# Towards a Robust Quantification of the Societal Impacts of Consumer-facing Cybercrime

**Markus Riek**

November 2017

Dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Economic and Political Sciences (Dr. rer. pol.)

Department of Information Systems
Westfälische Wilhelms-Universität Münster

Westfälische
Wilhelms-Universität
Münster

Inauguraldissertation zur Erlangung des akademischen
Grades eines Doktors der Wirtschaftswissenschaften
durch die Wirtschaftswissenschaftliche Fakultät der
Westfälischen Wilhelms-Universität Münster

Dekanin: Prof. Dr. Theresia Theurl
Erster Gutachter: Prof. Dr. Rainer Böhme
Zweiter Gutachter: Prof. Dr. Stefan Klein
Tag der mündlichen Prüfung: 14. November 2017
Tag der Promotion: 14. November 2017

# Summary

Consumer-facing cybercrime has become a pervasive threat to today's networked society. Profit-oriented criminals commit several kinds of fraud, identity theft, and extortion via electronic computer networks. While many countries realize that cybercrime is a serious problem, little is known about its impact on individuals and society as a whole. Several measurement problems have been identified. Police reports of cybercrime are known to be incomplete and inconsistent and survey-based estimates are suspected to be unreliable due to methodological flaws in the sampling and modeling of costs. Moreover, the coverage of impacts is incomplete because protection expenses and indirect costs are largely omitted. Indirect costs include lost opportunities, if consumers avoid technologies to keep away from cybercrime. Avoidance is assumed to cause considerable costs because worried consumers miss out on the benefits of technology. Yet, it has received little attention in research.

Recognizing the global scale of the cybercrime problem and the wide spread of unreliable estimates, the aim of this dissertation is the robust quantification of its societal impact. We conduct three empirical studies to advance the measurement in different directions.

The first study discusses robust estimation of direct costs. We develop a tailored survey instrument, which asks for monetary and non-monetary victim losses and protection expenses. Using primary data, collected from 6 394 adult Internet users in six EU member states, we study loss distributions and evaluate the robustness and precision of different summary indicators for estimating costs. Using our own harmonized loss indicator we find, inter alia, that scams have the severest impact on victims, as opposed to payment-related fraud, and that victim losses are dwarfed by protection expenses at the societal level. Furthermore, the study offers an evidence-based discussion of methodological choices regarding the instrument design and cost estimation in future surveys.

The second study provides empirical evidence of online service avoidance. We postulate a model of individual security behavior, which explains online service avoidance and protection behavior in reaction to cybercrime victimization and perceived risk of cybercrime. We validate the model on the societal level, using structural equation modeling in a secondary analysis of the Special Eurobarometer, an EU-wide population survey. A longitudinal replication of the study (2012 – 2014) demonstrates that cybercrime persistently affects avoidance of online banking, online shopping, and unknown websites. The results confirm the importance of avoidance for indirect costs and the model adds to the small body of information systems literature on negative behavioral outcomes.

The third study supplements the societal perspective with a micro level measurement of credit card avoidance by the victims of credit card fraud. We record longitudinal transaction data for 93 victims before and after a fraud incident, and we collect several attitudes of the victims in telephone interviews. Both types of data are combined in a linear mixed-effects model. The model predicts that a fraud incident leads to an average lost revenue of €2 per week and victim. Furthermore, it identifies informative communication during the fraud dispute handling to be a key measure for the credit card issuer to reduce these indirect costs due to avoidance.

# Acknowledgments

First and foremost I want to thank Prof. Dr. Rainer Böhme, who could not have been a better advisor during my time as a doctoral student. Rainer's passion for research and his extensive theoretical, methodological, and practical knowledge always guided my work towards the relevant questions. He taught me how to collect meaningful empirical data and document my results properly. He gave me the opportunity to work independently, was always available with helpful feedback, and reassured me when I believed everything was going wrong. I am extremely grateful for the opportunity to learn from such a great person during my work. I also thank Prof. Dr. Stefan Klein to evaluate my thesis and Prof. Dr. Wilfling to participate as a third reviewer in my disputation committee at University of Münster.

I had many great colleagues during my time at the University of Münster and Innsbruck. While I am very grateful that I had the opportunity to work with all of them, some deserve special thanks. First of all, Stefan Laube for the numerous scientific and personal talks we had during our the scientific career. It is really great to see how we developed from scientific greenhorns, over the first conference presentations and rejected journal papers, to the submission of our dissertations. Special thanks also to Svetlana Abramova, for never avoiding insightful discussions of my research models and persistently correcting and fine-tuning my texts. Also thanks to Pascal Schöttle and Cecilia Pasquini for reviewing many parts of my dissertation and Michael Fröwis for the good times in the office.

This work would not have been possible without the great collaboration I had with other researchers and non-academic partners. Before all, I want to thank Petra Silsbee and her colleagues from PLUSCARD for giving me the unique opportunity to collaborate with them in a study of victims of credit card fraud. I would also like to thank Marie Vasek and Tyler Moore who helped me a lot to get my scientific career started at the Southern Methodist University. Finally, I would like to thank the many colleagues of Michel van Eeten's group at the TU Delft for the many great discussions and the collaboration in the E-CRIME Project.

I would like to thank my parents, Edeltraud and Michael, for the many good qualities and values they gave me on the way, for always supporting me in the best possible way, and, maybe most importantly, for always providing a happy and loving home. I would also like to thank my brother Andy, sister-in-Law Laura, and my best friend Johannes for always supporting me.

Finally, I would like to specially thank my fiancée Laura, for her never ending support and motivation, for calming me down when it was necessary, for loving me through my absences, frustration, and grumpiness, and for putting happiness even in the most stressful days. I am the happiest person because I have you on my side.

# Contents

# List of Figures

# List of Tables

# List of Acronyms

(in alphabetical order)

### Statistical Terms

| | |
|---|---|
| **AMLI** | adjusted median loss indicator |
| **AVE** | average variance extracted |
| **CFA** | confirmatory factor analysis |
| **CFI** | comparative fit index |
| **CI** | confidence interval |
| **CR** | composite reliability |
| **ELI** | expected loss indicator |
| **GLMM** | general linear mixed-effects model |
| **HLI** | harmonized loss indicator |
| **ITS** | interrupted times-series analysis |
| **LMM** | linear mixed-effects model |
| **LRT** | likelihood ratio test |
| **MI** | modification indexes |
| **PLS** | partial least square |
| **RMSEA** | root mean square error of approximation |
| **SD** | standard deviation |
| **SEM** | structural equation modeling |
| **TLI** | Tucker Lewis index |
| **UCM** | unconditional sample mean |
| **WLSMV** | robust weighted least square |

## Theoretical Models and Constructs

| | |
|---|---|
| **ATU** | Attitudes Toward Using |
| **AV** | Avoidance Intention |
| **BI** | Behavioral Intention |
| **C-HIP** | Communication-Human Information Processing Model |
| **ET** | Expectancy Theory |
| **EXP** | Cybercrime Experience |
| **HBM** | Health Belief Model |
| **MA** | Media Awareness |
| **OSAM** | Online Shopping Acceptance Model |
| **PB** | Protection Behavior |
| **PCR** | Perceived Cybercrime Risk |
| **PEU** | Perceived Ease-of-Use |
| **PMT** | Protection Motivation Theory |
| **PU** | Perceived Usefulness |
| **RAT** | Routine Activity Theory |
| **RCT** | Rational Choice Theory |
| **TAM** | Technology Acceptance Model |
| **TPB** | Theory of Planned Behavior |
| **TR** | Trust |
| **TRA** | Theory of Reasoned Action |
| **TTAT** | Technology Threat Avoidance Theory |
| **UC** | User Confidence |
| **U** | Usage |
| **UTAUT** | Unified Theory of Acceptance and Use of Technology |

## Countries

| | |
|---|---|
| **DE** | Germany |
| **EE** | Estonia |
| **IT** | Italy |
| **NL** | the Netherlands |
| **PL** | Poland |
| **UK** | the United Kingdom |

## Other Acronyms

| | |
|---|---|
| **BC** | bank cards |
| **CNP** | card not present |
| **DIW** | Germany Institute for Economic Research |
| **DNS** | domain name system |
| **DoS** | denial-of-service |
| **EB** | Special Eurobarometer on Cyber Security |
| **EPS** | electronic payment systems |
| **GDP** | gross domestic product |
| **ICT** | information and communication technology |
| **IDT** | identity theft |
| **IS** | information systems |
| **ISCED** | International Standard Classification of Education |
| **MIT** | Massachusetts Institute of Technology |
| **NCVS** | National Crime Victimization Survey (in the US) |
| **OB** | online banking |
| **OOP** | out-of-pocket |
| **OS** | online shopping |
| **OSF** | online shopping fraud |
| **OSN** | online social networking |
| **PC** | personal computer |
| **PII** | personal identifiable information |
| **PP** | PayPal |
| **PSD2** | Second Payment Services Directive |
| **URL** | uniform resource locator |

# Chapter 1

# Introduction

## 1.1 Motivation

The sociologist Manuel Castells postulates that the world rapidly moves towards a networked society, "where the key social structures and activities are organized around electronically processed information networks" (Castells, 2008, p. 4). Indeed, in 2017, 80 % of individuals in developed countries use the Internet (ITU, 2017). This has transformed personal communication, work environments, financial transactions, knowledge transfer, and more (Castells, 2009).

Unfortunately, advantageous characteristics of the Internet, including its interconnectivity, anonymity, and global reach, also favor malicious behavior (Clough, 2015), and they have led to the emergence of cybercrime. The wide proliferation of payment-linked online services creates a large pool of targets for profit-oriented criminals (Reyns, 2013), and this is one driver behind the evolution of cybercrime into a serious industry (Moore et al., 2009). Offenses include traditional crimes, such as fraud or the trading of illegal goods, which are now committed via the Internet, and crimes unique to computer networks, such as hacking and ransomware attacks (European Commission, 2007). Recently reported examples include the following:

- The *WannaCry* ransomware, which encrypts data on personal computers (PCs) and demands a ransom payment in the cryptographic currency Bitcoin, equivalent to $ 300, to unlock infected PCs. The attack was launched in May 2017, and it infected at least 200 000 Windows computers in more than 150 countries. Victims included not only individual Internet users but also hospitals, universities, and the German railway company *Deutsche Bahn* (Goldman, 2017).

- The hacking of the large US credit bureau *Equifax*, which lost the social security numbers, birth dates, and addresses of 143 million Americans (roughly half of the US population) and 209 000 credit card credentials to unknown criminals (Krebs, 2017).

- The trading of illegal goods on darknet markets, such as *AlphaBay* and *Hansa*. The largest market, *AlphaBay*, had over 200 000 users, 40 000 vendors, and more than 350 000 listings for drugs, stolen identification documents, counterfeit goods, malware and hacking tools, and fraudulent services. *Hansa* was the third-largest market trading similar volumes. Both were taken offline in July 2017 by an internationally coordinated police operation (Europol, 2017).

**Societal Impact** It is hardly surprising that cybercrime is reported to be a serious problem. The United Kingdom's (UK's) National Crime Agency reports that the prevalence of cybercrime has surpassed the sum of all traditional crimes (NCA, 2016). While many other countries also report increasing levels, little is known about the associated costs for the victims and society as a whole (Levi, 2017). As for traditional crimes, reliable estimates are needed to inform policy making, set law enforcement priorities, and tailor public education campaigns (Anderson, 1999). Furthermore, the security community should use victim losses to evaluate the effectiveness of widely deployed security measures (Viega, 2012). However, most cost estimates are controversial.

Media reports, citing industry surveys with opaque methodologies, often proclaim “digital Pearl Harbors” and put cybercrime on one level with global drug trade (Florêncio et al., 2014). For example, CBS News writes that the overall costs of the *WannaCry* ransomware are estimated to end up at $ 4 billion, even though, four days after the attack, only $ 0.1 million had been paid by the victims, and patches were already available (Berr, 2017). The Center for Strategic and International Studies reports that costs related to cybercrime account for 0.41 % of the gross domestic product (GDP) in the EU, 0.61 % in the US, and even 1.60 % in Germany (McAfee and CSIS, 2014). Cybersecurity Ventures, an independent research and intelligence company, forecasts that global costs will grow from $ 3 trillion in 2015 to $ 6 trillion in 2021 (Morgan, 2016). These cost estimates translate to 4.41 % of the nominal global GDP in 2015 and 7.13 % in 2021 (OECD, 2014).

Academics studying information security economics are more skeptical and argue that many reports exaggerate costs (Florêncio and Herley, 2013; Anderson et al., 2013). Scholars of criminology share this assessment; they remark that cybercrime data is inconsistent and quantitative research is still very limited (Holt and Bossler, 2014; Rosenfeld and Weisburd, 2016). The wide range of existing estimates in industry reports underlines these assessments and highlights the challenges of reliable cybercrime measurement. Several problems have been identified.

**Problems of Quantification** Most fundamentally, comprehensive and reliable official records regarding the prevalence of cybercrime, for example, in police-recorded statistics, are rare and not comparable between countries (Van Dijk, 2015). This is due to conscious and unconscious underreporting by both consumers (Bidgoli and Grossklags, 2016) and organizations (Laube and Böhme, 2016) as well as a lack of common authoritative definitions of cybercrime (Arief et al., 2015).

Another problem concerns the estimation of impacts for observed crimes. While many scholars collect valuable data on particular types of criminal activity (e. g., Kanich et al., 2008), they do not observe consequences. This often limits the quantification of impacts to rough multiplications with average loss figures, which can only result in vague estimates. Note that already for the single *WannaCry* attack estimates of the costs differ by several orders of magnitude. Furthermore, individual studies typically focus on a single type of cybercrime and miss the bigger picture.

Victimization surveys are another option to collect data on cybercrime, and they are less affected by the aforementioned problems. Nevertheless, the reliable estimation of costs is complicated. Victim losses are concentrated among a small fraction of the population and loss distributions require specific modeling because the majority of victims loses only insignificant amounts, while others lose much more (Florêncio and Herley, 2013). Most survey-based cybercrime reports fail to apply concentration-aware sampling and robust statistical modeling to account for theses issues.

The last set of problems concerns the incomplete coverage of impacts. In addition to victim losses, impacts comprise protection expenses, which would not be necessary without cybercrime, and opportunity costs (Anderson, 1999). The latter include not only the lost time and productivity of criminals and victims but also lost opportunities caused by worried consumers who avoid information and communication technologies (ICTs) in order to avoid cybercrime.

**Costs of Avoidance** These hesitant or refusing consumers miss out on the benefits of a networked society, including convenient and inexpensive methods for handling financial transactions via online banking (Lee, 2009) or credit card payments (Chakravorti, 2003) as well as increased product availability and lower prices in e-commerce (Li and Huang, 2009). Anderson et al. (2013) conjecture that lost opportunities due to the individual avoidance of online services account for a substantial part of the cost of cybercrime. However, including avoidance in cost estimates adds another level of complexity because it requires the quantification of individual behavior at the societal level.

To date, behavioral models of avoidance in reaction to cybercrime, validated on the societal level, do not exist. Individual behavior is commonly studied in the information systems (IS) discipline; however, mostly to identify beliefs that lead to the adoption of ICT (Cenfetelli and Schwarz, 2011). Widely established models, such as the Technology Acceptance Model (TAM; Davis, 1989), exist, and they are used to study adoption in organizational contexts (Legris et al., 2003) and to a lesser extent for individual consumers (Anderson and Agarwal, 2010). Studies on inhibiting factors (Cenfetelli and Schwarz, 2011), and negative outcomes, such as IS discontinuance (Recker, 2016) or avoidance as a form of security behavior (Chen and Zahedi, 2016), are less common.

## 1.2 Research Goal and Contributions

Recognizing the global cybercrime problem and the wide spread of unreliable estimates of its costs, the aim of this dissertation is the robust quantification of the societal impact of consumer-facing cybercrime. Accordingly, the research is guided by three objectives:

1. To develop robust measurement methods and behavioral models to quantify the impact of cybercrime at the societal level.

2. To apply the developed methods and models using appropriate empirical data.

3. To derive evidence-based implications for policy making and business management.

To reduce the problem space, we focus on consumer-facing cybercrime, which targets or decisively involves individual consumers. This subset still includes a broad range of offenses, which differ with regard to the attacker's motivation, the ways in which they are conducted, and the impact on the victim. We exclude crimes that are emotionally, personally, or politically motivated, such as stalking, harassment, or the publication of illegal content. While those crimes are also conducted via electronic networks, and they may cause significant harm for the victims or society, the quantification of this harm is extremely challenging. Appreciating the existing problems of robust cost estimation, we focus on profit-oriented offenses, since their impact is easier to measure. Profit-oriented crimes comprise several kinds of fraud, identity theft, and extortion. We conduct three studies to provide quantitative evidence of their impacts.

**Studies** Chapter 4 studies the robust estimation of direct costs using victimization surveys. We develop a tailored instrument, which explicitly asks for monetary and non-monetary cybercrime losses and protection expenses. We collect representative data in a survey of 6 394 adult Internet users, covering seven types of consumer-facing cybercrime in six selected EU member states. Victims are consciously oversampled to increase the number of informative data points. We estimate loss distributions and evaluate different summary indicators with regard to their robustness and precision in depicting the impact of cybercrime. Using a specifically developed *harmonized loss indicator*, we compare costs between different types of cybercrime, cost categories, and countries.

The second study in Chapter 5 provides quantitative evidence of avoidance behavior. Acknowledging the importance of lost opportunities, we quantify online service avoidance in response to cybercrime exposure. We propose a parsimonious research model to explain protection behavior and avoidance intention of online shopping, online banking, and online social networking – three technologies that are widespread enough to allow for population-wide empirical studies. The model and three variants are validated using covariance-based structural equation modeling (SEM) in secondary analyses of three waves of the Special Eurobarometer on Cyber Security, a series of EU-wide population surveys (EB77.2, 2012; EB79.4, 2013; EB82.2, 2015).

Chapter 6 supplements the societal perspective with a study of credit card avoidance at the micro level. We measure the reactions of victims to credit card fraud in a natural experiment which is integrated into the credit card replacement process. We cooperate with PLUSCARD, a German payment card processor, to record weekly aggregates of transaction counts and revenue for 93 fraud victims, three months before and after the incident. In addition, PLUSCARD conducts telephone interviews after each incident to collect attitudes, intentions, and self-reported behavior based on a specifically developed questionnaire. We jointly analyze the transaction and interview data in a linear mixed-effects model (LMM) to measure avoidance and identify attitudes that explain it.

The three studies make several theoretical, methodological, and empirical contributions to the research on consumer behavior and the measurement of consumer-facing cybercrime.

### Theoretical Contribution

- **A model of individual security behavior in reaction to cybercrime.** Our literature review in Chapter 3 shows that avoidance, as a form of security behavior, is rarely studied, even though it is suspected to form a large part of the costs of cybercrime (Section 2.4.2). We synthesize suitable models from the IS discipline and insights from criminology to postulate a model of individual security behavior in reaction to cybercrime (Section 5.1). The core of the model adapts the perceived risk-extended TAM (Featherman and Pavlou, 2003) to explain the avoidance of online services. Protection behavior is added as another reaction to perceived risk, which itself is affected by cybercrime experience and media awareness. We further include user confidence as a moderator (Section 5.3.1), and we evaluate the avoidance of unknown websites as a related reaction to cybercrime (Section 5.3.3). Our model is able to explain consumer behavior, and it adds to the small body of IS literature on negative behavioral outcomes.

### Methodological Contributions

- **Validation of a behavioral model at the societal level.** A major methodological contribution is the empirical validation of the previously described model with multiple SEM analyses (Chapter 5.2). The analyses utilize the microdata of three representative EU-wide population surveys – the Eurobarometer reports. While we are not the first to validate a behavioral model using representative data, secondary analyses with data from a total of 57 000 Internet users, collected face-to-face in three successive years (2012 – 2014), are rare, if at all existing. We strengthen our contribution by proposing a trend analysis to study the persistence of structural links from a longitudinal perspective (Section 5.4). The good fit of a reduced version of our model, without media awareness, is confirmed by multiple approximate fit indexes for all years and further supported by an improved measurement model (Section 5.3.2).

- **An instrument tailored to measure costs of cybercrime for consumers.** Our study in Chapter 4 contributes to the estimation of direct costs for consumers. Based on a review of the short-comings in existing reports (Section 2.3.3), we are the first to develop an instrument that is specifically tailored to measure the victim losses and protection expenses of consumer-facing cybercrime (Section 4.1). Acknowledging that our data collection is limited to a single snapshot, we discuss the impact of central design choices, such as the exclusion of malware, on the resulting cost estimates to inform future victimization surveys in the context of cybercrime.

- **Discussion of robust indicators of aggregate costs.** Section 2.3.3 demonstrates that many survey-based cybercrime reports are unreliable because the particularities of loss distributions are ignored. We propose methods to derive aggregate costs figures, which handle zero-inflated and skewed distributions (Section 4.2). We evaluate the methods in terms of precision and robustness using the primary data, collected with our tailored instrument, and we discuss our own *harmonized loss indicator*, which provides robust cost figures (Section 4.3).
- **A combined measurement of attitudes, intentions, and actual behavior.** Our last methodological contribution is the combination of six months of longitudinal transaction data with responses to standardized interviews. While most behavioral studies are limited to intentions reported in surveys, we are able to study credit card transactions of fraud victims in a LMM analysis (Section 6.3.2). The LMM isolates the impact of an incident on the avoidance of the new credit card from random variations in spending levels between different weeks and victims. Thus, it can estimate the costs of avoidance in terms of lost revenue, and the inclusion of attitudes, collected in the interviews, can explain the avoidance behavior (Section 6.3.3).

**Empirical Contributions** Based on the collection of primary data (Chapters 4 and 6) and the analysis of secondary data using new methods (Chapter 5), this dissertation makes several empirical contributions. A selection of our findings is presented below.

- Losses of cybercrime victims are best modeled with zero-inflated, log-normal distributions, and their aggregation requires robust indicators (Section 4.2.2). The same holds for the distributions of protection expenses, which have similar, but less extreme, characteristics (Section 4.2.4).
- Scams have the severest impact on individual victims in terms of monetary and time-related losses. Identity theft with regard to payment-linked online services leads to the highest initial losses; however, the service providers largely reimburse the victims (Section 4.2.3).
- At the societal level, monetary losses and expenses of consumers are exceeded by the monetary equivalents of time-related costs. Aggregate protection expenses exceed the victim losses by more than five times in most countries (Section 4.2.5).
- The positive impact of victimization on the avoidance of online shopping, online banking, and unknown websites is consistently mediated by perceived risk of cybercrime (Section 5.4).
- Protection behavior, in the form of using different passwords and changing security settings, is directly influenced by cybercrime experience, not by perceived risk of cybercrime (Section 5.4).
- User confidence in conducting online transactions moderates the latent variable means of cybercrime experience, perceived risk, and avoidance. Interestingly, confident users have experienced more cybercrime, but they perceive less risk and avoid online services less (Section 5.3.1).
- Credit card fraud leads some victims to avoid payments with the new credit card. Our LMM predicts that this results in an average lost revenue of €2 per week and victim after the incident (Section 6.3.2).
- Victims of credit card fraud who felt well informed during the credit card replacement process use the new credit card significantly more, making communication a key measure to reduce indirect costs due to avoidance (Section 6.3.3).

Our contributions advance the quantification of consumer-facing cybercrime in many directions. Natural to all empirical studies our analysis have limitations. To achieve our goal of reliable quantification of societal impacts, we carefully discuss the impact of these limitations on our results. As the limitations strongly depend on the respective method and empirical data, we document them in the discussion of each analysis (in Chapters 4–6).

## 1.3 Preliminaries

### 1.3.1 Research Ethics

This dissertation studies individuals and in particular victims of cybercrime. Therefore, the compliance with human research ethics is an essential prerequisite of the data collection. Our analyses build around five victimization surveys. The three Eurobarometer reports analyzed in Chapter 5 have been conducted on behalf of the European Commission. Ethical considerations are documented in the respective technical reports (EB77.2, 2012; EB79.4, 2013; EB82.2, 2015). The collection of primary data, conducted by us and others for the analyses in Chapters 4 and 6, follow the ethical guidelines published by the United Nations Office (UNODC-UNECE, 2009). This section summarizes the main considerations, including: 1) the protection of respondents through ensuring informed consent and 2) the protection of confidentiality, privacy and anonymity of participants.

All participants are rational adults (18 or older) and gave informed consent to participate in the studies voluntarily. The international consumer survey (Chapter 4) has been conducted by the market research company Ipsos as part of the EU FP7 project E-CRIME. Ipsos has long experience in conducting survey research in an ethical and legal manner across European jurisdictions. Potential participants of the survey were provided with information on the purpose, intended beneficiaries, potential social impacts, and any risks of participation, prior to the interview. They were also informed that they could withdraw from the survey at any point. Informed verbal consent was given at the beginning of each telephone interview. The data collection for the case study of credit card fraud (Chapter 6) has been exclusively conducted by PLUSCARD. Written consent was given by the participants prior to the telephone interviews, via mail or a special website. To provide the basis for informed consent, potential participants were provided with an information letter on the purpose of the research, intended beneficiaries, data protection actions, and any risks of participation.

The confidentiality of the collected data and the anonymity of participants were of paramount importance in both data collection processes. All personal identifiable information (PII) has been removed from the data sets by the collecting party and transaction data has been aggregated to weekly bulks before it left PLUSCARD. Thus, all analyses are based on anomymized data sets.

The compliance with ethical and data protection requirements has been confirmed by independent parties. The consumer survey (Chapter 4) has been reviewed by an independent ethics board of the E-CRIME project. The case study of credit card fraud (Chapter 6) has been approved by the independent ethics board of the University of Innsbruck.

### 1.3.2 Notational Conventions

Monetary dollar amounts, e. g., \$ 300, refer to US Dollars, if not noted stated otherwise. £-amounts refer to pound sterling, as used in the United Kingdom. We use the short (American) scale for large numbers. Accordingly, one billion corresponds to $10^9$. Where necessary, we abbreviate large numbers using small letters: million (m), billion (bn), trillion (tn). We opted for this convention to avoid confusion with upper-case symbols for cost estimates in Chapter 4.

Significance levels of correlations and coefficients in the regression and path analyses are documented with the following notation: Significance: $^{***} = p < 0.001$, $^{**} = p < 0.01$, $^{*} = p < 0.05$, $^{\dagger} = p < 0.1$, $' = p < 0.15$. Accordingly, $^{***}$ represents a p-value $< 0.001$. Note that the last level $'$ ($p < 0.15$) is only used once for the analysis of mediation effects in Chapter 5 (see Table 5.4).

To support readability we use acronyms according to the following conventions. Acronyms are generally re-introduced in every chapter. The long form is used if a term only occurs once in a chapter. The acronyms for behavioral constructs (summarized on page xii) are written in the long form in hypothesis, discussion sections, and the conclusion.

For brevity, we do not include retrieval dates for online sources in the bibliography. However, all links were available on September 24th, 2017.

### 1.3.3 Publications and Collaborative Work

Parts of this dissertation are published in peer-reviewed academic journals, conferences, and workshops. Table 1.1 assigns the publications to two of the main chapters and orders them chronologically within each chapter. All papers have been written in collaboration with other researchers, whose contributions are briefly described in the remainder of this section.

**Table 1.1:** Peer-reviewed publications

| |
|---|
| Chapter 4: Estimation of Direct Costs |
| • Riek, M., Böhme, R., Ciere, M., Ganan, C., and van Eeten, M. (2016). Estimating the Costs of Consumer-facing Cybercrime: A Tailored Instrument and Representative Data for Six EU Countries. *Workshop on the Economics of Information Security (WEIS)*, University of California at Berkeley, Berkeley, USA. |
| Chapter 5: Quantitative Evidence of Indirect Impact |
| • Riek, M., Böhme, R., and Moore, T. (2014). Understanding the Influence of Cybercrime Risk on the E-Service Adoption of European Internet Users. *Workshop on the Economics of Information Security (WEIS)*, The Pennsylvania State University, State College, USA.<br>• Riek, M., Böhme, R., and Moore, T. (2016). Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transactions on Dependable and Secure Computing*, 13(2), pp. 261–273. © 2016 IEEE.<br>• Riek, M., Abramova, S., and Böhme, R. (2017). Analyzing Persistent Impact of Cybercrime on the Societal Level: Evidence for Individual Security Behavior. In: *Proceedings of the 37th International Conference on Information Systems (ICIS)*, Seoul, South Korea. |
| Related work |
| • Böhme, R., Laube, S., and Riek, M. (2018). A Fundamental Approach to Cyber Risk Analysis. *Variance*, 11(2), in press. |

The idea for the estimation of direct costs of consumer-facing cybercrime, reported in Chapter 4, originates in the EU research project E-CRIME (URL: `http://cordis.europa.eu/project/rcn/185498_en.html`). Within the project a multi-purpose victimization survey was conducted. I led the development of the measurement instrument, which was done in collaboration with all five authors of the WEIS 2016 paper and other partners from the E-CRIME consortium. The survey was conducted by the market research company Ipsos, which was also part of the E-CRIME consortium. I was responsible for checking the quality of the survey data, I conducted the statistical analysis, and I drafted the working paper. The work presented in Chapter 4 incorporates comments from the WEIS workshop and E-CRIME meetings and substantially extends the WEIS 2016 version, for example, by the inclusion of confidence intervals and an improved connection to the criminology literature.

The fundamental idea for a behavioral model of online service avoidance in response to cybercrime exposure, presented in Chapter 5, was proposed by Rainer Böhme as a follow-up from a paper he wrote together with Tyler Moore. I developed the research model in a working paper presented at WEIS 2014 and an improved version has been published in the IEEE TDSC in 2016. I had the idea to extend the avoidance model with protection behavior and to replicate the SEM analysis for additional Eurobarometer surveys. The extended research model and additional analyses are documented in the 2017 ICIS paper, which I wrote in collaboration with Svetlana Abramova. Chapter 5 integrates all papers and presents avoidance and protection behavior in a single integrated model. I conducted additional confirmatory factor analyses and SEM analyses for this integrated model.

## 1.4 Dissertation Outline

This dissertation is organized into seven chapters. Chapters 2 and 3 lay the foundation for the quantification of the societal impact of consumer-facing cybercrime. Chapter 2 defines consumer-facing cybercrime, classifies its potential societal impacts, reviews available data sources, discusses challenges of cost estimation, and finally presents existing evidence. Chapter 3 introduces theories of individual security behavior to quantify parts of the indirect impact of cybercrime. It starts with a fundamental summary of theories which explain individual behavior, reviews the application of two major IS models in the context of security, and provides an overview of less commonly used theories.

Chapters 4 and 5 examine cybercrime impact on the societal level using national representative surveys. Chapter 4 estimates direct costs of consumer-facing cybercrime in six EU countries. It describes the measurement instrument, primary data collection, and cost estimation procedure, before comparing cost estimates for a broad range of cybercrimes and along various dimensions. Chapter 5 provides quantitative evidence of the indirect impact of cybercrime due to individual avoidance of online services by EU Internet users. It formalizes a model of individual security behavior and validates this model in a secondary analysis of the Special Eurobarometer. A trend analysis replicates the results for three subsequent waves of the Eurobarometer.

Chapter 6 supplements the societal perspective with a case study of credit card fraud, as one instance of cybercrime. While the results are less general than in the two previous chapters, the case study enables the observation of cybercrime impact in a clearly defined context including actual behavioral data in addition to attitudes and intentions reported in a telephone survey.

Chapter 7 closes with a summary of the key results, practical implications, and an outlook to future research.

# Chapter 2

# Consumer-facing Cybercrime

This chapter introduces the background on consumer-facing cybercrime and the measurement of its societal impacts. Section 2.1 sets the scene with a historical perspective on the developments that lead to cybercrime. Section 2.2 conceptualizes consumer-facing cybercrime, as used in this dissertation. Section 2.3 introduces the quantification of its societal impacts; it classifies potential impacts, reviews available data sources, and discusses the challenges for robust estimates. Section 2.4 concludes the chapter with an overview of the existing estimates of consumer-facing cybercrime.

## 2.1 History

This section provides a brief historical overview of the main developments that lead to present-day cybercrime. It largely summarizes a more comprehensive representation by Brenner (2010). Accordingly, we refer to Brenner (2010) unless stated otherwise.

The concept of *computer crime* first appeared in the 1960s together with the use of mainframe computer systems. The first cases of illegal activity – manipulation and sabotage – were conducted by financially motivated insiders. Since the systems were not interconnected, and only a few people had access and sufficient skills to use them, the potential to commit computer crime was restricted.

The increasing availability of computers sparked the culture of *hacking*. Starting at the Massachusetts Institute of Technology (MIT), hacking spread to other academic centers in the US. In the beginning, students explored computer systems by manipulating them using clever and practical tricks. The ARPANET was the first packet-switching computer network that linked the mainframes of universities, research laboratories, and defense contractors in the US. Its introduction in 1969 and its expansions in the following years provided the first opportunities for remotely hacking computers. However, it was bound to 256 computers, limiting the hacker community to a small group.

Two dynamics substantially increased the opportunity for malicious activity; first, the spread of PCs in households and organizations which began in the 1980s and second, the on-going networking of these computers via the Internet in the 1990s. The opportunities of a global computer network lead to new forms of crime, including the first instances of malware.

The word malware combines *malicious* and *software* to describe software that is designed to infiltrate and/or damage a computer without the owner's knowledge and consent. Similar to hacking, malware was first used to experiment with the capabilities of computers and networks. While early instances, e. g., Robert Morris's worm (1988) and the WM.Concept virus (1995), were not implemented with a malicious intention, they infected PCs globally and caused considerable costs.

The "I love you" virus, which appeared in 2000, was even more destructive. It destroyed files on infected PCs and tried to steal passwords. The virus arrived as an attachment to a spam email, and it emailed itself to the complete address book of an infected PC. It spread around the globe in a few hours, infected about 45 m PCs in at least 20 countries, and it caused estimated damages of $ 8-10 bn. The major novelty of the attack was not technical, but psychological. The success of the simple "I love you" text in the email's subject pointed to the great opportunities for fraud on the Internet.

**Cybercrime** A basic principle of criminology is that crime follows opportunity (Wall, 2007). At the beginning of the 21st century, several factors were in favor of committing crimes via the Internet (Clough, 2015). The early use of hacking, malware, and spam emails demonstrated the potential of computer networks, the on-going proliferation of the Internet provided a pool of millions of targets, and the absence or ambiguity of laws made punishment unlikely.

Using the Internet, multiple geographically dispersed victims could be targeted simultaneously, crossing national and continental boarders (Goodman and Brenner, 2002). The anonymity hampered the prosecution of cybercriminals, since they could operate from any location in the world and cover-up tracks by using intermediate computers as proxies. In a hypothetical (but not unrealistic) example, malicious emails sent from a webserver in Russia may spread malware to conduct credit card fraud in the EU, while the whole process is controlled from a laptop connected to the wireless network of a beach hotel in the Philippines. The capabilities of computers and networks further provided simple and cost effective means to repeat attacks (Wall, 2007). Adding to the previous example, the attack may be repeated in the US, China, and other countries, or it could be used for other types of financial fraud with only a few modifications.

The emergence of digital payments and payment-linked online services further fueled criminal activity, as criminals realized that they could use their technical knowledge and skills to commit crimes for financial profit (Hunton, 2009). Organized groups emerged, in which criminals take specialized roles, including malware developers, hackers, and spammers. The division of labor has led to extensive gains in criminal productivity similar to Adam Smith's pin factory (Smith, 1827). According to Moore et al. (2009), cybercrime has taken off as a serious industry since about 2004.

In addition, digital underground markets have evolved, and they enable the exchange of criminal artifacts between organized groups or individual criminals (Franklin et al., 2007). The tools needed to conduct various types of cybercrime are easily accessible on these markets, and they allow for attacks to be performed without much training (Anderson et al., 2008). The combination of these developments led to a number of different types of attacks, which we subsume under cybercrime.

## 2.2 Definition

Even though, many forms of cybercrime have been observed around the globe for several years, a common definition is still missing. This section takes a practical approach to conceptualizing consumer-facing cybercrime. Section 2.2.1 first reviews the challenges in establishing a precise definition and Section 2.2.2 examines cybercrime from multiple perspectives. Finally, Section 2.2.3 conceptualizes consumer-facing cybercrime in the context of this dissertation.

### 2.2.1 Challenges

Cybercrime has been discussed in academic journals, computer magazines, and newspaper articles, yet diverse and inconsistent interpretations continue to exist (Barn and Barn, 2016). Authors from criminology (e. g., Van Dijk, 2015) and computer science (e. g., Arief et al., 2015) argue that there is still no agreement upon a clear definition. The word is often used as an umbrella term including all crimes associated with computers (Moore, 2010). A multitude of synonyms, such as computer crime, cyber-warfare, high-tech crime, or Internet crime, exist which often point to the same, but sometimes completely different offenses (Clough, 2015). To understand the problems of defining cybercrime we start at its etymological roots and then review the challenges reported in the literature.

**Etymological Roots** *Cyber*crime specifies a subset of crimes associated with the cyber domain. A *crime* can be defined as "[t]he violation of laws, or more precisely those social norms that have become subject to state control and legal sanctions reliant on punishment" (Calhoun, 2002, p. 100). In many cases, the act of doing something criminal must be accompanied by the intention to do so, in order to be classified as a crime (Law, 2015). Many countries compile crimes in a criminal code containing a catalog of offenses and the respective penalties. Finding an indisputable definition of crime is difficult because it is specific to national laws or theoretical frameworks (Henry and Einstadter, 2006). The consideration of the *cyber* component introduces further complications.

The etymologic roots of the term *cyber* are in the concept of cybernetics proposed as a scientific discipline by Wiener (1948). Cybernetics comprises "the entire field of control and communication theory, whether in the machine or in the animal" (Wiener, 1961, p. 11). Böhme et al. (2018) state that this origin barely suggests a precise definition of the term cyber, yet its current application is vast. It comprises "cyber space" as popularized by the science fiction short story "Burning chrome" (Gibson, 1987) as well as the establishment of the "US Cyber Command" in 2010. The latter was founded as a consequence of recognizing that cyber is a fifth domain of warfare next to land, sea, air, and space (Lynn, 2010). Similar to cyber-warfare, cybercrime is suggested to be a new domain of crime which requires special consideration in laws and criminal codes (Wall, 2007), to account for its unique properties.

**Challenges to Define Cybercrime** The main challenges to define cybercrime can be divided into three categories. First, descriptions and definitions have been developed by different organizations, countries, and scientific disciplines, as a result of the technical nature and global reach of cybercriminal attacks (Alkaabi et al., 2011). While computer scientists may be able to perfectly define the technical dimension of a cybercriminal act, such definitions may be hard to code into national laws and even more difficult to harmonize between countries.

Second, cybercrime often combines multiple criminal acts in a single attack. Malware, for example, is a multi-purpose tool supporting many kinds of attacks (Holt and Bossler, 2014). Ransomware is one kind of malware, used to encrypt data on the victim's PC and extort a ransom to unlock (Kharraz et al., 2015). Other kinds secretly steal account credentials to prepare identity theft or connect infected PCs to a botnet which enables other crimes (Tajalizadehkhoob et al., 2017). Some versions of the infamous *ZeuS* Malware are able to perform all three functions (Symantec, 2016b).

The third reason is the evolving nature of cybercrime, which is driven by innovation itself and in terms of social interaction with new technologies. Section 2.1 outlines the development of cybercrime from attacks against mainframe computers to complicated attack schemes, which involve malware, botnets, and underground markets. More recent innovations, such as the Internet of Things or cryptographic currencies, open up new opportunities. These dynamics require that cybercrime definitions are either continuously updated or vague enough to include new forms of crime automatically.

### 2.2.2 A Practical Approach

Recognizing the challenges of defining cybercrime precisely, we opt for a more practical approach. We start with an introduction of different perspectives on cybercrime, distinguish it from related concepts, and finally look at existing policy definitions.

**Perspectives on Cybercrime** Taking different perspectives can help to conceptualize cybercrime in the absence of a clear definition. A common classification uses three categories based on the role of computers and networks in the criminal act (Goodman, 1996; Brenner, 2010; Alkaabi et al., 2011; Clough, 2015). Accordingly, cybercrime includes:

1. Crimes in which computers or computer networks are the **target** of the criminal activity, such as hacking, malware, or denial-of-service (DoS) attacks.

2. Crimes in which the computer is used as a **tool or instrument** for committing crimes. For example, online fraud, harassment, dissemination of illegal content, or stalking.

3. Crimes in which the computer is an **incidental aspect** of the commission of the crime. For example, if it is used for communication or data storage.

The third category, i. e., the incidental aspect, is omitted by many authors who argue that the increasing use of computers and networks makes them an incidental aspect of almost any crime. Summarizing existing definitions, Alkaabi et al. (2011, p. 4) state that the “overridingly predominant view is clearly that for a crime to be considered as cybercrime, the computer or network or digital device must have a central role in the crime i.e., as target or tool”.

Wall (2015) agrees with the essential role of computers and networks, but suggests to add a second (orthogonal) dimension. The additional dimension concerns the impact of networks and in particular the Internet on criminal opportunity and behavior. Accordingly, cybercrimes can be classified into three types:

1. **Cyber-assisted crimes** are traditional crimes for which the Internet has *created more* opportunities because they can be conducted online. Examples include tax fraud or stalking.

2. **Cyber-enabled crimes** are traditional crimes for which the Internet has *enabled new* opportunities, e. g. illegal access (by hacking), selling of counterfeit goods, or large-scale fraud.

3. **Cyber-dependent crimes** are *new types* of crime for which the Internet has opened completely *new opportunities*, such as ransomware or DoS attacks.

Anderson et al. (2013) apply the same logic and distinguish (1) traditional crimes which may now be conducted online, (2) transitional crimes whose modus operandi has changed substantially as a result of the move online, and (3) new crimes that owe their existence to the Internet. They further add a fourth category, called **criminal infrastructure** (or platform crimes, respectively). The criminal infrastructure comprises crimes which do not extract money from the victims but rather facilitate other (primary) crimes. We detail this distinction when describing consumer-facing cybercrime in Section 2.2.3.

Further and less common perspectives classify cybercrimes based on the role of humans in the criminal act (Gordon and Ford, 2006) or from the perspective of its main stakeholders, i. e., attackers (Arief et al., 2015) versus defenders and victims (Arief and Adzmi, 2015).

**Differentiation from Related Concepts** We differentiate cybercrime from three related concepts: *hacktivism*, *cyber-terrorism*, and *cyber-warfare*. Since all three capitalize on cybercriminal tools to varying degrees, they are sometimes confused with cybercrime.

*Hacktivism* is a form of cyber activism (Milan, 2013). It predominantly covers operations that use hacking techniques against organizations and their information systems to promote ideas of political or social change. Common techniques comprise DoS attacks, website defacements, and data leakage. The informal group of activists “Anonymous” is often associated with acts of hacktivism. A prominent example is “Operation Payback” which took down websites of MasterCard, Visa, and PayPal after the services stopped processing payments for WikiLeaks, a platform which promotes freedom of information and publishes classified documents (Mackey, 2010). We differentiate *hacktivism* from cybercrime due to its ideological motivation and the fact that acts of *hacktivism* are bound to infrequent events which rarely result in high damages, even if they receive a lot of media attention.

*Cyber-terrorism* refers to the convergence of cyberspace and terrorism. Attacks are also politically or ideologically motivated, but have a *terroristic* component. Therefore, cyber-terroristic attacks instill terror on the target population, resulting in large-scale destruction or even death (Clough, 2015). An example may be hacking of air traffic control systems to cause the collision of planes (Denning, 2001). *Cyber-terrorism* can be distinguished from *hacktivism* mainly by the severity of its impact. However, boundaries are fuzzy and may depend on the perspective. For example, officials at MasterCard or Visa may refer “Operation Payback” as an act of *cyber-terrorism*. While such acts are likely punishable by national laws of the affected country, we differentiate *cyber-terrorism* from cybercrime because terrorists have a fundamentally different motivation than profit-oriented criminals.

*Cyber-warfare* describes the use of computer networks and information systems as sophisticated strategic weapons in inter-state conflicts. The computer worm “Stuxnet”, which destroyed centrifuges in an Iranian nuclear plant in 2010, is the first act of *cyber-warfare* known to cause physical damage across international boundaries (Lindsay, 2013). At least two characteristics make cyberattacks attractive for warfare. The greater opportunity to achieve particular goals, such as retarding the Iranian nuclear program, without causing collateral damage and the possibility to remain anonymous. Therefore, states capitalize on technology used or even developed by cybercriminals. Farwell and Rohozinski (2011) speculate that some states even outsource attacks to criminal organizations. Nevertheless, *cyber-warfare* needs to be distinguished from cybercrime because it requires the existence of an inter-state conflict.

**Policy Definitions** Legislative definitions of cybercrime are bound to the criminal codes of individual countries. To match the broad and international research goal of this dissertation we only consider policy definitions which shape national legislation. Furthermore, our focus is on publications in the EU, i. e., by the Council of Europe.

The Convention on Cybercrime (Council of Europe, 2001), also known as the Budapest Convention, is a binding international treaty intended to be adopted in national legislations to provide an effective framework to fight cybercrime internationally. The convention aims to harmonize national criminal law elements in the area of cybercrime, to provide procedural powers necessary for the investigation and prosecution, and to set up a fast and effective regime of international cooperation. It contains high-level definitions of different types of cybercrime, including: illegal access and interception, data and system interference, misuse of devices, computer-related forgery and fraud, as well as offenses related to copyright. As of 2017, 55 countries around the globe have ratified the treaty, including the USA, Canada, and Japan (Council of Europe, 2017).

In a subsequent communication by the European Commission, cybercrime is defined as all “criminal acts committed using electronic communications networks and information systems or against such networks and systems” (European Commission, 2007, p. 2). The communication further specifies three types of cybercrime:

1. **Traditional forms of crime**, which are committed via electronic communication networks and information systems. These include any kind of large-scale fraud, identity theft, or scams as well as the national and international trade of illegal goods via the Internet.
2. **Publication of illegal content** using electronic media. This includes child sexual abuse material, incitement to racial hatred or religious extremism, and counterfeit documents.
3. **Crimes which are unique to electronic networks**, most importantly, well-coordinated, large-scale attacks against information systems. This includes DoS attacks to interrupt online services and the distribution of malware.

The policy definition applies to all types of cybercrime that Alkaabi et al. (2011) found; however, the role of computers and networks as targets or tools is not considered. The definition rather focuses on the impact of the Internet on criminal opportunity, i. e., on the second perspective put forward by Anderson et al. (2013) and Wall (2015). Accordingly, it distinguishes traditional crimes committed via electronic networks (cyber-assisted) from crimes unique to electronic networks (cyber-dependent). While it does not specify cyber-enabled crimes explicitly, it includes the publication and dissemination of illegal content as an individual category.

### 2.2.3 Consumer-facing Cybercrime

Our conceptualization of consumer-facing cybercrime follows the policy definition summarized in the previous section. Given the focus in the dissertation, we exclude offenses that are not consumer-facing, and we consequently do not consider crimes solely targeted at organizations. However, in many cases, organizations and consumers are both affected by the same incident. A recent example is the 2017 data breach at Equifax – a large US credit bureau – which affected not only the credit bureau but also the customers whose credit card credentials were leaked (Krebs, 2017). Losses resulting from credit card fraud, as another example, may be incurred by consumers, the credit card issuer, or merchants, depending on the liability in a particular case. Our approach here is to limit the set of cybercrimes to the ones either targeted at consumers or in which consumers play a significant role.

The second restriction is the focus on profit-oriented crimes. We exclude politically motivated crimes, which comprise acts of hacktivism, cyber-terrorism, and other acts of hate speech or publication of illegal content. We also do not consider personally motivated crimes, such as bullying, harassment, or stalking, even though they may be also committed via online social networks (e. g., Juvonen and Gross, 2008).

We adapt Communication 267 (European Commission, 2007) and conceptualize consumer-facing cybercrime as follows:

> “all criminal acts *against arbitrary consumers* committed using electronic communications networks and information systems or against such networks and systems *to make a financial profit*”.

The remainder of this section supplements this working definition with a brief summary of different types of consumer-facing cybercrime. These have been identified by an integration of sources that operationalize consumer-facing cybercrime. We consider crimes listed in the taxonomy of Alkaabi et al. (2011), the framework of Anderson et al. (2013), and the EB82.2 (2015), which is a consumer survey to collect data on Internet users’ cybercrime experience in the EU.

Consumer-facing cybercrime can be broken down into two types of offenses: *primary crimes*, which extract money from the victim, and the *criminal infrastructure*, which supports the conduct of the primary crimes (Anderson et al., 2013).

**Primary Crimes** Based on the method to extract money, primary crimes can be further divided into three sets of primary offenses against consumers: fraud, identity theft (IDT), and extortion.

*Fraud* comprises a wide range of crimes. In an examination of its costs in the UK, Levi and Burrows (2008, p. 299) define it as “the obtaining of financial advantage or causing of loss by implicit or explicit deception; it is the mechanism through which the fraudster gains an unlawful advantage or causes unlawful loss.” Pratt et al. (2010) use a similiar definition of consumer fraud. We consider several fraudulent schemes, which are conducted via the Internet. They comprise the offer of non-existent, falsely represented, or counterfeit goods and services, and deceptions used to trick victims into transmitting funds or other items of value to the perpetrators.

*Identity theft* can be interpreted as one type of fraud. In a discussion of identity-related crimes, Koops and Leenes (2006, p. 556) define it as “fraud or another unlawful activity where the identity of an existing person is used as a target or principal tool without that person’s consent.” While this definition interprets IDT as a subcategory of fraud, both terms are often used interchangeably, in particular in the context of banking. Accordingly, the theft of credit card credentials is referred to as credit card fraud[1], and the illegal control of an online banking account is referred to as online banking fraud. The confusing use of terms emphasizes the challenges in finding common definitions of cybercrime. In this dissertation IDT is associated with payment-linked identities, including credit card credentials, online banking and online shopping accounts, and other payment services.

*Extortion* is mainly concerned with the use of malware to encrypt data or whole devices and then demanding a ransom payment to unlock them. While other forms of extortion exist, for example, with the publication of sexually explicit material (Wittes et al., 2016), the extortion with ransomware is the most common offense (Berr, 2017; Young and Yung, 2017).

**Criminal Infrastructure** The criminal infrastructure does not extract money from the victims, but supports the previously described crimes. Two central activities, part of the criminal infrastructure, relate to the use and operation of underground markets and botnets.

*Underground markets* provide an anonymous platform for trading various illegal goods, including criminal tools and services that are used to conduct primary offenses, as well as the loot of such offenses. For example, specialized “Phishermen” create copies of genuine bank websites to steal bank account numbers and passwords, and “Spammers” lure customers to these fake websites by distributing phishing emails (Moore et al., 2009). Both services can be purchased on underground markets. Furthermore, stolen identities in the form of accounts and credentials can be sold to other criminals who specialize on monetizing them (Franklin et al., 2007).

*Botnets* are networks of bots. A bot is PC that is infected with a malware which puts the PC under the central control of a criminal. While being a bot is typically not harmful (mostly not even detectable) for the users of infected machines, botnets provide the technical infrastructure for primary offenses and other parts of the criminal infrastructure, such as hosting phishing websites or sending out spam emails (Tajalizadehkhoob et al., 2017).

## 2.3 Quantification

This section provides the foundation for the quantification of the societal impacts of consumer-facing cybercrime. Section 2.3.1 classifies the societal impact of traditional crime and cybercrime. Section 2.3.2 reviews data sources in the context of consumer-facing cybercrime and Section 2.3.3 discusses the challenges of robust cost estimation.

[1] In accordance with this convention, we also refer to it as credit card fraud in the case study (Chapter 6).

### 2.3.1 Classification of Societal Impacts

A quantification of the societal impacts of crime requires the estimation of incurred costs. This section introduces two frameworks for structuring the societal impacts of crime (Anderson, 1999) and cybercrime (Anderson et al., 2013), and it discusses the particularities in the context of cybercrime.[2]

**Crime** Anderson (1999) criticizes the standard estimates of criminal activity because they only count crimes and largely neglect the associated costs, especially indirect costs such as private expenditures for crime-prevention and opportunity costs. He attempts to exhaustively estimate the overall burden of crime in the US, including all "costs that would not exist in the absence of illegal behavior under current U.S. law" (Anderson, 1999, p. 613). According to his framework costs can be structured in four categories:

1. **Transfers** of assets from the victims to the criminals (direct costs of the victims).
2. **Crime-induced production**, i. e., resources for products and activities that do not contribute to society except in their association with crime.
3. **Opportunity costs** of criminals and (potential) victims, including the losses in workers' productivity, the criminals' time, and the time (potential) victims spent on securing assets, looking for keys, and purchasing and installing crime-prevention measures.
4. **The value of risks to life and health** are implicit costs (in particular for violent crime). They include the fear of being injured or killed, the anger associated with the inability to behave as desired, and the agony or distress of being a victim of crime.

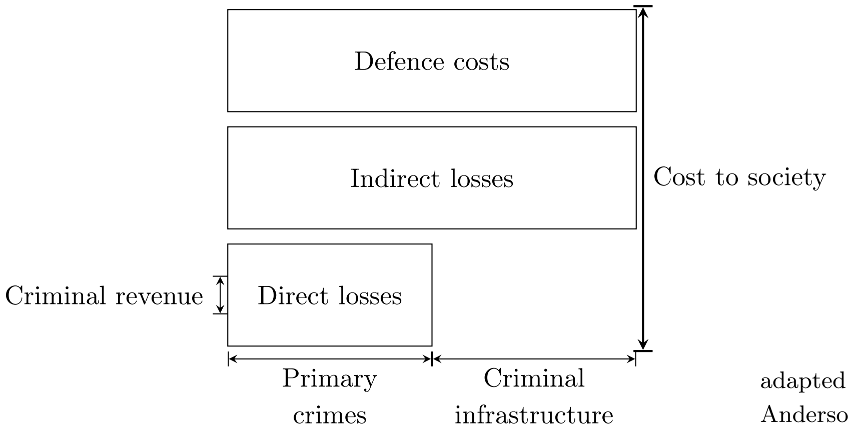
The majority of crimes create costs in multiple categories. For instance, a robbery creates a transfer of goods or money from the victim to the criminal, (possibly) health and psychic issues, and the opportunity cost of the time for both victim and offender. Anderson (1999) measured the burden of crime in the US for the year 1997, integrating various data sources. He finds that the gross annual cost ($ 1.71 tn) has the same order of magnitude as life insurance purchases and annual expenditures on health. Criminal revenues (through transfer of assets) only represent about a third of the overall cost, the other two thirds are opportunity costs, crime-related expenses, and diminished life quality.

A replication of the study in 2010 highlights the importance of societal impacts when measuring crime. While the number of reported crimes decreased between 1995 and 2010 by 53 %, the estimated gross annual cost of crime increased by $ 800 m during the same period (Anderson, 2012). However, a comparison between both studies should be interpreted with caution because of the following: changes in the sources, estimation methods of reporting agencies, and the availability of data.

**Cybercrime** Anderson et al. (2013) propose a similar framework for structuring the costs of cybercrime to society. The framework, illustrated in Figure 2.1, structures the costs along two dimensions. The first distinguishes between three costs to society: direct losses, indirect losses, and defense costs, similar to Anderson (1999). According to Anderson et al. (2013), *direct losses* are the monetary equivalent of losses, damage, or other suffering that the victim experiences as a consequence of a cybercrime incident. They can be further subdivided into primary and secondary losses; secondary losses are additional costs, for example, the effort to reset account credentials (for vendors and consumers), the distress that victims suffer, deferred purchases, and other inconveniences. *Indirect losses* are the monetary equivalent of the losses and opportunity costs imposed on society because cybercrimes are carried regardless of whether they are successful or not. They include

[2] Note that these are two different authors, despite the (coincidental) common surname.

spending for law enforcement agencies and the legal system, but also the individual avoidance of online services by worried consumer, and other missed business opportunities, such as the inability for banks to communicate with customers via emails. *Defense costs* are the monetary equivalent of prevention efforts, which are spent in anticipation of crimes.



adapted from,
Anderson et al. (2013)

**Figure 2.1:** Conceptual framework of the societal impact of consumer-facing cybercrime

The second dimension of the framework separates the two types of consumer-facing cybercrime: *primary crimes* and *criminal infrastructure* (cf. Section 2.2.3). While only primary crimes create revenue for the criminal, both types lead to defense costs and indirect losses. Money spent on spam filters, malware removal, or botnet take-downs can be attributed to the criminal infrastructure.

Anderson et al. (2013) also collect existing estimates for different types of cybercrime, and they aggregate them within their framework. Acknowledging the high uncertainty in many of their estimates, they refrain from providing an overall cost estimate. However, they find that indirect losses and defense costs exceed direct losses, in particular for transitional cybercrime (cyber-enabled) and crimes unique to computer networks (cyber-dependend).

**Comparative Analysis** The two frameworks have many analogies. Both separate societal impacts into direct, indirect, and defense costs. The definitions of direct costs differ, as the concept of *transfers* (Anderson, 1999) only corresponds to primary losses in the framework of Anderson et al. (2013). However, secondary losses may be covered under opportunity costs by Anderson (1999). Another difference between the frameworks is the coverage of opportunity costs. While Anderson (1999) focuses on the lost opportunity with regard to the production and time of criminals and victims, Anderson et al. (2013) highlight the lost opportunity when innovative online services are avoided. Since information and communication technology (ICT) can provide extensive benefits in many situations, they speculate that the costs of avoidance are crucial in the context of cybercrime.

Anderson et al. (2013) do not explicitly include the risks to life and health. Methods for quantifying such risks in monetary terms exist in criminology. Dolan et al. (2005) estimate intangible costs, such as pain, grief, and other suffering, as a result of violent crime. Dolan and Peasgood (2007) extend the work to include intangible costs in anticipation of such crimes. Cybercrimes may also have emotional, social, or even physical impacts (Arief et al., 2015). Modic and Anderson (2015) find that the perceived emotional impact of scams can exceed the perceived impact of monetary losses. While methods for quantifying emotions for traditional crimes may be transferred to the context of cybercrime, we believe that they are of subordinate importance to the quantification of profit-oriented crimes in this dissertation.

### 2.3.2 Data Sources

The robust quantification of the societal impacts of consumer-facing cybercrime must be based on reliable data. We survey the most relevant sources and discuss their main advantages and limitations.

**Police-recorded Statistics** The natural sources for quantifying crime are police-recorded statistics. The approach works well for many traditional crimes, in particular, if a police report is required for victims to receive insurance payments. In the context of cybercrime, however, a number of limitations and caveats cause police-recorded statistics to be doubted. The first is a lack of consensus on what constitutes a cybercrime. As an authoritative definition is missing (see Section 2.2.1), some offenses may be classified as cyber when in fact they are not, while others may be concealed within other crime statistics (Kerr, 2003). The international nature of cybercrime further impedes its correct geographic allocation.

The second limitation is underreporting (Van Dijk, 2015; Bidgoli and Grossklags, 2016). In Germany, only 64 426 out of (an estimated) 14.7 m cybercrime incidents (0.4 %) made it into the police-recorded statistics in 2013 (Rieckmann and Kraus, 2015). In the US, only 8 % of IDT victims stated that they have filed a report (Harrell, 2015). Perceptions that the incident was not significant, that the police could not help, or the fact that victims did not know how to report it, are the most common reasons for not reporting (Harrell, 2015; Rieckmann and Kraus, 2015).

Involved businesses, such as online shops or payment service providers, can observe incidents as well; however, they are often reluctant to share information publicly or with authorities (e. g., Laube and Böhme, 2016). Their reasons include worries about reputational damage or legal liabilities (Cavusoglu et al., 2004). Furthermore, they may lack of incentives to spend extra costs on reporting crimes when, to their knowledge, little is done with those reports by law enforcement agencies. In 2013, for example, only 2 % of businesses in the UK stated that they report cybercrime incidents to the police (McGuire and Dowling, 2013).

Other official entities, such as the Internet Crime Complaint Center in the US[3], have similar problems. While they may capture the range of existing offenses, reporting will always be incomplete. With regard to the estimation of the societal impacts of cybercrime, official statistics are further limited because they do not include defense costs and indirect losses.

**Direct Observation** Another source of empirical data is direct the observation of criminal activities. The approach is particularly appealing in the cyber context, where (semi-)automated tools can perform the data collection. The range of applications comprises the identification of malicious uniform resource locators (URLs) using passive domain name system (DNS) analysis (Bilge et al., 2014) and the control over portions of spam-sending botnets to measure their size and understand their modes of operation (Kanich et al., 2008). These sources help one understand particular types of cybercrime. However, they are strongly limited when it comes to cost estimation because they are designed to track attack trends, not the actual impacts.

Studies that attempt to obtain price quotes for criminal artifacts from underground markets or criminals' communication channels are subject to similar issues (e. g., Franklin et al., 2007; Thomas et al., 2013). While prices, for example, for malware, may indicate the amount of money that criminals handle, the success of attacks and the actual impact on victims cannot be observed. A few studies aim to analyze criminal value chains more comprehensively by incorporating information on the impacts. Levchenko et al. (2011), for example, analyze the spam value chain and McCoy et al.

[3] The Internet Crime Complaint Center is operated by the Federal Bureau of Investigation to establish a central and reliable point for reporting Internet-facilitated criminal activity (URL: `https://www.ic3.gov/`).

(2012) look at the business models of online pharmaceutical affiliate programs. While these studies are better suited to estimate costs, they are tailored to a particular type of cybercrime and miss the bigger picture.

Direct observation can be used to some degree to quantify defense costs and indirect losses. Indications of defense costs are revenues in the market for security products and services. However, the revenues neglect opportunity costs for the time spent by individuals and the salaries of employees working on security in organizations. An observation of indirect losses is possible in particular scenarios. Kosse (2013), for example, demonstrates that debit card use in the Netherlands dropped significantly on the day after media reports regarding debit card fraud.

**Victimization Surveys** Representative population surveys complete the canon of typical data sources. Unbelievably large estimates in many industry reports lead to a general suspicion of survey-based cybercrime reports in the security community (Ryan and Jefferson, 2003; Florêncio and Herley, 2013; Hyman, 2013). The criticism typically concerns the conducting entities' vested interest in exaggerating the results (e. g., Anderson et al., 2013) in a combination with opaque methodologies and the use of inappropriate methods. Indeed, most cybercrime reports are published by consultancies or security vendors, and the methodologies are often not publicly available.

Moreover, they inherit the main limitations of survey research. The cognitive bounds of the respondents, including the comprehension of cybercrime and memory of experiences (Tourangeau and Bradburn, 2010), and difficulties in reaching the relevant population (Florêncio and Herley, 2013) are possibly most important in the context of cybercrime. While cognitive bounds challenge the design of questionnaires and survey methods, the sampling issues render reliable data collection for large populations extremely cost intensive.

However, victimization surveys have many advantages in the context of cybercrime. They can uncover the "dark figure" of crimes – cases not reported to the police – enable a comparison between jurisdictions with different crime definitions, and collect information about the impacts of incidents directly (Van Dijk, 2015). Many larger countries already conduct periodic victimization surveys to measure traditional crime. The US National Crime Victimization Survey (in the US) (NCVS) for example, has been conducted annually since 1972 (Rand, 2006), and the British equivalent since 1982 (Jansson, 2007). Unfortunately, to date, cybercrimes are only partly covered in the periodic surveys, so far. We identify the most relevant surveys in Section 2.4.1.

Large-scale population surveys can also be used to quantify defense costs and indirect losses through avoidance behavior. They can measure perceptions, attitudes, and behavioral intentions, which makes them a useful tool for collecting data on behavior at an aggregate level.

### 2.3.3 Challenges of Robust Cost Estimation

When the appropriate data are collected, the remaining challenge is robust cost measurement. The most important challenges are sampling and the modeling of loss distributions.

Even though cybercrime is reported to be a serious and growing problem, it is still a rare phenomenon when surveying the general population. As (direct) losses are concentrated on the victims, a few respondents form a large part of the cost estimates in victimization surveys (Florêncio and Herley, 2013). As a result, a few respondents, who (un-)intentionally over report losses, potentially distort the overall estimate in a representative sample of 1 000 or more respondents. Larger samples and robust statistical methods can reduce the impact of this response error. Viega (2012) suggests the inclusion of cybercrime in traditional victimization surveys, which often use larger than a representative samples and benefit from the methodological experiences of national statistics bureaus

(Jansson, 2007). A prime example is the IDT supplement to the NCVS in the US, which yielded more than 60 000 responses and improved the reliability of cost estimates by re-confirming large loss amounts (> $ 1 000) during the interview (Harrell and Langton, 2013; Harrell, 2015).

The second challenge is the estimation of costs because, in most survey-based studies, the majority of victims loses nothing, while a few experience severe losses (Florêncio and Herley, 2013). Loss distributions are consequently zero-inflated. The large number of zero-losses may be explained by attempted but unsuccessful crimes, reflected, inter alia, in extremely small spam conversion rates (Kanich et al., 2008), or in the small number of credit card credentials that are actually used for fraud after a data breach (Graves et al., 2014). Harrell (2015) report that as much as 35 % of the victims of IDT did not experience a financial loss after the incident. Other relevant victimization surveys (Rieckmann and Kraus, 2015; Hernandez-Castro and Boiten, 2014; Symantec, 2016a) do not report the level of zero losses.

Furthermore, loss distributions are skewed even for non-zero losses. While the majority of victims loses small amounts, some high-value outliers report to losing much more. Florêncio and Herley (2013) demonstrate that, where available, the median loss is significantly smaller than the mean, indicating a skew to the right. Levi et al. (2017) report equivalent characteristics for fraud losses in the UK, and these are also present in all recent victimization surveys (Hernandez-Castro and Boiten, 2014; Rieckmann and Kraus, 2015). For instance, the average loss of IDT victims in the US is $ 1 343, with a median of $ 300 (Harrell, 2015). This renders estimates based solely on arithmetic means problematic.

## 2.4 Evidence of Societal Impacts

We present different types of existing evidence for the societal impact of cybercrime. Section 2.4.1 provides an overview of existing victimization surveys, and Section 2.4.2 summarizes the little data, available to measure indirect impacts due to avoidance.

### 2.4.1 Victimization Surveys

Victimization surveys primarily report the losses inflicted on the victims of cybercrime. While many surveys report the impact of cybercrime on businesses (e. g., Ponemon Institute, 2015; PwC, 2015), less work has been conducted for consumers. We summarize survey-based cybercrime reports in Table 2.1, with a focus on the EU and the US. Our selection is not exhaustive; however, we cover what we believe to be the most comprehensive efforts. Comparable overviews can be found for traditional crimes in the US (Anderson, 2012), academic studies on the costs of crime (Wickramasekera et al., 2015), and for some costs of cybercrime in developed countries (Levi, 2017).

Large-scale victimization surveys are typically conducted by public entities. In the US, Harrell and Langton (2013) and Harrell (2015) surveyed massive samples of more than 60 000 consumers regarding the impact of IDT in a supplement of the NCVS.[4] They find that the identity of 7 % of US consumers was "stolen"[5] in 2014, leading to overall costs of $ 15.4 bn – 0.08 % of the US gross domestic product (GDP). The most prevalent thefts are associated with credit cards and bank accounts. The losses include the money stolen by the criminals but also follow-up costs incurred

[4] While they cover various types of IDT, also including the misuse of personal information to receive medical care, a job, or government benefits (Harrell and Langton, 2013; Harrell, 2015), most are cybercrime.

[5] The term "identity theft" is suggestive in the sense that it blames the victims of not guarding their identifying information. We stick to this convention for its wide adoption, remarking that a technically more precise description for this kind of incidents is "authentication failure".

**Table 2.1:** Survey-based cybercrime reports

| Reg. | Y. | Report | Cybercrimes covered | Loss | Method |
|---|---|---|---|---|---|
| US | '14, '12 | Victims of Identity Theft (Harrell and Langton, 2013; Harrell, 2015) | Several types of identity theft | Yes | Available |
| EU | '14, '13, '12 | Special Eurobarometer on Cyber Security (EB77.2, 2012; EB79.4, 2013; EB82.2, 2015) | Identity theft, online shopping fraud (OSF), extortion, scams, malware, . . . | No | Available |
| DE | '15 | Cybercrime in Germany (Rieckmann and Kraus, 2015) | Identity theft, OSF, phishing, malware | Yes | Available |
| UK | '17 | Crime in England and Wales (Flatley, 2017) | Different types of fraud and computer misuse | No | Available |
| UK | '14 | Cybercrime in UK (Hernandez-Castro and Boiten, 2014) | "Online or computer-based fraud" and "online criminal activity" | Yes | Available |
| Glob. | '14, '13, '12 | Norton (Cyber crime) Report (Symantec, 2012; Symantec, 2013; Symantec, 2016a) | Not specified | Yes | Partly available |

Region (Reg.): United States (US), European Union (EU), Germany (DE), United Kingdom (UK).

by individual victims, such as legal fees or bounced checks. The methods used in both reports are comprehensively documented and the microdata is available for secondary research.

The Special Eurobarometer series on cyber security (EB) contains the largest cybercrime surveys in the EU (EB77.2, 2012; EB79.4, 2013; EB82.2, 2015). Representative data on the prevalence of various types of cybercrime has been collected in three subsequent years (2012 – 2014) for all 28 EU member states. Methods and microdata of the whole series are available. The most recent report covers IDT among other types, such as online shopping fraud, scams, and extortion (EB82.2, 2015). In comparison to the US, more consumers (9 %) have experienced Internet-related IDT in 2014.[6] While the EB series includes questions on perceptions and intentions, which could be use to analyze indirect losses, it does not ask for losses or other impacts directly related to victimization. Such surveys only exist on the national level in some countries.

In the UK, Hernandez-Castro and Boiten (2014) used Google Customer Surveys to ask 1 500 consumers about their losses to online fraud[7], finding the average loss for all consumers was £ 1.5 over the last two years, even though 83 % lost nothing. They asked for losses caused by *online criminal activity* (a similar term) in a second survey[8], surprisingly finding that while even more lost nothing (92 %), 2.3 % lost more than £ 10 000. Fraud and computer misuse are also included as experimental (not fully developed) statistics without costs in the latest victimization survey in the UK (Flatley, 2017). The Germany Institute for Economic Research (DIW) conducted a large scale victimization survey of more than 12 000 consumers tailored to cybercrimes (Rieckmann and Kraus, 2015). They report that the annual costs of cybercrime in 2015 in Germany were largely driven by malware infections and as high as € 3.4 bn (0.11 % of GDP).

In the private sector, security vendor Norton published a series of reports on consumer-facing

[6] We combined victims of identity theft (5 %; Question *QB8.1* (EB82.2, 2015)) and bank card or online banking fraud (6 %; Question *QB8.8* (EB82.2, 2015)) to compare the victimization to the US survey. Note that the types of IDT and the wording differ between both surveys.

[7] "How much money have you lost due to online or computer based fraud in the last two years ?" (Hernandez-Castro and Boiten, 2014).

[8] "How much money have you lost in the last year due to any kind of computer criminal activity ?" (Hernandez-Castro and Boiten, 2014).

cybercrime. The 2016 report estimates that global consumer losses to cybercrime are as high as \$ 150 bn (Germany: € 2 bn, UK: £ 1.7 bn, US: \$ 28.9 bn). On average consumers lose \$ 358 and 21 hours annually (Symantec, 2016a).[9] As information about the methodology, the sample, and the included crimes is not available, little can be said about the reliability of these figures.

Protection expenses are not covered in victimization surveys, but the size of the market for security products may be used as an anchor. The advisory firm Gartner estimates that global spending for cyber security products and services reaches \$ 86.4 bn in 2017 (7 % increase over 2016), and is expected to grow further (Gartner, 2017). Even though, the estimates include organizational spending, they point to the importance of protection expenses.

### 2.4.2 Indirect Costs through Avoidance

Lost opportunities due to individual avoidance of ICT are suspected to account for a substantial part of the overall cost of cybercrime (Anderson et al., 2013). Hesitant or refusing consumers, who avoid ICTs to keep away from cybercrime, miss out on the many benefits of technology and chose alternatives which are economically less efficient. Empirical evidence of indirect costs caused by avoidance is extremely rare.

Anderson et al. (2013) put a vague price tag on some parts. They estimate the costs of online banking avoidance in the UK with a "back-of-the-envelope" calculation. They multiply the 16 % of UK consumers, who reported to avoid online banking, with an unofficial estimate of a reduction of \$ 70 in support cost for every new online banking customer. This results in \$ 700 m indirect costs, caused by avoidance of online banking in the UK in 2010. The vague estimate should be seen as an upper bound. Nevertheless, the number indicates the potential scale of indirect costs, if all online services and technologies are considered.

A recapitulation of the socio-economic benefits of ICT backs up this indication. Online services provide extensive individual and socio-economic benefits to modern society. Online banking has introduced a convenient yet inexpensive and effective way of remotely handling financial transactions (Lee, 2009); e-commerce has increased product availability while decreasing trading costs (Li and Huang, 2009); and online social networks have deepened personal relationships worldwide (Amichai-Hamburger and Hayat, 2011). Reviewing the economic growth literature, Cardona et al. (2013) show that ICT increased labor productivity in the EU by at least 31 % (33 % in the US) since 1995. Brynjolfsson (1996) emphasizes the magnitude of the consumer surplus generated by online services, which provides additional social welfare not reflected in the traditional statistics. Brynjolfsson et al. (2003) demonstrate the importance of consumer surplus for the case of online book stores.

Only a few scholars study avoidance in reaction to cybercrime. Saban et al. (2002) conduct an exploratory study in three US cities, finding that exposure to spam emails reduces consumers' Internet purchases and the trust in online information. Smith (2004) proposes that expectancy theory can explain the negative effect cybercrime has on online shopping. However, he does not supply his propositions with any empirical data. Focusing on cybercrime in Europe, Böhme and Moore (2012) are first to conduct a secondary analysis of the 2012 EB survey, a pan-European population survey. Using a set of simple logistic regressions, they found that cybercrime experience, media exposure, and cybercrime concern decrease the likelihood of using online services. Their approach provides valuable insights, but lacks a theoretical model of behavior to formalizes multi-stage considerations of the effects and the measurement of latent variables.

[9] Earlier surveys report global average costs per consumer of \$ 298 in 2013 (Symantec, 2013) and \$ 197 in 2012 (Symantec, 2012).

# Chapter 3

# Individual Security Behavior

In the previous chapter, we uncover that online service avoidance is one reaction to cybercrime that potentially leads to high costs. However, research on security behavior largely neglects avoidance as a form of protection and focuses on more active responses (Chen and Zahedi, 2016). This corresponds to the general focus in information systems (IS) research on positive behavioral outcomes, most importantly the adoption and use of technologies. Negative outcomes, i. e., avoidance or discontinuance, are less commonly studied (Recker, 2016). Accordingly, enabling factors dominate over inhibiting factors in adoption studies. The latter are often simply treated as the antipoles of enablers, even though they may be inherently different (Cenfetelli and Schwarz, 2011).

This chapter introduces theories of security behavior with an emphasis on theories that can be used or adapted to study avoidance. We start fundamentally, with a multi-disciplinary background on explaining individual behavior in Section 3.1. The next two sections survey the applications of two central IS theories in the security context. Section 3.2 reviews the use of Technology Acceptance Model (TAM) to study the impact of perceived risk on the adoption of online services and security software. Section 3.3 introduces Protection Motivation Theory (PMT) to explain engagement in protective actions. Section 3.4 closes with an overview of less commonly used theories.

## 3.1 Explaining Individual Behavior

Individual behavior forms societies and economic systems, making it an essential part of the field of economic studies. Since the inception of modern economics, which dates back to Adam Smith (1723–1790), a large number of theories have been developed and structured in different schools of thought (Hunt, 2015). We do not want to engage in a fundamental discussion on the most appropriate school. Instead, we use selected theories to explain the mechanisms and influencing factors of individual decisions, and we ultimately map them to security behavior.

**Broader Context** According to the New Chicago School Model (Lessig, 1998), individual behavior is regulated by four constraints: laws, social norms, markets, and architectures. Laws regulate behavior through centralized enforcement by a state, and social norms control it through established morals in a society. Given a set of laws, norms, and the scarcity of resources, markets further regulate behavior through prices. The last set of constraints is associated with the architecture of the environment, which can be man-made or naturally existing. Individual behavior is regulated by all four constraints simultaneously and to different degrees. Outcomes at the societal level are grounded in microlevel behavior, which is formed by rational choices (Blume and Easley, 2008).

**Rational Choice** According to Wittek (2013) rational choice is used as an umbrella term for a variety of models that assume that individuals make cost-benefit calculations and choose the alternative with the highest expected utility. A narrower use of Rational Choice Theory (RCT) in neo-classical economics makes three key assumptions regarding rational individuals: they have selfish and stable preferences, they maximize their own utility, and they act independently based on full information. Assuming full information requires that individuals are aware of all alternatives, know probabilities and consequences of outcomes, and are not cognitively limited in the processing of this information.

Becker (1976) demonstrates that RCT-based models explain human behavior in a wide range of settings, including criminal motivation and behavior. Scott (2008) states that the use of RCT has lead to a variety of powerful economic models. The downside of RCT is that its assumptions are likely violated in real-life situations because unlimited cognitive capabilities and unrestricted information are hardly ever available. Therefore, individuals rarely make purely rational decisions.

**Bounded Rationality** Based on this criticism, Simon (1957) proposed a theory of bounded rationality and the concept of *satisficing*, which is a combination of the words: "satisfy" and "suffice". It postulates that rational decision makers are typically bound to *satisficing* rather than strict optimizing because of limited cognitive capabilities or incomplete information. A plethora of work followed in psychology and sociology to study the bounding factors in human decision processes more profoundly. Kahneman and Tversky (1979) propose the Prospect Theory, which states that individual decisions differ depending on the expectancy of gains or losses, and Gigerenzer and Goldstein (1996) emphasize the importance of heuristics for fast decisions under uncertainty. Kahneman (2003) summarizes many contributions within a framework of bounded rationality, highlighting the importance of framing effects, the heuristics that individuals use in uncertain situations, and loss aversion in choice under risk.

Kahneman (2003) further states that human decisions are made within one of two systems: *intuition* or *logical reasoning*. Similar dual-path models are proposed to distinguish between perceptions of risk as *feelings* or *rational analysis* (e. g., Loewenstein et al., 2001; Slovic and Peters, 2006). According to these models, individuals may not reason poorly, but rather act intuitively or emotionally. The consideration of bounded rationality has led to the new field of behavioral economics, which exists alongside the rational, neo-classical schools of thought.

**Explaining Behavior** Other psychological theories largely side-step the discussion on rationality and focus on explaining behavior over which individuals have self-control. The Theory of Reasoned Action (TRA; Fishbein and Ajzen, 1975), explains how *attitudes* and *subjective norms* form the intention to engage in a particular behavior. This intention ultimately predicts behavior. Attitudes are based on beliefs about the likelihood that behavior will result in desired consequences, and subjective norms combine normative beliefs with the will to comply (Ajzen and Fishbein, 1980). The Theory of Planned Behavior (TPB) improves the predictive power of TRA by adding a third antecedent of intention and behavior. *Perceived behavioral control* represents the judgment of how well an individual can execute the courses of action required by the intended behavior (Ajzen, 1991).

TRA and TPB are powerful predictive models, if three requirements are satisfied: the specificity of the measure of intention corresponds to that of actual behavior, intentions are stable between the time of measurement and the performance of behavior, and the implementation of intentions is under the volitional control of the individual (Madden et al., 1992). Both theories have been applied to several settings, including leisure activities (Ajzen and Driver, 1992) and health-related (Godin and Kok, 1996), or unethical behavior (Chang, 1998). TPB does not require a rational decision maker, since attitudes, subjective norms, and perceived behavioral control can be influenced by bounding factors, such as poor information, unconscious biases, or irrational processes (Ajzen, 2015).

**Mapping to Security Behavior** The technical architecture of computer networks and social norms are the main regulators of individual security behavior on the Internet. Furthermore, this behavior is likely shaped by bounded rationality. Bounding factors include the comprehension of all risks and benefits tied to the use of online services and the Internet. This is due to the complexity and ongoing innovation of software, computers, and networks. Many decisions are ad-hoc, for example, the decision as to whether an email should be opened or a website should be trusted, and they require the use of some heuristics. However, at the aggregate level, rational behavior in the wider sense may be observable. For instance, Internet users purchase security products to reduce the risk of cybercrime based on cost-benefit calculations, or they may avoid online services that are perceived to be more risky than beneficial to them.

The explanation of individual behavior in interaction with information and communication technology (ICT) is one of the core competences of the IS discipline. In comparison to economics and psychology, IS is still a young discipline. It largely builds on existing theories and contextualizes them in the ICT domain (e. g., Pavlou and Fygenson, 2006; Dinev and Hu, 2007). The remainder of this chapter presents IS models, which have been used to the study individual security behavior.

## 3.2 Technology Acceptance Model

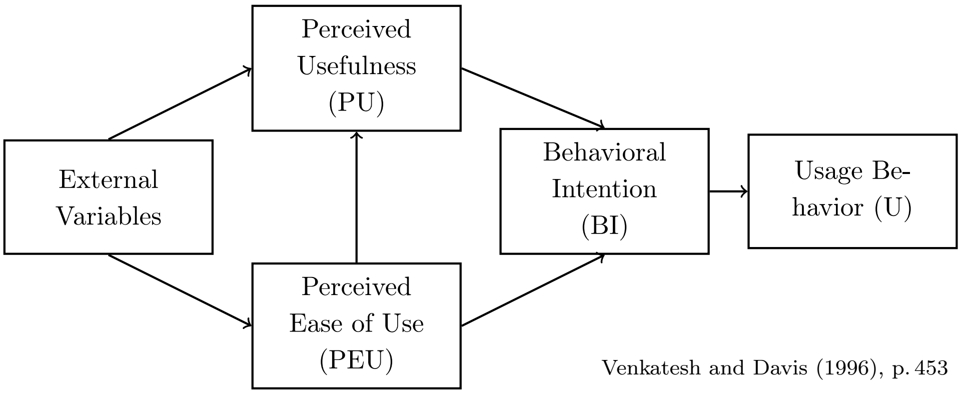
The TAM, proposed by Davis (1989), is among the most commonly used models of individual behavior in IS research. We introduce it in Section 3.2.1 and provide an overview of its applications for online service adoption. Thereafter, we present two kinds of security behavior that are studied using TAM. The perceived risk-extended TAM in Section 3.2.2 studies the negative impact of security concerns on the adoption of online services. Section 3.2.3 summarizes studies that build on TAM (and similar models) to study the adoption of protection technologies.

### 3.2.1 Origin

TAM is based on TRA and tailored to explain and predict the acceptance of ICTs. It replaces the general constructs, *attitudes* and *subject norms*, with the following two technology acceptance measures: *Perceived Ease-of-Use* (PEU) and *Perceived Usefulness* (PU). PEU is defined as "the degree to which a person believes that using a particular system would be free from effort"(Davis, 1989, p. 320), and PU is "the degree to which a person believes that using a particular system would enhance his or her job performance" (Davis, 1989, p. 320). TAM proposes that PEU and PU of a technology are the key variables of interest in explaining the *Attitudes Toward Using* (ATU) it. A positive ATU increases the *Behavioral Intention* (BI), which ultimately determines the actual *Usage* (U) of a technology.

TAM has been continuously refined. Figure 3.1 illustrates the parsimonious version of the model, that Venkatesh and Davis (1996) use to test different antecedents of PU and PEU. The ATU construct has been dropped from the model, and external variables, which influence PEU and PU, have been added. The core effects are the same: PEU increases PU, both increase the BI to use a technology, and BI predicts U. Legris et al. (2003) find that they are mostly convergent across TAM studies.

TAMs are usually validated empirically with either multiple regressions or structural equation modeling (SEM) approaches. The advantage of SEM lies in its ability to include latent variables and provide consistent parameter estimates (Urbach and Ahlemann, 2010). Latent variables – PEU, PU, and BI – are measured using factor analysis of multiple indicators, and the structural links are simultaneously estimated using path analysis.


Perceived Usefulness (PU)
External Variables
Behavioral Intention (BI)
Usage Behavior (U)
Perceived Ease of Use (PEU)

Venkatesh and Davis (1996), p. 453

**Figure 3.1:** Parsimonious version of the Technology Acceptance Model

**Applications** TAM's parsimony, robustness, and predictive power lead to its wide usage in empirical studies (Venkatesh and Davis, 2000). Even though, it has been constructed to explain employees' adoption of company-owned, work-related software (Davis, 1989), many studies show its applicability for a wide spectrum of other technologies (Legris et al., 2003; Yousafzai et al., 2007). Several extensions exist. TAM2 adds social influences and cognitive instrumental processes to the original model, to explain PU and BI (Venkatesh and Davis, 2000). Social influences comprise subjective norm, voluntariness, and image. Cognitive instrumental processes comprise job relevance, output quality, and result demonstrability. TAM3 further extends TAM2 to include antecedents of PEU (Venkatesh, 2000; Venkatesh and Bala, 2008). It focuses on managerial interventions to increase acceptance and effective utilization of ICT in organizations. The Unified Theory of Acceptance and Use of Technology (UTAUT), proposed by Venkatesh et al. (2003), intends to unify TAM and its extensions with competing theories to derive a combined model of use intention and behavior.

TAM and UTAUT models have been widely used in studies of online services. A literature review of 165 publications that consider the adoption of online banking between 1999 and 2012 shows that the majority applies either of the two models to test relations between the constructs (Hanafizadeh et al., 2013). A similar proliferation of acceptance models is found for online shopping adoption (Chang et al., 2005). Zhou et al. (2007) develop the Online Shopping Acceptance Model (OSAM), extending TAM for application in an online shopping scenario. Models to study the adoption of online social networking (OSN), however, mostly focus on other factors, such as network externalities (Lin and Lu, 2011) or connectedness and participation (Jiao et al., 2013). Nevertheless, a few studies also apply TAM in the OSN context. Shin and Kim (2008) extend it with *Perceived Involvement* and *Enjoyment*. Pinho and Soares (2011) show its applicability for a set of 150 students. However, they remark that the use of the parsimonious, unextended TAM model limits their study.

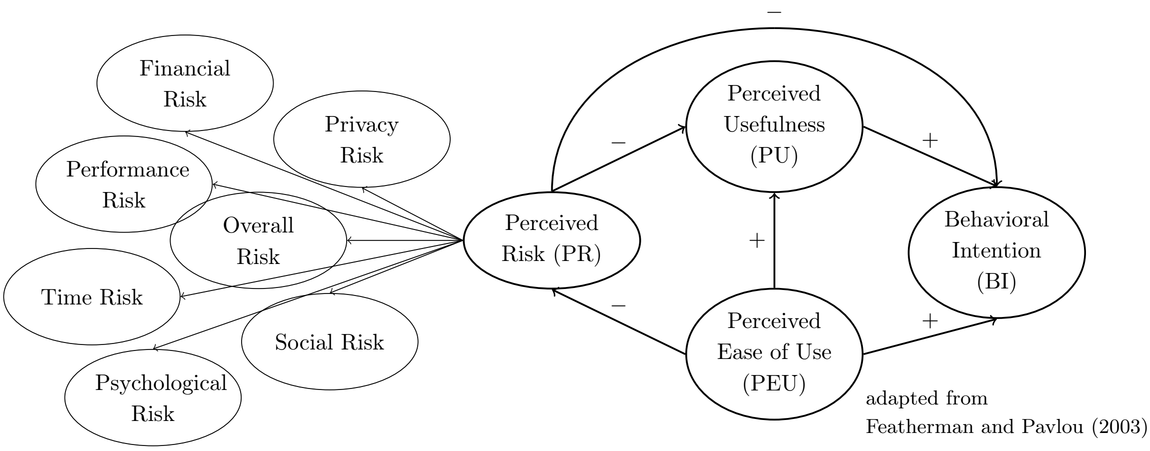
**Critique** The parsimony has been criticized to be an Achilles' heel of TAM. Bagozzi (2007) states that it is unreasonable to expect that one model can explain decisions and behavior fully across a wide range of technologies and adoption situations. Moreover, the large amount of independent attempts to expand TAM to adapt it to the constantly changing IT environments has lead to confusion regarding which iteration or modification is the most appropriate (Benbasat and Barki, 2007). In the context of individual security behavior, the basic TAM and UTAUT models miss at least one important factor – *Perceived Risk* – crucial for adoption in online scenarios (Featherman and Pavlou, 2003).

### 3.2.2 Perceived Risk Reducing Technology Acceptance

The negative impact of *Perceived Risk* (PR) on technology acceptance is one form of individual security behavior. The importance of PR in commercial transactions was already identified by Bauer (1960), who states that shopping always involves risk because the buyer's decision has uncertain consequences that can be unpleasant and are not perfectly predictable. The spatial and temporal separation between consumers and retailers and the open architecture of the Internet increase this uncertainty (Pavlou, 2003). Therefore, PR is more pronounced in online shopping than in traditional brick-and-mortar shopping (Tan, 1999).

Two forms of uncertainty are naturally present: *behavioral* and *environmental* (Pavlou, 2003). Behavioral uncertainty is concerned with the behavior of dubious and possibly malicious online merchants. Environmental uncertainty reflects a more general concern about the security of the Internet as a channel for commercial transactions. Both can increase the level of PR, as the customer is not able to monitor the seller's behavior or the security of the online transaction in general (Chiu et al., 2014). Since individuals feel threatened by uncertain situations and try to avoid them, PR potentially limits the intention to use online services (Gefen et al., 2003; Chiu et al., 2014).

**Perceived Risk-extended TAM** Consequently, PR likely accounts for variance in the BI variable of TAM, when applying it to online services (Pavlou, 2003). Featherman and Pavlou (2003) systematically integrate PR, as a multidimensional construct with several types of risk (as shown in Figure 3.2). The construct was originally introduced as a general PR construct by Cunningham (1967). Featherman and Pavlou (2003) find empirically that performance related risks, i. e., time, privacy, and financial risks, have the strongest influence on PR. Social risks, concerned with losing the current social status, were not found to have a significant influence.



adapted from
Featherman and Pavlou (2003)

**Figure 3.2:** *Perceived Risk* extended Technology Acceptance Model

Figure 3.2 illustrates that PR reduces the BI to use an online service directly and indirectly by reducing its PU. The negative impact exists for initial as well as repeated online shopping and is found to be larger for less experienced Internet users (Featherman and Fuller, 2003). PEU can mitigate the negative effects of PR because it reduces uncertainty and increases the user's confidence in using an online service (Featherman and Pavlou, 2003). Featherman et al. (2010) build on the PR extended TAM to test the impact of privacy risk on PEU and the BI to use e-commerce. They find that the PEU as well as the vendor's *credibility* and *capability* reduce privacy risk and increase adoption. The focus on e-commerce and the sole consideration of privacy risks, neglecting for example online fraud, limit their study. Martins et al. (2014) confirm the importance of risks by integrating the UTAUT model with the PR theory. They derive a combined model which is able to explain 81 % of the variance in usage behavior for 248 online banking customers and provide further evidence that financial, time, and privacy risks are the most salient concerns.

**Trust** Trust (TR) is often described to be the counterpart of perceived risk (e. g., Featherman and Pavlou, 2003) because trust in an online seller and the Internet in general reduces the PR of online transactions. Therefore, it can be another important factor in the adoption process of online services, mitigating behavioral uncertainty (Pavlou, 2003). A number of studies include TR (e. g., Jarvenpaa et al., 1999; McKnight et al., 2002; Gefen et al., 2003; Suh and Han, 2003; Lin, 2006). Montazemi and Saremi (2013) show the importance of TR for online banking adoption by conducting a meta analysis, which incorporates 26 SEM models into a single random effects SEM. Their aggregated findings suggest that TR is the most important factor for the initial use intention of online banking, outperforming the original TAM factors, PEU and PU. Metzger (2006) finds that having trust in an OSN provider is strongly linked to disclosure of information and participation in social networks.

**Studies of Online Service Adoption** Table 3.1 summarizes this subsection. It demonstrates that PR-extended technology acceptance models, especially TAM and UTAUT, are frequently applied to study adoption of different online services. The findings are mostly consistent. The general hypotheses of TAM – PU and PEU increase the BI to use a technology – are confirmed for online services. PR is an important negative factor in the initial and continuous use of online services (Chiu et al., 2014) and should be included, either as antecedent (e. g., Featherman and Pavlou, 2003; Im et al., 2011) of PU, PEU, and BI or as a moderating factor (e. g., Featherman and Fuller, 2003; Chiu et al., 2014). The negative influence of PR on BI or one of its antecedents, i. e., PEU or PU, is frequently shown. Finally, TR is shown to be reducing PR and increasing BI.

Most research using such models is conducted within the online banking domain, including comparative studies (e. g., Lee, 2009) and national applications around the globe (e. g., Wang et al., 2003; Riffai et al., 2012; Martins et al., 2014). TR is more frequently used in the context of online shopping (e. g., Gefen et al., 2003). However, some studies also use PR or both constructs (e. g., Faqih, 2011). The adoption of OSN is less frequently tested with technology acceptance models, however, some studies show their applicability (e. g., Shin, 2010).

### 3.2.3 Adoption of Protection Software

The second form of security behavior, analyzed with acceptance models, is the adoption of protection technology. This changes the focus of studies from negative impacts of PR on adoption of online services (as presented in the previous section) to positive impacts of PR on the BI to use protection technology. Anderson and Agarwal (2010) review the behavioral security literature. They show that TAM and its foundation TPB have been used to explain the adoption of security software.

Using a TPB-based model, Dinev and Hu (2007) analyze user intentions and behavior toward protective technologies. They find that *Threat Awareness* is a strong predictor of using protective technologies, whereas PEU and *Computer Self-efficacy* are not significant. They suggest that this is due to the difference between positive and protective technologies. The latter are used out of fear

**Table 3.1:** Literature on the influence of *Perceived Risk* on the adoption of online services

| **Year** | **Model** | **Method** | **Findings** | **Reference** |
|---|---|---|---|---|
| **e-Services** | | | | |
| 2003 | TAM-PR | SEM | PR ↘ PU, BI; PR as 2nd order construct | Featherman and Pavlou (2003) |
| 2003 | TAM-PR | ANOVA | PR ↘ PU, BI; PR moderates effects | Featherman and Fuller (2003) |
| **Online banking** | | | | |
| 2003 | eTAM | SEM | Credibility, PU, PEU ↗ BI | Wang et al. (2003) |
| 2006 | eTAM | SEM | PU, PEU, TR(Web Security) ↗ BI | Cheng et al. (2006) |
| 2009 | TAM-TPB-PR | SEM | PR ↘ ATU (ultimately BI) | Lee (2009) |
| 2011 | UTAUT-PR | SEM | PR ↘ BI | Im et al. (2011) |
| 2012 | eUTAUT | Correlation | PR moderates: PU, PEU ↗ BI | Riffai et al. (2012) |
| 2012 | TAM-IDT | PLS | PEU, TR(Web Security) ↗ BI | Giovanis et al. (2012) |
| 2013 | TAM-TR | Meta-SEM | TR ↗ BI | Montazemi and Saremi (2013) |
| 2014 | UTAUT-PR | SEM | PU, PEU, Comp. ↗ BI; PR ↘ BI | Martins et al. (2014) |
| **Online shopping** | | | | |
| 2003 | TAM-PR | PLS | TR ↗ PU, BI | Pavlou (2003) |
| 2003 | TAM-TR | SEM | TR, PU ↗ BI | Gefen et al. (2003) |
| 2010 | TAM-PR | SEM | PR(Privacy), Credibility, PEU ↗ BI | Featherman et al. (2010) |
| 2011 | TAM-TR | PLS | PR ↘ TR; TR ↗ BI | Faqih (2011) |
| 2012 | PT-PR | PLS | PR moderates effects | Chiu et al. (2014) |
| **Online social networking** | | | | |
| 2010 | TRA-TAM | SEM | PR (Security & Privacy) ↘ TR, BI | Shin (2010) |
| 2010 | eTAM | SEM | PR not considered | Kwon and Wen (2010) |
| 2013 | TAM-PR-TR | SEM | No effect for: PR on PU, BI | Alarcón-del Amo et al. (2014) |

Model: Extended TAM (eTAM), Trust (TR), Perceived Risk (PR), Prospect Theory (PT), Compatibility (Comp.)
Findings: Positive Effect (↗), Negative Effect (↘).

of negative consequences, for which awareness becomes a key determinant. In a comparative study the role of *Threat Awareness* is stronger in the US compared to South Korea (Dinev et al., 2009). Lee and Kozar (2008) show empirically that *attitude*, *subjective norm*, *perceived behavioral control*, and *denial of responsibility* significantly affect the intention of anti-spyware adoption. Burns and Roberts (2013) study protective behavior as a result of exposure to cybercrime in general. Their results indicate that the impact of privacy attitudes and normative beliefs is mediated by intention, whereas *perceived behavioral control* directly affects protective behavior.

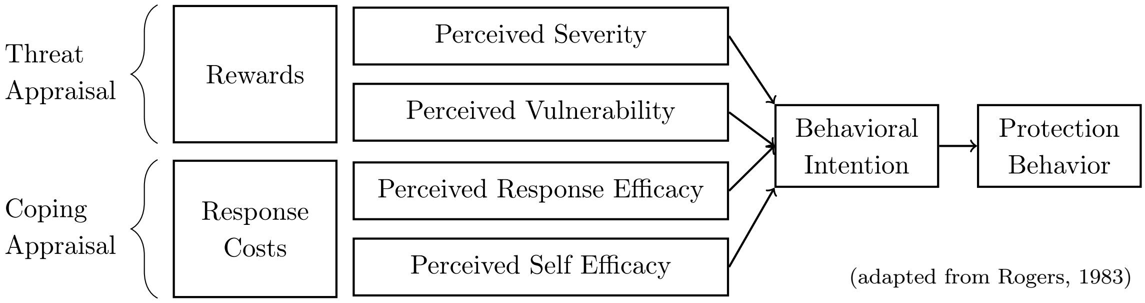
Mainly building on TAM, Kumar et al. (2008) study factors which affect the use of a firewall by home computer users. Their results suggest that attitude towards security and privacy protection technologies plays a more important role than PU in shaping users' BI. Johnston and Warkentin (2010) conjecture that individuals form perceptions of security technology not on the basis of performance gains, but rather on the basis of utility for threat mitigation. Shropshire et al. (2015) find that PEU, PU, and *organizational support* increase the BI to use protection technology in an organizational context. While these studies show that acceptance models can be used to study adoption of protection software, another stream of research is grounded on protection motivation.

## 3.3 Protection Motivation Theory

The PMT (Rogers, 1975) explains engagement in protection behavior with a threat and a coping appraisal. It is often applied to individual protection intention and behavior on the Internet. We introduce PMT in Section 3.3.1 and review its application in the context of security in Section 3.3.2.

### 3.3.1 Origin

Rogers (1975) proposed PMT to provide conceptual clarity to the understanding of fear appeals and their effects on attitude change. Rogers applied fundamental ideas of Richard Lazarus, who studied how people behave in and cope with stressful situations (Lazarus, 1966), to the context of fear appeals. A revision generalizes PMT to a more universal theory of persuasive communication using fear appeals (Rogers, 1983). However, the theory still emphasizes the cognitive processes that mediate behavioral change.



(adapted from Rogers, 1983)

**Figure 3.3:** Conceptual framework of the Protection Motivation Theory

PMT states that an individual's motivation or intention to protect them-self from harm are enhanced by four critical cognitions or perceptions: the *Perceived Severity* of the risk, the *Perceived Vulnerability* to the risk, the *Perceived Response Efficacy* of the risk-reduction behavior, and the *Perceived Self-efficacy* of performing this behavior. The first two cognitions create the threat appraisal and the last two the coping appraisal. Threat appraisals may be reduced by intrinsic or extrinsic rewards of performing the risky behavior and coping appraisals are reduced by the response cost. Consequently, PMT combines the assessment of threats (severity, vulnerability, and rewards) with coping factors (response efficacy, self efficacy, and responses costs) to explain individuals' motivation to protect themselves from negative outcomes.

Originally, PMT has been developed to study the impact of communications on health-related risks, including injury rehabilitation (Taylor and May, 1996), anti-smoking campaigns (Pechmann et al., 2003), and physical exercise campaigns (Milne et al., 2002). It has also been applied in other risk-related contexts, such as earthquake preparedness (Mulilis and Lippa, 1990). In a meta-analysis of 65 studies, Floyd et al. (2000) demonstrate that the main effects of threat and coping appraisals on behavioral intention and protection behavior hold with a moderate mean overall effect size.

### 3.3.2 Application in Online Security

PMT is mostly applied to study protection intention and behavior in response to cybercrime and security threats in an organizational context. Lee and Larsen (2009), for example, find that the four main cognitions have a significant influence on the decision of business executives in small and medium-sized enterprises to use anti-malware software. Johnston and Warkentin (2010) combine PMT with a social influence construct to investigate the influence of fear appeals on the compliance of students and university staff with recommendations to enact specific computer security actions. They find that the perception of a threat is an essential component of the motivation to use protection software and that fear appeals are most effectively communicated in a language suitable to the self-efficacy level of the recipients. Similarly, Ifinedo (2012) combine PMT with TPB to investigate employee's intention to comply with IS security policies. Using a partial least squares (PLS) analysis, they find that most PMT factors have a significant impact on individual compliance. Interestingly, *Perceived Severity* and *Response Costs* were not significant.

**Home Computer Users** Focusing on home computer users, Anderson and Agarwal (2010) find that protection intentions are influenced by a combination of cognitive, social, and psychological components and identify interventions that can positively influence protection intentions. Tsai et al. (2016) show that coping appraisals were the strongest predictors of online safety intentions, especially *Response Efficacy* and the extensions: *Habit Strength* and *Personal Responsibility.* Security knowledge has the strongest impact on coping appraisal which subsequently affects protection behavior (Srisawang et al., 2015). Hanus and Wu (2016) study the impact of security awareness on desktop security behavior. They find that security awareness significantly affects *Perceived Severity*, *Response Efficacy*, *Self-efficacy*, and *Response Cost.* In a meta-analysis of 28 studies, Sommestad et al. (2015) summarize that PMT is more powerful to explain security behavior if it is voluntary, the threat and coping appraisals are concrete, and the threat is directed at the computer users.

**Consideration of Avoidance** Naturally, PMT-based studies of individual protection focus on active protection behavior and neglect passive outcomes. The Technology Threat Avoidance Theory (TTAT) integrates PMT with the health belief model and risk analysis research to study avoidance behavior (Liang and Xue, 2009). TTAT explains threat avoidance as a form of individual coping (Lazarus, 1966) with malicious IT. It suggests that avoidance behavior is fundamentally different from adoption because "approach behavior always moves the current state toward the desired end state, while avoidance behavior has no affirmative direction as long as it separates the current state from the undesired end state" (Liang and Xue, 2009, p. 76). According to TTAT, individuals can perform two types of coping to deal with a threat: problem-focused, meaning the implementation of safeguarding measures, and emotion-focused, just accepting the threat.

Surprisingly, avoidance of risky situations, e. g., online banking, is not suggested as a coping alternative in TTAT. Furthermore, empirical applications only test the intention to use safeguards in different contexts (Liang and Xue, 2010; Arachchilage and Love, 2014), making them not significantly different from the PMT studies previously discussed.

We only find one study which is grounded in PMT and explicitly incorporates avoidance as security behavior. Chen and Zahedi (2016) integrate TTAT into a contextualized PMT model to study individuals' security perception and behavior. They specify three forms of coping: *protective action*, *seeking help*, and *avoidance* and test their model in a multi-group SEM analysis based on an online survey of 718 individual Internet users in the US and China. They find that all forms of coping are relevant. However, avoidance and seeking help are found to be more prevalent reactions to security concerns in China, whereas US citizens rather engage in protective action.

## 3.4 Related Theories

To complete the picture of theories on individual security behavior this section presents four theories, which are less commonly used. We outline each theory and show its application to security behavior.

**Expectancy Theory** Expectancy Theory (ET) was introduced by Vroom (1964) to understand individual motivation of employees to perform well in work tasks. It postulates that while the performance of employees is based on many individual factors, such as personality, skills, knowledge, and experience, all can be motivated by the same mechanisms. These mechanisms are a multiplicative function of three factors: *expectancy*, *instrumentality*, and *valence*. *Expectancy* concerns the perceived relationship between effort and performance, formulated as the belief that higher effort will yield better performance. *Instrumentality* concerns the relationship between performance and rewards, i. e., the belief that performing well results in receiving a higher payment, a promotion, or other recognition. Finally, *Valence* is the degree to which organizational rewards meet the individual's personal goals.

Some scholars apply ET in the context of security behavior. Smith (2004) states that ET can explain hesitation in adoptive behaviors associated with online purchases due to cybercriminal activities. Winkfield et al. (2017) create a theoretical model to understand the influence of leadership behaviors on employee compliance with non-technical IS security controls. However, both studies do not evaluate their model with empirical data. Burns et al. (2015) build on ET to assess the motivational influence of security education, training, and awareness programs. They find that two disparate security-related behaviors: proactive protection and psychological distancing can be explained by their model.

**Health Belief Model** An exact origin of the Health Belief Model (HBM) is not defined, but it is assumed that it was first used in 1950 by a group of public health service investigators in the US (Rosenstock, 1974). The HBM proposes that the likelihood of taking recommended preventive health action is influenced by several factors. An individual needs to believe that she was personally susceptible to a disease, that its occurrence would have an impact on some component of her life, and that taking a particular action would reduce her susceptibility, if the disease occurred. Taking preventive action entails overcoming important psychological barriers such as cost, convenience, pain, and embarrassment.

Liang and Xue (2009) integrate HBM in their TTAT model. Ng et al. (2009) study security behavior of computer users in the context of careful consideration of email attachments from a health belief perspective. They show that perceived susceptibility, perceived benefits, and self-efficacy are positive determinants of email related security behavior. On the other hand, security is usually viewed as an inconvenience, which may deter users from practicing safe behavior. Claar and Johnson (2012) use HBM to study computer security usage behavior in the home environment. Testing their model on a sample of 184 computer users they find that perceived vulnerability to security incidents and prior experience significantly contribute to the use of computer security.

**Communication-Human Information Processing Model** To structure research on digital warning messages, Wogalter (2006) proposes the Communication-Human Information Processing Model (C-HIP). The C-HIP model is a process model. It begins with a source that delivers a warning through a channel to a receiver. The reception of the warning may be paired with other environmental stimuli, which distract the receiver from the warning. The receiver goes through five information processing steps, which determine whether the warning results in behavioral change. The C-HIP model can be used to understand why warning messages are ineffective.

Egelman et al. (2008) use C-HIP to examine the effectiveness of active phishing warnings. They simulate a spear phishing attack to expose users to browser warnings. They find found that 97 % out of 60 participants fell for at least one phishing message. However, active phishing warnings were significantly more effective than passive warnings.

**Routine Activity Theory** Routine Activity Theory (RAT) was proposed as a theory in criminology by Cohen and Felson (1979) to analyze crime rate trends and cycles. It states that crimes require the meeting of a likely offender with a suitable target and the absence of a capable guardian against the crime. Cohen and Felson (1979) doubted that macro changes such as economic recessions and unemployment rates are the only factors for increasing crimes rates. Instead the increasing dispersion of activities away from households and families increases the opportunity for crime and thus generates higher crime rates. RAT is losely aligned with a set of theories and perspectives known as environmental criminology, which focuses on the importance of opportunity in determining the distribution of crime across time and space.

Some criminologists have tried to transfer the study of individual victimization using RAT in the context of the Internet and cybercrime (Holt and Bossler, 2008; Pratt et al., 2010). Kigerl (2012) uses RAT to analyze why some countries are more affected by cybercrime than others. While the theory has implications for victimization, it cannot really explain victim behavior or reactions to crime.

# Chapter 4

# Estimation of Direct Costs

Direct costs of consumer-facing cybercrime include victim losses and protection expenses. Reliable estimates of direct costs can inform policies, set law enforcement priorities, and tailor public education (Anderson, 1999). Furthermore, they can be used to evaluate the effectiveness of widely deployed security measures. In an anniversary note of the IEEE Security & Privacy magazine, Viega (2012, p. 16) concludes that a crucial goal of the security community must be "[. . . ] to figure out how well we're really doing, instead of leaving it to gut feelings and anecdotal evidence".

First steps towards reliable estimation have been made. Anderson et al. (2013) propose a framework of the social cost of cybercrime and use it to organize existing estimates. They find, for example, that protection expenses and indirect impacts largely exceed monetary losses of the victims. However, their analysis depends on many heuristics, assumptions, and extrapolations which are necessary to integrate different data sources in a single framework. Florêncio and Herley (2013) focus on cybercrime surveys. They remind us of methodological challenges when collecting data on rare phenomena with concentrated losses. They name sampling as a major issue of victimization surveys because representative samples are susceptible to be dominated by a few outliers.

We identify four shortcomings of current cost estimates: (1) the lack of primary data (2) collected with a tailored questionnaire that covers cost types systematically, (3) administered to consumers selected by concentration-aware sampling, (4) and evaluated with robust statistical methods.

We set out to address these issues by measuring the costs of profit-oriented cybercrime for consumers and present the following contributions to quantitative cybercrime research:

1. **Development of a measurement instrument.** We develop a survey instrument tailored to measure monetary and non-monetary costs of consumer-facing cybercrime with a victimization survey. More importantly, we discuss design choices in light of our resulting cost estimates.

2. **Representative data collection.** We use our instrument to collect primary data on the prevalence of seven types of consumer-facing cybercrime in six EU member states. We obtain a representative sample of Internet users in each country and oversample victims of cybercrime. The controlled oversampling is compensated by inverse probability weighting in the analysis.

3. **Assessment of cost estimation issues.** We study characteristics of the loss distributions for each type of cybercrime, in particular zero-inflation and skewness, and propose alternative statistical methods for the robust estimation of summary figures.

4. **Comparative analysis of cost estimates**. We include the cost factors *money* and *time* as well as the cost categories *victim losses* and *protection expenses* in the survey. We aggregate cost estimates and compare them along various dimensions to derive policy implications.

To the best of our knowledge, we are the first to estimate the costs of consumer-facing cybercrime using a specifically tailored instrument, data collection approach, and estimation method. However, economic and interview time constraints restricted us in the level of detail and limit the number of crimes and cost categories surveyed. Our analysis is also limited by the fact that the survey only offers a single snapshot without the option to implement iterations or split-sample designs. Our approach here is to discuss the constraints post-data and, where appropriate, derive lessons learned for future work.

The chapter is structured as follows. We develop the measurement instrument in Section 4.1 and present descriptive results of the victimization survey. Section 4.2 explores estimation issues and reports cost estimates. Finally, Section 4.3 discusses limitations, revisits central design choices in the light of our results, and derives implications based on a comparison of different estimates.

## 4.1 Measurement Instrument

Considering the critique and good practices in prior studies (summarized in Section 2.3), we develop a survey instrument tailored to estimate costs of consumer-facing cybercrime. The instrument enables the exploration of statistical issues and the comparison of cost estimates between different crimes, cost factors, categories, and countries. We start by setting up a framework of cost categories and cost factors in Section 4.1.1. Section 4.1.2 describes the sampling and fieldwork. Section 4.1.3 reports descriptive results on the prevalence of our selected types of consumer-facing cybercrimes in the six surveyed countries.

### 4.1.1 Framework of Costs

Reliable cost estimation needs to be based on a clear definition of costs. Where applicable, we call intentional consumer spending *expenses*, unintentional spending *losses*, and the aggregate of both *costs*. Our framework of cost factors and categories is illustrated in Figure 4.1.

The framework largely adapts previous work by Anderson et al. (2013) to measure the costs of cybercrime. It is coherent with cost categories used for traditional crime (Anderson, 1999; Dolan et al., 2005). We distinguish three aggregate *cost categories*: direct losses $\mathcal{L}$, indirect losses $\mathcal{I}$, and protection expenses $\mathcal{P}$. Each cost category can comprise a set of *cost factors* $\{M, T, C, S, \ldots\}$.

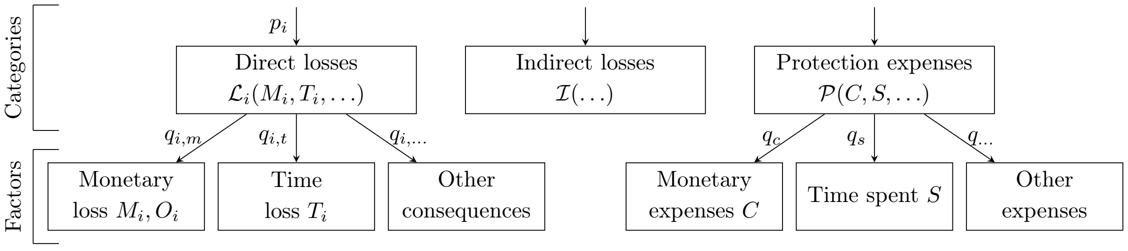


**Figure 4.1:** Model of cybercrime cost factors and aggregate cost categories

Direct losses of cybercrime victims $\mathcal{L}$ are further broken down to account for different types of cybercrime $i$ which occur with probability $p_i$. Accordingly, $\mathcal{L}_i$ represents the losses for one type of cybercrime and $\mathcal{L}$ for all crimes. Even though our framework allows for the inclusion of arbitrary cost factors, we only consider losses of money $\{M_i, O_i\}$ and time $\{T_i\}$ in this study. Monetary losses are the sum of primary and secondary losses, but further subdivided into initial losses $M_i$ and *out-*

*of-pocket losses* $O_i$. The latter represent the amount ultimately lost by the victim taking potential compensation payments into account.

Protection expenses $\mathcal{P}$ are spent in anticipation of crimes. Dolan and Peasgood (2007) refer to $\mathcal{P}$ as the costs of the fear of crime. As such, they do not necessarily require a criminal incident and potentially apply to all Internet users. $\mathcal{P}$ comprise the money spent $C$ and the time $S$ to learn about, implement, and maintain protection measures. Since incidents do not always lead to all consequences and not every person spends time or money on security, we allow every cost factor to materialize with probability $q$.

Indirect losses $\mathcal{I}$ are also not necessarily associated with a particular incident, but result from the overall prevalence of crime. They comprise social costs of the legal system, law enforcement, and the opportunity costs of the criminals' time (Anderson, 1999, 2012) as well as impacts of behavioral change, such as avoidance of online services by concerned Internet users (Chapter 5), market distortions, and the like. Although $\mathcal{I}$ are suspected to form a large part of the overall cost of cybercrime (Anderson et al., 2013), we do *not* attempt to measure them in this study because they are inherently different from $\mathcal{L}$ and $\mathcal{P}$ and require knowledge of the broader economic context, which cannot be expected from consumers.

Cybercrimes may also have emotional, social, or even physical impacts (Arief et al., 2015), denoted as *other consequences* or *other expenses* in Figure 4.2. Modic and Anderson (2015) for example, find that the perceived emotional impact of scams can exceed the perceived impact of monetary losses. Methods to quantify emotions in monetary terms have been developed for traditional crimes. Dolan et al. (2005), for example, estimate intangible costs, such as pain, grief and other suffering, as a result of violent crime. Due to economic and methodological constraints, chiefly interview time and the higher risk of re-victimization experiences associated with questions on emotional consequences, we neglect the quantification of emotional impact and focus on money and time.

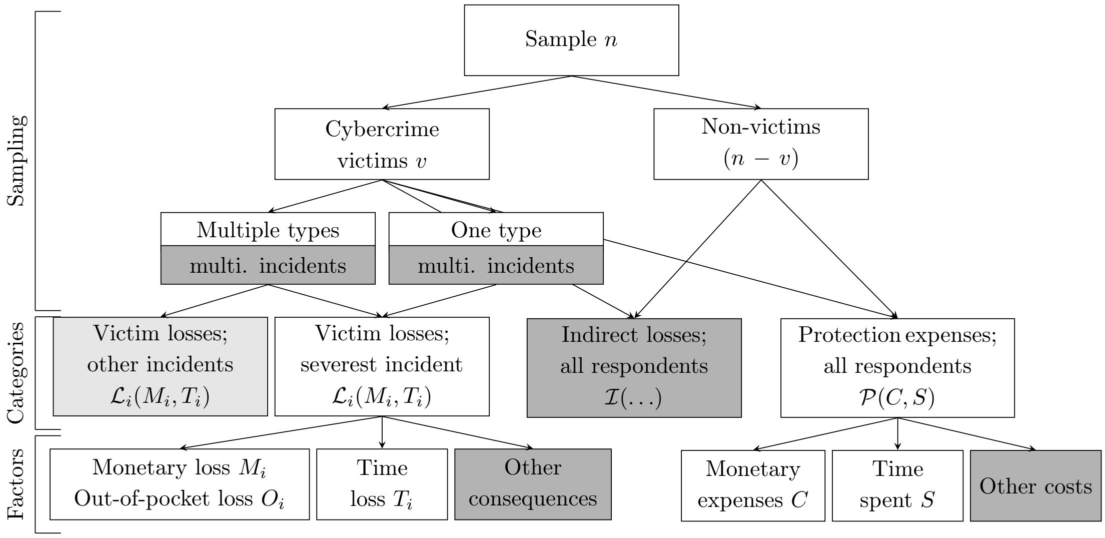
### 4.1.2 Fieldwork and Sampling

The survey was conducted as part of a larger multi-purpose survey within the European research project E-CRIME[1]. We collected representative data for adult Internet users in six European countries (in protocol order): Germany (DE), Estonia (EE), Italy (IT), the Netherlands (NL), Poland (PL), the United Kingdom (UK). This selection creates a diverse set of countries in terms of geographic location, maturity of the information and communication infrastructure, Internet usage, and cybercrime prevalence as reported in previous surveys (EB82.2, 2015).

Telephone interviews were carried out between July and October 2015 in the respective mother tongue for each country. Following the recommendations of our ethical reviewers, all respondents participated voluntarily, with informed consent, and were 18 years or older. The sampling was done in two phases. A representative sample per country was drawn with random digit dialing, an established technique in the target countries, with quotas set on age, gender, and region. Only respondents who reported to use the Internet for personal purposes at least once per month were interviewed. Overall 6 394 response sets have been collected. Because cybercrime victims are rare, even in a sample of monthly Internet users, we added 256 victims in a second sampling phase (oversampling), resulting in an overall subpopulation of 1 242 victims. The additional victims too, were reached using random digit dialing, but only surveyed if they reported to have experienced at least one type of cybercrime. The oversampling is accounted for in the analysis by inverse probability weighting. Demographics of the sample and the subpopulation of victims are reported in Appendix A.1.2.

Figure 4.2 illustrates the measurement instrument as used in the survey. White boxes represent

[1] URL: `http://ecrime-project.eu/`, grant number: 607775.



Gray boxes: not covered in the survey; Light gray boxes: covered based on assumptions.

**Figure 4.2:** Conceptual model of the measurement instrument

parts for which we collect data, gray boxes are *not* covered, and light gray boxes implicate a coverage based on assumptions. The lower part illustrates our coverage of cost factors and categories, as described in the previous section. The upper part visualizes our sampling choices.

Naturally, individuals may have experienced multiple types of cybercrime $i$, or multiple incidents of one type. Thus, $i$ can lead to $x \in \{1, 2, \ldots\}$ incidents. The optimal approach is an exhaustive measurement of all incidents $x$ for all types of cybercrime $i$ for every victim $v$. Due to economic constraints in the survey, we were not able to do this exhaustive data collection. We do not consider multiple incidents for a single type of crime, i. e., we set $x = 1$, assuming that multiple victimization of the same type of crime is rare. We record multiple victimization across different types of cybercrime but estimate costs only for the subjectively severest incident in the last five years (light gray rectangle in Figure 4.2). We discuss implications of this design choice for the cost estimation post-data in Section 4.3.2.

### 4.1.3 Prevalence of Consumer-facing Cybercrime

Section 2.2 demonstrates that consumer-facing cybercrime spans a wide range of offenses, which differ with regard to the attacker's motivation, the methods used, and the impact on the victims. Naturally, victimization surveys are best suited to study crimes with a direct relationship between the victim and the criminal. Table 4.1 shows our selection of seven profit-oriented types, along with the wording in the English version of the questionnaire.

We include four types of identity theft (IDT): IDT with regard to (wrt.) online banking (OB), bank cards (BC), PayPal (PP), and online shopping (OS). Furthermore, we ask for other types of fraud, i. e., online shopping fraud and scams, as well as extortion. The selection of crimes can be broadly categorized by the involvement of a third party. The first category concerns IDT of payment-linked services, the second contains crimes related to online shopping, and the third comprises scams and extortion which do not involve a third party. The wording is rather colloquial to be applicable across jurisdictions and as comprehensible as possible for the respondents (Van Dijk, 2015).

The selection is not exhaustive. We exclude emotionally and politically motivated offenses and

**Table 4.1:** Types of consumer-facing cybercrime with question wording

| *Thinking of the past 5 years, have you ever personally experienced any of the following* | |
|---|---|
| IDT wrt. OB | *Someone getting access to your bank account password (to buy something in your name, take money from your account, open a credit etc.)* |
| IDT wrt. BC | *Someone getting access to your bank card security numbers (to buy smthg. in your name)* |
| IDT wrt. PP | *Someone getting access to your PayPal password (to buy something in your name, or take money from your account)* |
| IDT wrt. OS | *Someone getting access to your online shopping account (e. g., Amazon etc.), to buy something in your name* |
| OS fraud | *Products or services which you have purchased online not being delivered, being defective or of different quality than advertised* |
| Extortion | *Someone extorting money from you to recover access to an account or your computer* |
| Scams | *Someone tricking you to transfer money to a fraudulent website* |
| Malware | *Do the following statements apply to you During the past 5 years, I have had malware/viruses on my computer* |

Identity theft (IDT), Online shopping (OS), Online banking (OB), Bank cards (BC), PayPal (PP).

crimes typically not targeted against consumers, such as denial-of-service (DoS) attacks. We also exclude malware and other criminal activities of the cybercriminal infrastructure (as defined by Anderson et al., 2013, p. 6) from the cost estimation and only record the prevalence of malware infections as an anchor to previous surveys (EB82.2, 2015). We discuss this design choice post-data in Section 4.3.2.

**Prevalence** Table 4.2 reports the prevalence of cybercrime in the six surveyed countries. We measure prevalence as defined by Lauritsen and Rezey (2013) for each type of cybercrime and in total. Inverse probability weights are applied per country to compensate for the oversampling of cybercrime victims. Accordingly, Table 4.2 represents the percentage of Internet users victimized over the last five years. The total prevalence includes multiple victimization. However, the majority of the victims (79.2 %) reported only one incident. 15.5 % experienced two incidents and only 5.3 % fell victim to more than two types of cybercrime.

**Table 4.2:** Cybercrime prevalence over the last five years by type of cybercrime $i$ and country $j$

| Cybercrime $i$ | DE | UK | NL | PL | EE | IT |
|---|---|---|---|---|---|---|
| IDT wrt. online banking | 1.4 % | 3.3 % | 1.4 % | 1.2 % | 1.0 % | 1.1 % |
| IDT wrt. bank cards | 3.5 % | 4.8 % | 2.0 % | 0.9 % | 1.7 % | 2.7 % |
| IDT wrt. PayPal | 2.0 % | 2.3 % | 0.7 % | 0.8 % | 0.4 % | 0.9 % |
| Online shopping fraud | 8.4 % | 9.0 % | 10.3 % | 9.7 % | 9.1 % | 5.0 % |
| IDT wrt. online shopping | 4.3 % | 4.1 % | 1.1 % | 0.9 % | 0.8 % | 1.9 % |
| Extortion | 5.1 % | 2.8 % | 1.1 % | 1.4 % | 0.6 % | 1.5 % |
| Scams | 5.0 % | 4.4 % | 2.3 % | 3.4 % | 1.7 % | 2.4 % |
| Total | 22.2 % | 21.6 % | 15.7 % | 13.9 % | 13.2 % | 12.1 % |
| *For comparison*: Malware | 51.5 % | 50.5 % | 48.8 % | 68.1 % | 55.7 % | 60.1 % |

Germany (DE), United Kingdom (UK), Netherlands (NL), Poland (PL), Estonia (EE), Italy (IT).

We find that total cybercrime is most prevalent in Germany (22.2 %) and the UK (21.6 %). Italy on the other end is least affected (12.1 %). OS fraud is the most prevalent type of cybercrime with prevalence rates of almost 10 % in all countries, except Italy, where it is only 5 %. Victims of OS fraud have been identified using a proxy which added additional constraints, i. e., reporting to have lost money and not being able to recover losses completely. Appendix A.1.1 discusses the proxy in detail. Thus, our results are still likely to underestimate the real extent of OS fraud. IDT wrt. BC is comparably high in the UK (4.8 %) and Italy (2.7 %). Extortion (5.1 %) and Scams (5.0 %) are have been mostly reported in Germany. Malware infections have been encountered by at least twice as many respondents than all other crimes combined, in Italy and Poland the ratio is even higher.

## 4.2 Cost Estimates

This section estimates costs for the cost factors and categories presented in our framework. Section 4.2.1 introduces our statistical model of cost factors and robust methods to estimate summary figures. Based on this, we estimate victim losses $\mathcal{L}$ in Section 4.2.1 and analyze the impact of different cybercrimes in Section 4.2.3. After that, we estimate protection expenses $\mathcal{P}$ of all Internet users in Section 4.2.4. Finally, Section 4.2.5 formalizes the aggregation of costs factors and presents aggregate estimates per country. A notational overview of all estimators and indicators is provided in Table A.4 in Appendix A.2.

### 4.2.1 Model of Cost Factors

In principle, all cost factors $\{M_i, T_i, C, S\}$ can be modeled with semi-continuous random variables. Such variables combine a continuous distribution of losses (or expenses) with point masses at one or more locations, in our case zero for no losses (or expenses). They are different from left-censored or truncated variables because the zeros are valid outcomes and not merely proxies for negative or missing responses (Min and Agresti, 2002).

**Victim Losses** Initial monetary losses of cybercrime victims $M_i$ can be modeled as a mixture of zeros, when no loss occurred, and a continuous distribution of positive values, representing the losses. We use the random variable $Y$ to represent the losses for an arbitrary type of cybercrime (e. g., $Y = M_{scams}$). Let $y \in [0, \infty[$ denote the realization of $Y$. For a set of $v$ victims we write $y_i$ as the loss incurred by victim $i \in \{1, \ldots, v\}$.

As a semi-continuous variable, $Y$ consists of two parts. The first part is defined by the probability of a loss, denoted as $q = P(y > 0)$. We define an indicator function $\mathbf{1}$ that models this probability. It takes an expression as single argument. Its value is one if the expression evaluates to true; otherwise it is zero. For example, $\mathbf{1}(2 > 1) = 1$. For the second part of the model, let $z \in ]0, \infty[$ be the realization of a random variable $Z$ which models the loss amount under the condition that a loss has occurred. The probability density function (pdf) of $Z$ is denoted as $g_\theta$, where $\theta$ is a vector of the mean and dispersion parameters. This results in the following mixture pdf for $Y$:

$$f(x) = (1 - q) \cdot \mathbf{1}(x = 0) + q \cdot g_\theta(x). \tag{4.1}$$

We call $q$ the condition and $Z$ the distribution of conditional losses. Both can be analyzed independently, or together. The compound loss distribution $Y$ models the unconditional losses for all victims.

**Indicators of Unconditional Losses** In principle, expected values for the distribution of unconditional losses $E(Y)$ can be written as the product of the probability to lose money $q$ and the expected value of the conditional loss distribution $E(g_\theta)$:

$$E(Y) = q \cdot E(g_\theta). \tag{4.2}$$

However, in practice we cannot make distribution assumptions which lend themselves to expressions of expected values. Closed-form estimators of central moments (i. e., the arithmetic mean), arguably the most common choice, are prone to fail if the distributions do not meet standard assumptions. Nevertheless, it is an objective to calculate robust single-figure summary statistics that are easy to interpret, compare, and aggregate.

Our literature review in Section 2.3.3 identified two common issues in the loss data, which (in combination) require more careful estimation. First, right-skewed conditional loss distributions $Z$, which are often driven by a few outliers reporting extreme values. In accordance with earlier studies, we also find five cases with loses between €10 000 and €17 000 in our data set and a single scam victim reporting losses of €30 000. Second, the unconditional loss distributions $Y$ are often zero-inflated because the majority of victims loses nothing. Indeed, many (severest) incidents in our data do not lead to a monetary loss, especially for incidents of extortion ($\hat{q} = 13.7\,\%$) and IDT wrt. online shopping ($\hat{q} = 17.9\,\%$). The skewed distributions call into question the use of the unconditional sample mean (UCM) $\bar{y}$ as headline indicator for unconditional losses. While the median $\tilde{y}$ is robust against outliers, its use as indicator is problematic because it is zero as soon as 50 % of the victims do not lose money. Thus, it cannot handle the zero-inflation in the data. Acknowledging both issues, we consider three alternative indicators for unconditional losses, which combine the loss condition $q$ with a summary statistic of the conditional losses.

First, the *expected loss indicator* (ELI) is a variant of the conditional distribution-based mean $\mu$ scaled by the probability of the condition $q$. This probability is estimated by the empirical relative frequency of a loss event, $\hat{q}$:

$$\text{ELI} = \hat{q} \cdot \mu. \tag{4.3}$$

The ELI is very similar to the UCM, but allows for more robust estimation by using the distribution-based mean $\mu$ for the conditional losses. This means the parameter vector $\hat{\theta}_\mathbf{i}$ of $g_\theta$ used to derive $\mu$ is estimated by fitting different heavy-tailed distributions to the point estimates of the reported losses using the maximum likelihood method.

Second, the *adjusted median loss indicator* (AMLI) uses a quantile of the conditional loss distribution as indicator. In contrast to the median $\rho_{50}$ (which is the 50 % quantile), the relevant quantile is shifted to the left by the empirical probability of a loss:

$$\text{AMLI} = \rho_{50-\lambda}, \text{ with shift } \lambda = \frac{1-\hat{q}}{2 \cdot \hat{q}}. \tag{4.4}$$

AMLI can be interpreted as the median of the unconditional distribution, estimated parametrically for the conditional part. It shares the aforementioned limitations of median-based estimators for distributions with more than 50 % zeros, but could be used in cases with smaller zero-inflation.

Third, the *harmonized loss indicator* (HLI) takes the conditional distribution-based median $\rho_{50}$ and scales it by the probability of the empirical condition $\hat{q}$:

$$\text{HLI} = \hat{q} \cdot \rho_{50}. \tag{4.5}$$

HLI values can be interpreted as expected losses of victims under the assumption of Bernoulli losses where the unknown shape of the loss distribution is simplified to its median.

In principle, time losses $T_i$, can also be modeled as semi-continuous variables, with a mixture distribution of a probability mass at zero and a continuous positive distribution. However, due to constraints in the questionnaire time losses are only recorded on an ordinal scale.

**Protection Expenses** Even though protection expenses $\mathcal{P}$ differ conceptually from victim losses $\mathcal{L}$ – i. e., $\mathcal{L}$ represents *unintentional* losses and $\mathcal{P}$ *intentional* expenses for security – their cost factors can be modeled in the same manner. Models of monetary expenses $C$ correspond to losses $M$ and time spent $S$ follows the time losses $T$.

Economic studies show that individual and household expenditures for durable goods can be modeled with two-part approaches (e. g., Duan et al., 1983; Xiao-Hua and Tu, 1999). Zero-inflation may be even higher for protection expenses, as current operating systems are often shipped with integrated security software, such as the "Windows Defender Antivirus". Our data supports that unconditional expenses for protection are zero-inflated. In three out of the six surveyed countries (the Netherlands, Italy, and Estonia) less than 50 % of Internet users spend money on security, in Estonia as low as 20 %. The time spent on protection $S$ might be zero-inflated and skewed, describing a spectrum from people who do not care to very concerned ones.

### 4.2.2 Losses of Cybercrime Victims

We estimate (un-)conditional losses $\{M_i, T_i\}$ for the $v = 1\,242$ victims. We derive summary statistics for each type of cybercrime $i$ across all six countries because the number of incidents with monetary losses is too small for country-specific figures. As an explanation, Appendix A.1.3 reports the number of incidents with monetary losses per type of cybercrime and country. Loss estimates for victims of multiple crimes are based on the severest incident.

Monetary losses $M_i$ are recorded as point-estimates or in ordinal categories, if the respondent could not recall an exact amount. Overall, 608 victims reported losses as point estimates and 104 (15.30 %) in one of nine ordinal categories.[2] We conservatively impute exact values for categorical and missing responses. We replace categorical responses with a distribution-based median for each loss interval (instead of the interval center) to account for the skewness of the distribution. The (lognormal) distributions have been fitted as described in the next paragraph.

Four victims *refused* to report the loss amount and 14 victims *didn't know*. We impute the overall median of the fitted loss distribution for refusals (0.36 %). Since the victims reported a loss, but no value, we believe this is the best approach. For the 14 *don't know* responses (1.32 %) we impute the median of the smallest loss category (€ [1:50]). We do not drop the cases because the respondents reported a loss and argue that the losses have been small if respondents cannot recall the amount.

**Fitting Loss Distributions** Data exploration clearly supports that all conditional loss distributions are skewed to the right. As an example, Figure 4.3 shows a histogram of the initial monetary losses of scam victims along with the pdfs of the candidate loss distributions.[3] We fit three heavy-tailed distributions: lognormal, gamma, and Weibull, which have been suggested for losses in the context of risk management (Dutta and Perry, 2006) and cybercrime (Florêncio and Herley, 2013). We also fit the normal distribution for comparison.

[2] Question 26a: "How much money would you say you have lost due to this incident altogether (including fees you may have had to pay, etc.)"; cost categories for €-countries and the UK in the respective currency: [1:50], [51:100], [101:200], [201:500], [501:1 000], [1 001:5 000], [5 001:10 000], [>10 000]. For Poland the categories are adjusted to equivalents in the national currency Zloty.

[3] The breaks in the histogram are based on the categorical intervals used in the survey. For a better visualization the x-axis is truncated at a loss of € 1 200, cutting off a part of the right tail (11 incidents).

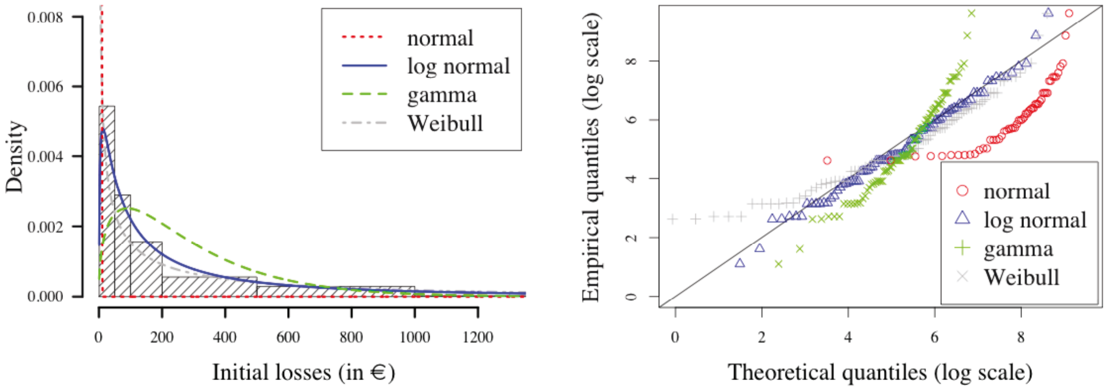


**Figure 4.3:** Conditional monetary losses of scam victims; Left: Histogram and candidate loss distributions, Right: Q–Q plot of candidate distributions on log scale.

We use weighted maximum likelihood estimation (Delignette-Muller and Dutang, 2015) to account for our sampling weights. The parameter estimates $\hat{\theta}_i$ of initial monetary losses for all types of cybercrime are reported in Appendix A.3.1 along with the relative goodness-of-fit indicators AIC and BIC for each candidate distribution. According to both, AIC and BIC, the lognormal distribution fits the loss data best for all types of crime, except IDT wrt. PayPal and extortion. For these two types the Weibull distribution performs slightly better ($\Delta$AIC $= +1$ for IDT wrt. PayPal and $\Delta$AIC $= +2$ for extortion). However, since the number of victims $v_i$ is very small in both cases ($v_i < 15$) and $\Delta$AIC is not substantial, we estimate all parameters using the lognormal distribution. Q–Q plots support its good fit for all types of cybercrime.[4] The right part of Figure 4.3 shows the Q–Q plot for loss distributions of scam victims, as one example. Across all types of crime we find deviations from lognormal mostly in the tails. While overestimations in the lower tail ($m_i < exp(3) \approx 20$ euro) are unproblematic, deviations in the upper tail need to be considered. In particular high losses to OS fraud, IDT wrt. OS and IDT wrt. OB may be slightly underestimated by the lognormal distributions.

**Monetary Loss Estimates** Table 4.3 reports the monetary loss estimates, structured in two parts. The left part compares empirical and distribution-based estimates for *conditional losses*. The right part adds the condition $\hat{q}_i$, to compare our indicators (ELI, AMLI, HLI) and the UCM for *unconditional losses*. All cost estimates are presented together with 90 % confidence interval (CI; in brackets) which are derived from non-parametric bootstrapping using the percentile method (Canty and Ripley, 2017). We ran an individual bootstrap with 10 000 samples for every estimator and indicator and accounted for the survey weights in the re-sampling process.

Table 4.3 shows that the empirical and distribution-based means ($\bar{m}_i$ and $\mu_i$) of the conditional losses exceed the respective medians ($\tilde{m}_i$ and $\rho_i$) consistently. For IDT wrt. OS, IDT wrt. OB, and OS fraud $\bar{m}_i$ exceeds $\tilde{m}_i$ more than three times, for scams even six times. An inspection of the data suggests that the large difference is driven by a single scam victim reporting a loss of € 30 000. The CIs of most estimates are large, but suggest that median estimates are more accurate than means. The CIs of $\mu_i$ also indicate that distributions-based mean estimates are often less accurate than their empirical counterparts $\bar{m}_i$. In particular when only few data points $v_l$ are used to fit the loss distribution, as is the case for IDT wrt. PP ($v_l$ =12), IDT wrt. OS ($v_l$ =17), and extortion ($v_l$ =14). Distribution-based medians $\rho_i$ are less prone to this issue and estimate more accurately than $\tilde{m}_i$.

[4] Additional histograms and Q–Q plots for the remaining types of cybercrime can be found in Appendix A.3.1.

**Table 4.3:** Initial monetary losses of cybercrime victims for each type of cybercrime $i$

| | **Condition** | | **Conditional** | | | | **Unconditional** | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Mean | | Median | | Mean-based | | Median-based | |
| Cybercrime | $v_l$ | $\hat{q}_i$ | $\bar{m}_i$ | $\mu_i$ | $\tilde{m}_i$ | $\rho_i$ | UCM | ELI | AMLI | HLI |
| IDT wrt. OB | 22 | 34 % | 2106<br>[830:4008] | 2585<br>[914:8177] | 630<br>[274:1102] | 466<br>[264:1022] | 710<br>[203:1396] | 872<br>[242:2745] | 0<br>[0:0] | 157<br>[71:345] |
| IDT wrt. BC | 69 | 34 % | 1165<br>[834:1578] | 1684<br>[1118:2835] | 403<br>[274:548] | 329<br>[217:477] | 400<br>[250:534] | 578<br>[330:940] | 0<br>[0:0] | 113<br>[66:160] |
| IDT wrt. PP | 12 | 24 % | 2039<br>[799:3808] | 4425<br>[1175:10356] | 1000<br>[274:2667] | 488<br>[234:1396] | 492<br>[170:1034] | 1068<br>[265:2690] | 0<br>[0:0] | 118<br>[51:375] |
| OS fraud | 488 | 91 % | 174<br>[126:207] | 131<br>[108:149] | 50<br>[46:50] | 54<br>[48:58] | 158<br>[118:192] | 119<br>[100:138] | 45<br>[42:51] | 49<br>[44:54] |
| IDT wrt. OS | 17 | 18 % | 452<br>[164:722] | 447<br>[131:959] | 93<br>[55:300] | 139<br>[72:242] | 81<br>[23:133] | 80<br>[19:174] | 0<br>[0:0] | 25<br>[10:44] |
| Extortion | 14 | 14 % | 197<br>[104:285] | 406<br>[157:860] | 131<br>[68:300] | 74<br>[28:156] | 27<br>[10:43] | 55<br>[16:123] | 0<br>[0:0] | 10<br>[3:22] |
| Scams | 90 | 45 % | 1078<br>[475:2048] | 783<br>[485:1436] | 176<br>[120:310] | 198<br>[158:287] | 488<br>[214:943] | 354<br>[213:662] | 0<br>[0:9] | 90<br>[69:133] |

Estimates in € based on the severest incident ($v = 1\,242$) over the last five years; 90 % CI (in brackets).

The right part of Table 4.3 compares indicators of unconditional losses. The UCM and the ELI consistently report the highest losses and largest CIs. Since they are based on the conditional means, they are strongly influenced by very large losses. The AMLI is more robust against large values in the right tail. However, in accordance with the empirical median, it is zero as soon as less than 50 % of the victims report losses. Thus, it cannot cope with the high zero-inflation, which exists for all types of cybercrime, except OS fraud. The HLI combines the advantages of both approaches. It is robust against outliers of conditional losses and the high zero-inflation of the condition. The comparatively narrow CIs also support the most accurate measurement for the HLI.

**Time Loss Estimates** $T_i$ is measured using an ordinal question with five categories, asking respondents how much time they have spent to deal with the incident.[5] 28 responses are missing due to *don't know* responses and 12 victims refused to provide an answer. We impute zero for *don't know* responses (2 %), assuming that respondents who cannot answer a categorical question most likely lost an insignificant amount of time. For the refusals (0.83 %) we impute the central category [1:10] hours (hrs), which is also the modus and median of the empirical distribution.

Table 4.4 reports the empirical distributions of $T_i$ for each type of cybercrime in hours. We observe that, as expected, time losses are unlikely to be zero-inflated, since the vast majority of cybercrime victims ($> 90\,\%$) loses time, independent of the type. All seven distributions have two peaks suggesting that time losses follow a bimodal distribution, such that victims either lose a few hours [<10] or a lot more [>20].

However, the results may also indicate that our choice of categories includes too many responses in the highest category and needs to be refined. Collecting point-estimates for $T_i$ (as we did for $M_i$), would be the best approach to understand the distribution of time losses, and we encourage future research in this direction. Without further knowledge about the distribution we estimate time losses by the mean of the categorical interval centers UCM and compute CIs using the approach described in the previous section. Scams lead to the highest losses of time, with a mean of 9.57 hours.

[5] Question 29: "How much time have you spent trying to solve the problem (please think of the total number of hours you have personally spent)"; categories: [0] hours, [0:1] hours, [0:10] hours, [10:20] hours, [>20] hours.

**Table 4.4:** Distribution of time losses $T_i$ for each type of cybercrime $i$

| **Cybercrime** | **0 hrs** | **[0:1] hrs** | **[1:10] hrs** | **[10:20] hrs** | **[> 20] hrs** | **UCM** | **90 % CI** |
|---|---|---|---|---|---|---|---|
| IDT wrt. online banking | 2.5 % | 30.9 % | 44.9 % | 4.5 % | 17.2 % | 7.88 hrs | [6.2:10.1] |
| IDT wrt. bank card | 1.6 % | 34.6 % | 45.1 % | 8.3 % | 10.3 % | 8.45 hrs | [6.9:11.2] |
| IDT wrt. PayPal | 9.6 % | 29.0 % | 42.5 % | 6.8 % | 12.1 % | 8.22 hrs | [7.3:9.6] |
| Online shopping fraud | 3.4 % | 26.7 % | 50.6 % | 5.5 % | 13.8 % | 7.13 hrs | [6.6:7.9] |
| IDT wrt. online shopping | 1.3 % | 32.2 % | 44.0 % | 7.4 % | 15.1 % | 7.01 hrs | [5.6:8.5] |
| Extortion | 6.4 % | 26.5 % | 40.0 % | 10.4 % | 16.7 % | 8.89 hrs | [7.6:10.9] |
| Scams | 5.3 % | 30.4 % | 35.1 % | 8.5 % | 20.7 % | 9.57 hrs | [8.1:10.8] |

UCM: Unconditional sample mean based on the severest incident ($v = 1\,242$) over the last five years.

### 4.2.3 Cybercrime Impact Map

To compare impacts between different types of cybercrime, we analyze monetary losses $M_i$ and time losses $T_i$ jointly in a *cybercrime impact map*, as depicted in Figure 4.4. Each type of cybercrime $i$ is represented by a black circle. The further crimes move to the upper right of the map, the higher are the overall losses $\mathcal{L}_i$ incurred by the victims.

The UCM of each $T_i$ defines the location of crimes on the x-axis and the HLI estimates for $M_i$ (and $O_i$) define the location on the y-axis. We distinguish between initial monetary losses $M_i$ and out-of-pocket (OOP) losses $O_i$, which represent the victim's ultimate monetary losses after compensation payments. Compensation is measured on an ordinal scale with six brackets representing the percentage of losses, victims were able to recover.[6] We calculate point estimates for $O_i$ by multiplying each initial loss with the interval center of each compensation level. The summary figures for OOP losses are then estimated by the HLI for each type of cybercrime.[7] $O_i$ define a second location for each type of cybercrime on the y-axis (white diamonds).

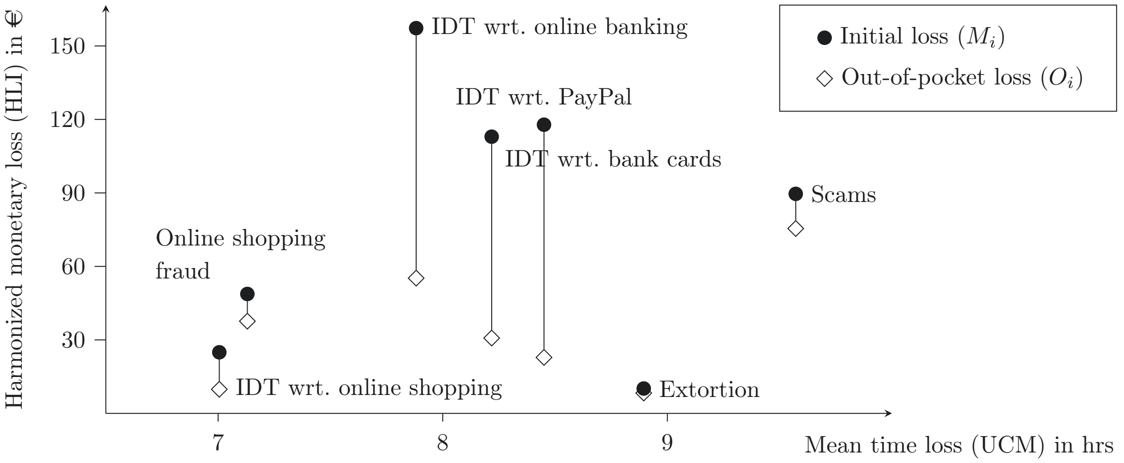


**Figure 4.4:** Cybercrime impact map for our seven types of cybercrime $i$

The impact map illustrates that the seven types of cybercrime fall into three categories, which correspond to the categories of third party involvement (cf. Section 4.1.3). The first category com-

[6] Question 31: "To what extent were you able to get your money back"; scale levels: [0], [0,25 %], [25 %,50 %], [50 %,75 %], [75 %,100 %], [100 %].

[7] Appendix A.3.2 shows parameter estimates $\hat{\theta}_i$ for the distribution of OOP losses $O_i$.

prises incidents in the context of online shopping and is characterized by the lowest combined impact for consumers. OS fraud and IDT wrt. online shopping lead to comparably small monetary losses (also small compensation) and are least time consuming.

The second category relates to payment and financial services, comprising IDT wrt. online banking, bank cards, and PayPal. These crimes lead to the highest initial losses, but service providers cover a large parts of the costs through compensation payments. Consequently, OOP losses are comparable to the other types of cybercrime. While we suspected that receiving compensation requires more time, we could not find evidence for this effect in our data.

The third category of crimes – extortion and scams – does not involve a third party. These crimes turn out to be most time-consuming and the victims do not receive any compensation.[8] Interestingly, losses to extortion were the smallest of all crime types until the field time (2015). This may have changed with the recent increase in ransomware attacks (Berr, 2017). According to our impact map, scams are the most *dangerous* type of cybercrime for consumers because they lead to the highest OOP loss and require most time to deal with.

### 4.2.4 Protection Expenses

We study protection expenses $\mathcal{P}$ for all respondents in each country ($n = 6\,394$). The majority of Internet users (90.77 %) has some protection software installed on their computers and a substantial fraction (61.76 %) purchased commercial products. We estimate expenses $C$ and the time consumers spend to protect $S$ using the same approach as for victim losses (cf. Section 4.2.2).

**Fitting Expense Distributions** We first impute exact values for categorical and missing responses. 1 523 categorical responses[9] are replaced by the lognormal median of each categorical interval. Two responses were not imputed because respondents reported expenses > € 10 000, which seem unrealistic for personal protection expenses and significantly exceed the highest point estimates (€ 5 000). For the 49 *refusals* (0.77 %) the median of the conditional expense distribution is imputed. Because respondents reported expenses, but no value, we believe this is the best possible approach. For the larger number of 658 *don't know* responses (10.29 %) we conservatively imputed no expenses, arguing that consumers know whether they have spent money on security products.

We fit six distributions to the point estimates of conditional protection expenses, one for each country $j$. Appendix A.3.3 shows the parameter estimates $\hat{\theta}_j$ for each country along with relative quality indicators AIC and BIC. The AIC and BIC suggest best fit of the lognormal distribution for Germany, Italy, and the UK and a Gamma or Weibull distributions for Estonia, the Netherlands, and Poland. The differences in the indicators are small and the Q–Q plots for Estonia, the Netherlands, and Poland also support good fit for the lognormal distribution, in particular in the upper tail. Therefore, in the interest of consistency, we model all conditional expenses using the lognormal distribution. As for cybercrime losses we overestimate a few values in the lower tail $< 2.5 \approx log(€\,12)$ and slightly underestimate in the upper tail. The empirical quantiles are characterized by steps, which are formed by common replies for round values (prices), such as $3.91 \approx log(€\,50)$.[10]

[8] The compensation for scams is likely caused by consumers who classified bank related incidents, e. g. IDT wrt. bank cards or IDT wrt. online banking, as scams. The majority of scam victims, who received compensation, reported the incident to the bank and got all losses recovered.

[9] Question 35: "Overall, during the past 5 years, how much money would you say you have spent on protection software (for example, anti-virus or firewall)"; cost categories for €-countries and the UK in the respective currency: [1:50], [51:100], [101:200], [201:500], [501:1 000], [1 001:5 000], [5 001:10 000], [>10 000]. For Poland the categories are adjusted to equivalents in Zloty.

[10] Histograms of the empirical distributions and Q–Q plots for all countries can be found in Appendix A.3.3.

**Expense Estimates** Table 4.5 presents the expense estimates. We report monetary protection expenses $C_j$ against the backdrop of the characteristics of cybercrime losses $M$. The conditional estimates and unconditional indicators for $C_j$ are in principle more reliable because they are based on a larger subsample (see $n_s$), are less prone to zero-inflation (see $\hat{q_j}$), and include fewer extreme data points in the upper tail (max €5 000).

**Table 4.5:** Protection expenses $C_j$ (and time $S_j$) by country $j$

| | | | Conditional | | | | Unconditional (Unc.) | | | | Time (hrs) | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Country | | Cond. | Mean | | Median | | Mean-based | | Median-based | | Cond. | Unc. |
| | $n_\mathrm{s}$ | $\hat{q_j}$ | $\bar{c_j}$ | $\mu_j$ | $\tilde{c_j}$ | $\rho_j$ | UCM | ELI | AMLI | HLI | $\hat{s_j}$ | UCM |
| DE | 597 | 54 % | 224<br>[201:247] | 217<br>[200:231] | 150<br>[150:200] | 155<br>[145:163] | 121<br>[107:135] | 118<br>[107:126] | 49<br>[32:59] | 84<br>[77:89] | 84 % | 21.00<br>[20:23] |
| EE | 173 | 20 % | 141<br>[113:145] | 158<br>[126:176] | 100<br>[100:100] | 91<br>[70:95] | 28<br>[21:29] | 31<br>[23:35] | 0<br>[0:0] | 18<br>[13:19] | 56 % | 12.49<br>[11:14] |
| IT | 452 | 46 % | 192<br>[167:208] | 190<br>[169:202] | 100<br>[100:100] | 118<br>[108:125] | 89<br>[76:97] | 88<br>[76:94] | 0<br>[0:0] | 55<br>[48:59] | 78 % | 14.91<br>[14:16] |
| NL | 476 | 48 % | 226<br>[214:242] | 237<br>[224:254] | 200<br>[200:200] | 164<br>[156:177] | 108<br>[100:118] | 113<br>[104:124] | 0<br>[0:23] | 79<br>[73:86] | 69 % | 18.74<br>[17:20] |
| PL | 628 | 60 % | 124<br>[115:133] | 137<br>[123:150] | 86<br>[86:92] | 82<br>[76:87] | 75<br>[68:81] | 83<br>[73:91] | 31<br>[25:37] | 49<br>[45:53] | 73 % | 16.64<br>[15:18] |
| UK | 609 | 58 % | 262<br>[241:279] | 262<br>[243:277] | 195<br>[195:195] | 184<br>[171:192] | 151<br>[137:163] | 151<br>[138:161] | 72<br>[59:82] | 106<br>[97:112] | 67 % | 14.78<br>[14:17] |

Condition (Cond.); Estimates in € based on the full sample ($n = 6\,242$); 90 % CI (in brackets).

The main characteristics of $C_j$ and $S_j$ are also similar to cybercrime losses. The conditional means ($\bar{c_j}$ and $\mu_j$) exceed the respective medians ($\tilde{c_j}$ and $\rho_j$) in all countries and are less accurate, as indicated by the CIs. Accordingly, the mean-based indicators (UCM and ELI) report the highest unconditional estimates. Differences between estimates are substantially smaller and the CIs narrower than for cybercrime losses. The AMLI performs better, at least for Germany, Poland and the UK where more than 50 % of the respondents spent money on protection measures. As for the cybercrime losses, HLI figures are smaller than ELI (and UCM) in all countries. Overall, the results indicate that protection expenses can be measured more reliably in surveys than victim losses.

The time $S_j$ consumers have spent to manage protection measures in the last year, is measured on an ordinal scale with five categories[11]. 150 *don't know* responses (2.15 %) and 37 refusals (0.53 %) are conservatively imputed with zeros, i. e. no time. Overall, 73.82 % reported to have spent time to manage protection measures. The fraction is the smallest in Estonia (56 %) and highest in Germany (84 %). In contrast to time losses $T_i$, the empirical distribution of $S_j$ is unimodal with a single maximum in one of the smaller categories. We estimate that over the last five years, Internet users spent between 12.5 and 21 hours to protect themselves.[12]

### 4.2.5 Aggregate Cost Estimates

We propose a general utility function $U(\mathbb{X})$ to aggregate cost factors. $U(\mathbb{X})$ models the *disutility* or *badness* of costs, losses, and other consequences with realizations $u \in [0, \infty[$. It takes a vector of cost factors $\mathbb{X}$ as input and evaluates to positive, monetary values. The results are monotonically

[11] Question 35a: "And now, thinking of the past 12 months, how much time did you spend learning about and installing protection software"; categories: [0] hours, [0:1] hours, [1:10] hours, [10:20] hours, [>20] hours.

[12] To align the time frames, all UCM estimates for time expenses $S_j$ are multiplied by five.

increasing in every element of the input $\mathbb{X}$. Furthermore, $U$ is defined such that an individual is indifferent between alternative a) nothing happens and b) experiencing $U = 100$ *and* receiving € 100.

We first explain $U$ for the protection expenses $\mathcal{P}(C, S)$. Let $C$ and $S$ be semi-continuous random variables modeling costs and time spent for protection with realizations $c, s \in [0, \infty[$. Furthermore, let $\alpha \in [0, \infty[$ be a conversion factor that converts time to monetary values, such as a minimum wage. Then, we can define the aggregate protection expenses $\mathcal{P}$ as a linear combination of $C$ and $S$:

$$\mathcal{P} = C + \alpha \cdot S. \tag{4.6}$$

Losses of individual types of cybercrime $\mathcal{L}_i$ follow the same disutility function $U$ and can be summarized using the same principle. To calculate the total cybercrime losses $\mathcal{L}$, all types of cybercrime need to be aggregated. Assuming that the processes of falling victim to different types of crime are independent, we weigh $\mathcal{L}_i$ with the probability of being victimized $p_i$. $M_i$ models the monetary losses and $T_i$ the time to deal with an incident of type $i$ with realizations $m_i, t_i \in [0, \infty[$ . The total cybercrime losses $\mathcal{L}$ are the sum over all weighted disutilities:

$$\mathcal{L} = \sum_{i \in \{I\}} p_i \cdot \mathcal{L}_i = \sum_{i \in \{I\}} p_i \cdot (M_i + \alpha \cdot T_i). \tag{4.7}$$

Recall, that monetary cost factors $C_j$ and $M_i$ follow the structure of $Y$ (described in Section 4.2.1) and are summarized with the harmonized loss indicator (HLI).[13] Time costs $S_j$ and $T_i$ are summarized by the UCM. We set the conversion factor $\hat{\alpha}_j$ to be the minimum hourly wage for each country $j$ (state: Jan. 2015; Schulten, 2015).[14] The minimum wage is a common and rather conservative conversion factor, already used in the context of information security (e. g., Herley, 2009).

**Results** Table 4.6 reports aggregated cybercrime losses $\mathcal{L}_j$ and protection expenses $\mathcal{P}_j$ for all Internet users older than 18 over a time period of five years. $\mathcal{L}_j$ are calculated using initial monetary losses $M_j$ (not OOP losses $O_j$), following the rationale that at the societal level all consumers pay for the victim compensation through higher service fees.

**Table 4.6:** Aggregate cost estimates by country $j$

| **Country** | | **Cybercrime losses** | | | | | **Protection expenses** | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | $\hat{\alpha}_j$ | $M_j$ | $O_j$ | $T_j$ | $\hat{\alpha}_j \cdot T_j$ | $\mathcal{L}_j$ | $C_j$ | $S_j$ | $\hat{\alpha}_j \cdot S_j$ | $\mathcal{P}_j$ |
| DE | 8.50 | 18.67<br>[16:27] | 10.10<br>[9:18] | 2.40<br>[2:3] | 20.40<br>[19:21] | 39.07<br>[35:47] | 84.44<br>[77:59] | 21.00<br>[20:23] | 178.51<br>[168:194] | 262.94<br>[253:279] |
| EE | 2.34 | 10.18<br>[9:14] | 6.00<br>[5:9] | 1.17<br>[1:1] | 2.75<br>[3:3] | 12.93<br>[12:16] | 17.70<br>[13:0] | 12.49<br>[11:14] | 29.23<br>[27:33] | 46.93<br>[44:51] |
| IT | 7.38 | 10.90<br>[9:15] | 5.58<br>[5:10] | 1.22<br>[1:1] | 9.02<br>[8:9] | 19.92<br>[18:24] | 54.80<br>[48:0] | 14.91<br>[14:16] | 110.01<br>[101:122] | 164.81<br>[156:176] |
| NL | 9.21 | 12.76<br>[11:18] | 7.36<br>[6:12] | 1.46<br>[1:2] | 13.48<br>[12:14] | 26.25<br>[24:31] | 78.84<br>[73:23] | 18.74<br>[17:20] | 172.58<br>[156:188] | 251.42<br>[235:267] |
| PL | 2.42 | 11.94<br>[11:17] | 7.51<br>[7:12] | 1.44<br>[1:2] | 3.48<br>[3:4] | 15.41<br>[14:20] | 49.23<br>[45:37] | 16.64<br>[15:18] | 40.27<br>[37:44] | 89.51<br>[87:93] |
| UK | 8.06 | 22.83<br>[19:35] | 11.13<br>[9:24] | 2.43<br>[2:3] | 19.62<br>[18:21] | 42.45<br>[38:54] | 106.08<br>[97:82] | 14.78<br>[14:17] | 119.15<br>[111:134] | 225.23<br>[217:241] |

Estimates in €, except T and S in hours; $\mathcal{L}_j$ extrapolated to full sample; 90 % CI (in brackets).

[13] Appendix A.3.4 compares HLI and UCM estimates for monetary costs.

[14] Because Italy did not have a national minimum wage in 2015, we follow Francesco Riccardi (2014) and use € 7.38, which is 51 % of the median wage. The same approach has been used to calculate the minimum wage in Germany.

With aggregated losses equivalent to €22.83, the average UK consumer has lost most money to cyber criminals in the last five years and also incurred the highest total losses ($\mathcal{L}_{\text{UK}} =$€42.45). German Internet users spend most on protection ($\mathcal{P}_{\text{DE}} =$€263). Across all countries protection expenses $\mathcal{P}_j$ are substantially higher than cybercrime losses $\mathcal{L}_j$. Even monetary expenses for protection $\mathcal{C}$ alone exceed the overall cybercrime losses $\mathcal{L}_j$ by factor two in all countries except Estonia. In the Netherlands consumers spend almost ten times more on protection than they lose.

Table 4.6 also indicates that protection rather costs time than money, with Poland being the only exception. The monetary equivalent of the time spent on protection $\hat{\alpha}_j \cdot S_j$ is at least twice the monetary expenses $C_j$ in Germany, Italy, and the Netherlands. For cybercrime losses the results are mixed, but tend towards more losses of time $\hat{\alpha}_j \cdot T_j$, particularly in comparison to OOP losses $O_j$. Obviously, these results highly depend on the choice of the time conversion factor $\hat{\alpha}$. However, our conservative choice of $\hat{\alpha}_j$ underpins the importance of time losses and expenses for overall costs.

## 4.3 Discussion

Our results raise several points for discussion. We first discuss limitations in Section 4.3.1. Then, we evaluate our design choices post-data and make suggestions for future studies in Section 4.3.2. Section 4.3.3 compares cost estimates along multiple dimensions and derives policy implications.

### 4.3.1 Limitations

Population surveys can only measure what average consumers can observe, understand, and report with sufficient precision. In the domain of cybercrime, this mainly concerns the ability to distinguish different attack techniques and attribute computer problems to criminal versus other causes. Economic (budget) and methodological (e. g., respondent's attention span) constraints further limit the instrument design and the data collection. We took several measures to prioritize the collection of loss data, including: 1) representative sampling of Internet users, i. e., excluding the offline population, 2) oversampling of victims of cybercrime, 3) a reference period of five years, and 4) asking for the severest incident in the case of multiple victimization. Although we identify a total of 1 242 victims, we only find a few incidents with monetary losses for some types of cybercrime. We decide to fit loss distributions across countries and thus do not account for between-country variation. Still, for some types of crime we could only use a small number of cases (less than 20). This reinforces the challenges of collecting data on cybercrime and calls for a careful reporting of results.

Constraints in the questionnaire design also limit our results and partly bias our estimates. We do not collect data on multiple incidents of the same type of crime and identify victims of online shopping fraud with a proxy. As a result, we can only present prevalence rates and underestimate the total incidence of the selected types of cybercrime. Moreover, this introduces a downward bias to our aggregated loss estimates. As a natural limitation of a consumer survey, we do not observe costs incurred by other parties. These include business spending, e. g., for fraud departments, customer support, or security measures, as well as social costs for the legal system and crime prevention agencies. We also miss potential losses for excluded types of cybercrime, i. e., parts of the criminal infrastructure, most importantly malware, and crimes which are not profit-oriented.

Acknowledging these limitations, we can and do not claim to provide an exhaustive measurement of all costs of consumer-facing cybercrime in the surveyed countries. Following the cautious remarks put forward by Anderson et al. (2013), we do not calculate a single cost estimate, but use our results to discuss central choices in the instrument design and compare cost estimates across crimes, cost factors, cost categories, and countries.

### 4.3.2 Design Choices

**Exclusion of Malware** Malware subsumes a wide variety of malicious software (Emigh, 2006). Depending on the purpose some types are more visible to victims than others. In the case of ransomware, for example, an infection is obvious: the malware encrypts data on the victim's computer and extorts a ransom to regain access (e. g., Kharraz et al., 2015). Other types of malware secretly steal credentials to log into the victim's accounts and may only become observable if the offender successfully conducts identity theft. If the malware connects the victim's computer to a botnet an infection may never be recognized (Tajalizadehkhoob et al., 2017). The great variety of types and visibilities makes it difficult for ordinary Internet users to comprehend what malware is and what constitutes an infection. For example, should a browser warning or notification from an anti-virus software be reported as infection Since malware often operates together with other offenses (Holt and Bossler, 2014), accurate measurement is further complicated by accountability issues. A victim of ransomware may report an incident of extortion, a malware infection, or both.

Driven by these concerns we let respondents report malware or virus infections, but do not ask for associated costs. Confirming results of the most recent Special Eurobarometer Report on Cyber Security (EB; EB82.2, 2015), we find that malware is significantly more prevalent than all other types of cybercrime. However, country-specific prevalence varies substantially between our survey and the EB. For instance, malware infections are reported by 28 %*pts.* more Internet users in Poland, but 17 %*pts.* less users in Italy in our data. Part of this variation can be explained by differences in the data collection, question wording, and time horizons. While we ask Internet users if they had malware/viruses on their *computer* in the *last five years*, the EB asks if they have *ever* "[d]iscovered malicious software (viruses, etc.) on [their] *device*" (EB82.2, 2015, p. 56). However, the results also support our reasoning that it is difficult for respondents to decide if their experiences constitute a malware infection. In a control question in our survey, 41 % of all respondents who reported malware/virus infections, also stated that they *don't know what it is.*[15]

We have to conclude that measuring malware prevalence based on a single question is highly unreliable and so would be associated cost estimates. Nevertheless, excluding the measurement of malware to avoid this uncertainty underestimates the overall costs of cybercrime, e. g., for clean-up efforts or damaged devices. We believe that future research needs to address the role of malware in relation to primary crimes, its perception by Internet users, and how it can be measured, before it can be reliably included in cybercrime victimization surveys.

**Severest Case** Recall that we collected costs for the severest incident over the past five years if respondents fell victim to multiple types of cybercrime (21 % of all victims). We opt for the severest incident for two reasons. The first is information retrieval. The severest incident tends to be better memorized by the victim because it is more likely to be noticed and discussed when it occurs. This leads to better initial encoding and greater rehearsal of the incident information in the victim's memory increasing retrieve-ability in a survey, especially in a long reference period of five years (Tourangeau and Bradburn, 2010). The second reason is the concentration of losses. We aim to include as many victims with financial losses in the sample as possible. We find that (across all crimes) the zero-inflation levels are smaller for the victims with multiple incidents (61.6 %) compared to victims with one incident (69.4 %). Considering our objective to study loss data in detail, we conclude that it is beneficial to ask for the severest incident because we were able to collect additional data points to calculate loss estimates.

[15] Question 21.2 "How informed do you consider yourself to be about each of the following" Malware: heard about it and know what it is; heard about it but I don't know what it is; never heard about it.

For aggregation we impute unobserved losses with summary values obtained from all victims who reported only one or the severest incident for the respective type of crime. While this rule introduces an upward bias on losses, it is safe to interpret our estimates as upper bounds. Studies with larger sample sizes (such as Harrell, 2015; Rieckmann and Kraus, 2015) might still opt for the most recent incident to obtain more accurate estimates, which are comparable to other reports.

**Harmonized Loss Indicator** Our data reinforces earlier findings that losses of cybercrime victims are zero-inflated (Harrell, 2015) and skewed to the right (Florêncio and Herley, 2013; Levi et al., 2017) with strong empirical evidence. Most victims report no losses, many lose little, and a few lose a lot. Adding to this, we show that protection expenses have similar characteristics. While many Internet users spent no money on protection, some spent a considerable amount.

We propose a *harmonized loss indicator* (HLI) to derive summary figures of both cost categories: *victim losses* and *protection expenses.* The HLI scales the conditional distribution-based median of costs by the condition of incurring this cost (cf. Eq. 4.5). It proves to be more accurate than sole mean or median-based methods because it handles the zero-inflation and the skewed distributions simultaneously. Furthermore, it is robust against high value outliers. The statistical interpretation of HLI figures is not straightforward and extrapolated numbers should be handled with high caution. However, it enables a robust comparison of estimates as done in Section 4.3.3.

Table A.8 in Appendix A.3.4 compares aggregate HLI figures to mean-based estimates. HLI figures of victim losses are 2.5 to 3.4 times smaller than mean-based estimates in every country and the CIs indicate a higher accuracy. The difference is less substantial for protection expenses, for which HLI figures are only 1.1 to 1.4 smaller. We conclude that victim losses are more difficult to measure than protection expenses because the distributions have more extreme characteristics (wrt. zero-inflation and high value outliers) and less data points are available.

Future surveys may still derive aggregate statistics based on the sample mean, in particular if enough data points are available. However, we strongly encourage a careful analysis of cost data and reporting of medians and zero-inflation levels along with mean estimates.

### 4.3.3 Implications

**Types of Cybercrime** We estimate losses for seven types of cybercrime. Identity theft and fraud related to online shopping lead to the smallest losses of money and time. Online shopping fraud is still a considerable problem because of its high prevalence rates in all countries. Identity theft related to financial or payment service accounts leads to the highest monetary losses. However, the victims often receive substantial financial compensation, reducing the ultimate out-of-pocket losses to those individuals considerably. Interestingly, we do not find evidence that compensated victims lose more time than those who do not receive compensation. While this situation seems acceptable for individual victims, service providers need to socialize the costs by increasing prices. This way, all consumers bear cybercrime losses in the form of an indirect tax. Scams and extortion turned out to be most time consuming for the victims. The high prevalence and high out-of-pocket losses of scams indicate that they have the severest impact on the average consumer.

The results imply that law enforcement should prioritize the fight against scams and extortion because they cause large losses for the victims and, in the words of the Routine Activity Theory (RAT), lack a capable guardian who protects individual consumers (Yar, 2005). Financial and payment providers need to take responsibility as such a guardian to secure their services, also to reduce their own losses.

**Cost factors and categories** We find that time is a substantial cost factor. The monetary equivalent of the time lost by victims exceeds monetary out-of-pocket losses in all countries, except Estonia and Poland. The time individuals spent on protection also exceeds monetary expenses everywhere, except in Poland. These results may be positively biased because 1) we only measure time costs using an ordinal question with five categories and 2) derive monetary equivalents using a country-wide conversion factor. On the contrary, many respondents reported time losses in the highest category (>20 hours) and with the minimum wage we use a conservative conversion factor. Furthermore, most incidents (even the ones without monetary losses) go along with some loss of time, e. g., for discovery, initial investigation, and reporting.

Consequently, clear instructions regarding effective protection measures, the provision of help, and efficient processes to report incidents can reduce a large part of the costs of cybercrime. However, future work also needs to study the role of time in greater detail, e. g., with exact loss estimates and subjective monetary equivalents. Some Internet users may even enjoy upgrading and securing their own computer and would not perceive this time as lost.

With regard to cost categories, we find that aggregated protection expenses always exceed victim losses; in most countries more than fives times. The difference may be explained by a general risk aversion of consumers but also by protection against unobserved types of cybercrime. Indeed, protection software rather protects against the criminal infrastructure, e. g., malware and spam, not so much against our selection of primary crimes. Therefore, we can not evaluate the effectiveness of protection expenses and can only speculate that consumers behave with protective aims.

This reinforces previous suggestions by Anderson et al. (2013) to increase law enforcement and prosecution efforts in order to deter cybercrime. However, Levi et al. (2017) cautions that reactive investigation of crimes in hard-to-reach countries may lead to wasted expenditures in practice.

**Countries** We finally compare cybercrime prevalence and costs across the six surveyed countries. Despite of the highest protection expenses in Germany and the UK, we also find the highest prevalence and losses in both countries. Losses are largely driven by scams and extortion in Germany and identity thefts in the UK. Italian, Estonian, and Polish consumers on the other end, lose considerably less money to cyber-criminals, even though they spend less money and time on protection.

This contradiction might be explained by RAT. Applying RAT at the national level, Kigerl (2012) argues that wealthier nations with higher levels of Internet use, such as Germany and the UK, are subject to a higher cybercrime activity. Williams (2016) obtains similar results for online identity theft. Our data supports this hypothesis, but we believe that language is another important factor. Most consumer-facing cybercrimes, require some communication with the victim and thus a translation of, e. g., spam emails into the respective national language. A rational criminal targets the largest possible markets, making English and German speaking countries (the latter also include Austria and parts of Switzerland) most attractive. Estonia, with less than 1.5 bn citizens and a very distinctive language, is less attractive. Our data supports this speculation about criminal decision making, as Estonians lose the least to cybercrime, even though they spend least on protection. The Netherlands however, are an exception as Dutch Internet users report high protection costs, medium levels of victimization, and rather small losses. Sophisticated legislation, law enforcement, and consumer education are a potential explanation. Indeed, the Netherlands are among the leading European countries in terms of “cyber-regulation” (BSA, 2015) and consumers report to be best informed about cybercrime in the latest EB survey (EB82.2, 2015).

Our country-level results suggest that larger and wealthier countries need to devote more resources to fight cybercrime and educate consumers. Among the surveyed countries, the Netherlands may be seen as a role model for such efforts.

# Chapter 5

# Quantitative Evidence of Indirect Impact

In addition to victim losses and protection expenses, cybercrime is suspected to lead to individual avoidance of information and communication technology (ICT). Section 2.4.2 shows that avoidance causes considerable indirect costs to society because consumers miss out on the benefits of ICT and chose alternatives which are economically less efficient.

Understanding and measuring avoidance behavior is an intricate endeavor. Section 3.1 demonstrates that individual behavior is influenced by factors of bounded rationality and regulated by several constraints, including, social norms, laws, and technology-mediated architectures. Time-dependent changes of perceptions and behavior in dynamic environments add further uncertainty. The issues are often neglected by researchers for justified reasons, including a lack of applicable theory or reliable data. However, established online services can be studied empirically at the aggregate level with accepted behavioral theories and using longitudinal methods.

We make a first step towards finding persistent security behavior at the societal level. By synthesizing information systems (IS) theories (surveyed in Sections 3.2 and 3.3) with insights from criminology, we devise a research model that explains individual security behavior in reaction to cybercrime. The model includes avoidance of online shopping, online banking, and online social networking. These established online services are widespread enough to allow for population-wide empirical studies. It also considers active protection actions, such as using different passwords.

We validate the model of individual security behavior and its three variants using covariance-based structural equation modelling (SEM) in a secondary analysis of the Special Eurobarometer on Cyber Security (EB), a representative EU-wide survey (EB77.2, 2012). We replicate the study in two subsequent waves (EB79.4, 2013; EB82.2, 2015) and perform a trend analysis to test for the stability of structural links. This provides us with the rare opportunity to study security behavior at the societal level from a longitudinal perspective. Our results add to the emerging research on negative outcomes of security behavior (Chen and Zahedi, 2016), with four main contributions:

1. **A model of individual security behavior.** We develop a theoretical model to study avoidance of three major online services: online shopping, online banking, and online social networking and three forms of protection behavior in reaction to cybercrime.

2. **Validation on the societal level.** We validate the model using SEM in a secondary analysis of three EB waves, enabling us to analyze representative samples of 27 EU member states for the years 2012–2014.

3. **Test of three model variants.** Furthermore, we test three variants of the model: a moderation analysis of user confidence, an improved measurement model, and avoidance of unknown websites as a more general form of avoidance.

4. **Longitudinal replication.** We develop a longitudinal approach to verify the robustness of the model in terms of its measurement model and overall fit. A trend analysis of the structural links confirms that security behavior is persistent across the three waves of the EB.

The contribution of the study within this dissertation is the measurement of avoidance behavior in reaction to cybercrime at the societal level. While we do not derive cost estimates, we provide strong empirical evidence that cybercrime experience and perceived risk lead to avoidance of online shopping, online banking, and unknown websites. Protection behavior, i. e., using different passwords or changing security settings, is triggered only by cybercrime experience.

The chapter is structured as follows. Section 5.1 develops our research model and describes its measurement using the EB data. Section 5.2 introduces the analysis method and validates the model for the first EB wave in 2012. Section 5.3 documents results for three variants. Section 5.4 replicates the study in a longitudinal approach for the second and third wave (2013 and 2014). Finally, Section 5.5 summarizes the results, discusses limitations, and derives implications for theory and practice.

## 5.1 Methodology

This section develops our model of individual security behavior. Section 5.1.1 starts with a summary of criminology studies in the context of crime, risk perception, and reactions. Section 5.1.2 integrates the results with behavioral models from IS research and Section 5.1.3 introduces the EB surveys which are relevant for the measurement of the model.

### 5.1.1 Perceived Risk in Criminology

Fear of crime is considered to be multidimensional in nature consisting of two components: a rather rational risk perception and a rather emotional feeling of being unsafe (Ferraro and LaGrange, 1987). This distinction corresponds to the dual path models which explain behavior under risk (see Section 3.1). In correspondence with Protection Motivation Theory (PMT), rational risk is often operationalized as the product of the probability of victimization and the severity of the crime. While the two components are known to be interrelated, dependencies between them are still unclear (Rader et al., 2007). We focus on perceived risk and do not intend to clarify the relation here. We consider fear of crime to be implicitly included, assuming that emotional reactions also influence how people react to cybercrime. However, we encourage future research to clarify the risk–fear relationship.

**Antecedents** We consider three antecedents of perceived risk of crime: prior experiences, media reports, and demographic factors. The examination of prior experiences reveals mixed results. Most scholars find strong effects (e. g., Tyler, 1984; Skogan, 1987; Liska et al., 1988; Wittebrood and Junger, 2002; Visser et al., 2013). Still, some find just weak or no effects (e. g., McGarrell et al., 1997). Gainey et al. (2010) summarize that the examination of the link between victimization experiences and perceived risk is not conclusive. Assuming that perceived risk is a function of the probability of getting victimized and the severity of the crime (Ferraro and LaGrange, 1987), we suspect that experiencing crime leads to increased concern about it. Visser et al. (2013) provide evidence for this effect based on representative EU-wide surveys, conducted in 2006 and 2008. Alshalan (2006) finds that cybercrime experience increases the fear of cybercrime in a study of 987 US households.

The literature on the impact of media reports on risk perception is also controversial (Heath and Gilbert, 1996). In a review, Wahlberg and Sjoberg (2000) find that media coverage influences risk perception, especially if reports are repeated over time. Jackson (2011) argues logically that the media plays a role in individual perception of vulnerability and severity, as it is the primary source of information about the extent, nature, and seriousness of crimes. As crime reports tend to be rather sensational and alarming, also in the context of cybercrime (Florêncio et al., 2014), they are likely to increase public risk perception (Wahlberg and Sjoberg, 2000).

The majority of research is conducted for TV news. Studies find that watching TV reports increases the feeling of being unsafe (Heath and Gilbert, 1996), especially if they resonate personal experiences (Chiricos et al., 2000), cover sensational crimes (Liska and Baccaglini, 1990; Jackson, 2011), and/or are broadcasted frequently (Chiricos et al., 2000). Local crime news tend to have a stronger effect on the risk perceived by individuals (Heath and Gilbert, 1996), especially for people living in high crime places (Chiricos et al., 2000). Wahlberg and Sjoberg (2000) suggest that the media needs to be considered as an influencing factor, along with prior victimization, experiences in the social environment, or demographic factors.

Demographics are important in measuring offline fear of crime, as different social groups are found to have different perceptions of the risks of victimization (Visser et al., 2013). Women, elderly, and Caucasians tend to be more fearful compared to their respective counterparts (Hale, 1996). However, other studies find different effects because the influence of demographic factors can change substantially, depending on the particular situation and offense (Heath and Gilbert, 1996).

### 5.1.2 Model of Individual Security Behavior

We combine these insights from criminology with behavioral models from IS research and ideas put forward in Böhme and Moore (2012), concerning the indirect costs of cybercrime. The resulting model explains the impact of cybercrime exposure on the avoidance of online services and on protection behavior. We synthesize the different research streams to formalize causal links between higher order constructs as direct and indirect (mediated) effects.

The research model, as depicted in Figure 5.1, has different parts. The right part builds on the basic elements of the perceived risk-extended Technology Acceptance Model (TAM; Featherman and Pavlou, 2003) and Unified Theory of Acceptance and Use of Technology (UTAUT) models (Martins et al., 2014). In both models *Perceived Risk* reduces the *Behavioral Intention* to adopt (and use) a system. Due to our focus on the impact of cybercrime, we incorporate the constructs as *Perceived Cybercrime Risk* (PCR) and *Avoidance Intention* (AV). We invert the originally negative effect of *Perceived Risk* on *Behavioral Intention* proposed in TAM and UTAUT and hypothesize a positive effect of PCR on AV. In other words, Internet users, who perceive higher levels of cybercrime risk, are more likely to avoid online services.

This main effect coincides with the PMT-based models suggested by Liang and Xue (2009) and Chen and Zahedi (2016), who propose a structural link between perceived threats and avoidance as coping behavior. Avoidance behavior can be defined as: "[a]voiding the use of the Internet in various degrees, especially avoiding sensitive activities such as online banking, in order to avoid online security threats" (Chen and Zahedi, 2016, p. A2).

Our literature review also demonstrates that *Protection Behavior* (PB) is a frequent response to perceived (cybercrime) risk. PB subsumes all "protective countermeasures to reduce or eliminate the risk of Internet security attacks" (Chen and Zahedi, 2016, p. A2). Therefore, we add it as a second reaction to PCR.

The left part of Figure 5.1 represents the criminological extension of the research model. *Cy-*

*bercrime Experience* (EXP) and *Media Awareness* (MA) are included as antecedents, which directly increase PCR. Both also have an indirect positive impact on AV and PB, which is fully mediated by PCR. Thus, becoming a victim of cybercrime or hearing about it in the media increases individual perception of cybercrime risk and ultimately leads to avoidance of online services and/or triggers protection efforts. The theoretically derived directions of the causal links are further enforced by explicit statements in the EB questions (e. g., "Has concern about cybercrime made you change the way you use the Internet ?"[1]).

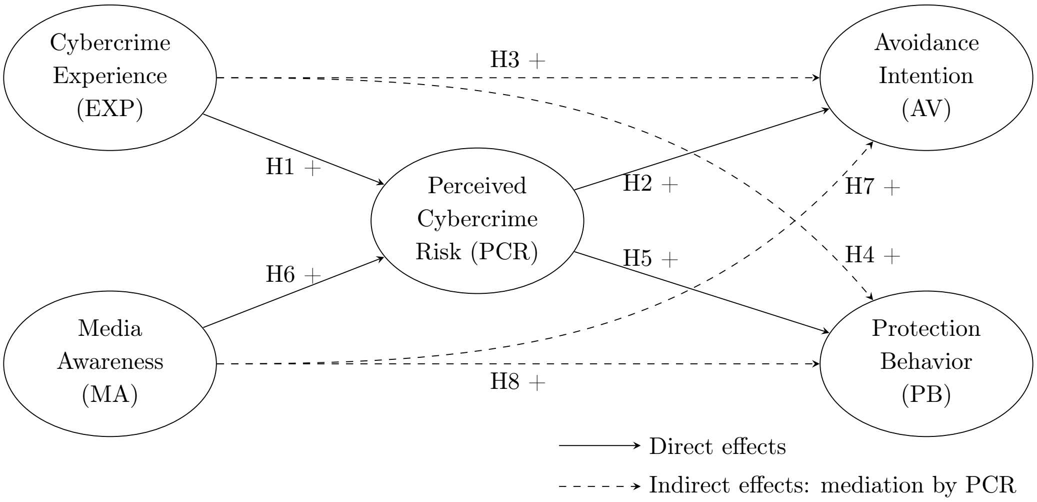


**Figure 5.1:** Research model in path model notation

Even though, the research model contains a total of eight different hypotheses, it is parsimonious in that it focuses on the impact of PCR on AV and PB. It neglects the positive TAM factors: *Perceived Usefulness* and *Perceived Ease-of-use*, and additional factors from PMT, e. g., *response efficacy*. While this limits its predictive power, the model can be validated using the EB surveys. The remainder of this subsection formulates the eight hypotheses of the model.

**H1+: Cybercrime Experience increases Perceived Cybercrime Risk.**
Prior victimization as an antecedent increasing perceived risk of crime is controversial among criminologists. However, perceived risk is assumed to be a function of the probability to get victimized and the severity of the criminal act (Ferraro and LaGrange, 1987). We argue that cybercrime experience increases the perceived probability to get victimized and therefore also perceived risk. We suspect that the effects are stronger in the online context, due to higher degrees of uncertainty in the Internet, caused by spatial and temporal separation of users and services (Pavlou, 2003).

**H2+: Perceived Cybercrime Risk increases Avoidance Intention to use online services.**
Technology acceptance studies find negative effects of perceived risk on the adoption of online services in several different scenarios. Featherman and Pavlou (2003) show that financial, performance and privacy risks are the most influential risk factors. As consumer-facing cybercrime is likely to increase these risks, we assume that it is a major factor increasing perceived online risk and ultimately reducing online service adoption and use.

**H3+: Cybercrime Experience increases Avoidance Intention to use online services. The effect is fully mediated by Perceived Cybercrime Risk.**
Saban et al. (2002) show that cybercrime experience decreases the likelihood of repeated online

[1] EB: Question 7 (EB77.2, 2012).

shopping. Böhme and Moore (2012) confirm the negative effects for online banking and general online participation. We agree with their findings, but hypothesize that the effect is fully mediated by *Perceived Cybercrime Risk*. Accordingly, *Cybercrime Experience* increases *Perceived Cybercrime Risk*, which ultimately increases *Avoidance Intention* of online services.

**H4+: Perceived Cybercrime Risk increases Protection Behavior.**
Protective actions are another reaction to cybercrime. Anderson and Agarwal (2010) show that TAM and the Theory of Planned Behavior are frequently used in the IS literature to explain the adoption of security software. Other studies build on PMT to understand individual protection behavior (e. g., Lee and Larsen, 2009; Ifinedo, 2012; Johnston and Warkentin, 2010). While perceived risk is often conceptualized as perceived security risk, we argue that *Perceived Cybercrime Risk* is equally applicable.

**H5+: Cybercrime Experience increases Protection Behavior. The effect is fully mediated by Perceived Cybercrime Risk.**
Studies on the impact of security incidents or, as we label it, *Cybercrime Experience* are less common. This is most likely due to the difficulty of recruiting victims. Applying the same logic as for **H3**, we hypothesize that *Cybercrime Experience* increases *Perceived Cybercrime Risk*, which ultimately increases *Protection Behavior*.

**H6+: Media Awareness increases Perceived Cybercrime Risk.**
Media reports are found to increase the perceived risk of traditional crime, especially if the news cover local crimes and are repeated over time. Cybercrimes are likely to be perceived as local crimes because the Internet is an open and global infrastructure in which all users can be affected. Thus, we suspect that these effects occur online as well. Furthermore, cybercriminal attacks are often reported in a rather spectacular way and victimization statistics are likely to be overestimated (Florêncio and Herley, 2013), which further contributes to an increasing perception of cyberrisk.

**H7+: Media Awareness increases Avoidance Intention to use online services. The effect is fully mediated by Perceived Cybercrime Risk.**
Böhme and Moore (2012) remark that Internet users, who have heard about cybercrime in news reports or from colleagues, are less likely to bank online than those who have not heard such reports. Kosse (2013) finds that newspaper articles about skimming significantly reduce the use of debit cards on the same day. In analogy to *Cybercrime Experience*, we hypothesize that this avoidance effect is fully mediated by *Perceived Cybercrime Risk*. In other words, *Media Awareness* increases *Perceived Cybercrime Risk*, which ultimately increases *Avoidance Intention* of online services.

**H8+: Media Awareness increases Protection Behavior. The effect is fully mediated by Perceived Cybercrime Risk.**
Many adoption studies include social norms into their models to explain use intention and behavior of technologies (e. g., Venkatesh and Davis, 2000; Johnston and Warkentin, 2010). We argue that social norms are influenced by *Media Awareness*. Consequently, *Media Awareness* affects individual *Protection Behavior* and the effect is mediated by *Perceived Cybercrime Risk*.

### 5.1.3 Measurement Model Development

The theoretical constructs in our research model (*Cybercrime Experience*, *Media Awareness*, *Perceived Cybercrime Risk*, (Behavioral) *Avoidance Intention*, and *Protection Behavior*) are measured using questions in the EB surveys. This section briefly introduces the EB series and the questions used in the SEM analysis. Descriptive statistics focus on responses given in the first wave in 2012.

Trends for the remaining years are presented in Section 5.4 as part of the longitudinal replication.

**Special Eurobarometer on Cyber Security** The Special Eurobarometer reports on Cyber Security comprise three survey waves to measure the prevalence and perception of consumer-facing cybercrime in Europe. They also include consumer attitudes and behavior in the context of IT security. The first report was published by the European Commission in July 2012 as part of a series of publications to raise cybercrime awareness and encourage the provision of counter measures (EB77.2, 2012). All three surveys were conducted in at least 27 EU member states. In 2013, Croatia joined the EU and has been added to the series as the 28th member state (EB79.4, 2013). The fieldwork was conducted in March 2012, May and June 2013, and October 2014.

The sampling and data collection is consistent across all three waves. Respondents are 15 years or older and were interviewed face-to-face in their respective mother tongues. Using stratification by country as well as random route and closest birthday rules within countries, all surveys can be considered to be a representative cross-section of European citizens above the age of 15. The first wave yielded a total of 26 593 responses. The subsequent surveys collected more response sets (27 680 in 2013 and 27 868 in 2014) due to the inclusion of Croatia.

All EB surveys are based on a standardized questionnaire and relevant answers are reported on binary and ordinal scales. The ordinal scales are either 3-point frequency scales reporting a vague count of cybercrime experience (“never”, “occasionally”, “often”) or 4-point rating scales that measure cybercrime concern by the strength of agreement with a statement (“not at all”, “not very”, “fairly”, “very”). Additionally, “don’t know” and “refusal” are possible responses for both types of questions. Outliers do not need to be considered and the 4-point rating scales are interpreted as being equidistant. Table 5.1 reports descriptive statistics of the relevant questions for the population of Internet users for all three EB waves.[2]

**Indicators** *Cybercrime Experience* is measured by five ordinal indicators. Internet users have been asked how frequently they have experienced five different cybercriminal attacks: identity theft, spam emails, online shopping fraud, illegal content, and unavailable online services.[3] In 2012, almost half of the Internet users (49.8 %) stated that they have encountered one form of cybercrime at least occasionally. Individual types of attacks, except spam emails, have not been encountered by more than 80 % of the respondents. Even spam emails have never been experienced by 62.1 %. This surprisingly high number is likely to be biased by the question wording “How often have you received emails fraudulently asking for money or personal details ?” (EB77.2, 2012, p.46), which excludes a large amount of spam emails.

*Media Awareness* represents the extent to which people are exposed to news reports about cybercrime from different media sources. Respondents are asked on a binary scale whether they have seen or heard about cybercrime from TV, radio, newspapers, or the Internet.[4] The majority heard about cybercrime from TV (66.7 %), one third from newspapers (33.3 %) or the Internet (34.2 %), and about one quarter from the radio (22.9 %). Note that the question block to measure *Media Awareness* has been discontinued in 2013.

*Perceived Cybercrime Risk* is measured using six ordinal indicators. Internet users reported their concern of victimization regarding six different types of cybercrime: identity theft, spam emails,

[2] Note that small differences to the figures presented in Riek et al. (2016) for the year 2012 are probably due to the fact that the original study eliminated a few more cases to account for missing values in the moderation analysis.

[3] Question QE10: “Cybercrimes can include many different types of criminal activity. How often have you experienced or been a victim of the following situations ?” (EB77.2, 2012, p. Q5).

[4] Question QE8: “Cybercrimes can be defined as any crimes which are committed via the Internet. In the last 12 months, have you seen or heard anything about cybercrime from any of the following ?” (EB77.2, 2012, p. Q4).

**Table 5.1:** Descriptive statistics of Eurobarometer questions used for latent variable measurement

| **ID** | **Latent variable (scale)/ indicator** | **Answers** | | |
|---|---|---|---|---|
| | Year | 2012 | 2013 | 2014 |
| | Number of respondents (normalized weights) | 18 809 | 18 983 | 20 213 |
| **EXP** | **Cybercrime Experience (Ordinal)** | | | |
| | "How often have you experienced or been victim of... ?" – At least occasionally | | | |
| exp1 | Identity theft | 8.16 % | 6.42 % | 6.95 % |
| exp2 | Receiving spam emails (or phone calls) | 37.87 % | 31.64 % | 31.25 % |
| exp3 | Online shopping fraud | 12.41 % | 9.97 % | 12.62 % |
| exp5 | Encountering illegal material | 15.24 % | 14.39 % | 14.60 % |
| exp6 | Unavailable online services (due to cyber-attacks) | 12.78 % | 11.81 % | 7.71 % |
| **MA** | **Media Awareness (Binary)** | | | |
| | "In the last 12 month, have you heard about cybercrime from ... ?" – Yes | | | |
| ma1 | Television | 66.68 % | - | - |
| ma2 | Radio | 22.89 % | - | - |
| ma3 | Newspaper | 33.30 % | - | - |
| ma4 | Internet | 34.21 % | - | - |
| **PCR** | **Perceived Cybercrime Risk (Ordinal)** | | | |
| | "How concerned are you about becoming a victim of... ?" – At least fairly | | | |
| pcr1 | Identity theft | 61.26 % | 51.70 % | 67.99 % |
| pcr2 | Receiving spam emails (or phone calls) | 48.04 % | 43.19 % | 55.93 % |
| pcr3 | Online shopping fraud | 48.97 % | 42.11 % | 55.74 % |
| pcr4 | Encountering child pornography | 50.64 % | 43.62 % | 52.22 % |
| pcr5 | Encountering content of racial hatred | 40.72 % | 34.73 % | 46.13 % |
| pcr6 | Unavailable online services (due to cyber-attacks) | 42.70 % | 37.38 % | 50.94 % |
| **AV** | **(Behavioral) Avoidance Intention (Binary)** | | | |
| | "Has concern about security issues made you change the way you use the Internet ?" – Yes | | | |
| avS | You are less likely to use online shopping | 17.73 % | 16.80 % | 13.35 % |
| avB | You are less likely to use online banking | 14.60 % | 14.78 % | 12.15 % |
| avN | You are less likely to online social networking | 36.78 % | 34.09 % | 12.15 % |
| avU | You only visit websites you know and trust | 33.92 % | 32.11 % | 35.67 % |
| **PB** | **Protection Behavior (Binary)** | | | |
| | "Has concern about security issues made you change the way you use the Internet ?" – Yes | | | |
| pbA | You have installed anti-virus software | 51.4 % | 46.0 % | 60.6 % |
| pbB | You use different passwords for different websites | 25.1 % | 24.3 % | 31.5 % |
| pbS | You have changed security settings (e. g., in your browser, ... ) | 16.4 % | 16.3 % | 17.6 % |
| **USE** | **Online Service Use (Binary)** | | | |
| use1 | Online shopping | 52.63 % | 50.42 % | 56.75 % |
| use2 | Online banking | 48.40 % | 48.44 % | 54.00 % |
| use3 | Online social networking | 51.86 % | 53.38 % | 59.99 % |

Base: EU Internet users above the age of 15.

online shopping fraud, encountering child pornographic content or content of racial hatred, and unavailable online services.[5] The types overlap with the crimes measuring cybercrime experience,

[5] Question QE11: "And how concerned are you personally about experiencing or being a victim of the following cybercrimes ?" (EB77.2, 2012, p. Q6).

except for illegal content, which is further divided into child pornography and content of racial hatred. Most respondents are fairly or not very concerned. Concerns are higher for identity theft (61.2 %) and rather low for accidentally encountering content of racial hatred (40.7 %). Alshalan (2006) shows that a reason for this difference is the perceived severity of the cybercrime type, as encountering illegal material usually does not cause as much direct harm on the individual as, for example, identity theft.

*Avoidance Intention* is measured by three binary questions which causally linked to *Perceived Cybercrime Risk*. Respondents are asked whether they are less likely to use a particular online service due to concerns about cybercrime.[6] Table 5.1 shows that 17.7 % are less likely to do online shopping and 14.6 % are less likely to do online banking. Avoiding the sharing personal information on the Internet, which is used as a proxy for online social network usage, is substantially higher (36.8 %). Each binary indicator is directly included as a dependent variable in the analysis and three models are tested separately, one for each online service.

*Protection Behavior* is measured in the same manner as *Avoidance Intention*, by three binary statements causally linked to *Perceived Cybercrime Risk*. Each indicator represents one self-reported reaction to cybercrime. The most common response is installing anti-virus software. 51.4 % of Internet users reported that they installed anti-virus software in 2012. The use of different passwords and changing security settings are least prevalent reactions (25.1 % and 16.4 %, respectively).

## 5.2 Results

We use covariance-based SEM to fit one model for each form of avoidance and protection behavior. We describe the statistical method in Section 5.2.1. Then, we report results of the SEM analysis for the first EB wave (EB77.2, 2012) structured along the two-step approach introduced by Anderson and Gerbing (1988). First, the quality of the measurement model is reported in Section 5.2.2 to prove construct validity and reliability. Second, structural parameters are estimated in Section 5.2.3.

### 5.2.1 Statistical Method

SEM is a multivariate analysis technique which performs factor analyses and simultaneously estimates regression coefficients. Linear regression only allows for explaining variables to directly influence the outcome. SEMs by contrast can handle multi-stage effects between (groups of) predictors, while explicitly accounting for measurement error and multi-collinearity (Hair, 2010). It is frequently used in the social science to explain human decision making and also popular in IS research to measure technology acceptance (cf. Table 3.1 in Section 3.2.2).

We use a single-level, cross-sectional SEM. Such models can be either covariance-based – here and in the following just referred to as SEM – or variance-based – referred to as partial least square (PLS) analysis. While both approaches pursue similar goals, SEM is better suited to confirming theories and PLS to developing theories and making predictions (Henseler et al., 2009). We use the covariance-based SEM technique to confirm our hypotheses, as we empirically test our theoretically derived model using the fit indexes introduced in the next paragraph. Non-normal data, another common reason for using PLS (Ringle et al., 2012), is accounted for by the robust weighted least square (WLSMV) estimation method developed for non-normal, categorical indicators (Finney and DiStefano, 2006). A small sample size, another prominent reason for the use of PLS (Henseler et al., 2009), is not an issue in our analysis.

[6] Question QE7: “Has concern about security issues made you change the way you use the Internet in any of the following ways?” (EB77.2, 2012, p. Q4).

We use the statistic software Mplus for the parameter estimation because it provides all features required to analyze the EB data in a secondary analysis. First, it supports the WLSMV estimation method (Muthen et al., 1997), which is considered to be the best available approach for categorical, non-normal distributed indicators, given a large sample (Finney and DiStefano, 2006). Second, it allows for the correct analysis of a complex sample, such as the EB survey. This includes the simultaneous consideration of sampling weights and country fixed effects. Third, it can handle missing values for individual indicators using pairwise exclusion. In addition to these data-related features, Mplus supports testing mediation (Section 5.2.3) and moderation effects (Section 5.3.1).

**Model Fit Evaluation** The traditional test statistic in SEM is the chi-squared ($\chi^2$) test, which assesses the difference between the model implied covariance matrix and the sample covariance matrix. As the $\chi^2$ statistic is strongly influenced by the sample size, it may fail for large samples (N>5 000), even when the differences between the observed and the predicted covariances are only marginal (Kline, 2010, p. 201). This is likely to happen in our analysis of about 18 000 cases. The $\chi^2$ statistic is also criticized because it assumes the existence of a perfectly fitting model, which is implausible in typical SEM applications (Steiger, 2007). Due to these issues, we only report $\chi^2$ values, but do not consider them for model fit evaluation. Instead, we evaluate the overall goodness-of-fit with multiple approximate fit indexes. The variety of existing indexes can be broadly categorized into *absolute* and *incremental* fit indexes.

Absolute fit indexes can be interpreted as proportions of the covariances in the sample data matrix explained by the model (Kline, 2010, p. 195). We report the root mean square error of approximation (RMSEA) along with its 90 % confidence interval (CI) as an absolute fit index. The RMSEA was first referenced in (Steiger, 1990). It uses the $\chi^2$ statistic corrected for model parsimony and larger sample sizes. The RMSEA is scaled as a badness-of-fit statistic on a scale from 0 to 1. A value of 0 indicates perfect model fit and 1 worst model fit. While different cut-off values have been proposed, e.g., close to 0.06 (Hu and Bentler, 1999) or a stringent upper limit of 0.07 (Steiger, 2007), there is a general consensus that models with a RMSEA<0.05 provide good fit to the data (Schumacker and Lomax, 2004; Kline, 2010). Yu and Muthén (2002) confirm this threshold for categorical variables.

Incremental fit indexes indicate the relative improvement in model fit compared with a statistical baseline model, typically the independence model (Kline, 2010, p. 195). They are also known as comparative fit indexes or relative fit indexes. We report the comparative fit index (CFI), which was introduced by Bentler (1990) and the Tucker Lewis index (TLI), initially developed for factor analysis by Tucker and Lewis (1973). Values for both statistics range between 0 and 1 with increasing values indicating better model fit. A value larger than 0.9 is needed in order to ensure that misspecified models are not accepted (Hu and Bentler, 1999). Values >0.95 are recognized as indicative of good fit (Hu and Bentler, 1999; Schumacker and Lomax, 2004; Kline, 2010). Yu and Muthén (2002) confirm the 0.95-threshold for TLI and CFI scores of categorical outcomes.

**Confirmatory Factor Analysis** In addition to the overall model fit, construct reliability and validity needs to be analyzed in a confirmatory factor analysis (CFA). We use the three criteria suggested by Fornell and Larcker (1981) to evaluate reliability and validity.

First, the standardized factor loadings should be significant and exceed 0.5. IS scholars (e.g., Straub et al., 2004) typically suggest a cut-off value of 0.707 because loadings $>$ 0.707 indicate that the construct explains more than half of the variation in the indicator. However, CFA models can be accepted if factors do not explain this much variance for all indicators. In their heavily cited book on multivariate data analysis, Hair et al. present rules of thumb "suggesting that loadings should be at least .5 and ideally .7 or higher." (Hair, 2010, p. 819). Our secondary analysis of a heterogeneous data set unavoidably contains more noise than data collected in a controlled setup. We measure indicators on short scales and use constructs which are created post-hoc from semantically diverse items. This unexplained variance attenuates the factor loadings. Hence, we accept the 0.5 cut-off.

The second criterion, construct reliability, is tested using the composite reliability (CR) indicator. As CR takes into account that indicators can have different loadings, it is more suited in our analysis than the commonly used indicator Cronbach's Alpha (Hair, 2010). The CR should exceed 0.8.

Third, the average variance extracted (AVE), which represents the amount of indicator variance that is accounted for by the underlying items of the construct, should be greater than 0.5. This indicates that the construct explains more than half of the variance of its indicators (Hair, 2010).

In addition to these criteria, the model needs to be tested for discriminant validity to ensure that constructs do not measure the same phenomenon. To confirm discriminant validity, the square root of AVE should be greater than the between construct correlations (Henseler et al., 2009).

### 5.2.2 Measurement Model

**Data Preparation** Before the CFA and SEM analyses can be conducted, the data needs to be prepared. 8 583 cases (out of the total of 26 593) are excluded from the analysis because respondents reported that they do not use the Internet at all. 172 cases (0.96 %) are removed because they contain "Don't Know" responses for all questions related to *Perceived Cybercrime Risk* (PCR) and/or *Cybercrime Experience* (EXP). Another 640 "Don't Know" responses (3.6 %), measuring cybercrime experience, are changed into "Never", assuming that respondents, who do not know whether they experienced cybercrime, have not experienced it. The remaining 1 275 incomplete cases (7.17 %) are handled by Mplus using pairwise deletion. Ultimately, our analysis is based on 17 773 cases which represent 18 605 EU Internet users (using normalized weights).

**Table 5.2:** Reduced model: standardized factor loadings

| **Latent Variable** | **Indicator** | **Mean** | **SD** | **Loading** | **SE** | **Z-Score** | $R^2$ |
|---|---|---|---|---|---|---|---|
| Cybercrime Experience | exp1 | 0.093 | 0.324 | 0.776$^{***}$ | 0.041 | 19.0 | 0.602 |
| | exp2 | 0.486 | 0.676 | 0.556$^{***}$ | 0.025 | 21.9 | 0.309 |
| | exp3 | 0.138 | 0.380 | 0.769$^{***}$ | 0.030 | 26.0 | 0.591 |
| | exp4 | 0.175 | 0.431 | 0.724$^{***}$ | 0.042 | 17.3 | 0.524 |
| | exp5 | 0.140 | 0.379 | 0.740$^{***}$ | 0.046 | 16.0 | 0.548 |
| Perceived Cybercrime Risk | pcr1 | 2.739 | 0.973 | 0.821$^{***}$ | 0.007 | 113.9 | 0.674 |
| | pcr2 | 2.455 | 0.976 | 0.820$^{***}$ | 0.008 | 99.6 | 0.672 |
| | pcr3 | 2.448 | 0.967 | 0.805$^{***}$ | 0.010 | 77.6 | 0.648 |
| | pcr4 | 2.535 | 1.092 | 0.801$^{***}$ | 0.009 | 86.9 | 0.642 |
| | pcr5 | 2.310 | 0.979 | 0.823$^{***}$ | 0.007 | 124.6 | 0.677 |
| | pcr6 | 2.318 | 0.989 | 0.795$^{***}$ | 0.007 | 119.3 | 0.632 |

Model fit: N=17 773; $\chi^2(df)$=254(70); RMSEA=.012 (.011 – .014), TLI=.980, CFI=.984

**Confirmatory Factor Analysis** We first evaluate the measurement model using the criteria presented in Section 5.2.1. Results of the CFA for the baseline model are reported in Appendix B.1. The overall goodness-of-fit indexes show acceptable fit (bottom of Table B.1) and almost all indicators meet the first criterion – significant factor loadings greater than 0.5. The only exception is ma1, which measures awareness of cybercrime from TV. This points to problems with the measurement of the *Media Awareness* (MA) construct. Table B.2 shows that the second and third criterion are not met by MA, which has unacceptable reliability and validity scores (CR = 0.66, AVE = 0.38). Several modification indexes (MI) underpin the negative influence of MA on the fit of the overall model. The problems are likely raised by measuring the latent variable on four binary indicators. Given that the phrasing of the questions does not reflect our understanding of cybercrime awareness very well (since hearing about cybercrime from multiple sources may not increase awareness), we exclude MA from the structural analysis. Nevertheless, we suspect that media reports influence the behavior of Internet users and encourage further research on this aspect, using appropriate instruments.

We conduct a second CFA for a reduced model without MA. The MIs further imply that a positive measurement error correlation should be added between pcr4 and pcr5 (MI: 28, E.P.C.Std.: 0.155). Since both questions measure a form of illegal content (pcr4: child pornography, pcr5: content promoting racial hatred[7]) and are likely to be interpreted similarly by the respondent, the correlation is legitimate. Table 5.2 reports standardized factors loadings for the reduced model and Table 5.3 the remaining fit criteria. All goodness-of-fit indicators indicate good model fit. The constructs fulfill the reliability and validity requirements, i. e., meet the three suggested criteria. The AVE for EXP is 0.49 in the reduced model. Due to the secondary nature of our analyses, we consider it close enough to the target value of 0.5 to be deemed acceptable.

**Table 5.3:** Reduced model: reliability and discriminant validity

| | **Reliability** | | **Correlations (lower-left)** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | CR | AVE | EXP | PCR | avS | avB | avN | pbA | pbP | pbS |
| EXP | 0.82 | 0.49 | **0.700** | (.021) | (.045) | (.033) | (.012) | (0.024) | (.024) | (.036) |
| PCR | 0.92 | 0.66 | .263$^{***}$ | **0.812** | (.019) | (.017) | (.028) | (0.029) | (.015) | (.029) |
| avS | - | - | .061 | .170$^{***}$ | - | (.035) | (.032) | (.025) | (.021) | (.028) |
| avB | - | - | .170$^{***}$ | .127$^{***}$ | .577$^{***}$ | - | (.050) | (.027) | (.017) | (.033) |
| avN | - | - | .145$^{***}$ | .092$^{***}$ | .305$^{***}$ | .297$^{***}$ | - | (.046) | (.046) | (.038) |
| pbA | - | - | .317$^{***}$ | .066$^{*}$ | .011 | .073$^{**}$ | .450$^{***}$ | - | (.025) | (.043) |
| pbP | - | - | .174$^{***}$ | .047$^{**}$ | −.027 | .010 | .414$^{***}$ | .557$^{***}$ | - | (.033) |
| pbS | - | - | .075$^{*}$ | .006 | −.026 | −.038 | .453$^{***}$ | .427$^{***}$ | .532$^{***}$ | - |

Cybercrime Experience (EXP), Perceived Cybercrime Risk (PCR), Avoidance Intention: Online shopping (avS), Online banking (avB), Online social networking (avN), Protection Behavior: Anti-virus (pbA), Different passwords (pbP), Changed security settings (pbS).

To confirm discriminant validity, the square root of AVE (noted in bold font on the diagonal of Table 5.3) should be greater than the between construct correlations (Henseler et al., 2009). This is satisfied for all constructs in the reduced model. Table 5.3 shows that correlations between most constructs are generally low, but highly significant ($p < 0.001$). The low correlations can be traced to the secondary analysis and the heterogeneous data set which includes multiple countries, languages, and cultures. However, the measurement model analysis shows that the reduced model can be reliably and validly measured based on the EB data.

### 5.2.3 Structural Models

The structural parameters are estimated using the reduced measurement model. To test our hypotheses, we evaluate overall model fit in accordance to the threshold for approximate fit indexes

[7] pcr4 – Question QE11.4: "Accidentally encountering child pornography online" (EB77.2, 2012, p. Q6); pcr5 – Question QE11.5: "Accidentally encountering material which promotes racial hatred or religious extremism" (EB77.2, 2012, p. Q6).

identified in Section 5.2.1 and then check the effect size and significance of path coefficients. The lower part of Table 5.4 reports approximate fit indexes for each model. All indicate good fit of the six models, with a slightly better fit for avoidance intention models compared to protection behavior models. Avoidance of online shopping (avS) models fit best and installing anti-virus software (pbA) fit worst. The path coefficients, their standard errors (in brackets), and the level of significance are documented in the upper part of Table 5.4, enabling the evaluation of the hypotheses.

**Table 5.4:** Structural models: path coefficients (SEs) and fit indexes

| | **Avoidance Intention (AV)** | | | **Protection Behavior (PB)** | | |
|---|---|---|---|---|---|---|
| **Path** | avB | avS | avN | pbA | pbP | pbS |
| EXP → PCR | 0.258$^{***}$<br>(0.020) | 0.258$^{***}$<br>(0.020) | 0.260$^{***}$<br>(0.020) | 0.258$^{***}$<br>(0.020) | 0.259$^{***}$<br>(0.020) | 0.262$^{***}$<br>(0.021) |
| PCR → AV/PB | 0.093$^{***}$<br>(0.023) | 0.167$^{***}$<br>(0.020) | 0.061$^{*}$<br>(0.027) | −0.010<br>(0.027) | 0.006<br>(0.016) | −0.016<br>(0.031) |
| EXP → AV/PB | 0.142$^{***}$<br>(0.034) | 0.020<br>(0.044) | 0.121$^{***}$<br>(0.011) | 0.063<br>(0.035) | 0.161$^{***}$<br>(0.026) | 0.317$^{***}$<br>(0.028) |
| EXP$\xrightarrow{\text{PCR}}$AV/PB | 0.024$^{***}$<br>(0.005) | 0.043$^{***}$<br>(0.006) | 0.016$^{*}$<br>(0.007) | −0.003<br>(0.007) | 0.002<br>(0.004) | −0.004<br>(0.008) |
| EXP$\xrightarrow{\text{tot.}}$AV/PB | 0.166$^{***}$<br>(0.031) | 0.063$'$<br>(0.043) | 0.137$^{***}$<br>(0.012) | 0.061<br>(0.037) | 0.162$^{***}$<br>(0.023) | 0.313$^{***}$<br>(0.024) |
| Model fit: $\chi^2$ (*df*) | 143 (51) | 138 (51) | 201 (51) | 194(51) | 166(51) | 191(51) |
| RMSEA | .010 | .010 | .013 | .013 | .011 | .12 |
| (90% CI) | .008 - .012 | .008 - .012 | .011 - .015 | .011 - .014 | .009 - .013 | .011 - .014 |
| TLI / CFI | .990/.993 | .991/.993 | .985/.988 | .988/.985 | .988/.991 | .986/.989 |

Cybercrime Experience (EXP), Perc. Cybercrime Risk (PCR), AV: Online shopping (avS), Online banking (avB), Online social networking (avN), PB: Anti-virus (pbA), Different passwords (pbP), Changed security settings (pbS).

*Cybercrime Experience* increases *Perceived Cybercrime Risk* significantly in all three avoidance models, providing strong support for **H1**. The effect size may be positively biased by context effects because the PCR battery directly succeeds the EXP battery, question blocks QE11 and QE10 in EB77.2 (2012), and same question bias because both batteries contain almost exclusively the same answer categories (Tourangeau and Bradburn, 2010). The bias might explain the comparably high path coefficient between EXP and PCR. We believe that the general effect is justified, but its size must be confirmed by future studies.

The EB data also provides support for **H2**, *Perceived Cybercrime Risk* increases *Avoidance Intention* among all three online services. We observe the biggest effect size for the impact on avoidance of online shopping (avS: $\beta = 0.167$, $p < 0.001$). A smaller, but still highly significant effect is observed for the avoidance of online banking (avB: $\beta = 0.093$, $p < 0.001$). Avoidance of online social networks (avN: $\beta = 0.061$), measured by publishing less personal information online, is significant at the $p < 0.05$ level.

Indirect effects of *Cybercrime Experience* on *Avoidance Intention* are found for all online services: online banking (avB: $\beta = 0.024$, $p < 0.001$), online shopping (avS: $\beta = 0.046$, $p < 0.001$), and online social networking (avN: $\beta = 0.02$, $p < 0.05$), supporting **H3**. Full mediation by PCR is only found for the avoidance of online shopping, as the direct effect is not significant (avS: $\beta = 0.02$, $p < 0.653$). The effect size of the total effect is small and only marginally significant ($p < 0.15$). Significant direct effects are observed for EXP on avoidance of online banking and online social networking, but the total effects are partially mediated by PCR.

The right part of Table 5.4 reports path coefficients for *Protection Behavior* (PB). The structural links support **H1** for the PB models, with very similar effect sizes for all three forms of protection. In contrast to AV, the impact of PCR on PB is not significant. Consequently, **H4** is not supported by the data. We also have to reject the full mediation hypothesis (**H5**) regarding the impact of EXP on PB. Indirect effects are not significant in any model. Interestingly, we find a direct effect of EXP on using different passwords (pbP: $\beta = 0.161$, $p < 0.001$) and changing security settings (pbS: $\beta = 0.317$, $p < 0.001$). Installing anti-virus software (pbA) is neither influenced by PCR nor by EXP. While this may be a surprising result, we conjecture it is due to the high proliferation of anti-virus software, which the majority of Internet users reports to install preventively (see Table 5.1). Hypotheses **H6** and **H7** were not tested because the MA construct could not be measured reliably.

## 5.3 Model Variants

We study three variations of the research model to make additional robustness checks and obtain further explanations of Internet users' avoidance behavior. Specifically, Section 5.3.1 analyses the moderating role of Internet users' confidence in online transactions using a multi-group analysis. Section 5.3.2 proposes an improved measurement model based on a new set of questions available in the third EB wave. Finally, Section 5.3.3 considers avoidance of unknown websites as a fourth, more general, form of avoidance not directly associated with a particular online service.

### 5.3.1 Moderation by User Confidence

Computer and Internet literacy can moderate user interaction with technology. Hsu and Chiu (2004) show how one's belief in Internet self-efficacy positively influences the use of online services. In the context of security behavior, Chen and Zahedi (2016) find that perceived security self-efficacy has a negative impact on avoidance behavior. To test for these moderation effects of *User Confidence* (UC), we extend the research model with two additional hypotheses. The first concerns the moderation of path coefficients and the second the moderation of factor means. Figure 5.2 illustrates the hypotheses in an extended path model.

**H9: User Confidence moderates the effects between higher order constructs, in that the effects are smaller for confident users.**
Various authors (e. g., Featherman and Fuller, 2003) emphasize that understanding how different consumer segments perceive and evaluate risks is essential for explaining adoption. Therefore, we suspect that the UC in handling online transactions moderates the effects (**H1** – **H3**), proposed in the original research model. We hypothesize that the effects EXP has on PCR are smaller for more confident users, as they feel more secure about their online behavior and perceive less uncertainty.

**H10: User Confidence moderates the effects, in that the means of latent variables for Perceived Cybercrime Risk and Avoidance Intention are smaller for confident users.**
In addition to different effect sizes we suspect that UC influences the means of the constructs in our model. In particular, we hypothesize that more confident Internet users perceive less cybercrime risk and are also less likely to avoid online services.

**Measurement of User Confidence** UC is measured using a single ordinal indicator, which represents the self-reported confidence to conduct online transactions on a 4-point rating scale[8]. Responses in the EB show that more than two thirds of EU Internet users (68.99 %) are at least

[8] QE5 How confident are you about your ability to use the Internet for things like online banking or buying things online ? ("very confident", "fairly confident", "not very confident", "not at all confident").

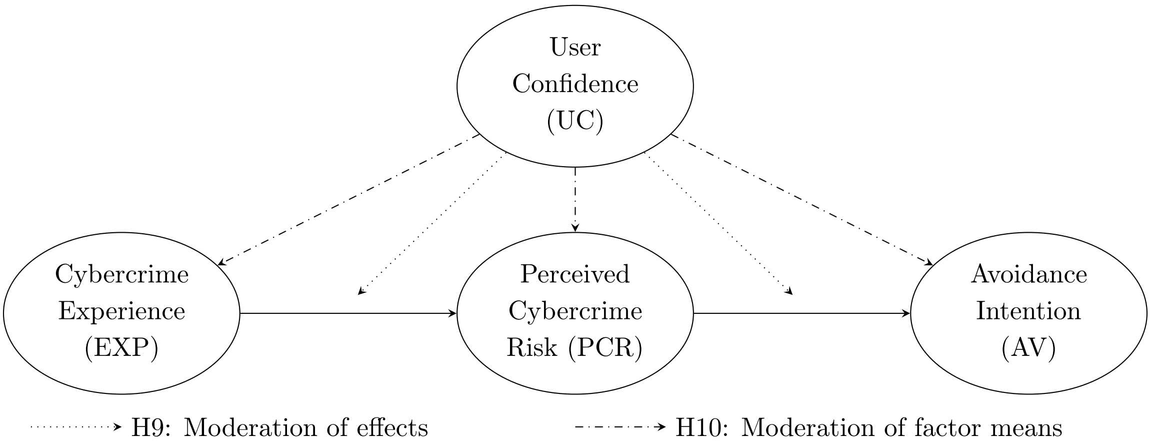

User Confidence (UC)
Cybercrime Experience (EXP)
Perceived Cybercrime Risk (PCR)
Avoidance Intention (AV)
H9: Moderation of effects
H10: Moderation of factor means

**Figure 5.2:** Extension of the research model by moderation of *User Confidence*

fairly confident and more than one quarter (26.7 %) are very confident in conducting online transactions. We split the sample into very confident ($N = 4\,972$) and not at all confident (unconfident) Internet users ($N = 2\,196$). To reduce the amount of noise and heterogeneity, we exclude the central categories, i. e., "fairly" and "not very" confident users, from the multi-group analysis.

Table B.5 (in Appendix B.3) compares descriptive statistics of the relevant indicators between the three groups of very confident, unconfident, and all Internet users.[9] Confident users consistently report higher rates of cybercrime experience and media awareness. We find the biggest differences for reception of spam emails, which is reported by half (52.94 %) of the confident, but only one fifth (20.54 %) of the unconfident Internet users, and similarly for having read about cybercrime on the Internet, which is also much more likely for confident users. Unconfident users, on the other hand, report higher levels of perceived risk for every form of cybercrime. For example, 67.03 % are personally concerned to become a victim of identity theft (in contrast to 54.12 % of the confident users). Unconfident Internet users are also at least twice as likely to reduce their use of online shopping and online banking due to security concerns.

**Multi-group Analysis** We study the moderation effects of user confidence in a multi-group analysis. We use the general-to-specific approach proposed by Millsap and Yun-Tein (2004) to test measurement invariance between different models. Meade et al. (2008) show that for large samples, the chi-square difference test is biased to reject invariance. This corresponds to the problems of the $\chi^2$ goodness-of-fit statistic, discussed in Section 5.2.1. We report $\chi^2$ differences, but use a CFI-based difference test to evaluate model invariance, as suggested by Millsap and Yun-Tein (2004). According to the test, a CFI change ($\Delta\text{CFI} <= 0.002$) confirms measurement invariance between two models.

Table 5.5 reports the results of invariance tests in the multi-group analysis. The overall goodness-of-fit indexes confirm acceptable fit for all models and all three online services. The baseline model (Mod A) includes both groups with all parameters freely estimated in each group. To test measurement invariance, factor loadings and thresholds are fixed in the invariant model (Mod B). Modification indexes suggest a partly invariant model, with the thresholds of pcr3 being free to vary between groups. Byrne et al. (1989) show that moderation effects can be tested on partly invariant models if at least two intercepts and loadings are fixed.

[9] The minor deviations for all Internet users in comparison to the descriptives statistics in Table 5.1 are due to the exclusion of a few cases with missing values for user confidence.

**Table 5.5:** Moderation of *User Confidence*: measurement invariance

| **Model** | $\chi^2$ **(*df*)** | **CFI** | **TLI** | **RMSEA (90% CI)** | $\Delta\chi^2$ **(*df*)** | $\Delta CFI$ |
|---|---|---|---|---|---|---|
| **Avoidance Intention: Online shopping** | | | | | | |
| Mod A: Baseline | 168 (102) | .995 | .994 | .013 (.009 – .017) | | |
| Mod B: Invariant | 215 (123) | .993 | .993 | .014 (.011 – .017) | 75.03 (21) | .002 |
| Mod C: Fixed path coef. | 233 (126) | .992 | .992 | .015 (.012 – .018) | 20.02 (3) | .001 |
| Mod D: Fixed factor means | 265 (126) | .990 | .989 | .017 (.014 – .020) | 31.57 (3) | .003 |
| **Avoidance Intention: Online banking** | | | | | | |
| Mod A: Baseline | 167 (102) | .995 | .994 | .013 (.009 – .016) | | |
| Mod B: Invariant | 213 (123) | .993 | .993 | .014 (.011 – .017) | 73.67 (21) | .002 |
| Mod C: Fixed path coef. | 228 (126) | .992 | .992 | .015 (.012 – .018) | 19.46 (3) | .001 |
| Mod D: Fixed factor means | 265 (126) | .990 | .989 | .017 (.014 – .020) | 33.36 (3) | .003 |
| **Avoidance Intention: Online social networking** | | | | | | |
| Mod A: Baseline | 192 (102) | .993 | .991 | .015 (.012 – .019) | | |
| Mod B: Invariant | 238 (123) | .992 | .991 | .016 (.013 – .019) | 75.05 (21) | .001 |
| Mod C: Fixed path coef. | 237 (126) | .992 | .991 | .015 (.012 – .018) | 09.13 (3) | .000 |
| Mod D: Fixed factor means | 276 (126) | .989 | .988 | .018 (.015 – .021) | 26.86 (3) | .003 |

The invariance of path coefficients is tested by fixing them to be equal between groups (Mod C) and comparing the model fit to Mod B. Table 5.5 shows that Mod C is invariant to Mod B because ΔCFI <= 0.002 for all online services. The chi-square-based DIFFTEST ($\Delta\chi^2$ (*df*)), provided by Mplus for WLSMV estimation, also shows the lowest values for this model alternation confirming that reactions of confident and unconfident Internet users do not differ significantly. Consequently, **H9** needs to be rejected.

**Table 5.6:** Moderation of *User Confidence*: multi-group analysis

| **Paths** | **Online banking (avB)** | | **Online shopping (avS)** | | **OSN (avN)** | |
|---|---|---|---|---|---|---|
| LV means | Unconfident | Confident | Unconfident | Confident | Unconfident | Confident |
| EXP→PCR | 0.232$^{***}$<br>(0.027) | 0.315$^{***}$<br>(0.027) | 0.234$^{***}$<br>(0.028) | 0.315$^{***}$<br>(0.027) | 0.233$^{***}$<br>(0.027) | 0.315$^{***}$<br>(0.027) |
| PCR→AV | 0.036<br>(0.028) | 0.138$^{***}$<br>(0.037) | 0.100$^{***}$<br>(0.030) | 0.197$^{***}$<br>(0.049) | 0.010<br>(0.034) | 0.074<br>(0.045) |
| EXP→AV | 0.190$^{***}$<br>(0.040) | 0.208$^{***}$<br>(0.031) | 0.032<br>(0.053) | 0.119$^{*}$<br>(0.057) | 0.277$^{***}$<br>(0.045) | 0.093$^{**}$<br>(0.033) |
| EXP$\xrightarrow{\text{PCR}}$AV | 0.008<br>(0.007) | 0.043$^{***}$<br>(0.011) | 0.024$^{**}$<br>(0.008) | 0.062<br>(0.016) | 0.002<br>(0.008) | 0.023<br>(0.014) |
| EXP$\xrightarrow{\text{tot.}}$AV | 0.198$^{***}$<br>(0.037) | 0.252$^{***}$<br>(0.036) | 0.055<br>(0.053) | 0.181$^{**}$<br>(0.058) | 0.279$^{***}$<br>(0.044) | 0.117$^{***}$<br>(0.003) |
| EXP | 0.00<br>(*fixed*) | 0.785$^{**}$<br>(0.267) | 0.00<br>(*fixed*) | 0.891$^{**}$<br>(0.297) | 0.00<br>(*fixed*) | 1.162$^{***}$<br>(0.271) |
| PCR | 0.00<br>(*fixed*) | −0.506$^{***}$<br>(0.140) | 0.00<br>(*fixed*) | −0.531$^{***}$<br>(0.142) | 0.00<br>(*fixed*) | −0.621$^{***}$<br>(0.143) |
| AV | 24.38% | 9.05% | 27.25% | 11.42% | 29.84% | 39.36% |

Mediation: EXP$\xrightarrow{\text{PCR}}$AV, total effect: EXP$\xrightarrow{\text{tot.}}$AV; SEs in brackets; Cybercrime Experience (EXP), Perceived Cybercrime Risk (PCR), Avoidance Intention (AV), Online social networking (OSN).

The invariance of factor means and intercepts is tested by fixing the factor means for all latent variables and the thresholds for the respective question on online service avoidance (Mod D).

Table 5.5 shows that this constrained model exceeds the ΔCFI threshold in all three domains, indicating a significant deviation from the invariant model (Mod B). This confirms that latent variable means differ between confident and unconfident Internet users.

To illustrate the differences, factor means are fixed to zero for unconfident users and freely estimated for confident users. The lower part of Table 5.6 reports the results. It shows that confident users report significantly more EXP ($p<0.01$), but significantly less PCR ($p<0.001$) and a smaller AV of online shopping and online banking. The moderation effect is different for online social network participation, i. e., publishing personal information online, as unconfident users do not reduce their participation in social networks as much as confident users. Consequently, **H10** is accepted for online shopping and online banking, but rejected for online social networking. This suggests a distinction between security and privacy risks to be investigated in future work.

### 5.3.2 Improved Measurement Model

A major limitation of secondary analyses is the dependence on an existing instrument, which is not tailored to the analysis. In our case the EB surveys limit us to the six types of cybercrime, available to measure individual *Cybercrime Experience* and *Perceived Cybercrime Risk*. Fortunately, the 2014 wave of the EB adds four types of cybercrime, enabling an improvement of the measurement model by including more appropriate types as indicators for the two constructs.

**Indicator Selection** The left part of Table 5.7 shows the four new types of consumer-facing cybercrime (exp7, pcr7, exp8, pcr8, exp9, pcr9, exp10, and pcr10) and their question wording. All new types target ordinary Internet users and potentially lead to substantial monetary losses, making them highly relevant for our study of individual security behavior. The increased pool of indicators with a total of ten different types of cybercrime, allows us to remove less suitable crimes from the measurement model (exp2, pcr2, exp4, pcr4, exp5, pcr5, exp6, pcr6). We argue for the omission of these indicators due to one or multiple of the following reasons: 1) they only cause insignificant harm, 2) they are not primarily targeted against individual Internet users, or 3) they are not observable for them.

**Table 5.7:** Improved measurement model (14'): indicators with original question wording

| **Additional cybercrime indicators** | | **Removed cybercrime indicators** | |
|---|---|---|---|
| exp7, pcr7 | "Your social media or email account being hacked" | exp2, pcr2 | "Receiving emails or phone calls fraudulently asking for access to your computer, logins or personal details (including banking or payment information)" |
| exp8, pcr8 | "Being a victim of bank card or online banking fraud" | exp5, pcr5 | "Accidentally encountering child pornography online" |
| exp9, pcr9 | "Being asked for a payment in return for getting back control of your device" | exp4, pcr4 | "Accidentally encountering material which promotes racial hatred or religious extremism" |
| exp10, pcr10 | "Discovered malicious software (viruses, etc.) on your device" | exp6, pcr6 | "Not being able to access online services (e. g. banking services or public services) because of cyber-attacks" |

In the cases of accidentally encountering extremist material (exp4, pcr4) and child abuse material (exp5, pcr5), Internet users are affected only indirectly. Though the possession of the material can be illegal, the recipients who encounter it accidentally are not the primary victims. In the majority of cases, their harm is insignificant compared to the harm caused to the primary victims. Other crimes are barely observable for individual Internet users, partly because they are also not targeted at them. This concerns in particular inaccessible online services, due to cyber-attacks (exp6, pcr6). Spam emails (exp2, pcr2) are targeted against consumers and their reception is commonly reported in the EB (31.3 % in 2014). We still decide to exclude spam emails from the improved measurement model because the harm of pure reception is hardly significant and research shows that the vast majority of spam emails are not successful (Kanich et al., 2008). Following our discussion in Section 4.3.2, we choose not to include the new indicator malware infections (exp10, pcr10), since infections are not always detectable for the victim and do not necessarily cause significant harm.

**Measurement Model** The improved measurement model includes the following five types of cybercrime: identity theft in the context of online shopping, online shopping fraud, hacked accounts, bank card or online banking fraud, and extortion. All of them are targeted against individual Internet users and can cause significant harm. Descriptive statistics are presented together with standardized factor loadings in Table 5.8. Online shopping fraud is the most commonly experienced type in the EU with 12.62 % of Internet users reporting some experience. The prevalence of the remaining types of cybercrime ranges between 6.95 % for identity theft on the lower and 8.35 % for extortion on the upper end. Nevertheless, most Internet users are (fairly or very) concerned about experiencing identity theft (67.99 %), but less about extortion (47.19 %) and online shopping fraud (55.74 %).

**Table 5.8:** Improved measurement model (14'): descriptives and standardized factor loadings

| **Descriptive statistics** | | | **Standardized factor loadings** | | | |
|---|---|---|---|---|---|---|
| ID | Latent variable (scale)/ indicator | Answer | Loading | SE | Z-Score | $R^2$ |
| **EXP** | **Cybercrime Experience (Ordinal)** | | | | | |
| "How often have you experienced or been victim of... ?" – At least occasionally | | | | | | |
| exp1 | Identity theft | 6.95 % | 0.855$^{***}$ | 0.014 | 59.76 | 0.731 |
| exp3 | Online shopping fraud | 12.62 % | 0.696$^{***}$ | 0.053 | 13.09 | 0.484 |
| exp7 | Hacking of private accounts | 7.71 % | 0.767$^{***}$ | 0.031 | 24.96 | 0.588 |
| exp8 | Online banking/bank card fraud | 7.10 % | 0.776$^{***}$ | 0.044 | 17.48 | 0.602 |
| exp9 | Extortion | 8.35 % | 0.623$^{***}$ | 0.045 | 13.96 | 0.388 |
| **PCR** | **Perceived Cybercrime Risk (Ordinal)** | | | | | |
| "How concerned are you personally about becoming a victim of... ?" – At least fairly | | | | | | |
| pcr1 | Identity theft | 67.99 % | 0.834$^{***}$ | 0.013 | 66.74 | 0.696 |
| pcr3 | Online shopping fraud | 55.74 % | 0.776$^{***}$ | 0.013 | 58.513 | 0.602 |
| pcr7 | Hacking of private accounts | 60.25 % | 0.832$^{***}$ | 0.010 | 82.53 | 0.691 |
| pcr8 | Online banking/bank card fraud | 63.36 % | 0.844$^{***}$ | 0.011 | 78.57 | 0.712 |
| pcr9 | Extortion | 47.19 % | 0.812$^{***}$ | 0.010 | 79.80 | 0.659 |

Model fit: N=18 693; $\chi^2(df)$=158(90); RMSEA=.006 (.005 – .008), TLI=.977, CFI=.985.

We conduct a new CFA analysis for the improved measurement model (14') using the data from the third EB wave in 2014. Table 5.8 also reports the CFA results. The overall fit indexes at the bottom confirm that the improved model provides a good fit to the data. All goodness-of-fit indexes exceed the respective values for the original (reduced) model in 2012. The first criterion for construct reliability and validity (significant standardized factor loadings $> 0.5$) is met by both improved constructs. Table B.3 in the appendix shows that the second and third criterion are also met, as CR exceeds 0.8 and AVE exceeds 0.5 for both constructs. Furthermore, Table B.3 confirms discriminant validity for the improved measurement model.

We compare CFA results for the improved measurement model to the original measurement model in 2014, fitted as part of the longitudinal repetition in Section 5.4.3. The improved model provides better fit in all goodness-of-fit indexes and CR and AVE scores indicate better reliability.

**Structural Models** We finally analyze the structural models. According to the $\chi^2$ statistics and the RMSEA, the improved model is better than the original one in 2012 for all forms of AV and PB. The approximate fit indixes, CFI and TLI show mixed results with only marginal differences. Overall, the differences in goodness-of-fit are only small. The structural links confirm the results of the original model, underlining its robustness.

The impact of EXP on PCR is positive and highly significant for all forms of avoidance and protection. PCR leads to avoidance of online shopping (avS: $\beta = 0.148$, $p < 0.001$) and banking (avB: $\beta = 0.135$, $p < 0.001$). We also find a fully mediated impact of EXP on both services (avS: $\beta = 0.042$, $p < 0.001$ and avB: $\beta = 0.038$, $p < 0.001$). Avoidance of online social networking (avN) is neither influenced by EXP nor by PCR. The marginal effect found in the original model is insignificant in the improved measurement model. PB is triggered directly by EXP in the case of using different passwords (pbP: $\beta = 0.090$, $p < 0.001$) and changing security settings (pbS: $\beta = 0.230$, $p < 0.001$).

**Table 5.9:** Improved measurement model (14'): structural models

| | **Path coefficients** | | | | **Model fit** | | | |
|---|---|---|---|---|---|---|---|---|
| AV | EXP→PCR | PCR→AV | $\text{EXP}\xrightarrow{\text{PCR}}\text{AV}$ | EXP→AV | $\chi^2$ (*df*) | RMSEA (90 CI) | CFI | TLI |
| avS | $0.283^{***}$<br>(0.0340) | $0.148^{***}$<br>(0.0240) | $0.042^{***}$<br>(0.0090) | −0.003<br>(0.0440) | 97 (42) | .008 (.006–.010) | .991 | .988 |
| avB | $0.282^{***}$<br>(0.0330) | $0.135^{***}$<br>(0.0200) | $0.038^{***}$<br>(0.0070) | 0.032<br>(0.0330) | 100 (42) | .009 (.006–.011) | .990 | .987 |
| avN | $0.282^{***}$<br>(0.0330) | 0.047<br>(0.0270) | 0.013<br>(0.0080) | 0.017<br>(0.0280) | 116 (42) | .010 (.008–.012) | .988 | .984 |
| PB | EXP→PCR | PCR→PB | $\text{EXP}\xrightarrow{\text{PCR}}\text{PB}$ | EXP→PB | | | | |
| pbA | $0.282^{***}$<br>(0.0350) | 0.037<br>(0.0270) | 0.010<br>(0.0070) | −0.052<br>(0.035) | 103 (42) | .009 (.007–.011) | .989 | .985 |
| pbP | $0.281^{***}$<br>(0.0340) | 0.019<br>(0.0350) | 0.006<br>(0.0110) | $0.090^{***}$<br>(0.020) | 101 (42) | .009 (.006–.011) | .990 | .986 |
| pbS | $0.282^{***}$<br>(0.0340) | 0.021<br>(0.0260) | −0.006<br>(0.0080) | $0.230^{***}$<br>(0.0190) | 95 (42) | .008 (.006–.010) | .988 | .987 |

Cybercrime Experience (EXP), Perceived Cybercrime Risk (PCR), Avoidance Intention (AV): Online shopping (avS), Online banking (avB), Online social networking (avN), Protection Behavior (PB): Anti-virus (pbA), Different passwords (pbP), Changed security settings (pbS).

### 5.3.3 Avoidance of Unknown Websites

The third variant extends the model with avoidance of unknown websites (avU) as a fourth form of *Avoidance Intention*. We justify the inclusion of avU with the statement by Liang and Xue (2009) that individual avoidance behavior has no affirmative direction, as long as it separates the current state from an undesired end-state (i. e., becoming a victim).

In our context, individuals may keep using familiar and well-known online service providers, but avoid unknown websites which offer the same service. The facilitating role of familiarity and trust has been studied repeatedly in the context of online shopping. Gefen and Straub (2000) already demonstrate their importance in online purchase decisions. Lim (2003) classifies sources of perceived risk in B2C e-commerce, finding that uncertainty regarding an unknown vendor is equally important as the general risk of online shopping. In a similar vein, brand image (online and offline) is found to be an essential source, reducing perceived risk and facilitating the adoption of online services (Chen and He, 2003; Kwon and Lennon, 2009).

**Measurement Model** In analogy to *Avoidance Intention* for the three online services, we measure avU with a binary question: "…you only visit websites you know and trust." Descriptive statistics for avU are reported in Table 5.1 along with the other indicators. About one third of EU Internet users (33.9 % in 2012 and 35.7 % in 2014) reported to only visit websites they know and trust.

To include avU, we conduct an additional CFA analysis comprising all outcome variables. We do not report the results here in detail, since avU has already been included in the CFA analysis for the improved measurement model (Section 5.3.2) and is included in all CFAs which are part of the longitudinal repetition (Section 5.4). In summary, the CFAs confirm good fit to the data in terms of overall goodness-of-fit and all constructs are measured validly and reliably.

**Structural Model** The structural model for avU, measured using the improved measurement model based on the data for 2014, provides good fit to the data. The approximate goodness-of-fit indexes all indicate a good model fit: $\chi^2\,(df) = 91\,(42)$, RMSEA $= 0.008\,(0.006-0.010)$, TLI=0.988, CFI=0.991. The characteristics of the structural links in the avU models are similar to avoidance intention of online banking (avB) and online shopping (avS). Accordingly, EXP increases PCR ($\beta = 0.283$, $p < 0.001$), which ultimately increases avU ($\beta = 0.157$, $p < 0.001$). The indirect effect of EXP on avU is mediated by PCR and highly significant ($\beta = 0.051$, $p < 0.001$).

Interestingly, we find a direct and negative effect of EXP on the avU $\beta = -0.066$, $p < 0.01$, which is small, but still significant. While reverse causality between both constructs might explain the effect, we cannot study this in detail, at least with the current data set. We encourage future studies to shed more light on this observation and include avU in the longitudinal repetition to check the persistence of this form of avoidance.

## 5.4 Longitudinal Repetition

The two additional waves of the EB enable a repetition of the SEM analysis in 2013 and 2014. We develop a longitudinal approach to validate the robustness of the behavioral model and study time-dependent changes of perceptions and behavior. Section 5.4.1 outlines our approach and Section 5.4.2 presents descriptive statistics from a longitudinal perspective. Section 5.4.3 reports results for the measurement models and Section 5.4.4 for the structural models. Finally, Section 5.4.5 discusses trends in the structural links.

### 5.4.1 Approach

Longitudinal studies are characterized by repeated observations of the same units on the same outcomes at different points in time (Singer and Willett, 2003). In the best case, they are based on panel data, where an initial sample, the panel, is pre-selected and data is collected at several occasions (Steel and McLaren, 2008). While panel studies enable in-depth analysis of inter- and intra-individual changes over time, they require substantial resources, which are rarely affordable for sampling at the societal level. Another option often used in the social science are time-series analyses of aggregated measures (Bernal et al., 2017). Time-series analysis can explain time-variant changes on an aggregated level, but require numerous observations (50 or more) to estimate parameters (Box and Pierce, 1970). Unfortunately, the EB data is only available for three points in time.

Trend studies are a viable alternative if the research questions concern aggregated effects at the societal level. The design allows to draw on independent samples for each measurement, provided that these samples represent the same population (Steel and McLaren, 2008). The EB data is collected independently from different subjects, but with the same sampling methods and instrument for the same population (see first paragraph in Section 5.1.3). Even though not without limitations, the data can be used to check the robustness of the research model and examine time-variant differences in aggregated effects, i. e., on the pan-European level.

An essential consideration for longitudinal research design is the time metric, i. e., the data collection interval (Steel and McLaren, 2008). The metric must fit to the characteristics of the sample and the phenomena to be studied (Singer and Willett, 2003). While some dynamics are best studied over days or weeks, aggregated effects of online service avoidance among the general population can be expected to change slowly. The absence of seasonal effects in cybercrime attacks reduces the need for equidistant sampling intervals. Even data from a few waves allows us to observe relevant trends in such a scenario (Kehr and Kowatsch, 2015).

Our approach uses the same SEM analysis to evaluate the robustness of the model and observe trends over time. The study is structured into two phases. The first phase replicates the SEM analysis (as conducted in Section 5.2) for the two subsequent waves. We estimate and evaluate the research models for all three EB waves individually. In the second phase we validate the persistence of aggregated effects by comparing CIs of the structural links for each hypothesis.

### 5.4.2 Data

The trend analysis is based on all three EB waves. Table 5.1 (in Section 5.1.3) reports descriptive statistics of the relevant indicators. The question wording did not change. The only differences we find, are that the order of *Cybercrime Experience* (EXP) and *Perceived Cybercrime Risk* (PCR) related questions has been swaped in the 2014 wave and that the questions measuring *Media Awareness* have been discontinued in 2013. The questionnaires are available in the technical appendices of the respective EB reports (EB77.2, 2012; EB79.4, 2013; EB82.2, 2015).

**Marginal Trends of Relevant Indicators** EXP is measured by five indicators, one for each type of cybercrime. Although the original question wording does not set an explicit time frame, we can assume that most respondents have an implicit horizon or fading memory (Tourangeau and Bradburn, 2010). Otherwise, it is difficult to explain that reported experience of cybercrime decreased between 2012 and 2014. Broken down by type of crime, we find the biggest difference for the reception of spam emails (exp2), which drops from 37.9 % of Internet users in 2012 to 31.3 % in 2014. Online shopping fraud (exp3), on the other end, remained on the same level (12.5 %).

PCR is measured independently for each of six types of cybercrime. While less than half of the respondents reported concern (except for pcr1: Identity theft) in 2012, all concern rates drop substantially between -5 %-pts. and -10 %-pts. in 2013. However, they increase above the 2012 level in 2014 (+9 %-pts. to +17 %-pts.). This "bumpy" nature of measuring cybercrime further challenges the robustness of the model over time. On the other hand, it highlights the importance of continuous refinement of measurement instruments and models, as done in Section 5.3.2.

*Avoidance Intention* (AV) is measured by three binary statements, which are causally linked to PCR through the question wording.[10] Marginal statistics show that avoidance of online shopping

[10] Question QE7: "Has concern about security issues made you change the way you use the Internet in any of the following ways ?" (EB77.2, 2012, p. Q4).

(avS) and online banking (avB) decreases slightly (-2 %-pts. to -4 %-pts.) from 2012 to 2014 and substantially (-25 %-pts.) for online social networking (avN).

*Protection Behavior* (PB) is measured in the same manner as AV. Each indicator represents one self-reported reaction to cybercrime. The most common response is installing anti-virus software (pbA). 51.4 % and 60.6 % of Internet users reported pbA in 2012 and in 2014, respectively. The use of different passwords (pbP) is less prevalent (25.1 %), but also increased (+6 %-pts.) over time. Changing security settings (pbS) is least prevalent (16.4 %) and increased only slightly (1 %-pt.).

**Contradiction of Avoidance and Adoption Trends** National trends of online service adoption may contradict with our findings regarding avoidance behavior (Section 5.2). To illustrate this contradiction, Figure 5.3 shows trends in the marginal statistics of national adoption levels for online shopping and online banking in the 27 EU member states. While levels vary between member states, increasing adoption trends of both services can be clearly observed from 2012 to 2014.

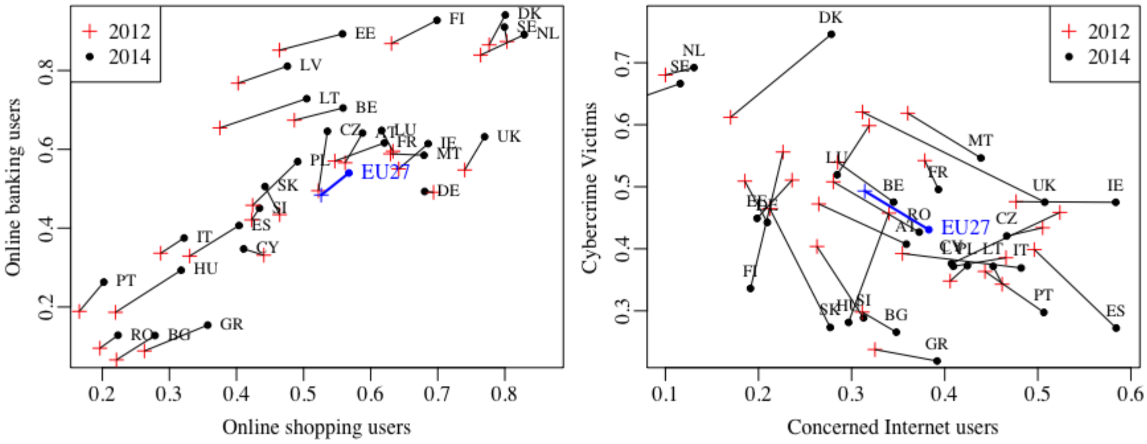


**Figure 5.3:** Comparison of EU member states in 2012 and 2014: users of online shopping and online banking (left), fraction of Internet users reporting concerns about and experience of cybercrime (right); Sources: EB77.2 (2012); EB82.2 (2015), authors' analysis

Figure 5.3 also shows that about a half of the European Internet users reported experience of some form of cybercrime in 2012. While experiences vary between countries, we see a downward trend on average. On the other hand, the public concern about cybercrime has grown from 2012 to 2014. Comparing the country-level trends, two contradictions are apparent and challenge hypotheses H1 and H2 regarding the impact of cybercrime on avoidance behavior. First, even though reported cybercrime experience dropped on average, cybercrime concern increased in 19 countries (and on average). Second, cybercrime concern and online service adoption increased simultaneously, despite the proposed avoidance effect.

Obviously, this simple interpretation of aggregated figures in two snapshots does not consider time lag effects and neglects that ongoing adoption may also increase the population of potentially concerned users. Still, the contradictions and the dynamic environment further challenge the robustness of the research model and call for a longitudinal perspective in the study of security behavior.

### 5.4.3 Measurement Models

**Data Preparation** Since the sampling and data collection is consistent in all three EB waves, we perform the same actions as in 2012 to prepare the data for the SEM analysis in the subsequent waves. We drop 9 535 cases from the 2013 wave because respondents reported that they do not use the Internet (8 988 cases in 2014). We also remove 108 cases for the 2013 survey because they contain “don’t know” or “refusal” responses in all questions related to PCR or EXP (187 for 2014). 526 further “don’t know” responses for EXP are recoded to “no experience” (602 in 2014). The remaining missing values (774 in 2013 and 1 472 in 2014) are handled by the SEM software Mplus using pairwise exclusion. To be consistent, we do not consider Croatia (the 28th member state) in the analysis. In total, our analysis is based on 18 037 cases for 2013, which represent 18 875 Internet users using normalized weights (18 693 for 2014 representing 20 081 Internet users).

**Table 5.10:** Longitudinal replication: standardized factor loadings

| | **2012** | | | **2013** | | | **2014** | | |
|---|---|---|---|---|---|---|---|---|---|
| | Loading | Z-Score | $R^2$ | Loading | Z-Score | $R^2$ | Loading | Z-Score | $R^2$ |
| exp1 | 0.714*** | 20.00 | 0.510 | 0.698*** | 20.87 | 0.487 | 0.736*** | 31.94 | 0.542 |
| exp2 | 0.623*** | 23.70 | 0.388 | 0.664*** | 18.30 | 0.441 | 0.704*** | 22.71 | 0.496 |
| exp3 | 0.745*** | 31.97 | 0.555 | 0.627*** | 15.83 | 0.393 | 0.655*** | 15.72 | 0.429 |
| exp5 | 0.694*** | 18.60 | 0.482 | 0.675*** | 16.73 | 0.456 | 0.700*** | 26.48 | 0.490 |
| exp6 | 0.703*** | 16.50 | 0.494 | 0.682*** | 13.62 | 0.465 | 0.721*** | 20.52 | 0.520 |
| pcr1 | 0.822*** | 112.70 | 0.676 | 0.851*** | 103.44 | 0.724 | 0.825*** | 63.31 | 0.681 |
| pcr2 | 0.820*** | 102.33 | 0.672 | 0.827*** | 71.51 | 0.684 | 0.822*** | 102.49 | 0.676 |
| pcr3 | 0.807*** | 77.51 | 0.651 | 0.816*** | 99.75 | 0.666 | 0.786*** | 51.08 | 0.618 |
| pcr4 | 0.800*** | 86.17 | 0.640 | 0.821*** | 73.94 | 0.674 | 0.863*** | 75.05 | 0.745 |
| pcr5 | 0.822*** | 123.78 | 0.676 | 0.824*** | 93.22 | 0.679 | 0.839*** | 108.22 | 0.704 |
| pcr6 | 0.795*** | 121.42 | 0.632 | 0.819*** | 79.74 | 0.671 | 0.752*** | 76.29 | 0.566 |
| Model Fit | $\chi^2(df)$=341(106);<br>RMSEA=.011 (.010 – .013),<br>TLI=.966, CFI=.977; | | | $\chi^2(df)$=326(106);<br>RMSEA=.011 (.009 – .012),<br>TLI=.957, CFI=.970; | | | $\chi^2(df)$=329(106);<br>RMSEA=.011 (.009 – .012),<br>TLI=.946, CFI=.963; | | |

**Confirmatory Factor Analyses** We conduct two additional CFA analyses, one for each year. The lower part of Table 5.10 reports overall fit of the CFA analysis. The approximate fit indexes for the reduced models exceed the thresholds for good fit discussed in Section 5.2.1. The 90 % CI for the RMSEA index (noted in brackets) further supports the good fit.

The upper part of Table 5.10 reports standardized factor loadings, significance levels and standard errors in brackets, Z-Scores and $R^2$ values for each indicator. We include results for 2012 for comparison. All measurement models meet the criteria proposed by Fornell and Larcker (1981). The standardized factor loadings for all indicators are $> 0.5$ and significant, meeting the first criterion. The second and third criteria are reported in Table 5.11. All latent variables meet the second criterion (CR $> 0.8$). Overall, PCR indicators perform better than EXP. The third criterion (AVE $> 0.5$) is met by all latent variables, except for EXP in 2013, which is only 0.47. Due to the secondary nature of our analyses and the satisfied threshold criteria in 2012 and 2014, we acknowledge this negligible deviation and consider it close enough to the target value of 0.5 to be deemed acceptable.

We finally check for discriminant validity to ensure that different constructs do not measure the same phenomenon. Since the square root of AVE (noted in bold font on the diagonal in Table 5.11) is greater than the between construct correlations (Henseler et al., 2009), we can confirm discriminant validity for all constructs in all years. Overall, correlations between constructs (lower-left of the diagonal in Table 5.11) are small.

**Table 5.11:** Longitudinal replication: reliability and discriminant validity

| **Constructs** | | **Scores** | | **Correlations (lower-left)** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Year | Name | CR | AVE | EXP | PCR | avS | avB | avN | avU | pbA | pbP | pbS |
| '12 | EXP | 0.82 | 0.49 | **.700** | (.021) | (.045) | (.033) | (.012) | (.023) | (.024) | (.024) | (.036) |
| | PCR | 0.92 | 0.66 | .263$^{***}$ | **.812** | (.019) | (.017) | (.028) | (.020) | (.029) | (.015) | (.029) |
| | avS | - | - | .061 | .170$^{***}$ | - | (.035) | (.032) | (.053) | (.025) | (.021) | (.028) |
| | avB | - | - | .170$^{***}$ | .127$^{***}$ | .577$^{***}$ | - | (.050) | (.044) | (.027) | (.017) | (.033) |
| | avN | - | - | .145$^{***}$ | .092$^{***}$ | .305$^{***}$ | .298$^{***}$ | - | (.047) | (.046) | (.046) | (.038) |
| | avU | - | - | .001 | .132$^{***}$ | .087 | .096$^{*}$ | .327$^{***}$ | - | (.046) | (.041) | (.041) |
| | pbA | - | - | .317$^{***}$ | .066$^{*}$ | .011 | .073$^{**}$ | .450$^{***}$ | .203$^{***}$ | - | (.025) | (.043) |
| | pbP | - | - | .174$^{***}$ | .047$^{**}$ | $-.027$ | .010 | .414$^{***}$ | .329$^{***}$ | .557$^{***}$ | - | (.033) |
| | pbS | - | - | .075$^{*}$ | .006 | $-.026$ | $-.038$ | .453$^{***}$ | .394$^{***}$ | .427$^{***}$ | .532$^{***}$ | - |
| '13 | EXP | 0.80 | 0.45 | **.671** | (.020) | (.041) | (.063) | (.023) | (.023) | (.031) | (.030) | (.019) |
| | PCR | 0.93 | 0.68 | .228$^{***}$ | **.825** | (.016) | (.023) | (.028) | (.015) | (.017) | (.017) | (.026) |
| | avS | - | - | $-.013$ | .177$^{***}$ | - | (.049) | (.049) | (.036) | (.023) | (.030) | (.045) |
| | avB | - | - | .146$^{*}$ | .195$^{***}$ | .578$^{***}$ | - | (.046) | (.022) | (.023) | (.026) | (.050) |
| | avN | - | - | .243$^{***}$ | .103$^{***}$ | .280$^{***}$ | .294$^{***}$ | - | (.017) | (.041) | (.033) | (.033) |
| | avU | - | - | $-.008$ | .114$^{***}$ | .131$^{***}$ | .059$^{**}$ | .324$^{***}$ | - | (.032) | (.019) | (.028) |
| | pbA | - | - | .384$^{***}$ | .087$^{***}$ | .041$^{\dagger}$ | .069$^{**}$ | .459$^{***}$ | .201$^{***}$ | - | (.029) | (.018) |
| | pbP | - | - | .245$^{***}$ | .085$^{***}$ | $-.019$ | $-.017$ | .350$^{***}$ | .318$^{***}$ | .549$^{***}$ | - | (.027) |
| | pbS | - | - | .037$^{\dagger}$ | .057$^{*}$ | .019 | $-.046$ | .459$^{***}$ | .446$^{***}$ | .432$^{***}$ | .534$^{***}$ | - |
| '14 | EXP | 0.83 | 0.50 | **.707** | (.035) | (.032) | (.029) | (.029) | (.013) | (.028) | (.020) | (.034) |
| | PCR | 0.92 | 0.66 | .246$^{***}$ | **.812** | (.025) | (.022) | (.031) | (.011) | (.033) | (.031) | (.030) |
| | avS | - | - | .049 | .133$^{***}$ | - | (.023) | (.040) | (.034) | (.052) | (.033) | (.042) |
| | avB | - | - | .019 | .133$^{***}$ | .558$^{***}$ | - | (.039) | (.021) | (.026) | (.032) | (.024) |
| | avN | - | - | .160$^{***}$ | .015 | .346$^{***}$ | .283$^{***}$ | - | (.021) | (.028) | (.029) | (.042) |
| | avU | - | - | .031$^{*}$ | .110$^{***}$ | .221$^{***}$ | .208$^{***}$ | .307$^{***}$ | - | (.022) | (.018) | (.024) |
| | pbA | - | - | .326$^{***}$ | .024 | .098$^{\dagger}$ | .055$^{*}$ | .391$^{***}$ | .175$^{***}$ | - | (.029) | (.027) |
| | pbP | - | - | .186$^{***}$ | .016 | .100$^{**}$ | .068$^{*}$ | .396$^{***}$ | .220$^{***}$ | .508$^{***}$ | - | (.029) |
| | pbS | - | - | .074$^{*}$ | $-.003$ | .154$^{***}$ | .092$^{***}$ | .455$^{***}$ | .356$^{***}$ | .393$^{***}$ | .456$^{***}$ | - |

Diagonal: $\sqrt{\text{AVE}}$; Upper-right: SE's of the correlations. Cybercrime Experience (EXP), Perceived Cybercrime Risk (PCR), AV: Online shopping (avS), Online banking (avB), Online social networking (avN), PB: Anti-virus (pbA), Different passwords (pbP), Changed security settings (pbS).

### 5.4.4 Structural Models

After validating the replicated measurement models, we test structural models for the different forms of avoidance intention and protection behavior. We estimate a total of 21 individual models, one for each year and each form of avoidance or protection behavior.

**Avoidance Intention** The right part of Table 5.12 reports approximate fit indexes for each model. The left part reports standardized path coefficients and their standard errors (in brackets). We find that the 2013 wave performs worst in terms of overall fit. By contrast, the structural models for 2014 perform best. A comparison of different forms of avoidance shows that online shopping (avS) models fit the data best and models for online social networking avoidance (avN) fit worst. However, the differences between years and forms of avoidance are small and the fit indexes indicate an acceptable fit for all three models and in all three years.

To evaluate the robustness of the model to temporal changes, we look at changes of individual effects over time. We report direct (EXP→AV) and indirect effects (EXP$\xrightarrow{\text{PCR}}$AV) for the impact of cybercrime experience on avoidance of online services. While effect sizes are rather small, we are able to check the persistence of signs and significance of path coefficients.

**Table 5.12:** Longitudinal replication: structural models for *Avoidance Intention*

| | **Path coefficients (SEs)** | | | | **Model fit** | | | |
|---|---|---|---|---|---|---|---|---|
| Year | EXP→PCR | PCR→AV | EXP$\xrightarrow{\text{PCR}}$AV | EXP→AV | $\chi^2$ (*df*) | RMSEA (90 CI) | CFI | TLI |
| Online shopping (avS) | | | | | | | | |
| 2012 | 0.258 *** <br> (0.020) | 0.167 *** <br> (0.020) | 0.043 *** <br> (0.006) | 0.020 <br> (0.044) | 139 (51) | .010 (.008–.012) | .993 | .991 |
| 2013 | 0.223 *** <br> (0.020) | 0.189 *** <br> (0.016) | 0.042 *** <br> (0.007) | −0.051 <br> (0.039) | 145 (51) | .010 (.008–.012) | .989 | .986 |
| 2014 | 0.243 *** <br> (0.034) | 0.133 *** <br> (0.026) | 0.032 *** <br> (0.007) | 0.017 <br> (0.031) | 92 (51) | .007 (.004–.009) | .994 | .993 |
| Online banking (avB) | | | | | | | | |
| 2012 | 0.258 *** <br> (0.020) | 0.093 *** <br> (0.023) | 0.024 *** <br> (0.005) | 0.142 *** <br> (0.034) | 143 (51) | .010 (.008–.012) | .993 | .990 |
| 2013 | 0.223 *** <br> (0.020) | 0.173 *** <br> (0.036) | 0.039 *** <br> (0.008) | 0.108 <br> (0.067) | 159 (51) | .011 (.009–.013) | .987 | .983 |
| 2014 | 0.243 *** <br> (0.034) | 0.140 *** <br> (0.023) | 0.034 *** <br> (0.0070) | −0.011 <br> (0.026) | 98 (51) | .007 (.005–.009) | .994 | .992 |
| Online social networking (avN) | | | | | | | | |
| 2012 | 0.260 *** <br> (0.020) | 0.061 * <br> (0.027) | 0.021 * <br> (0.010) | 0.121 *** <br> (0.011) | 202 (51) | .013 (.011–.015) | .988 | .985 |
| 2013 | 0.225 *** <br> (0.020) | 0.054 <br> (0.033) | 0.012 <br> (0.008) | 0.226 *** <br> (0.030) | 169 (51) | .011 (.009–.013) | .986 | .982 |
| 2014 | 0.244 *** <br> (0.035) | −0.022 <br> (0.033) | −0.005 <br> (0.008) | 0.161 *** <br> (0.030) | 127 (51) | .009 (.007–.011) | .990 | .987 |
| Unknown websites (avU) | | | | | | | | |
| 2012 | 0.258 *** <br> (0.020) | 0.145 *** <br> (0.025) | 0.037 *** <br> (0.008) | −0.040 <br> (0.027) | 140 (51) | .010 (.008–.012) | .993 | .991 |
| 2013 | 0.223 *** <br> (0.020) | 0.125 *** <br> (0.015) | 0.028 *** <br> (0.008) | −0.042 <br> (0.023) | 164 (51) | .011 (.009–.013) | .987 | .984 |
| 2014 | 0.244 *** <br> (0.034) | 0.116 *** <br> (0.014) | 0.028 *** <br> (0.006) | −0.001 <br> (0.017) | 126 (51) | .009 (.007–.011) | .990 | .987 |

Cybercrime Experience (EXP), Perceived Cybercrime Risk (PCR), Avoidance Intention (AV).

We confirm **H1**: *Cybercrime Experience* has a significant positive effect on *Perceived Cybercrime Risk* in all years. The largest effects are found in 2012 ($\beta = 0.260$, $p < 0.001$) but they remain on a high level in the following years. We cannot see any impact following the swap in the order of the question batteries for EXP and PCR in 2014. While this supports the robustness of our findings, there remains a risk that the large effects are partially caused by questionnaire effects, in particular same question bias (Tourangeau and Bradburn, 2010).

We also find further support for **H2**: *Perceived Cybercrime Risk* has a significant and positive effect on avoidance intention of online shopping, online banking, and unknown websites in all three years. For avoidance intention of online social networks, we only find a small effect ($\beta = 0.061$, p < 0.05) for 2012, which disappears (is not significant) in the following years.

We can partially confirm **H3**: *Cybercrime Experience* has a positive indirect impact on the *Avoidance Intention* of online shopping, online banking, and unknown websites in all three years. The effects are fully mediated by PCR in the case of online shopping and unknown websites. In the case of online banking, we only find a partial mediation for 2012 because the direct effect is also significant $\beta = 0.142$, $p < 0.001$. The subsequent years also support the full mediation hypothesis. The mediation hypothesis cannot be confirmed for avoidance of online social networking.

**Protection Behavior** Table 5.13 reports the SEM results for *Protection Behavior* (PB). The overall fit of the models is slightly worse compared to the avoidance models. The worst fit indexes are observed in 2013. Among the different types of protection behavior, installing anti-virus software (pbA) fit worst in all years.

**Table 5.13:** Longitudinal replication: structural models for *Protection Behavior*

| | **Path coefficients (SEs)** | | | | **Model fit** | | | |
|---|---|---|---|---|---|---|---|---|
| Year | EXP→PCR | PCR→PB | $\text{EXP}\xrightarrow{\text{PCR}}\text{PB}$ | EXP→PB | $\chi^2$ (*df*) | RMSEA (90 CI) | CFI | TLI |
| Installing anti-virus software (pbA) | | | | | | | | |
| 2012 | 0.258$^{***}$<br>(0.020) | −0.010<br>(0.027) | −0.003<br>(0.007) | 0.063<br>(0.035) | 194(51) | .013(.011-.014) | .988 | .985 |
| 2013 | 0.223$^{***}$<br>(0.020) | 0.057$^{*}$<br>(0.027) | 0.013$^{*}$<br>(0.006) | 0.005<br>(0.019) | 209(51) | .013(.011-.015) | .982 | .976 |
| 2014 | 0.244$^{***}$<br>(0.034) | −0.019<br>(0.031) | −0.005<br>(0.008) | 0.069$^{*}$<br>(0.034) | 141(51) | .010(.008-.012) | .988 | .984 |
| Using different passwords (pbP) | | | | | | | | |
| 2012 | 0.259$^{***}$<br>(0.020) | 0.006<br>(0.016) | 0.002<br>(0.004) | 0.161$^{***}$<br>(0.026) | 166(51) | .011(.009-.013) | .991 | .988 |
| 2013 | 0.227$^{***}$<br>(0.020) | 0.034<br>(0.021) | 0.008<br>(0.005) | 0.228$^{***}$<br>(0.034) | 188(51) | .012(.010-.014) | .984 | .979 |
| 2014 | 0.246$^{***}$<br>(0.035) | −0.028<br>(0.037) | −0.007<br>(0.009) | 0.187$^{***}$<br>(0.026) | 125(51) | .009(.007-.011) | .990 | .987 |
| Changing security settings (pbS) | | | | | | | | |
| 2012 | 0.262$^{***}$<br>(0.021) | −0.016<br>(0.031) | −0.004<br>(0.008) | 0.317$^{***}$<br>(0.028) | 191(51) | .012(.011-.014) | .989 | .986 |
| 2013 | 0.228$^{***}$<br>(0.020) | −0.002<br>(0.019) | 0.000<br>(0.004) | 0.391$^{***}$<br>(0.032) | 183(51) | .012(.010-.014) | .985 | .981 |
| 2014 | 0.246$^{***}$<br>(0.035) | −0.059<br>(0.041) | −0.014<br>(0.011) | 0.344$^{***}$<br>(0.033) | 102(51) | .008(.006-.010) | .992 | .990 |

Cybercrime Experience (EXP), Perceived Cybercrime Risk (PCR), Protection Behavior (PB).

Concerning structural links, the data also supports **H1** for all PB models, with very similar effect sizes for EXP on PCR in all three years. **H4** is not supported by the data, since the impact of PCR on PB is not significant. We also have to reject the full mediation hypothesis regarding the impact of EXP on PB (**H5**), since indirect effects are not significant in any model. While we find marginal effects for **H4** and **H5** in 2013, we neglect them due to the bad reliability of the measurement model in this year. As for the original model in 2012, we find a positive direct effect of EXP on PB, which is highly significant for using different passwords (pbP) and changing security settings (pbS) in all years. The path coefficients for pbS consistently exceed the coefficients of pbP. pbA is not influenced by EXP nor by PCR, in any year.

In summary, *Protection Behavior* is rather influenced by *Cybercrime Experience*, whereas *Avoidance Intention* is driven by *Perceived Cybercrime Risk*. The improved measurement model for 2014 further underlines the robustness of these results.

### 5.4.5 Trend Analysis

To test for time-dependent changes in the structural links, we compare effect sizes for each hypothesis and each form of avoidance and protection behavior across all models (12, 13, 14, and the improved measurement model 14'). We calculate 95 % CIs for the standardized path coefficients and visually analyze pairwise overlaps in Figure 5.4. If CIs do not overlap, we can conjecture that the effects have changed significantly. Since the effects for avN are only marginally significant in 2012 and insignificant in the other models, we neglect it in the trend analysis. Each subfigure in Figure 5.4 reports the results for one hypothesis (in rows) and one form of avoidance or protection (in columns). Each dot represents an individual path coefficient in the respective year and the black line delineates the corresponding CI. The dashed green lines depict the CI of the baseline model in 2012.

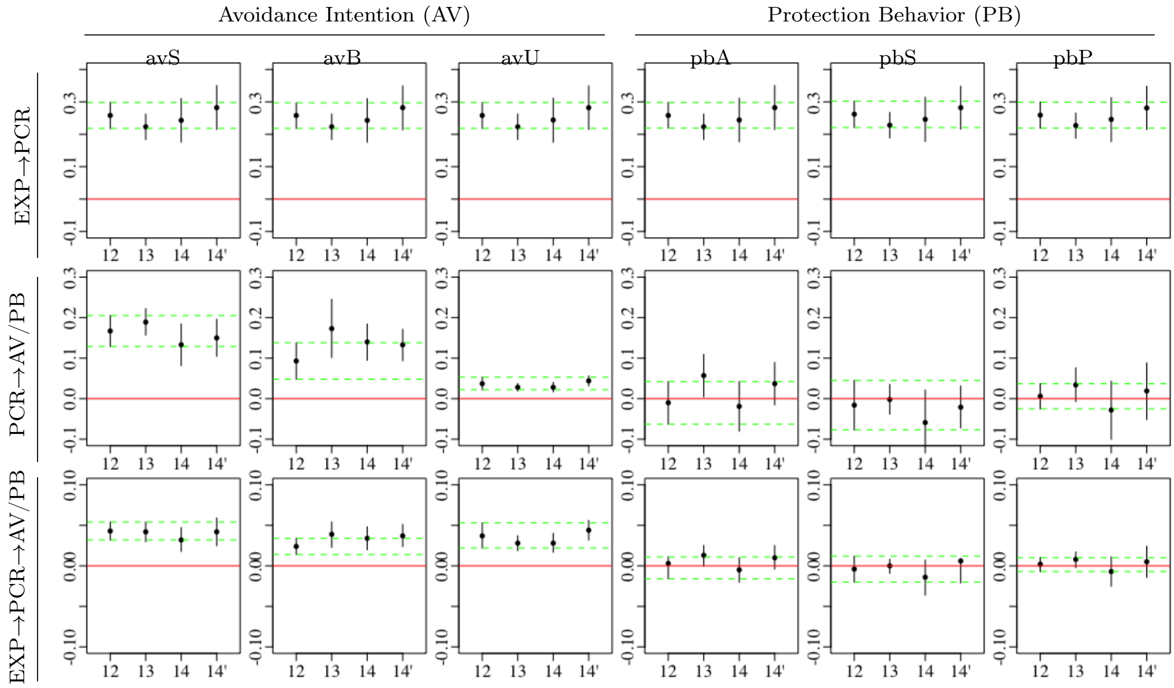


**Figure 5.4:** Trends in structural links for the core hypotheses (rows) over the four models (x-axis in each tile); effect size with 95 % CI (y-axis in each tile), reference CI of the 2012 model (dashed green line in each tile)

Overall, the largest effect sizes are observed in the top row for the impact of EXP on PCR (**H1**). The tiles in the middle row demonstrate that the impact of PCR is significant for AV (**H2**), but insignificant for PB (**H4**). The bottom row represents the indirect impact of EXP on AV (**H3**) and PB (**H5**). Overall, these effects show a pattern similar to the direct effects of PCR on both constructs, but with smaller effect sizes. We can confirm (**H3**), but have to reject (**H5**). Note that even though the effects are very small, they are still highly significant for all avoidance models in the left part of Figure 5.4.

Comparing the CIs between the different models, we cannot identify significantly different effect sizes. While we only visualize the CI of the baseline model (the dashed green line), all other CIs overlap in a pairwise comparison. We conclude that the structural links are stable across the different models and that the impacts of cybercrime exposure on online service avoidance and protection behavior by EU Internet users are persistent over time.

## 5.5 Discussion

The large set of results raises several points for discussion. First, Section 5.5.1 summarizes the results, before we discuss their robustness and limitations in Section 5.5.2. Sections 5.5.3 and 5.5.4 derive theoretical and practical implications.

### 5.5.1 Results

This chapter presents a theoretically derived model to explain the impact of exposure to consumer-facing cybercrime on online service avoidance and protection behavior. We provide empirical support for the model and its multiple variants using a SEM analysis based on three representative pan-European samples collected from 2012 to 2014.

Our empirical results confirm three out of five tested hypotheses regarding the impact of cybercrime experience and perceived cybercrime risk on the avoidance of online shopping, online banking, and unknown websites (**H1**, **H2**, **H3**). In short, cybercrime experience leads to perceived cybercrime risk, which ultimately leads to either of the three forms of avoidance intention. The effects are persistent over time and for an improved measurement model (14'). Avoidance of online social networks is only marginally influenced by perceived cybercrime risk in 2012, but this effect becomes insignificant in the remaining models. Therefore, we need to reject **H2** and **H3** for this form of avoidance. We also cannot confirm our hypotheses on protection behavior. Perceived cybercrime risk has no significant impact on protection behavior (**H5**) and impacts of cybercrime experience are not mediated by perceived cybercrime risk (**H4**). However, cybercrime experience has a direct impact on two forms of protection behavior: changing security settings and using different passwords.

The positive influence of media awareness on perceived risk, avoidance intention, and protection behavior (**H6**, **H7**, **H8**) is suggested by related research, but not empirically validated because the construct could not be reliably measured. The moderation by user confidence is partly confirmed. Structural links are invariant (**H9**), but latent variable means for perceived cybercrime risk and avoidance of online banking and shopping are significantly higher for unconfident users (**H10**).

### 5.5.2 Robustness and Limitations

A secondary analysis of a complex data requires special consideration regarding the robustness of the results. We use reflective multi-item measures for the perceived risk construct, which is originally identified as multi-dimensional (Featherman and Pavlou, 2003), and interpret cybercrime experience as a reflective construct, even though it might be formative. Since goodness-of-fit indexes support our measurement models, we believe that the research model can explain the EB data. The replication over time and the measurement with an improved set of indicators provides further confidence. Still, the good reliability and validity scores of perceived cybercrime risk and the acceptable scores of cybercrime experience should be confirmed with validated measurement scales in future research.

We find high heterogeneity in the data set, which is likely caused by variation between countries and interviews conducted in different languages. Our analysis accounts for between-country variation using fixed-effects in the model, but we do not study the impact of cultural and national characteristics in-depth, e.g., with a multi-level design. The heterogeneity in combination with short (ordinal) answer scales results in low correlations between indicators and constructs. Moreover, a rather vague question wording, common for large scale population surveys, can only provide tendencies of avoidance intention and protection behavior, but does not record precisely defined behavior. Despite all these limitations, path coefficients for avoidance of online shopping, online banking, and unknown websites as well as changing security settings and using different passwords are highly significant in the original model and persistent in all three waves of the EB.

Another limitation of a secondary data analysis is the inability to influence the instrument design. Our research model is parsimonious in the sense that it focuses on perceived cybercrime risk as the single factor influencing avoidance and protection. It neglects other factors commonly used in adoption theories, such as *Perceived Usefulness* and *Perceived Ease-of-use*. These factors likely have a positive effect on adoption, hence a negative effect on avoidance of online services. It also neglects factors of PMT, such as *Perceived Response Efficacy* or *Perceived Self Efficacy*, which influence protection behavior. Unfortunately, we could not include any of them in our population-wide analyses because they are not measured in the EB surveys.

In summary, our results are limited but provide a step towards understanding cybercrime impact and building principled theory in the context of individual security behavior. By testing our research model using secondary data of a complex multi-national sample, our study overcomes limitations of similar work, most importantly, non-representative sampling. Using the EB surveys, our results are based on three enormous data sets, which include a total of more than 57 000 responses of individual Internet users, collected with industry standard sampling and interviewing methods. Specialized software packages and robust estimation methods prove to be powerful in solving statistical issues for complex samples with categorical indicators and ensure the validity and reliability of our results, allowing for theoretical and practical implications.

### 5.5.3 Theoretical Implications

**Relevance of Perceived Risk for Online Service Avoidance** We provide empirical evidence that the perceived risk-extended TAM (Featherman and Pavlou, 2003) can be applied to explain online service avoidance from a cybercrime perspective at the societal level. By adding a perceived cybercrime risk construct, our model reinforces earlier suggestions (e. g., Chen and Zahedi, 2016) to consider negative factors when studying technology acceptance and security behavior. The SEM results confirm the positive influence of perceived risk of cybercrime on avoidance intention of online banking, online shopping, and unknown websites for EU Internet users.

Perceived risk of cybercrime has the strongest impact on the avoidance of online shopping. Pavlou (2003) proposes that online shopping includes behavioral uncertainty due to dubious merchants, in addition to the environmental uncertainty of the Internet. The higher level of uncertainty and the low switching costs reduce customer loyalty in online shopping, thus making it easier to avoid it. By contrast, switching costs are higher with online banking and customers usually interact with a single bank. Accordingly, the perceived risk is largely based on environmental uncertainty once trust in the online banking provider is established. The importance of trust in online banking adoption (even exceeding traditional TAM factors) has also been found in other studies (e. g., Montazemi and Saremi, 2013). This may explain the lesser effect of perceived risk of cybercrime on the avoidance of online banking. Looking at the antecedents of cybercrime risk, we find a positive effect of prior cybercrime experience on the avoidance of online services, which is mediated by perceived cybercrime risk for online shopping, online banking, and unknown websites in all years.

**Contradiction of Avoidance and Adoption Trends** The persistence of the avoidance effects suggests revisiting the contradictions between avoidance behavior and marginal trends in online service adoption, discussed in Subsection 5.4.2. Media coverage is a potential explanation for the simultaneous decrease in reported cybercrime experience and increase in perceived cybercrime risk. It has been shown that the media is a powerful tool in forming public opinion and risk perception, particularly regarding crimes (Wahlberg and Sjoberg, 2000; Jackson, 2011). While media awareness was part of the original research model, it could not be measured reliably with the questions available in the EB surveys. Moreover, the collection of data on media reception has been discontinued in 2013. Thus, we can only speculate about the existence of such an effect. The simultaneous persistence in avoidance and the growing adoption of online services may be explained by different forms of avoidance behavior, which are not entirely observable with our general measurement instrument. Liang and Xue (2009) state that avoidance behavior comprises various actions to evade an undesired end state, in our case victimization. Consumers may adopt different coping mechanisms and avoidance strategies in order to protect themselves against cyber risk. A clear conceptualization of online service avoidance, similar to the work by Recker (2016) for IS discontinuance, is necessary to fully understand this type of security behavior. Our extension of the original research model already makes a first contribution by showing that avoidance of unknown websites is one possible coping mechanism.

**Avoidance Intention of Online Social Networking** The use of online social networking (OSN) is not affected by cybercrime, as measured in the EB. We find the smallest effect (significant at $p < 0.05$) in 2012 which disappears entirely in the following years. The small influence may be due to measuring OSN avoidance with a proxy and general shortcomings of the secondary analysis. However, we explain this result by the context of the EB instrument, which focuses on security-related issues and types of crime. It largely neglects privacy-related issues, which arguably play a more significant role for social networking (Krasnova et al., 2009). The results highlight the inherently different characteristics of social networking in comparison to online banking and online shopping. While the latter two are fairly standardized routine activities with a direct link to financial transactions, social networking is a hedonic service used for personal pleasure, which requires users to share information and interact with others (Turel, 2015). Consequently, other types of cybercrime, for example, cyber-bullying and cyber-stalking, or concerns of data misuse by OSN providers are better indicators for perceived risk in online social networks (Krasnova et al., 2009). The fact that the avoidance models for online social networking fit the data worst in all waves, supports this argument and highlights the need for more appropriate models.

**Moderation of User Confidence** The moderation analysis shows that the strength of the effects in our model is not driven by unobserved variance in user's confidence during online transactions. Differences are found in factor means, as confident Internet users perceive significantly less cybercrime risk and are less likely to change their online behavior even though they report more cybercrime experience. The higher level of existing experience can be explained by different usage patterns. Confident Internet users surf more frequently, which increases their chance of becoming victimized but also their ability to identify cybercriminal attacks. Unconfident users, by contrast, perceive more cybercrime risk and demonstrate a higher intention to avoid online banking or shopping. Even though this result was expected, it might be puzzling in combination with the fact that unconfident users reported less cybercrime experience. How can a lower level of cybercrime experience lead to more perceived risk if the effects are the same? We believe that this discrepancy can be explained by missing factors in the model, i. e., media awareness or other social influences. If, as hypothesized and shown in the literature review, media awareness increases perceived cybercrime risk and the effect is stronger for unconfident Internet users, it can explain the higher factor means. Our data is too noisy to confirm this finding empirically and we recommend further research in this direction.

**Summary** Taking a step back, the prevalence of cybercrime and the persistence of aggregate effects emphasize the importance of studying individual security behavior at the societal level. We can summarize three theoretical implications for IS research on security behavior. First, IS scholars should shift the focus of avoidance models from customers avoiding a particular vendor to the population of all Internet users avoiding a technology in general. Second, this shift requires dedicated models and a clearer conceptualization of online service avoidance as a behavioral construct. Third, primary data at the societal level is needed to evaluate these models.

### 5.5.4 Practical Implications

Given an analysis at the societal level, practical implications are mainly directed towards policy makers. However, they also provide valuable information for online service providers. We show that the reduction of perceived risk of cybercrime facilitates increased online service use. Furthermore, Internet users tend to visit well-known and trusted websites and confident users generally perceive less risk and are more likely to use online services. These findings point to two sets of actions to facilitate online service use and regulate the market structure for B2C e-commerce.

**Facilitate Online Service Use** To increase Internet users' confidence in dealing with cybercrime risk, their digital literary needs to be improved. Public awareness about cybercriminal threats should be ensured, but, more importantly, Internet users need to be educated to make informed decisions to deal with these threats. Therefore, policy makers should establish trusted sources of authoritative advice regarding cybercrime and protective behavior, for example, in the form of official websites. Positive examples should be used on these websites to encourage secure behavior, as scary messages may increase perceived risk and lead to avoidance rather than secure use. Service providers should implement clear and easy-to-use services to support the confidence building process.

Another obvious action to reduce perceived risk is to limit victimization by continuously improving defense measures and intensifying law enforcement. All actions need to be credibly communicated to assure that the risk reduction in online transactions is correctly perceived by large parts of the population. Policy makers can create incentives such as trustmarks, standards, or security certificates, to foster security investments and encourage clear communication. Service providers can offer financial compensation to victims or consumer satisfaction guarantees to reduce the perceived risk.

**Market Structure of B2C E-commerce** Our new form of avoidance shows that reducing perceived risk may not always be the rational choice for all providers. We find that concerned consumers tend to visit websites they already know and trust. Such dynamics foster existing network economics which favor larger providers (Shapiro and Varian, 1998, p. 173) because a certain (perceived) level of cybercrime limits consumer choices and drives them towards well-known, trusted online brands. Put differently, negative consequences of ICT at the societal level may lead to positive outcomes for some market participants. In the most extreme scenario, cybercrime catalyzes a Matthew effect (Merton, 1968) in B2C e-commerce, resulting in very few large providers. This subtle interaction is relevant for business strategies and, more importantly, economic studies of online market structures aiming to inform policy makers, since beneficiaries of cybercrime may have few incentives to fight it alone or in joint efforts.

# Chapter 6

# Case Study: Credit Card Fraud

Internet payment systems are a basic requirement of many online services by enabling fast and convenient online payments. Despite the availability of several electronic alternatives, credit cards remain a widely used method (Vasiu and Vasiu, 2015). The European Central Bank reports that credit card transfers grew substantially between 2000 and 2012 with an annual rate of more than 5 % (ECB, 2014). Credit cards yield various individual and economic benefits, including convenience, reliability, and limited consumer liability in cases of fraudulent use (Chakravorti, 2003). However, the prevalence of fraud may lead individual users to avoid online payments or drives them towards other electronic payment systems (EPS), such as PayPal or Bitcoin, for payments on the Internet.

We can broadly differentiate two types of credit card transactions: *card present*, which is typically the case for point-of-sale transactions in a physical store, or *card not present* (CNP), necessary for transactions via the Internet. The ongoing proliferation of online shopping and credit cards as a popular payment method make CNP transactions an attractive target. Criminals obtain credit card credentials by breaking security measures of merchants or directly from the victim using phishing emails. Credentials can be monetized through various techniques, typically including illegal purchases. We call this type of cybercrime *credit card fraud* in this chapter, as the term is typically used by banks and credit card companies. Note that we refer to the same crime as *identity theft with regard to credit cards* in Chapter 4.

The prevalence of credit card fraud can be observed at many stages of the criminal value chain. Large data breaches hit companies around the globe (Edwards et al., 2016; Wheatley et al., 2016), often including breaches of credit card information. In 2014, for example, credit card information was stolen at two large US retailers. 40 m customers lost their data at Target (Krebs, 2014b) and 56 m at Home Depot (Krebs, 2014a). The trading of such information in underground online markets is continuously observed by researchers (e. g. Franklin et al., 2007; Thomas et al., 2013). Moreover, victimization surveys report that credit card fraud is a common criminal offense in the EU (e. g. EB82.2, 2015) and the US (Harrell, 2015). Our results in Section 4.1.3 confirm that Germany is among the highly affected countries in Europe, with more than 4 % of the Internet users reporting an incident between 2010 and 2015.

The prevalence of credit card fraud has motivated research and development of computer-assisted detection and prevention systems, which help credit card processors to contain fraud (West and Bhattacharya, 2016). Indeed, those systems are able to identify and block many fraudulent CNP transactions, often before they are processed. Nevertheless, the credit card usually has to be replaced, once credentials are compromised. Therefore, fraud incidents raise inconvenience to costumers and costs to the issuer, even if fraudulent payments are not processed. Considerably little research concerns the measurement of these costs. A report by the Smart Card Alliance tabulates all types of costs against the affected stakeholders, which comprise *acquirers* who process credit card payments for the *merchants*, *issuers* who process payments for *card holders*, and the *payment brands* (Smart Card Alliance, 2015). The main “cost” for the card holder is the inconvenience of the fraud dispute handling and the replacement of the compromised credit card. Tangible costs for the issuer include the operation of an anti-fraud department, expenses for customer communication, and the replacement of compromised cards. However, they also include less tangible, indirect costs, if customers avoid the replacement cards. We show in Chapter 5 that cybercrime experience and perceived risk consistently lead to the avoidance of online shopping, online banking, and untrusted websites. In the context of credit card payments avoidance may materialize in a fewer transactions, smaller revenues, or in the worst case for the issuer, complete customer drop-outs.

Some empirical evidence for such behavior has been collected in cross-sectional surveys. A survey among 2 500 US consumers reports that 8 % of Target and 8 % of Home Depot customers stopped using their credit cards after the large data breaches at both retailers became public (Stanton, 2015). The majority of consumers turned to cash payments (Home Depot: 48 %, Target: 62 %). Others stated that they switched to another credit card (Home Depot: 17 %, Target: 11 %). The Aite Group LLC, an industry research and advisory firm, conducted three international surveys concerning consumer reaction to credit card fraud in general (Inscoe, 2012, 2014; Knieff, 2016). They find that about half of the credit card owners surveyed in Germany report to use other payment methods after experiencing fraud, at least in some situations. In 2014, 22 % reported that they do not use the replacement card (36 % in 2012). In 2016, still 25 % report to use it less. Several explanations exist why customers avoid using the replacement card, including a loss of confidence in the security of credit card payments, the inconvenience of changing to a new card, or the intermediate change to other payment methods.

Only very few scholars try to understand avoidance behavior in the payment choice context. Somanchi and Telang (2017) study the impact of fraudulent transactions on the probability that customers terminate relationships with a large US bank after a fraud incident. They find that the probability to terminate contracts increases significantly for fraud victims. The increase is between 1 and 3 percentage points if the incident cannot be attributed to a perpetrator. Using an analytic approach, Graves et al. (2014) study the replacement decision for credit cards which have been exposed in data breaches but not yet compromised. They suggest that issuers have to decide carefully, as progressive replacement of exposed cards may be more costly than accepting the risk that these cards may lead to losses in the future. Unfortunately, they can only speculate about indirect costs of avoidance.

Surveys and academic studies provide interesting insights into victim reactions, but many important aspects of behavioral change and factors which influence this change are missing. The broad cross-sectional surveys (e. g. EB82.2, 2015; Harrell, 2015) reach a large population, but do not report reactions to fraud incidents. The Aite Group relies on self-reported behavior for reactions and only collects small samples. Existing academic studies lack empirical data of individual behavior (Graves et al., 2014) or have a different focus (Somanchi and Telang, 2017).

We fill many of these research gaps and contribute to behavioral research in the context of credit card payments, by answering the following two research questions:

1. Does credit card fraud lead to avoidance of credit card payments after the incident ?

2. What factors explain this avoidance behavior of the victims ?

In order to answer the research questions, we develop a research design which allows us to perform an intervention study in the form of a natural experiment. We collaborate with PLUSCARD a

German payment card processor to recruit a total of 93 victims of credit card fraud in Germany. For every victim, we record weekly aggregates of credit card transactions for a period of three months before and after the incident. Furthermore, we collect general attitudes towards the credit card as a payment method as well as perceptions and reactions related to the fraud incident, using standardized telephone interviews. We combine the transaction data (outcome variable) with self-reported attitudes (predictors) in a linear mixed-effects model (LMM). This allows us to identify a total of five different factors which have a significant impact on credit card use after the fraud incident. We find that security related attitudes have a negative impact on credit card use, but that good communication with the victims during the fraud dispute handling can compensate at least for parts of the negative effect. Our approach is limited in that we do not have a control group and a rather small sample size. However, we have the rare opportunity to jointly analyze self-reported attitudes and actual behavior in a clearly defined context and derive managerial implications for the fraud dispute handling as done by credit card issuers.

Accordingly, this chapter supplements the broad perspective on the societal impact of cybercrime with an in-depth case study of credit card fraud and its impact on the victims' behavior. The focus on a specific scenario allows us to overcome many limitations of large scale survey research. Most importantly, we identify victims objectively, i. e., do not depend on self-reported victimization, and analyze reactions to cybercrime with actual behavioral data. In addition, the case study allows us to cross-check previous findings on costs and reactions associated with cybercrime in the clearly defined context of credit card payments and credit card fraud.

This chapter is structured as follows. Section 6.1 develops the design of the intervention study. Section 6.2 presents descriptive statistics of the sample, interview results, and aggregated transaction data. Section 6.3 integrates self-reported and actual behavior in the mixed model analysis. Finally, Section 6.4 closes with a discussion of limitations, implications, and future work.

## 6.1 Research Design

This section develops our research design and documents the data collection. We start with a survey of related work in Section 6.1.1. Then, Section 6.1.2 presents the research design and Section 6.1.3 describes how the data collection is integrated into the fraud dispute handling. Section 6.1.4 summarizes the fieldwork.

### 6.1.1 Impact of Fraud on the Avoidance of Payment Methods

We show in Chapter 5 that cybercrime experience and perceived risk consistently lead to the avoidance of online shopping, online banking, and untrusted websites. In the context of payment cards, Kosse (2013) finds that newspaper articles about skimming reduce offline debit card use on the same day, but does not lead to long-lasting economic effects. Others find that consumers are likely to switch to other methods, if their confidence in the security of credit cards is undermined (Cheney, 2010; Sullivan, 2010). Effective reporting of fraud prevention efforts, on the other hand, can increases the quality of customer relationships and loyalty towards banks (Hoffmann and Birnbrich, 2012).

While all these studies suggest that security incidents reduce the use of payment methods, Kahn and Liñares-Zegarra (2016) state that the results are not yet conclusive. They point to some studies which only find a weak or even no impact of security incidents on individual use of payment methods. One problem is that many studies rely on general perceptions of security, reported in surveys, without the consideration of actual incidents. Explicitly including experience, Kahn and Liñares-Zegarra (2016) study the impact of identity theft for the 2009 Survey of Consumer Payment Choice.

Interestingly, they find that some types of identity theft have a positive impact on credit card use, in contrast to negative impacts on checks and online banking bill payments. Still, a major gap remains in their study, which is the lack of data on actual behavior in the form of credit card use. The only study which includes actual behavior is Somanchi and Telang (2017), who analyze the impact of fraudulent transactions on the probability that customers terminate relationships with a large US bank within six months after the incident. They use five years of data for half a million customers and find a significant increase in the termination probability for fraud victims. The probability is even greater if the fraud could not be investigated and attributed to a malicious third party.

### 6.1.2 Intervention Study

To answer our research questions, we conduct an intervention study. We analyze transaction data of victims of credit card fraud in a natural experiment. In natural experiments, the treatment varies through a naturally occurring or unplanned event (the fraud incident), which is exogenous to the outcome variable (credit card use). Such experiments are often used to study the impact of population wide health interventions (Craig et al., 2012), state laws, or other government interventions (Meyer, 1995). While in principle less powerful than studies with random selection, natural experiments are a viable alternative if random selection is not feasible. This is obviously the case for victims of credit card fraud, since only a fraction of credit card holders is affected and victimization cannot be randomized (in an ethical manner).

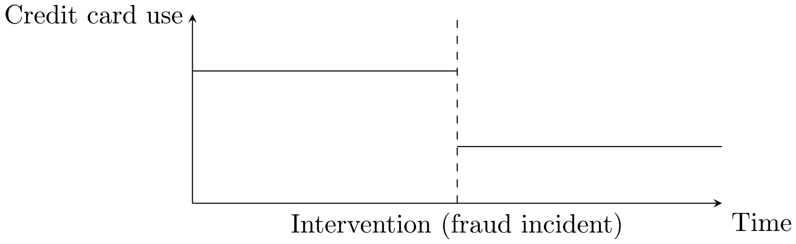


**Figure 6.1:** Conceptual model of the intervention study

We study weekly credit card use (outcome) for victims of credit card fraud before and after an incident, as depicted in Figure 6.1. The intervention is the fraud incident and the subsequent replacement of the credit card. Intervention effects can occur along two different dimensions: level (intercept), trend (slope), or also in variation. They can be immediate or delayed and they can be continuous or drift back towards the old level. We expect to see an abrupt downward change in the use level after the incident, which is persistent until the end of the observation period. Accordingly, we expect to see a change in the intercept, but not in the slope.

Various techniques exist to study the impact of an intervention. An important stream of research is interrupted times-series analysis (ITS; Tryon, 1982). ITS has been particularly used to study the impact of interventions for large populations (Bernal et al., 2017). While applications for smaller samples haven been suggested (Fok et al., 2015), we chose to study the intervention effects using a LMM. LMMs have several advantages. They provide a flexible modeling approach for repeated measures of the same subjects under different conditions and for small samples (West et al., 2014, p. 9). Furthermore, they allow for the inclusion of predictor variables with fixed and random effects, to examine the impact of additional factors on credit card use.

We conduct standardized telephone interviews among the victims to supplement the analysis of transaction data. We record attitudes towards the credit card as a payment method and perceptions of the incident and the replacement process to uncover factors influencing the potential avoidance behavior. Building on constructs proposed by Featherman and Pavlou (2003) and the model of security behavior (Chen and Zahedi, 2016), we test several factors with an impact on credit card use. Positive factors comprise perceived benefits of the credit card as a payment method, including perceived usefulness and perceived ease-of-use, but also positive perceptions of the fraud dispute handling. Negative factors mainly include indicators related to perceived risk.

### 6.1.3 Integration into the Credit Card Replacement Process

To collect empirical data, we collaborate with PLUSCARD, a German payment card processor. Our study resembles a natural experiment, as the data collection is integrated into the credit card replacement process, which is initiated by PLUSCARD after each (confirmed) fraud incident. A simplified representation of the credit card replacement process and the integration of the data collection are illustrated in Figure 6.2 and explained in the remainder of this subsection.

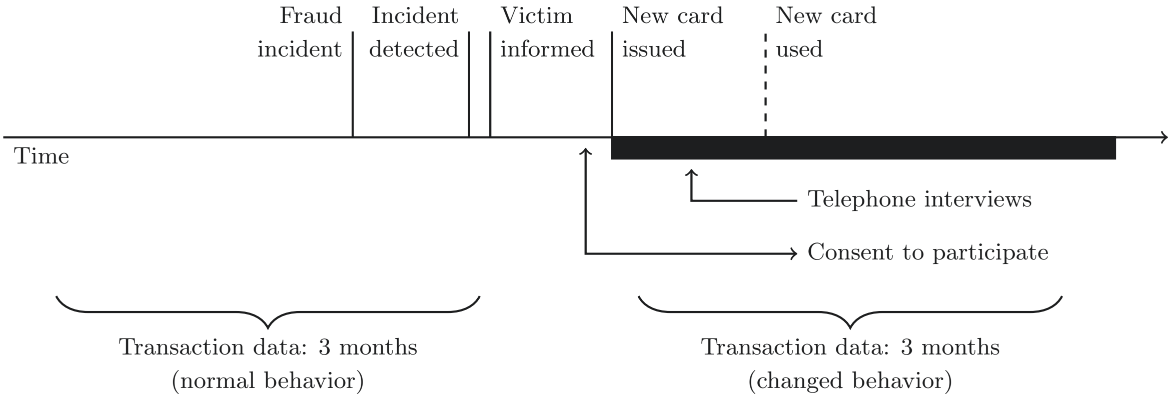


**Figure 6.2:** Study integration into the processing of credit card fraud incidents

Figure 6.2 shows the simplified process of the credit card replacement schematically above the horizontal time line. The process is initiated by an incident of credit card fraud. A potentially fraudulent CNP transaction is either detected by the fraud prevention systems operated by PLUSCARD or reported by a customer. In the former case, PLUSCARD blocks the credit card and tries to confirm the transaction by calling the customer. If the transaction is not verified, the credit card is permanently blocked. In some cases, incidents are only detected after fraudulent payments have already been processed. In those cases, PLUSCARD investigates the liability for the fraudulent transaction. Similar to our findings concerning compensation payments after identity theft of financial accounts (see Section 4.2.3), victims are generally reimbursed. In our sample all victims with losses received compensation payments. All victims are notified about the incident (and whether they are liable or not) by mail. The letters are issued automatically, once an incident is confirmed. Furthermore, a new credit card is issued immediately and send to the victim on the next day.

To integrate the study, PLUSCARD approaches victims after they have been notified about the fraud incident with an additional letter. The letter provides information regarding the purpose of the study and asks for consent to participate. Victims can give their consent by mail or by using a specially designed online form, which was integrated into PLUSCARD's website during the time of the fieldwork. A financial compensation of €10, for the time needed to conduct the telephone interview, is transferred to the victim's credit card account after the study.

The standardized telephone interviews are conducted by specially trained agents in PLUSCARD's internal call-center. This has three major advantages. First, the agents are informed about the study and have all relevant information regarding the fraud incident and the credit card replacement process. Second, victims do not need to communicate with an external call-center. Third, personal identifiable information (PII) never leaves PLUSCARD. The questionnaire covers behaviors, perceptions, and attitudes and has been designed in collaboration with PLUSCARD. The transaction data is recorded for each customer using the fraud detection systems operated by PLUSCARD. The recording started three months before the incident and ended three months after the replacement card has been received for each victim.

The privacy and anonymity of participants is of paramount importance. We follow the ethical standards presented in Section 1.3.1 and use several measures to guarantee privacy and anonymity through-out the data collection process. Participants provide written consent for: 1) being called in the telephone survey, 2) the analysis of aggregates of their transaction data, and 3) extraction of demographic information. Moreover, they explicitly agree with a data protection agreement. Transaction data is recorded in weekly bulks which include a transaction count and the total revenue for one week. Three types of transaction data are recorded: total, Internet, and PayPal transactions PLUSCARD collects and aggregates the survey results and the transaction data and integrates both in a single data set. Before the data set is made available to the researcher, all PII is removed. The procedure ensures that the analysis is conducted on a fully anonymized data set.

### 6.1.4 Fieldwork

The fieldwork started in December 2016 (week 51) with the first wave of invitation letters sent to all credit card owners and ended in June 2017 (week 25) with the last telephone interviews.[1] The recording of transaction data extends the fieldwork because all victims with fraud incidents between August 2016 (week 32) and March 2017 (week 13) have been invited to participate.

Figure 6.3 illustrates several aspects of the fieldwork for the complete time frame of the data collection. The x-axis shows the week number (in a "year.week" notation) and each line on the y-axis represents a single participant, chronologically ordered by the time of the fraud incident.

In total, 93 out of 756 approached victims gave consent to participate in the study (see Subsection 6.2.1). Blue circles mark the weeks in which victims were invited. The first wave was sent in week 51 (13.12.2016). Four additional waves were sent in January, February and March 2017 to reach more victims. The purple circles mark the date of the telephone interviews. In most cases, victims were interviewed a few weeks after the incident. Some interviews were considerably delayed because victims could not be reached. 13 participants could not be reached at all.

Figure 6.3 also illustrates the distribution of fraud incidents (marked by red crosses) over the period of the fieldwork, starting with first incidents reported in week 32 (August 2016). Incidents are spread throughout the whole data collection period, but victimization varies over time. Weekly rates range from 0 victims, e. g., in week 43 (2016) to 8 victims in week 52 (2016). Monthly rates range from 2 in February (2017) to 17 in August (2016).

The horizontal lines depict the time frame for which transaction data is recorded. Observation starts 13 weeks before the incident and ends 13 weeks after the replacement card was sent, which translates to approximately six month of transaction data for each victim. This results in an overall observation period of 60 weeks, starting in week 19 (01.05.2016) and ending in week 26 (25.06.2017).

The lines also provide first information on the individual use of the credit cards before and after

[1] We count all weeks according to the convention used by Microsoft Excel. Accordingly, all days until the first Saturday of the year count as week 1 and the last week of every year is week 53.

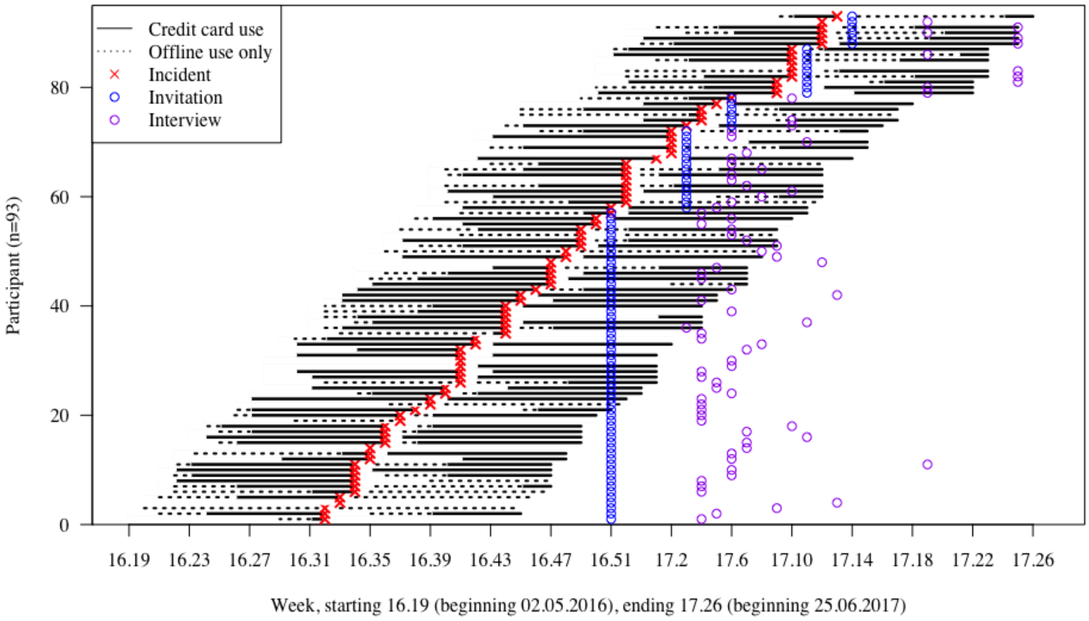


**Figure 6.3:** Fieldwork and data collection

the incident. Dotted lines indicate that the card was only used offline and solid lines indicate online use or both. Therefore, dashed lines turn into solid lines, once the credit card is also used online. The beginning of each line marks the first use after the beginning of the observation period or the fraud incident. Accordingly, white spaces indicate that credit cards have not been used, since either of the two points in time. Without going into much detail, we can observe diverse behavior before and after the incident. While some victims use the new card immediately after the incident, others refrain from using it online or at all.

## 6.2 Data

This section presents descriptive statistics. We first describe the sample in Section 6.2.1. Then, we present self-reported statistics for perceptions, behavior, intentions, and attitudes in Section 6.2.2. Finally, Section 6.2.3 reports actual behavior in the form of aggregated transactions.

### 6.2.1 Sample Demographics

All participants are victims of credit card fraud on a card that is operated by PLUSCARD. Since PLUSCARD processes payments for about a third of the banks in one of the major German saving bank associations, it has access to a large part of the German credit card market. The banking association as well serves about a third of the overall German population. In total, PLUSCARD processes payments for about 2.5 m cards which belong to one of approximately 200 saving banks in the association. Furthermore, PLUSCARD provides back-office services for 2 m additional cards.

Only 14 individual saving banks agreed to take part in the study, reducing the pool of customers and potential victims. The participating banks are spread across seven states in north, west, and east Germany. They vary in size with less than 2 000 credit cards issued by the smallest bank and almost 35 000 by the largest bank. The total population of credit card owners in our sample is a little smaller than 150 000.

**Table 6.1:** Demographics of the sample and all credit card owners

| Variable | Selected victims | | | Credit card owners | |
|---|---|---|---|---|---|
| | Interviewed | Participated | Rejected | Participating banks | All |
| N (count) | 80 | 93 | 663 | 150 000 | 2.5 m |
| Card (proportion Visa) | 43.8 % | 45.2 % | 54.6 % | 49.2 % | 41.4 % |
| Gender (proportion male) | 65.0 % | 67.7 % | 57.1 % | 57.5 % | 57.0 % |
| Average age (in years) | 48 | 48 | 45 | 49 | 49 |
| Average revenue (in 2016) | € 3 758 | € 3 769 | € 3 097 | € 2 394 | € 2 304 |

While this still seems to be a large population to sample from, only a small fraction of customers fall victim to credit card fraud. Furthermore, some victims were not contacted because they 1) were younger than 18 years, 2) were not using their credit card before the incident, 3) had a special platinum or business card, or 4) had an explicit no-contact agreement with the bank. Ultimately, a total 756 suitable victims have been contacted. 93 victims gave consent to participate in the study and 80 were interviewed by phone, leading to a response rate of 12.3 % (10.6 % for the phone interviews). The sample demographics for both groups of participants are shown in Table 6.1 and contrasted to unresponsive victims and the overall population of credit card owners.

PLUSCARD operates two types of credit cards, VISA and Mastercard. Compared to customers at the participating banks, the sample contains less VISA cards (-5.4 %-pts.). However, compared to customers at all banks, more VISA card users are in the sample (+2.4 %-pts.). The majority of customers are men (proportion: 57 %) and even more men (proportion: 65 %) participated in the study. The average age of participants is slightly younger (48 years) compared to all customers (49 years). Due to the exclusion of minors, it is greater than the overall German average, which was 44 years and three months in 2015 (Altenhoven, 2017). The average revenue in 2016 (for each group) is substantially higher for the selected victims. This is a result of the selection of participants, which excludes victims who have not used the credit card in the six months before the incident.

**Table 6.2:** Additional demographics for the interviewed victims

| Variable | Answers | | | | |
|---|---|---|---|---|---|
| **Education** | Tertiary | Lower sec. (2) | Upper sec. (3A) | Post-sec. (4A) | Sec. stage tert. (6) |
| (ISCED-Level) | 30.4 % | 26.6 % | 22.8 % | 15.2 % | 3.8 % |
| **Profession** | Full-time | Pension | Part-time | Other | Student |
| | 61.3 % | 16.2 % | 13.8 % | 4.8 % | 2.5 % |
| **Area of living** | Village | Town | City | Suburbs | Other |
| | 35.0 % | 32.5 % | 18.8 % | 8.8 % | 2.5 % |

Other professions include: apprentices, house wifes, no profession, and non-response.

The telephone interviews allowed us to collect additional demographic information for the interviewed victims, presented in Table 6.2. Education levels are reported using the International Standard Classification of Education (ISCED). A translation of ISCED to the German education system is available in Destatis (2016, p.80). The education level in the sample is rather high, with almost 50 % of respondents having higher than secondary education (tertiary, post-secondary, and second stage tertiary). The remaining participants have at least a secondary education level (lower secondary or upper secondary). The majority works full or part-time (75.1 %) and a substantial part is retired (16.2 %). Participants are likely living outside large cites. 67.5 % report to live in towns or villages, only 27.6 % live in cities or suburbs. Overall, we collected a rare sample of rather old credit card users. More than 50 % of the respondents older than 50 years.

### 6.2.2 Descriptive Statistics of Interview Responses

We report two types of the interview results. Section 6.2.2.1 presents self-reported behavior, perceptions, and intentions. Section 6.2.2.2 reports attitudes towards online shopping and credit card payments. Both sections order the results chronologically along the card replacement process, i. e., before, during, and after the incident. All questions have been translated to English in this chapter, the original German questionnaire can be found in Appendix C.1.1.

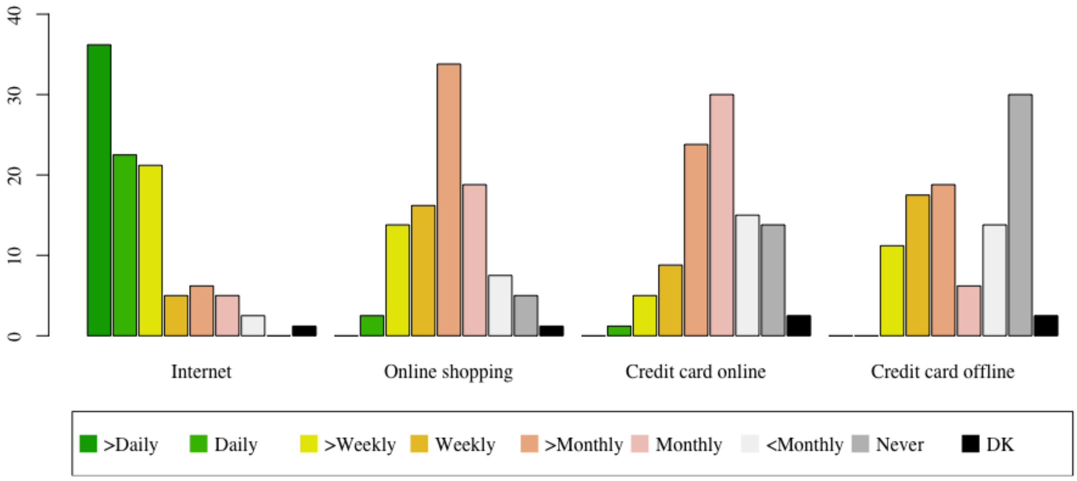


**Figure 6.4:** Self-reported behavior: average use during the three months before the incident

#### 6.2.2.1 Self-reported Behavior, Perceptions, and Intentions

This section reports behavior in the form of individual use statistics of credit card payments, the Internet, and online shopping before the incident. Furthermore, it provides information on perceptions of the fraud incident and use intentions in the future.

**Behavior Before the Fraud Incident** Figure 6.4 reports *self-reported* statistics regarding the use of the Internet and online shopping[2] as well as the credit card for Internet and offline payments[3]. Exact values are reported in Table C.1 (in the appendix). The Internet is frequently used by the vast majority of respondents. 58.7 % use it at least daily and additional 26.2 % use it at least weekly. The use of online shopping is less frequent. Still, more than 80 % use shop online at least monthly and almost 40 % state to use it at least weekly. The credit card is only partly used for payments on

[2] "On average, how often have you used [the Internet for personal purposes|online shopping] during the three months before the incident ?" (translated from the German questionnaire; Appendix C.1.1 p. 158 and p. 160).

[3] "On average, how often have you paid with your credit card [on the Internet|outside of the Internet] during the three months before the incident ?" (translated from the German questionnaire; Appendix C.1.1 p. 163 and p. 155).

the Internet. 13.8 % report that they never use their credit card online and another 15 % use it less than monthly. Most respondents use it either monthly or several times per month (45 %).

The distribution of credit card use for offline payments is characterized by two peaks. While 30 % of respondents never use the credit card offline, almost 30 % use it at least weekly. This points to two different groups of respondents. A first group, which only uses the card online, and a second group, which also uses it frequently offline.

**Table 6.3:** Self-reported behavior: additional use statistics

| Question | No | Yes | DK | NA |
|---|---|---|---|---|
| Do you use your credit card when you are abroad ?[a] | 18.8 % | 78.8 % | 2.5 % | 0.0 % |
| Do you own other credit cards ?[a] | 75.0 % | 25.0 % | 0.0 % | 0.0 % |
| Do you use these other credit cards [...] outside of the Internet ?[a] | 3.8 % | 21.2 % | 0.0 % | 75.0 % |
| Do you use online banking ?[b] | 18.8 % | 80.0 % | 0.0 % | 1.2 % |
| Are you already registered for S-ID-Check, [...] ?[c] | 60.0 % | 26.2 % | 13.8 % | 0.0 % |

Original (German) question wording in Appendix C.1.1 [a]: p. 156, [b]: p. 159, [c]: p. 170.

We also ask for the payment method that is mainly used for offline payments nationally and abroad. Results are reported in Table C.2 (in the appendix). More than 50 % of the respondents mainly use a debit card or cash to pay in shops. Only 8.8 % reported that they mainly use the credit card. However, 36.2 % use multiple payment methods, which may include the credit card as well. Other credit cards have not been reported as the main payment method.

Table 6.3 reports additional use statistics. The use of the credit card is more common for international payments. Almost 80 % of respondents use it to pay abroad. 40 % report to use it as the main payment method, followed by cash (30 %) and multiple payment methods (15 %). A substantial part (25 %) also has *another* credit card and almost all of them (21 %) use it for offline payments. Online banking is used by most respondents (80 %). However, only 26.2 % are registered for the new two-factor-authentication method for online credit card payments called S-ID-Check. Furthermore, 13.8 % have never heard of S-ID-Check.

**Use of Payment Methods on the Internet** Table 6.4 reports respondents' knowledge and use of different Internet payment methods. The first three (invoice, direct debit, and prepay) represent rather traditional forms of payment, whereas the remaining three (PayPal, Giropay, and "SOFORT Überweisung") rely on electronic payment systems (EPS).

**Table 6.4:** Knowledge and use of Internet payment methods

| Payment method | Never heard | Not used | Used (no reference period) | ECC* |
|---|---|---|---|---|
| "Which of the following traditional payment methods have you used on the Internet ?" | | | | |
| Invoice | 0.0 % | 15.0 % | 85.0 % | 84.9 % |
| Direct debit | 0.0 % | 37.5 % | 62.5 % | 74.9 % |
| Prepay | 0.0 % | 42.5 % | 57.5 % | 65.1 % |
| "Which of the following electronic payment systems have you used on the Internet ?" | | | | |
| PayPal | 0.0 % | 23.8 % | 76.2 % | 69.9 % |
| Giropay | 23.8 % | 67.5 % | 8.8 % | – |
| "SOFORT Überweisung" | 5.0 % | 50.0 % | 45.0 % | 59.6 % |

Original (German) question wording in Appendix C.1.1 pp. 164–166; *: "Heard of or used . . .".

Traditional payment methods are known to all respondents and have been used by the majority already. Invoice payments are most common (85 %). Among the EPS, PayPal is most prominent. It is known by all respondents and widely used (76.2 %). “SOFORT Überweisung” is also widely known (95 %), but only used by less than half of the respondents. Giropay, developed by the banking association, is known by 76.2 % but is only rarely used (8.8 %). Our results are generally consistent with a consumer survey (N=1 005) conducted in 2012 in Germany (ECC, 2012). Although not exactly comparable, we add the ECC results as an individual column to Table 6.4. Knowledge of PayPal and “SOFORT Überweisung” is reported more often in our sample, which is likely a result of the time difference in data collection periods. Giropay is not collected in ECC (2012).

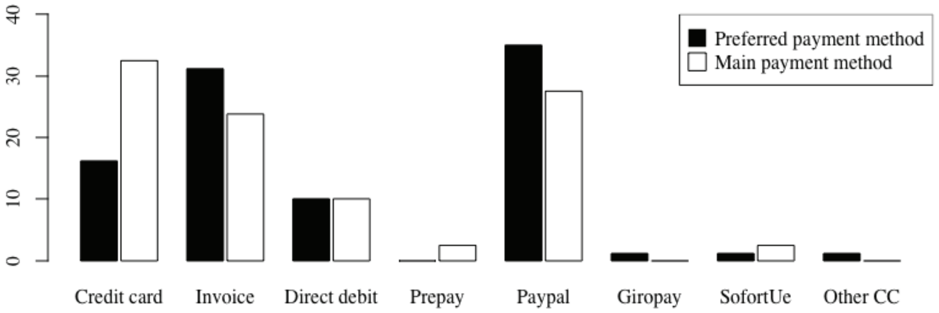


**Figure 6.5:** Preferred payment method versus mainly used payment method

In addition to knowledge and use of these online payment methods, we also ask for the preferred and mainly used methods. In a screening question, 97.5 % of respondents reported that they have a preferred method for Internet payments. Figure 6.5 illustrates that invoice and PayPal are the mostly preferred, followed by the credit card. Nevertheless, the credit card is mainly used for Internet payments, followed by PayPal and invoice. Direct debit is less important (10 %) and other payment methods are rarely preferred and used. All responses are reported in Table C.3 (in the appendix).

**Perception of the Fraud Incident** We collect several types of information regarding the incident, most importantly loss statistics. Table 6.5 reports the empirical distributions of three types of losses: 1) primary monetary, 2) additional monetary, and 3) time. Primary losses represent the money that was attempted to be stolen. Note that all primary losses have been reimbursed by PLUSCARD or could be blocked before the payment was processed. For comparison we include actual losses, recorded by PLUSCARD, along with the self-reported statistics. Categorical and missing values in the self-reported data have been imputed with conservative assumptions, using a similar approach as in Chapter 4 for population-wide cost estimates.

**Table 6.5:** Empirical distributions of losses incurred by the victims

| **Loss type** | **Quantiles** | | | | | | |
|---|---|---|---|---|---|---|---|
| | 0 % | 25 % | Median | 75 % | 100 % | Mean | Zero-inflation |
| Primary (self-reported) in € | 0.0 | 0.0 | 1.5 | 350.0 | 8900.0 | 471.8 | 49 % |
| Primary *(actual)* in € | 0.0 | 0.0 | 0.0 | 200.0 | 3959.2 | 239.9 | 52 % |
| Additional (self-reported) in € | 0.0 | 0.0 | 0.0 | 0.0 | 75.0 | 3.3 | 92 % |
| Time (self-reported) in hours | 0.0 | 0.0 | 0.5 | 5.5 | 50.0 | 4.7 | 29 % |

Many aspects of the loss distributions correspond to our findings in Section 4.2.2: losses of time are more prevalent than monetary losses, victims are always compensated, and zero-inflation is high (about 50 %). As many victims do not lose anything, even before reimbursement, loss distributions are also skewed to the right reflected in the large difference between mean and median estimates. In addition to the previous findings, we see that actual losses are smaller than self-reported losses and that additional costs are only a small fraction of the losses. We collected some additional information on the incident. 9 % of the victims detected the fraud themselves, otherwise it was detected by PLUSCARD. 11.2 % reported the incident to the police. 31.2 % reported to have avoided the credit card after the incident and used another payment method instead.

**Behavioral Intention After the Fraud Incident** We also report the intention to use the new credit card and online shopping in the three months after the incident in Table 6.6. Most people want to use the new credit card in the same way as before (70 % online and 66.2 % offline). Interestingly, even 3.8 % reported that they want to use their new credit card more often on the Internet. However, a substantial portion ($> 25$ %) wants to use it less or never. The reported intention for change is weaker for online shopping, for which 83.8 % of respondents report no change intention.

**Table 6.6:** Use intention after incident

| **Question** | **Never** | **Less** | **Same** | **More** | **NA** |
|---|---|---|---|---|---|
| "How often do you intend to use . . . " | | | | | |
| your new credit card for payments on the Internet ?[a] | 11.2 % | 13.8 % | 70.0 % | 3.8 % | 1.2 % |
| online shopping during the upcoming months ?[a] | 2.5 % | 13.8 % | 83.8 % | 0.0 % | 0.0 % |
| your new credit card for payments outside of the Internet ?[b] | 16.2 % | 17.5 % | 66.2 % | 0.0 % | 0.0 % |
| "How often have you used . . . " | | | | | |
| your new credit card in comparison to the old one ?[c] | 6.2 % | 17.5 % | 73.8 % | 1.2 % | 1.2 % |
| online shopping since the incident ?[d] | 8.8 % | 10.0 % | 75.0 % | 3.8 % | 2.5 % |

Original (German) question wording in Appendix C.1.1 [a]: p. 187, [b]: p. 191, [c]: p. 183, [d]: p. 184.

Since some interviews took place many weeks after the incident, we also asked for changed behavior in the time between incident and interview. The lower part of Table 6.6 shows that the reported change for this time is very similar to the future use intention. The stronger tendency to unchanged behavior (same) may be explained by the short time frame between the incident and the interview for some respondents. Thus, some may not have had the time to change their behavior.

#### 6.2.2.2 Attitudes

To identify factors which may influence avoidance of the credit card, we report attitudes towards online shopping, the credit card as a payment method, and the processing of the incident. Applying the same structure as in the previous section, attitudes are presented along the fraud process.

**The Credit Card as a Payment Method** We first report attitudes concerning the credit card as a payment method, followed by a few security related statements regarding online shopping in general. Attitudes concerning the credit card as a payment method have been collected using nine Likert scale items, which cover various credit card characteristics. Each item measures the agreement with a statement on a six-point scale, ranging from "totally disagree" (1) to "totally agree" (6). Table 6.7 reports the results.

Overall, respondents state that using the credit card on the Internet is beneficial for them (85 % agree and 55 % totally agree). This seems to be driven by the wide acceptance of the credit card

**Table 6.7:** Attitudes towards the credit card as a payment method

| **Statement** | **Disagree** | | | **Agree** | | | |
|---|---|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | **5** | **6** | **NA** |
| The credit card is accepted wherever I shop online. | | | | | | | |
| *widely accepted* | 1.2 % | 2.5 % | 1.2 % | 7.5 % | 17.5 % | 63.7 % | 6.2 % |
| Compared to other payment methods, I have better chargeback options when I use the credit card. | | | | | | | |
| *better reimbursement* | 10.0 % | 2.5 % | 6.2 % | 15.0 % | 15.0 % | 17.5 % | 33.8 % |
| The credit card makes payments on the Internet easier for me. | | | | | | | |
| *easier payments* | 5.0 % | 2.5 % | 2.5 % | 12.5 % | 13.8 % | 60.0 % | 3.8 % |
| Payments with the credit card take longer than with other payment methods. | | | | | | | |
| *longer payments* | 43.8 % | 20.0 % | 5.0 % | 6.2 % | 6.2 % | 8.8 % | 10.0 % |
| Other payment methods are more secure than the credit card. | | | | | | | |
| *less secure* | 18.8 % | 12.5 % | 5.0 % | 27.5 % | 13.8 % | 10.0 % | 12.5 % |
| The credit card is an inexpensive payment method. | | | | | | | |
| *inexpensive* | 8.8 % | 7.5 % | 10.0 % | 22.5 % | 20.0 % | 26.2 % | 5.0 % |
| Other payment methods lead to less additional costs. | | | | | | | |
| *o. paym. cheaper* | 23.8 % | 7.5 % | 12.5 % | 16.2 % | 13.8 % | 21.2 % | 5.0 % |
| Using the credit card on the Internet has substantive benefits for me. | | | | | | | |
| *overall useful* | 2.5 % | 6.2 % | 2.5 % | 15.0 % | 15.0 % | 55.0 % | 3.8 % |
| People, who are important to me, think that I should pay with the credit card on the Internet. | | | | | | | |
| *should use* | 20.0 % | 11.2 % | 2.5 % | 20.0 % | 10.0 % | 3.8 % | 32.5 % |

Original (German) question wording in Appendix C.1.1 p. 169.

as a payment method (almost 90 % agree) and its ease-of-use for online payments (more than 85 % agree). The comprehensive chargeback options are unknown to a third of all participants. With regard to costs and security answers are more evenly distributed. The credit card is predominantly perceived to be an inexpensive payment method, on the other hand more than half of the respondents state that other payment methods lead to less additional costs. With regard to security, about 25 % strongly agree (5 and 6) that other payment methods are more secure and more than 30 % strongly disagree (1 and 2).

Additional attitudes regarding online shopping are reported as an agreement to four binary statements in Table C.4 (in the appendix). Interestingly, more than 70 % of the respondents reported to *only* buy at online shops which offer their preferred payment method. As many respondents have already renounced a product because the vendor did not offer their preferred payment method. Also in line with that, 64 % do not buy at shops they do *not* know.

**Processing of the Incident** Five items collect attitudes on the incident and the card replacement process. Each item measures perception by recording the agreement with a statement on a six-point Likert scale. Items have been answered by the majority of respondents. Table 6.8 reports the results.

The responses show that the vast majority of the victims felt well informed (70 % totally agree) and is satisfied with the replacement process (76.2 % totally agree). Only very few think that it is cumbersome to use the new credit card (15 % strongly agree). Responses are more evenly distributed

**Table 6.8:** Perception of the incident

| **Statement** | **Disagree** | | | **Agree** | | | |
|---|---|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | **5** | **6** | **NA** |
| I felt well informed during the credit card replacement process. | | | | | | | |
| *well informed* | 5.0 % | 0.0 % | 1.2 % | 10.0 % | 12.5 % | 70.0 % | 1.2 % |
| I am more concerned about the security of my credit card after the incident. | | | | | | | |
| *more concerned* | 20.0 % | 10.0 % | 5.0 % | 18.8 % | 18.8 % | 26.2 % | 1.2 % |
| I understood what happened, and I can protect myself better in the future. | | | | | | | |
| *can protect self* | 22.5 % | 6.2 % | 13.8 % | 15.0 % | 6.2 % | 35.0 % | 1.2 % |
| I am completely satisfied with the credit card replacement process. | | | | | | | |
| *satisfied process* | 2.5 % | 2.5 % | 1.2 % | 5.0 % | 8.8 % | 76.2 % | 3.8 % |
| I think it is cumbersome to use my new credit card everywhere. | | | | | | | |
| *cumbers. use new cc* | 55.0 % | 12.5 % | 8.8 % | 6.2 % | 7.5 % | 7.5 % | 2.5 % |

Original (German) question wording in Appendix C.1.1 p. 186.

for security related attitudes. While 45 % strongly agree that they are more concerned about the security of their new credit card, 30 % strongly disagree. In the same way, 35 % totally agree that they can protect themselves in the future, while 22.5 % totally disagree.

**After the Incident** We also collect attitudes regarding credit card payments and online shopping after the incident. Again, these were recorded on a six-point Likert scale, which measured the agreement to six different statements.

**Table 6.9:** Attitudes towards credit card payment and online shopping after the incident

| **Statement** | **Disagree** | | | **Agree** | | | |
|---|---|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | **5** | **6** | **NA** |
| I intend to shop only at trusted or well-known websites. | | | | | | | |
| *shop at trusted webs.* | 3.8 % | 3.8 % | 5.0 % | 11.2 % | 27.5 % | 45.0 % | 3.8 % |
| I intend to stop buying particular products and services on the Internet. | | | | | | | |
| *not buy some products* | 36.2 % | 6.2 % | 12.5 % | 17.5 % | 10.0 % | 13.8 % | 3.8 % |
| For many of my payments on the Internet, the credit card is the only option. | | | | | | | |
| *card only option* | 15.0 % | 6.2 % | 10.0 % | 22.5 % | 17.5 % | 23.8 % | 5.0 % |
| I think it is cumbersome to try new payment methods on the Internet. | | | | | | | |
| *cumbersome to try new paym.* | 15.0 % | 6.2 % | 7.5 % | 10.0 % | 20.0 % | 37.5 % | 3.8 % |
| I can avoid credit card fraud, if I use my credit card less often on the Internet. | | | | | | | |
| *can avoid fraud* | 23.8 % | 5.0 % | 8.8 % | 18.8 % | 16.2 % | 21.2 % | 6.2 % |
| The bank protects me from credit card fraud. | | | | | | | |
| *bank prot. fraud* | 6.2 % | 5.0 % | 2.5 % | 12.5 % | 20.0 % | 48.8 % | 5.0 % |

Original (German) question wording in Appendix C.1.1 p. 188.

Table 6.9 reports the results. The items are overall more balanced than for the other attitudinal questions. About 60 % of the victims agree that they can avoid fraud, if they use their credit card less on the Internet. However, almost 65 % state that the credit is the only option and even more think that it is cumbersome to try new payment methods (67.5 %). Almost half the respondents totally agreed that their bank protect them from credit card fraud. With regard to online shopping, 40 % agree that they intend to stop buying some products online, substantially more intend to shop only at trusted or well-known websites (83.7 %).

### 6.2.3 Actual Behavior

We present actual behavior in the form of aggregated transactions. The approach is similar to interrupted time-series designs and intervention studies to analyze the aggregated data visually before and after the intervention (e. g., Bernal et al., 2017). In our case, the fraud incident is this intervention and we analyze weekly transactions and revenues over the whole sample in Figure 6.6.

Weeks are normalized for each victim such that the incident took place in week 0 (marked by a red vertical line). The preceding weeks are labeled week -13 to -1 and the following weeks 1 to 13 (x-axes). This numbering should not be confused with week numbers in 2016 and 2017. We have calculated mean statistics of credit card use for each week preceding and following the incident for the 93 participants (y-axes). The green lines represent credit card use for Internet payments, the blue lines for offline payments, and the black lines total use, which is the sum of the former two. The dashed lines represent overall averages over the 13 weeks. In addition to total use, we report PayPal adjusted use, indicated by gray lines. Paypal transactions can be identified if customers use their PLUSCARD credit card for payments with their PayPal account. Therefore, we can only adjust for *observable* PayPal transactions, not for cases where customers use their bank account directly.

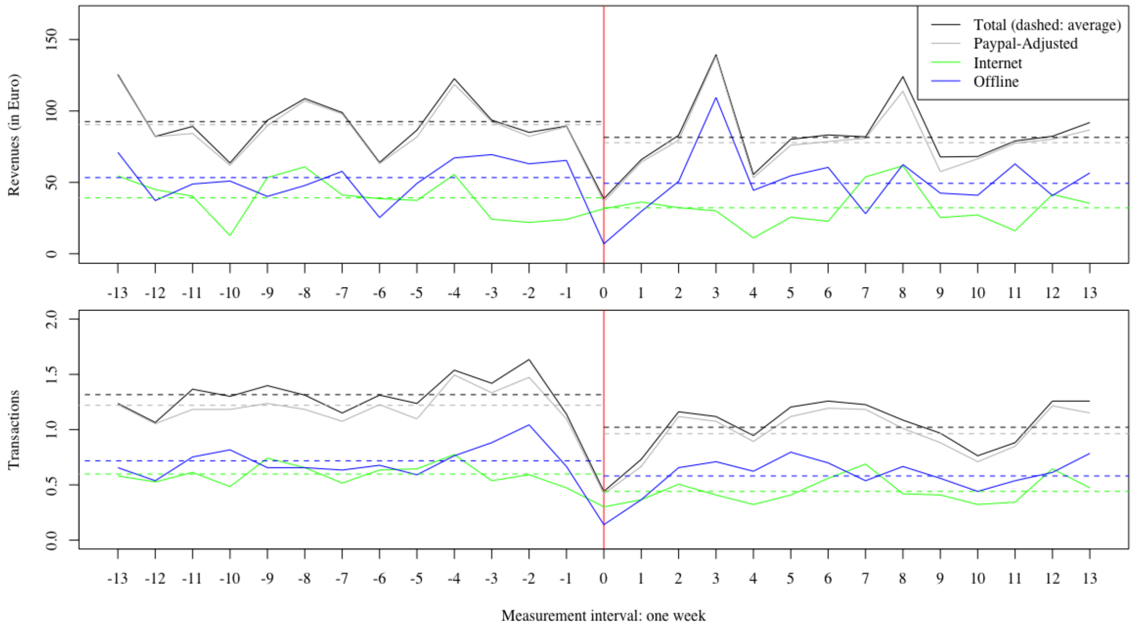


**Figure 6.6:** Average weekly transactions normalized to incident

Figure 6.6 shows that the weekly averages (in the upper part) fluctuate between one and two transactions before the incident. The averages of PayPal-adjusted transactions are only marginally smaller and behave very similar. Internet transactions account for roughly the half of the total transactions and seem more stable than the offline transactions. Average weekly revenues (in the lower part) behave similarly. While the measurement scale naturally causes a higher variation (between € 60 and € 120), they also seem fairly stable over time. Again, averages of PayPal-adjusted revenue are marginally smaller and Internet revenue accounts for roughly half of the total revenue.

Credit card use drops substantially during the week of the incident, but grows immediately in the following two weeks. The sharp drop is due to the block on the old credit card and the time that is needed to deliver the new card. Interestingly, no decrease can be observed for weekly revenue of Internet transactions in the week of the incident. The overall average drops from 1.32 total transactions per week before the incident to 1.02 transactions after the incident. Similarly, average revenue drops from € 95.5 to € 81.5.

## 6.3 Results

This section presents the results of the mixed model analysis. Section 6.3.1 first formalizes the modeling approach and Section 6.3.2 presents our baseline model, i. e., the simplest model to explain the impact of the fraud incident on credit card use. Finally, we analyze the inclusion of additional explanatory variables in Section 6.3.3.

### 6.3.1 Linear Mixed-effects Model

We opt for a LMM and a general linear mixed-effects model (GLMM) approach to test for changes in weekly credit card use after the incident and analyze which factors influence these changes. Both techniques provide a flexible modeling approach for repeated measures of the same subjects under different conditions. They involve the estimation of covariance parameters to capture the likely correlation, caused by repeated measures of the same outcome for the same subject. They are linear in the parameters and allow for the simultaneous inclusion of predictor variables and random effects (West et al., 2014, p.9).

Our LMM has two levels. The lower level contains weekly observations of credit card use $y_{i,t}$ per subject $i$. Accordingly, it represents within-individual change over time. The upper level contains all observations for each subject to model individual differences in the change. The number of subjects in the baseline model is $N = 93$. This is later reduced to 80 because not all participants were interviewed in the telephone survey. The number of observed weeks for each subject is $M = 27$, ranging from 13 weeks before to 13 weeks after the incident. The data set is balanced, since the number of observations for each individual is equal and at fixed points in time. The total number of observations for individual credit card use is $M \cdot N = 2\,511$ (2 160 for interviewed victims).

$Y_{i,t}$ models credit card transactions per subject and week, with realizations $y_{i,t}$. We allow for the inclusion of a set of predictors $X_j$, with index $j \in \{1, \ldots, P\}$ and coefficients $\beta_j$. $P$ is the total number of predictors in a model. The predictors include the incident ($incident_{i,t}$), which can be interpreted as $x_{i,t,1}$. Moreover, it comprises attitudes towards the credit card and the perception of the incident. Realizations $x_{i,t,j}$ of general attitudes are the same for each week within a subject. $\theta_t$ and $\gamma_i$ are random effects to model variation between weeks and individual spending levels, $\theta_t$ and $\gamma_i$ respectively. $\theta_t$ is relative to the incident. Both are assumed to be normally distributed. $\epsilon_{i,t}$ denotes the residuals. The whole model can be formalized as follows:

$$y_{i,t} = \beta_0 + \sum\nolimits_{j=1}^{P} (x_{i,t,j} \cdot \beta_j) + \theta_t + \gamma_i + \epsilon_{i,t}, \tag{6.1}$$

We use three outcome variables $C_{i,t}$, $R_{i,t}$, and $U_{i,t}$ as instances of credit card use $Y_{i,t}$ for the $i$-th subject in week $t \in \{1 \ldots M\}$. Realizations $c_{i,t}$ represent the absolute count of transactions for one subject in one week. $r_{i,t}$ represent the respective aggregated revenue, which is log-transformed in the estimation process, i. e., included as $log(r_{i,t})$. $u_{i,t}$ is a binary usage indicator included with a logit link in the logistic regression model. The models only differ in the outcome variable and the link function that is used in the regression.

### 6.3.2 Baseline Model of Credit Card Avoidance

The *baseline model*, as shown in Equation 6.2, is the simplest model that explains the impact of the fraud incident on credit card avoidance:

$$y_{i,t} = \beta_0 + incident_{i,t} \times \beta_1 + \theta_t + \gamma_i + \epsilon_{i,t}. \tag{6.2}$$

It includes a single predictor $incident_{i,t}$ to mark the incident for each subject and two random effects ($\theta_t$ and $\gamma_i$), which model random variation between weeks and subjects. The dummy variable $incident_{i,t}$ is zero before the incident and one starting with the week of the incident. Unexplained variance is captured by $\epsilon_{i,t}$. Credit card use $Y_{i,t}$ is instantiated by three outcome variables: transaction count $C_{i,t}$, aggregated revenue $R_{i,t}$, and binary usage indicator $U_{i,t}$.

**Data preparation** Prior to fitting the baseline model, we check for outliers in the transaction data. We conduct a visual analysis of the relative frequency of weekly transactions (left part of Figure 6.7) and a histogram of weekly log-revenues (right part of Figure 6.7). The frequency plot shows one or two potential outliers with 20 and 27 transactions in a single week. In-depth investigation reveals that two customers (called: $A$ and $B$) account for these high use weeks. $A$ has one week with 20 and one with 27 transactions and $B$ a single week with 20 transactions. We study individual spending behavior of both manually to determine if the numbers may be reasonable. As a result, we keep the value for $B$ because her spending level is generally high, including six weeks with at least ten transactions. Customer $A$ never used the credit card more than four times per week, except for the two outliers. To remove them, we impute five transactions for customers $A$ in the two outlying weeks. The histogram on the right shows that no outliers exist in weekly revenues, if those are log transformed (using: $log(r_{i,t} + 1)$). Both figures clearly show a very high portion of zero transaction weeks.[4] The credit cards were not used in 55 % of all observed weeks.

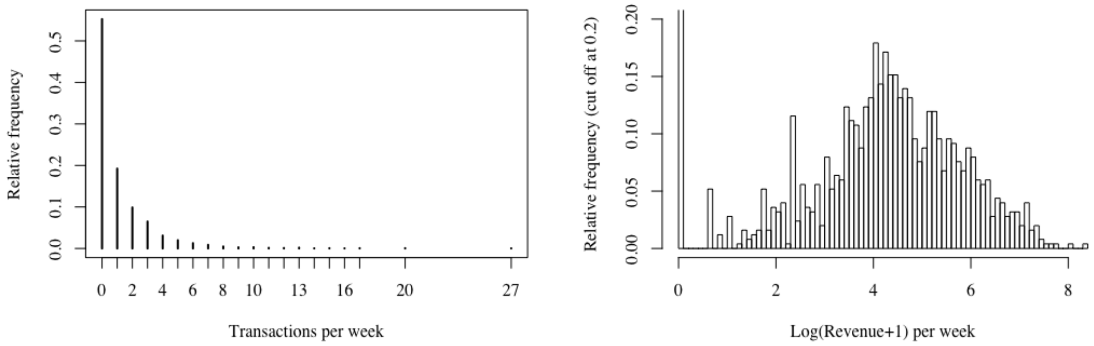


**Figure 6.7:** Empirical distribution of weekly credit card use

[4] The frequency is cut off at 0.2 for revenues in the right part of Figure 6.7 to improve illustration.

**Model fitting** In order to check the robustness of the baseline model comprehensively, we fit models for all three outcome variables $\{C_{i,t}, R_{i,t}, U_{i,t}\}$, two samples (*participating* victims and *interviewed* victims) and two types of transactions (*total* and *Paypal-adjusted*). Total transactions contain all recorded transactions, online and offline. Paypal-adjusted transactions are based on the total transactions, but subtract (observable) PayPal payments. The two samples comprise all participating victims ($N$=93) and the subsample of interviewed victims ($N$=80).

Models of weekly transaction counts $C_{i,t}$ as outcome, are fitted with a quasi-Poisson distribution (Bolker et al., 2012). This accounts for over-dispersion in the count data, which is caused by the zero-inflation and some high spending weeks. Using the function proposed by Scrucca (2004), we find that the variance is 3.83 times larger than what would be expected without over-dispersion (3.66 times for interviewed victims). Revenue models $R_{i,t}$ are fitted using a linear model with a restricted maximum likelihood procedure (Bates et al., 2015) and binary use models $U_{i,t}$ with a mixed-effects logistic regression. The setup includes twelve different models, all reported in Table 6.10.

**Table 6.10:** Baseline mixed-effects models of credit card avoidance

| | | **Transactions** $C_{i,t}$ | | **Revenue** $R_{i,t}$ | | **Use** $U_{i,t}$ | |
|---|---|---|---|---|---|---|---|
| Effect | Variable | Total | Adjusted | Total | Adjusted | Total | Adjusted |
| Sample: 93 participating victims | | | | | | | |
| | $\beta_0$ | $-0.318^{*}$<br>(0.137) | $-0.399^{**}$<br>(0.140) | $2.138^{***}$<br>(0.162) | $2.065^{***}$<br>(0.161) | $-0.141$<br>(0.202) | $-0.271$<br>(0.201) |
| | *incident* | $-0.228^{***}$<br>(0.069) | $-0.229^{***}$<br>(0.069) | $-0.337^{**}$<br>(0.098) | $-0.339^{**}$<br>(0.096) | $-0.409^{***}$<br>(0.124) | $-0.412^{***}$<br>(0.118) |
| Random | *week* ($\theta_t$) | 0.015 | 0.014 | 0.026 | 0.023 | 0.039 | 0.029 |
| (SD) | *subj.* ($\gamma_i$) | 1.383 | 1.452 | 1.967 | 1.951 | 3.003 | 2.999 |
| Sample: 80 interviewed victims | | | | | | | |
| | $\beta_0$ | $-0.359^{*}$<br>(0.149) | $-0.378^{*}$<br>(0.148) | $2.101^{***}$<br>(0.175) | $2.058^{***}$<br>(0.173) | $-0.186$<br>(0.220) | $-0.243$<br>(0.214) |
| | *incident* | $-0.204^{**}$<br>(0.070) | $-0.214^{**}$<br>(0.069) | $-0.290^{**}$<br>(0.098) | $-0.291^{**}$<br>(0.099) | $-0.344^{**}$<br>(0.123) | $-0.354^{**}$<br>(0.121) |
| Random | *week* ($\theta_t$) | 0.013 | 0.012 | 0.020 | 0.021 | 0.026 | 0.022 |
| (SD) | *subj.* ($\gamma_i$) | 1.432 | 1.406 | 2.042 | 1.992 | 3.159 | 2.993 |

Table 6.10 enables the evaluation of the baseline model for the different samples, types of transaction data, and outcome variables. The incident *incident* is significant at the $p < 0.01$ level for all outcome variables in all models. In principle, results are the same for both samples, but significance levels tend to decrease for the smaller sample of interviewed victims. The consideration of *PayPal-adjusted* transactions marginally increases the $\beta$-coefficient of *incident* in all models. However, without further investigation we deem the pairwise differences ($\Delta\beta \leq 0.01$) as negligible. standard deviations (SDs) are reported for the random effects. The random effect for between subject variation (*subject*) explains substantially more variance, than variation between weeks (*week*). Variation of individual spending is about two orders of magnitude larger than between week variation in all models. We checked for seasonality by including absolute weeks as a fixed effect, but did not observe a seasonal patterns. The normalization of weeks around each individual incident further reduces potential seasonal effects. In summary, the results provide strong evidence that the incident reduces credit card use in the following weeks and that the baseline model captures this effect.

**Correspondence with Self-reported Data** As a robustness check, we test the impact of self-reported credit card use and use intentions (online and offline) on actual transactions. Before including indicators into the LMM model, we impute values for the small portion of missing responses, at most 2.5 % of the cases for a single indicator (see Figure 6.4 and Table 6.6). To avoid list-wise exclusion we impute "<Monthly" for missing use responses and "Never" for missing intentions.

We include different indicators of self-reported behavior and intentions $x_{i,t,2}$ from the survey individually into the LMM, as shown in Equation 6.3 and validate the robustness of the model by an evaluation of the $\beta_2$-coefficients for each individual indicator.

$$y_{i,t} = \beta_0 + incident_{i,t} \times \beta_1 + x_{i,t,2} \times \beta_2 + \theta_t + \gamma_i + \epsilon_{i,t}. \tag{6.3}$$

Table 6.11 reports the $\beta_2$-coefficients of the additional factor for each extended model and demonstrates that self-reported use of the credit card (before the incident) explains actual use for all three outcome variables ($C_{i,t}$, $R_{i,t}$, and $U_{i,t}$). The same holds for self-reported use between the incident and the interview, which was asked only for Internet payments. The behavioral intention to use the new credit card for Internet payments is marginally significant in all three models. The intention to use the new credit card offline has some positive impact, significant at the p<0.1 level for $C_{i,t}$ and $R_{i,t}$. Overall, it is not surprising that actual credit card use is more influenced by self-reported use, than by future use intentions.

**Table 6.11:** Impact of self-reported credit card use and intention on actual credit card use

| | **Use before incident** | | | **Use after incident**$^A$ | | | **Use intention** | | |
|---|---|---|---|---|---|---|---|---|---|
| Variable | $C_{i,t}$ | $R_{i,t}$ | $U_{i,t}$ | $C_{i,t}$ | $R_{i,t}$ | $U_{i,t}$ | $C_{i,t}$ | $R_{i,t}$ | $U_{i,t}$ |
| Internet | $0.459^{***}$ | $0.447^{***}$ | $0.624^{***}$ | $0.699^{***}$ | $0.746^{***}$ | $0.942^{***}$ | $0.648^{**}$ | $0.662^{*}$ | $0.777^{*}$ |
| Offline | $0.456^{***}$ | $0.600^{***}$ | $0.699^{***}$ | - | - | - | $0.368^{\dagger}$ | $0.417^{\dagger}$ | 0.409 |

$^A$Self-reported use after incident and before the interview.

Even though not reported in Table 6.11, the impact of the incident on credit card use (*incident*) is highly significant (p<0.001) in all extended models. An exceptions are intentions to use the new credit card offline (p<0.007) in revenue and binary use models ($R_{i,t}$ and $U_{i,t}$). The expected influence of self-reported behavior and intentions on actual transactions further supports the ability of the baseline model to explain behavioral change after the fraud incident.

### 6.3.3 Combined Model with Explanatory Factors

Additional questions in the telephone interviews enable us to examine why individuals' credit card use changes after the fraud incident. To identify relevant factors we use a two-step strategy. We first select candidates by including factors into the baseline model individually and checking the significance of their impact on credit card use (5 % $\alpha$-level). The approach is the same as in the previous section, formalized in Equation 6.3. In the second step, we test the combination of multiple factors within a single model and exclude unnecessary factors using step-wise exclusion.

**Selection of Candidate Indicators** We consider a total of 18 attitude questions as candidate indicators. All attitudes are measured using Likert scale items with six levels, ranging from "totally disagree" to "totally agree". We interpret missing values as "don't know" responses and impute them as a seventh category in the center of the scale. Thus, we assume that respondents who did not give an answer neither agree nor disagree with a statement. We believe that this approach introduces the smallest bias to our estimates while preserving the sample size. Two attitudes towards the credit card as a payment method (*better reimbursement* and *should use*) are excluded from the analysis due to the high number of missing values (>30 %; see Table 6.7).

We fit models for all three types of credit card use $\{C_{i,t}, R_{i,t}, U_{i,t}\}$ for each candidate, based on total transactions (as opposed to PayPal-adjusted transactions). Responses are interpreted as continuous and casted to binary. Consequently, we fit 120 individual models. Table 6.12 summarizes the results for attitudes towards the credit card as a payment method. Each cell is based on a complete model, but only reports a single $\beta$-coefficient and significance level (for $\beta_2$ in Equation 6.3) for the impact of the respective indicator. Before analyzing the $\beta$-coefficients, we conduct basic sanity checks of the remaining model parts, most importantly, the impact of the incident on credit card use. We find that the impact of the fraud incident on credit card use is always negative and significant (*incident* $\leq -0.204$ with p<0.007 in all models). Accordingly, the inclusion of individual indicators does not fundamentally change the effects in the baseline model.

**Table 6.12:** Impact of attitudes towards the credit card on credit card use

| | **Interval scales** | | | **Binary scales** | | |
|---|---|---|---|---|---|---|
| Attitude | $C_{i,t}$ | $R_{i,t}$ | $U_{i,t}$ | $C_{i,t}$ | $R_{i,t}$ | $U_{i,t}$ |
| *widely accepted* | 0.062 | −0.013 | −0.010 | 0.313 | 0.024 | 0.060 |
| *easier payments* | 0.132 | 0.064 | 0.127 | 0.436 | 0.157 | 0.415 |
| *longer payments* | −0.108 | −0.087 | −0.155 | −0.310 | −0.318 | −0.519 |
| *less secure* | $-0.131^{\dagger}$ | $\mathbf{-0.214}^{**}$ | $\mathbf{-0.217}^{*}$ | −0.402 | $\mathbf{-0.770}^{*}$ | $-0.763^{\dagger}$ |
| *inexpensive* | $0.133^{\dagger}$ | $\mathbf{0.170}^{*}$ | $0.194^{\dagger}$ | 0.462 | 0.521 | 0.626 |
| *o. paym. cheaper* | $\mathbf{-0.149}^{*}$ | $\mathbf{-0.152}^{*}$ | $\mathbf{-0.241}^{**}$ | $-0.510^{\dagger}$ | $-0.582^{\dagger}$ | $\mathbf{-0.848}^{*}$ |
| *overall useful* | $\mathbf{0.216}^{*}$ | $0.182^{\dagger}$ | $\mathbf{0.277}^{*}$ | $0.782^{\dagger}$ | 0.557 | $1.041^{\dagger}$ |
| *cumbersome to try new paym.* | −0.022 | 0.002 | −0.069 | −0.020 | 0.025 | −0.196 |
| *can avoid fraud* | −0.041 | −0.099 | −0.070 | 0.090 | −0.191 | 0.062 |
| *bank prot. fraud* | $0.136^{\dagger}$ | $0.176^{\dagger}$ | $\mathbf{0.233}^{*}$ | $\mathbf{0.743}^{*}$ | $0.765^{\dagger}$ | $\mathbf{1.122}^{*}$ |
| *card only option* | $\mathbf{0.143}^{*}$ | $\mathbf{0.159}^{*}$ | $0.165^{\dagger}$ | $\mathbf{0.620}^{*}$ | $0.647^{\dagger}$ | $0.735^{\dagger}$ |

Responses recorded on Likert scale items (1-6), included as numeric (left) and binary (>3; right). Question wording and descriptives for upper part in Table 6.7 (lower part in Table 6.9).

Five attitude indicators have no significant impact on credit card use, including positive factors (*widely accepted* and *easier payments*), negative factors (*longer payments* and *can avoid fraud*), and rather general statements (*cumbersome to try new paym.*). A reason could be that many statements led to strong agreement, which does not separate respondents in the sample very well by variance at the end of the scale. Six indicators have a significant impact on credit card use on the numeric scale. Negative factors comprise the attitude that the credit card is less secure than other payment methods (*less secure*) and that other payment methods lead to less additional costs (*o. paym. cheaper*). Positive factors incorporate the overall attitude that using the credit card on the Internet has substantive benefits (*overall useful*), that the bank protects their customers from fraud (*bank prot. fraud*), and that the credit card is the only option for some Internet payments (*card only option*). Believing that the credit card is an inexpensive payment method (*inexpensive*) is only marginally significant in the revenue model. The impact measured on binary scales is similar with a tendency towards smaller significance levels.

**Table 6.13:** Impact of the incident interaction with perceptions and attitudes on credit card use

| | **Interval scales** | | | **Binary scales** | | |
|---|---|---|---|---|---|---|
| Variable | $C_{i,t}$ | $R_{i,t}$ | $U_{i,t}$ | $C_{i,t}$ | $R_{i,t}$ | $U_{i,t}$ |
| *well informed* | $-0.182^{\dagger}$ | $-0.254^{\dagger}$ | $-0.292^{\dagger}$ | $-0.528$ | $-0.700$ | $-0.855$ |
| interaction | $\mathbf{0.294}^{***}$ | $\mathbf{0.443}^{***}$ | $\mathbf{0.542}^{***}$ | $\mathbf{0.699}^{***}$ | $\mathbf{1.164}^{***}$ | $\mathbf{1.481}^{***}$ |
| *more concerned* | $-0.083$ | $-0.121^{\dagger}$ | $-0.139$ | $-0.241$ | $-0.364$ | $-0.351$ |
| interaction | $-0.042^{\dagger}$ | $-0.022$ | $-0.027$ | $-0.193^{\dagger}$ | $-0.219$ | $-0.330$ |
| *can protect self* | $-0.033$ | $-0.054$ | $-0.014$ | $-0.301$ | $-0.427$ | $-0.242$ |
| interaction | $0.039^{\dagger}$ | $0.057^{\dagger}$ | $0.063$ | $0.050$ | $0.071$ | $0.014$ |
| *satisfied process* | $-0.129$ | $-0.200$ | $-0.247$ | $-0.554$ | $-0.917$ | $-1.147$ |
| interaction | $\mathbf{0.229}^{***}$ | $\mathbf{0.316}^{***}$ | $\mathbf{0.479}^{***}$ | $\mathbf{0.982}^{***}$ | $\mathbf{1.457}^{***}$ | $\mathbf{2.156}^{***}$ |
| *cumbers. use new cc* | $-0.012$ | $-0.039$ | $-0.011$ | $-0.245$ | $-0.333$ | $-0.249$ |
| interaction | $-0.027$ | $-0.011$ | $-0.041$ | $-0.002$ | $0.041$ | $-0.114$ |
| *shop at trusted webs.* | $-0.065$ | $-0.112$ | $-0.080$ | $-0.224$ | $-0.610$ | $-0.316$ |
| interaction | $-0.012$ | $0.024$ | $0.025$ | $-0.010$ | $0.202$ | $0.324$ |
| *not buy some products* | $-0.019$ | $-0.065$ | $-0.049$ | $0.059$ | $-0.164$ | $0.027$ |
| interaction | $-0.026$ | $0.020$ | $0.019$ | $-0.175$ | $-0.092$ | $-0.130$ |
| *card only option* | $\mathbf{0.160}^{*}$ | $\mathbf{0.177}^{*}$ | $0.183$ | $\mathbf{0.746}^{*}$ | $\mathbf{0.797}^{*}$ | $\mathbf{0.926}^{*}$ |
| interaction | $-0.035$ | $-0.034$ | $-0.034$ | $\mathbf{-0.259}^{*}$ | $-0.289$ | $-0.375$ |
| *can avoid fraud* | $-0.000$ | $-0.053$ | $-0.018$ | $0.209$ | $-0.028$ | $0.266$ |
| interaction | $\mathbf{-0.087}^{***}$ | $\mathbf{-0.087}^{*}$ | $\mathbf{-0.102}^{*}$ | $\mathbf{-0.252}^{*}$ | $-0.314$ | $-0.397$ |

Responses recorded on Likert scale items (1-6), included as numeric (left) and binary (>3; right). Question wording and descriptives for the upper part in Table 6.8 (lower part in Table 6.9).

**Selection of Candidate Indicators with Interaction** The other indicators are directly related to the fraud incident because they concern its perception (upper part of Table 6.13) or attitudes after the incident (lower part of Table 6.13). To account for the relationship with the incident, indicators are included with an interaction term. The inclusion with interactions terms changes the main effects in some models. Therefore, we first check for significant coefficients and than investigate changes in the remaining parts of the relevant models. Table 6.13 shows that three perceptions of the incident are not significant (*more concerned*, *can protect self*, and *cumbers. use new cc*). However, we find highly significant positive impacts of feeling well informed during the fraud dispute handling (*well informed*) and being satisfied with the process (*satisfied process*). Detailed investigation of both models exhibits that the impact of the incident on credit card use remains unchanged (*incident*: $\leq -0.779$ with p<0.001 for all models).

The impact of attitudes after the incident is reported in the lower part of Table 6.13. We include *card only option* and *can avoid fraud* again with an interaction because the question wording explicitly relates to the incident (see Table 6.9). For *card only option* the interaction is not significant, probably indicating that the question was perceived as a general statement by most respondents. However, the interaction term reinforces the positive influence of *card only option* on credit card use. Thinking that fraud can be avoided (*can avoid fraud*) decreases the use of the credit card significantly after the incident. Attitudes towards only shopping (*shop at trusted webs.* and *not buy some products*) have no significant impact on credit card use.

In summary, we select five individual predictors (*bank prot. fraud*, *less secure*, *o. paym. cheaper*, *inexpensive*, and *overall useful*) and four predictors, with an interaction with the incident (*well informed*, *satisfied process*, *card only option*, and *can avoid fraud*), to be included in the combined model. Five of them have a negative and four a positive impact on credit card use. We acknowledge that our choice of an $\alpha$-level of 5 % means that one out of 20 $\beta$-coefficients may lead to an erroneous inclusion of individual predictors. However, the nine identified candidates are significant in multiple models. Moreover, they will be further examined in the combined model, reducing the risk of false inclusion.

**Derivation of the Combined Model** We derive a combined model, using a step-wise exclusion. We start with a "full" model, which includes all nine candidate indicators and remove insignificant indicators successively. We derive the combined model only for revenue models $R_{i,t}$ because they are the main variable on interest. The process is summarized in Table 6.14, which reports (from top to bottom) predictors, interactions, random effects, and fit indicators. We include the information criteria AIC and BIC as well as the pseudo $R^2$ measure, suggested by Nakagawa and Schielzeth (2013), for marginal and conditional $R^2$. Marginal $R^2$ concerns the variance explained by the (fixed) predictors and conditional $R^2$ the variance explained by the combination of predictors and random factors. We use a combination of all model fit criteria to select the best model.

The selection process is documented column-wise (from the left to right) in Table 6.14. In the full model on the very left, only three predictors are significant (*less secure*, and the interaction terms for *well informed* and *can avoid fraud*). Problems are caused by pairwise collinearity between two sets of individual factors, concerning the fraud dispute handling (Models 2a/b: *well informed* and *satisfied process*) and costs of the credit card (Models 4a/b: *o. paym. cheaper* and *inexpensive*). Table C.5 (in the appendix) shows that the absolute pairwise correlations for both sets of factors are exceed 0.5 and are larger than all other correlations. The correlation between similar factors with regard to the security of the credit card (Models 3a/b: *less secure* and *bank prot. fraud*) is only $-0.19$. Due to the similar context, we still examine all the three sets individually to exclude less suitable factors. To do so, we exclude the factors alternately from the model and select the superior factor by looking at AIC and BIC scores. Then, we make a likelihood ratio test (LRT) for the reduced model to check if it differs significantly.

We start with predictors of the fraud dispute handling in Mod2a. The predictor *satisfied process* has a significant impact in the model without *well informed.* The interaction with *incident* significantly increases credit card use after the incident. The same holds, vice versa, for *well informed.* AIC and BIC scores suggest to exclude *satisfied process* from the model and the LRT shows that the reduced model (Mod2b) is not significantly different ($\chi^2$=0.898, df=2, p=0.638). Consequently, we exclude *satisfied process.* Then, we look at security related attitudes. Believing, that the bank protects their customers from fraud (*bank prot. fraud*) is not significant, even if the potential collinear factor *less secure* is excluded from the model (Mod3a). Therefore, we exclude *bank prot. fraud* from the model and only consider *less secure* as a predictor of credit card use (Mod3b). The LRT demonstrates that the reduced model (Mod3b) is not significantly different ($\chi^2$=1.216, df=1, p=0.270). Furthermore, the marginal pseudo-$R^2$ increases in the reduced model. We finally check for the two cost related attitudes, *o. paym. cheaper* and *inexpensive* in Mod4a and Mod4b. If one of them is excluded, the impact of the other one becomes significant. We chose to keep *inexpensive* because it has slightly better AIC and BIC scores and explains more variance. Again, the LRT shows that the reduced model (Mod4b) is not significantly different ($\chi^2$=1.255, df=1, p=0.263).

After removing collinearity, we check the remaining predictors (*overall useful*, *card only option*, *can avoid fraud*). We exclude *overall useful*, as it is not significant in any model. For *card only option*, we remove the interaction term because the interaction is not significant. The BIC score, which values parsimonious models, shows an increase in quality for the final model and the LRT reassures that the reduced model (FinM) is not significantly different ($\chi^2$=0.543, df=1, p=0.762).

The final model (FinM) has five predictors, which explain credit card use in terms of weekly

**Table 6.14:** Step-wise derivation of a combined mixed-effects model

| | | Dispute handling | | Security attitudes | | Cost attitudes | | |
|---|---|---|---|---|---|---|---|---|
| **Variable** | **FullM** | **Mod2a** | **Mod2b** | **Mod3a** | **Mod3b** | **Mod4a** | **Mod4b** | **FinM** |
| *(Intercept)* | 2.799$^{*}$<br>(1.165) | 2.557$^{*}$<br>(1.121) | 2.579$^{*}$<br>(1.141) | 1.769<br>(1.125) | 2.715$^{*}$<br>(1.142) | 3.426$^{**}$<br>(1.050) | 2.321$^{*}$<br>(1.095) | 2.735$^{**}$<br>(0.943) |
| *incident* | −2.372$^{***}$<br>(0.467) | −1.851$^{***}$<br>(0.454) | −2.251$^{***}$<br>(0.431) | −2.251$^{***}$<br>(0.431) | −2.251$^{***}$<br>(0.431) | −2.251$^{***}$<br>(0.431) | −2.251$^{***}$<br>(0.431) | −2.283$^{***}$<br>(0.380) |
| *well informed* | −0.192<br>(0.172) | | −0.288$^{*}$<br>(0.127) | −0.244<br>(0.130) | −0.243$^{*}$<br>(0.121) | −0.241<br>(0.123) | −0.258$^{*}$<br>(0.121) | −0.271$^{*}$<br>(0.120) |
| *can avoid fraud* | −0.002<br>(0.071) | −0.001<br>(0.071) | 0.001<br>(0.071) | −0.059<br>(0.068) | 0.009<br>(0.071) | 0.010<br>(0.072) | 0.007<br>(0.071) | 0.011<br>(0.071) |
| *satisfied process* | −0.135<br>(0.164) | −0.261$^{*}$<br>(0.122) | | | | | | |
| *card only option* | 0.145<br>(0.078) | 0.150<br>(0.078) | 0.151<br>(0.078) | 0.123<br>(0.079) | 0.168$^{*}$<br>(0.076) | 0.169$^{*}$<br>(0.077) | 0.164$^{*}$<br>(0.077) | 0.179$^{*}$<br>(0.070) |
| *bank prot. fraud* | 0.123<br>(0.096) | 0.123<br>(0.096) | 0.099<br>(0.089) | 0.128<br>(0.091) | | | | |
| *less secure* | −0.185$^{*}$<br>(0.082) | −0.187$^{*}$<br>(0.080) | −0.194$^{*}$<br>(0.081) | | −0.207$^{*}$<br>(0.081) | −0.194$^{*}$<br>(0.082) | −0.220$^{**}$<br>(0.081) | −0.231$^{**}$<br>(0.080) |
| *o. paym. cheaper* | −0.083<br>(0.073) | −0.083<br>(0.072) | −0.082<br>(0.073) | −0.106<br>(0.075) | −0.083<br>(0.073) | −0.134$^{*}$<br>(0.065) | | |
| *inexpensive* | 0.101<br>(0.086) | 0.101<br>(0.086) | 0.104<br>(0.087) | 0.077<br>(0.089) | 0.126<br>(0.085) | | 0.171$^{*}$<br>(0.075) | 0.175$^{*}$<br>(0.075) |
| *overall useful* | 0.070<br>(0.095) | 0.069<br>(0.094) | 0.068<br>(0.095) | 0.110<br>(0.097) | 0.070<br>(0.096) | 0.079<br>(0.097) | 0.070<br>(0.096) | |
| Interactions | | | | | | | | |
| *well informed* | 0.399$^{***}$<br>(0.090) | | 0.441$^{***}$<br>(0.063) | 0.441$^{***}$<br>(0.063) | 0.441$^{***}$<br>(0.063) | 0.441$^{***}$<br>(0.063) | 0.441$^{***}$<br>(0.063) | 0.442$^{***}$<br>(0.063) |
| *can avoid fraud* | −0.087$^{*}$<br>(0.036) | −0.089$^{*}$<br>(0.036) | −0.086$^{*}$<br>(0.036) | −0.086$^{*}$<br>(0.036) | −0.086$^{*}$<br>(0.036) | −0.086$^{*}$<br>(0.036) | −0.086$^{*}$<br>(0.036) | −0.087$^{*}$<br>(0.036) |
| *satisfied process* | 0.055<br>(0.082) | 0.316$^{***}$<br>(0.058) | | | | | | |
| *card only option* | −0.006<br>(0.039) | −0.016<br>(0.039) | −0.006<br>(0.039) | −0.006<br>(0.039) | −0.006<br>(0.039) | −0.006<br>(0.039) | −0.006<br>(0.039) | |
| Random effects (variance) | | | | | | | | |
| subject | 1.497 | 1.495 | 1.506 | 1.622 | 1.531 | 1.576 | 1.557 | 1.568 |
| week | 0.019 | 0.018 | 0.019 | 0.019 | 0.019 | 0.019 | 0.019 | 0.019 |
| Model fit | | | | | | | | |
| N | 2160 | 2160 | 2160 | 2160 | 2160 | 2160 | 2160 | 2160 |
| marginal $R^2$ | 0.113 | 0.107 | 0.111 | 0.09 | 0.106 | 0.098 | 0.102 | 0.100 |
| conditional $R^2$ | 0.381 | 0.375 | 0.381 | 0.381 | 0.381 | 0.381 | 0.381 | 0.381 |
| AIC | 9079 | 9094 | 9076 | 9079 | 9075 | 9075 | 9074 | 9071 |
| BIC | 9181 | 9185 | 9167 | 9164 | 9160 | 9155 | 9154 | 9139 |

revenue $R_{i,t}$, in addition to the fraud incident *incident*. Feeling well informed during the fraud process significantly increases credit card use after the incident (*well informed*: 0.442$^{***}$). The effect is reinforced, if the credit card is reported to be the only option for Internet payments (*card only option*: 0.179$^{*}$) and perceived to be generally inexpensive (*inexpensive*: 0.175$^{*}$). Opposing factors are most importantly the incident itself (*incident*: −2.283$^{***}$), but also the attitude that the credit card is less secure than other payment methods (*less secure*: −0.231$^{**}$), and that fraud can be avoided if the credit card is used less online (*can avoid fraud*: −0.087$^{*}$). In summary, we have evidence that security related factors reduce the use of the credit card, while a good customer communication and a lack of (inexpensive) alternatives mitigate the impact.

**Model diagnostics** We make two residual plots to examine model assumptions. The left part of Figure 6.8 shows a fitted vs. residual plot and the right part a Q–Q Plot of the residuals. Both plots illustrate that the residuals are not normally distributed, as is assumed for a LMM. The deviation from normality in the residuals is caused by the high level of zero-inflation in weekly transactions. This is illustrated by the negative line, which forms in the fitted vs. residual plot. In 55 % of all weeks victims did not use their credit card. One measure to counter zero-inflation is further aggregation of observation periods. However, we find that zero-inflation would still be 43 % if credit card use is aggregated for two weeks (35 % for four weeks).

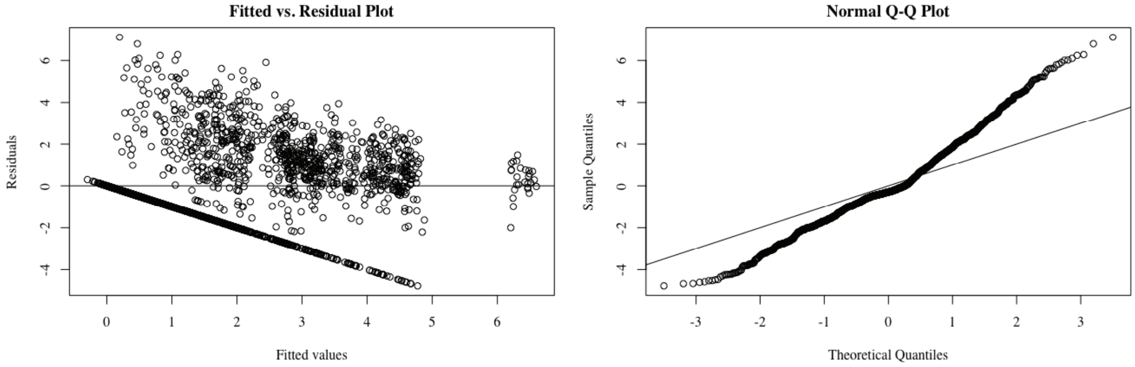


**Figure 6.8:** Average weekly transactions: normalized to incident

The deviation from normality affects the standard errors of the coefficients in the model and potentially biases significance levels. The latter have been calculated with the R package *lmerTest* based on Satterthwate approximations (Kuznetsova et al., 2015). To check the robustness of the significance levels against the backdrop of the non-normal residuals, we bootstrap confidence intervals (CIs) for the coefficients in the final model. We run four individual bootstraps with 10 000 samples, one for every significance level (0.001, 0.01, 0.05, 0.1). CIs are obtained using the percentile method and reported in Table C.6 (in the appendix). We check for every coefficient, at which (upper or lower) confidence level its sign changes. We find that the bootstrap significance levels are the same for most predictors, including: *(Intercept)*, *incident*, *well informed* (and its interaction with *incident*), and *less secure*. Moreover, coefficients are more significant for *card only option* (**), *inexpensive* (**), and the interaction of *can avoid fraud*(**). The results provide support that the effects in our model are significant, despite the non-normal residuals.

**Prediction of lost revenue** We use the final model to predict the average lost revenue per victim and week that can be accounted to the incident. Therefore, we calculate the difference between two predicted outcomes, one with the incident ($incident_{i,t}$=1) and one without the incident ($incident_{i,t}$=0). We set all remaining explanatory variables $x_{i,t,j}$ to the overall average and the random effects $\theta_t$ and $\gamma_i$ to zero. To account for the high variation between customers, we make predictions for three different types: the average customer, a high, and a low spender. We identify high (and low) spenders with 90 % (and 10 %) quantiles of the normal distribution ($\mu$=2.74, $\sigma$=1.21) for between subject variation in the intercept.

For the average customer the incident reduces predicted weekly revenue from € 8.18 to € 6.12, leading to average weekly losses of € 2.06. Over the observation period of 13 weeks predicted average losses add up to € 26.78 per average victim. Average weekly losses are smaller for low spenders (44 cents) and substantially higher for high spenders (€ 9.70). This highlights the importance of a frictionless fraud dispute handling with high spending customers. The aggregated average revenues, illustrated in Figure 6.6, do not show a clear upward trend, indicating that a fraction of the losses will persist after the observation period. This is further supported by the fact that two victims did not order the replacement card and 13 victims did not use the new card after the incident.

## 6.4 Discussion

### 6.4.1 Limitations

A limitation of our study is the lack of control groups. At least two control groups may be relevant. First, customers without credit card replacement and second, customers with ordinary credit card replacement, i. e., for whom the credit card expired. The first group helps to control for unobserved variance in credit card use during the fieldwork. It is less important in our study design, since the long data collection period, which spans more than a year in total, limits the impact of seasonality and the LMM enables the estimation of within-individual trends. The second group enables separation of two potential impacts: the fraud incident and the general inconvenience of credit card replacement. We do not know if some customers drop-out or use the new card less, after ordinary replacement. While we can not control for this, we include a dedicated question into the model: “I think it is cumbersome to use my new credit card everywhere”. Only 7.5 % of the victims totally agree with the statement (55 % totally disagree) and it is not a significant indicator of credit card use in the LMM. This indicates that using the replacement card is not a substantial inconvenience for the customers.

A second limitation is the small sample size. We only managed to recruit 80 victims to participate in the study. While this is a small sample size, it is always difficult to study behavior of cybercrime victims because only a small portion of individuals is affected. Even though we have a small sample we have very detailed information for every individual, including responses in the telephone survey and aggregated transaction data. As the sample reflects customer characteristics at the participating banks, we can derive practical implications.

### 6.4.2 Implications

Our baseline model shows that the replacement of compromised credit cards after fraud incidents leads to less individual credit card use. We find a decrease in different use statistics, including the transaction count, aggregate revenue, and for the binary usage indicator. The combination of standardized interviews with the analysis of actual transaction data allows us to identify and evaluate factors, which influence this individual behavior.

From a theoretical perspective we find that individual security-related attitudes are a key driver in reducing credit card use. In line with our findings for avoidance of online services (in Chapter 5), this highlights the importance of avoidance as security behavior in the context of credit card payments. Furthermore, we can highlight the importance of collecting actual data, wherever possible. Our loss statistics show that consumers tend to over-report losses. And our model results show that behavioral intentions are less accurate in predicting actual behavior compared to self-reported use.

**Management** Our results have practical implications for credit card issuers which help to reduce the negative impact of inevitable fraud incidents. A key measure is the communication with the victims. We find that being well informed during the fraud dispute handling had the strongest positive impact on using the new credit card after the incident. Descriptive statistics show that PLUSCARD is handling this communication very well, as 70 % of the victims totally agree that they were well informed. However, there is still potential to improve the communication. 37 % also strongly agree that they can avoid fraud, if they use their credit card less on the Internet. While this is not necessarily true, it has a significant negative impact on actual credit card use after the incident. An additional information leaflet sent out during the fraud dispute handling may be used to educate customers, on how to behave more securely, while continue using the credit card to the full extent. Currently, almost 30 % strongly disagreed that they understood what happened and are able to protect themselves.

Improving the general image of the security of credit card payments will also increase credit card use. Arguably, this is more difficult to implement for a single issuer. The general attitude that the credit card is less secure proved to be a significant predictor of less credit card transactions. Almost 25 % totally agree that it is less secure than other payment services. This is particularly interesting, since all victims were fully compensated for their losses. Better information on the victim's rights and charge-back options in general and in cases of fraud incidents may reduce this information asymmetry. Currently, more than 30 % of the victims are unaware of their charge-back options.

**Policy Making** Considering the broader (policy) perspective, we discuss our results in light of the revised European Second Payment Services Directive (PSD2). Inter alia, PSD2 aims to make the European payment market more secure, improve consumer rights, and promote the use of innovative payment methods (European Commission, 2015). Its requirements have to be implemented by all EU member states by 13 January 2018. Under PSD2, the liability of consumers for non-authorized payments is reduced and their right for refund is increased. Given the importance of security perceptions, these changes may have a positive impact on credit card use. However, it is important that these improvements are reported to consumers in order to have an impact. Other indicators demonstrate that this process takes time. We find that only 26.2 % of the victims used the new two-factor-authentication method S-ID-Check during the time of the fieldwork. Even though, it is required for card not present transactions under PSD2 and was implemented by PLUSCARD in late 2015.

The removal of surcharges for card payments in PSD2 may be beneficial for credit card issuers, since it makes the credit card more attractive for offline payments. Our results show that more than 40 % of the victims strongly agree that the credit card is the only option for many Internet payments and this attitude is a strong predictor of credit card use before and after the incident. Moreover, the credit card is reported to be the main payment method online by the majority of respondents, even though it is not the preferred one. From the perspective of an issuer it is essential to ensure the wide acceptance of the credit cards by online merchants and its attractiveness for offline payments.

In summary, our results show that communication with fraud victims, customers, and consumers in general are the key measures to increase credit card use. An informative fraud dispute handling can reduce the magnitude of indirect losses after incidents of credit card fraud significantly. Customer and consumer education regarding the security and liabilities of credit card payments can lead to more use in general.

# Chapter 7

# Conclusions

The aim of this dissertation is the robust quantification of the societal impacts of consumer-facing cybercrime. Chapters 2 and 3 lay the foundation. Chapter 2 delineates consumer-facing cybercrime and reviews methods for estimating its societal impacts, and Chapter 3 introduces models to explain individual security behavior, with a focus on avoidance. Based on this, Chapters 4 to 6 report the results of three empirical studies to quantify direct costs and indirect impacts. Chapter 4 discusses robust estimation of the direct costs of a broad range of different types of cybercrime in six EU member states. Chapter 5 develops a theoretical model of individual security behavior, and it provides quantitative evidence of online service avoidance in reaction to cybercrime at the societal level. Finally, Chapter 6 combines actual behavior and self-reported attitudes to estimate the costs of credit card avoidance in reaction to credit card fraud.

This chapter concludes the dissertation with a consolidation of the results in Section 7.1, a summary of evidence-based implications for policy making and business management in Section 7.2, and suggestions for future work in Section 7.3.

## 7.1 Summary of Results

Section 7.1.1 consolidates our results for direct costs. Section 7.1.2 and 7.1.3 summarize the results for indirect impacts due to the avoidance of online services and credit card payments, respectively.

### 7.1.1 Robust Estimation of Direct Costs

Direct costs of consumer-facing cybercrime comprise monetary and non-monetary costs in two categories: victim losses and protection expenses. Chapter 4 studies the robust estimation of direct costs based on primary data, which were collected with a specifically tailored instrument in a representative victimization survey in six EU member states. Several measures were used to prioritize the collection of loss data, including: the representative sampling of Internet users (i. e., excluding the offline population), the conscious oversampling of victims of cybercrime, a reference period of five years, and asking for the severest incident in the case of multiple victimization.

We analyze loss distributions and discuss methodological choices to derive reliable cost figures. Our results offer evidence-based suggestions for the instrument design and robust estimation of costs in the context of cybercrime. Furthermore, they enable a comparative analysis of robust cost figures along multiple dimensions.

**Methodological Choices** We find that the inclusion of malware in victimization surveys is problematic. Our empirical results suggest that many Internet users do not comprehend what a malware infection is, if it is surveyed only with a single question. Since malware is typically used as a tool for other types of cybercrime, such as extortion, it further raises accountability issues when costs should be estimated. Completely excluding malware underestimates the overall costs, ignoring, for example, clean-up and damaged devices. However, its role and comprehension by consumers must be better understood, before it can be reliably included in victimization surveys.

Regarding the estimation of costs, our results reinforce that loss distributions of cybercrime victims are zero-inflated and skewed to the right. Therefore, many victims lose nothing, some lose little, and a few lose substantial amounts. Zero-inflated, log-normal distributions prove to fit the data best. In addition to the results for victim losses, we provide empirical evidence that protection expenses of all consumers have similar, but less extreme, characteristics.

We discuss different indicators to derive robust cost figures and propose a *harmonized loss indicator* (HLI), which scales the conditional distribution-based median of costs by the condition of incurring this cost. The HLI can handle zero-inflation, skewness, and outliers in the distributions, and it proves to be more accurate than sole mean or median-based methods.

**Comparison of Cost Estimates** Among the seven types of cybercrime included in the survey, scams have the severest impact on individual victims, considering monetary and time-related costs. Identity theft of payment-linked accounts leads to the highest initial losses, which are largely compensated by the respective service provider. Incidents in relation to online shopping have the least severe impact on the victims; however, in most countries they are more prevalent than the other types of consumer-facing cybercrime included in our survey.

At the societal level, costs of time are higher than monetary costs. This is reflected not only in the time victims spend dealing with incidents, but also in the time that all consumers spend on protection. Overall, aggregate victim losses are dwarfed by the expenses for protection measures – more than fives times in most countries. As we do not observe all types of cybercrime, including parts of the criminal infrastructure, for example, malware and spam, we can not evaluate the effectiveness of protection expenses and can only speculate that consumers behave with protective intentions.

A comparison of the six countries provides further insights. Despite of the highest protection expenses in Germany and the UK, we also find the highest prevalence and losses in both countries. In Germany, losses are largely driven by scams and extortion, whereas in the UK identity thefts are the primary cause. We conjecture that both countries are highly targeted by criminals because their languages are widespread, and they provide a large pool of comparably wealthy Internet users.

**Cross-checking Results** Our case study of credit card fraud in Chapter 6 enables cross-checks for some of the previous findings. Based on actual loss data, recorded in the fraud detection systems of the credit card issuer, we can confirm that loss distributions of credit card fraud are zero-inflated and skewed to the right. Furthermore, in our sample, all victims who lost money have been reimbursed, which confirms that payment service providers likely compensate victims for losses from cybercrime.

### 7.1.2 Avoidance of Online Services

The avoidance of online services is suspected to form a large part of the overall cost of cybercrime. Chapter 5 provides quantitative evidence of avoidance behavior by individual consumers in response to cybercrime exposure. We develop a theoretical model of individual security behavior and validate it using three pan-European surveys.

**A Model of Individual Security Behavior** Based on a synthesis of different research streams, we postulate a multi-stage model of individual security behavior in reaction to cybercrime exposure. The core of the model adapts the perceived risk-extended Technology Acceptance Model (TAM; Featherman and Pavlou, 2003) to explain the avoidance of online services. Protection behavior is added as another reaction to perceived risk, and both cybercrime experience and media awareness are included as its antecedents. Thus, the model links four forms of *Avoidance Intention* and three forms *Protection Behavior* to the following influencing factors: *Cybercrime Experience*, *Media Awareness*, and *Perceived Cybercrime Risk*. The impact of *Cybercrime Experience* and *Media Awareness* on both outcome variables is proposed to be mediated by *Perceived Cybercrime Risk*. *User Confidence* in online transactions further moderates the effects and the latent variable means.

**Validation at the Societal Level** The model is validated in a latent variable path analysis. We use structural equation modeling in secondary analyses of the Special Eurobarometer on Cyber Security (EB), which is a representative population survey conducted in 2012 in 27 EU member states. The reliability and validity scores indicate better measurement of the *Perceived Cybercrime Risk* construct in comparison to *Cybercrime Experience*. *Media Awareness* could not be reliably measured on the EB data. *Avoidance Intention* is measured for online shopping, online banking, online social networking, and unknown websites. *Protection behavior* is measured by three forms of protection, using anti-virus software, changing security settings, and using different passwords. Approximate goodness-of-fit indexes suggest good fit for the reduced model, without *Media Awareness*.

The availability of more appropriate types of cybercrime as indicators for experience and perceived risk in the third EB wave enabled the evaluation of an improved measurement model in 2014. The good fit confirms the robustness of the model. A trend analysis over all three waves of the EB demonstrates the persistence of structural links from a longitudinal perspective (2012 – 2014). While the study has limitations due to the secondary analysis and the complex sample (discussed in Section 5.5.2), it provides robust results for more than 57 000 EU Internet users.

**Empirical Findings** *Cybercrime Experience* consistently increases *Perceived Cybercrime Risk*, which ultimately leads to the avoidance of online shopping, online banking, and unknown websites. In other words, risk perception fully mediates the impact of experience on avoidance. *Perceived Cybercrime Risk* has a stronger impact on the avoidance of online shopping, compared to online banking. This may be explained by higher levels of uncertainty in online shopping due to dubious merchants. Online banking includes less uncertainty once trust in the bank is established. These conjectures are supported by the persistent avoidance of unknown websites.

Cybercrime does not influence the avoidance of online social networking, as measured in the EB. We believe that the context of the EB survey, rather than the inadequacy of our theoretical model, can explain this result. The EB focuses on security-related types of crime, and it neglects privacy-related issues, which are important for social networking (see discussion on page 81). While online banking and online shopping have a direct link to financial transactions, social networking is a hedonic service used for personal pleasure, and it requires the sharing of information and interaction with others. Other types of crime may consequently be more relevant when studying avoidance of online social networking.

The persistence of effects for online banking and online shopping may contradict the increasing adoption trends for both services. We conjecture that unobserved forms of avoidance explain this contradiction. As avoidance can comprise various actions to evade an undesired end state, consumers may adopt different coping mechanisms and strategies to protect themselves (Liang and Xue, 2009). This calls for a clear conceptualization of online service avoidance, similar to the work by Recker

(2016) for information systems (IS) discontinuance. Our extension of the original research model makes a first contribution by demonstrating that the avoidance of unknown websites is one possible coping mechanism.

The moderation analysis suggests that the strength of the effects in our model is not driven by unobserved variance in Internet users' confidence during online transactions. Differences are found in the factor means, since confident Internet users perceive significantly less cybercrime risk, and they are less likely to change their online behavior, even though they report more cybercrime experience. The higher level of experience found for confident users can be explained by different usage patterns: using the Internet more frequently increases their chances of becoming victimized, and also their ability to identify cybercriminal attacks. By contrast, unconfident users perceive more cybercrime risk, and they demonstrate a higher intention to avoid online banking or online shopping. We believe that this discrepancy can be explained by missing factors in the model, i. e., media awareness or other social influences, which increase perceived risk.

*Protection Behavior* is not influenced by *Perceived Cybercrime Risk*; however, two forms – using different passwords and changing security settings – are directly triggered by *Cybercrime Experience.*

**Summary** Taking a step back, the prevalence of cybercrime and the persistence of aggregate avoidance effects emphasize the importance of studying individual security behavior at the societal level. IS scholars should shift the focus of avoidance studies from customers avoiding a particular vendor to the population of all Internet users avoiding a technology in general. This shift requires dedicated models and a clearer conceptualization of online service avoidance as a behavioral construct. We suggest next steps in Section 7.3.

### 7.1.3 Avoidance of Credit Card Payments

The estimation of costs due to avoidance behavior is possible at the micro level. Chapter 6 supplements the societal perspective in Chapters 4 and 5 with a study of the avoidance of credit card payments after an incident of credit card fraud.

**Study Design** We develop a study design, which is integrated into the credit card replacement process after a fraud incident in the form of a natural experiment. In cooperation with PLUSCARD, a German payment card processor, we record weekly aggregates of transaction counts and revenue for 93 fraud victims, three months before and after the incident. In addition, PLUSCARD collects attitudes, intentions, and self-reported behavior with telephone interviews using a specifically developed questionnaire. The collected data provides the rare opportunity of combining the longitudinal measurement of actual behavior with different attitudes affecting this behavior. We combine both types of data in a linear mixed-effects model (LMM). Building on the complete longitudinal data set, the LMM analysis isolates the impact of the incident from random variation between different weeks and victims. Furthermore, it allows for the inclusion of attitudes in the same model.

**Results** Our results provide strong evidence that some victims of credit card fraud avoid credit card payments after an incident. We find a reduction of overall weekly transactions and revenues in the weeks after the incidents, and in the telephone interviews about 20 % of the victims reported that they are using their new credit card less. The LMM demonstrates that the impact of the fraud incident on the avoidance of the credit card is significant for transaction counts, revenues, and a binary usage indicator. The model also enables a prediction of average losses for the credit card issuer in terms of lost revenue. We find that the incident leads to average losses of €2.06 per week and per victim. However, substantial variation exists between victims.

The inclusion of attitudes into the LMM identifies factors that influence avoidance behavior. *Feeling well informed* during the fraud dispute handling significantly increases credit card use after the incident, and the effect is reinforced, if the credit card is reported to be the *only option* for Internet payments and perceived to be generally *inexpensive*. Opposing factors are most importantly the incident itself, as well as the attitude that the credit card is generally *less secure* than other payment methods, and that *fraud can be avoided* if the credit card is used less online.

In summary, the fraud incident and security-related concerns reduce the use of the credit card, while informative customer communication and a lack of alternatives can compensate this effect.

## 7.2 Implications

Based on the consolidated results, we derive key implications with the aim of reducing the societal impact of cybercrime. The first set of implications in Section 7.2.1 concerns policy making and the second set in Section 7.2.2 relates to business management.

### 7.2.1 Policy Making

The implications for policy making comprise evidence-based recommendations for priorities in the fight against consumer-facing cybercrime and actions to reduce its societal impact.

**Fighting Consumer-facing Cybercrime**

- **Law enforcement priorities.** Our results in Section 4.2.3 indicate that policy making and law enforcement should prioritize actions against scams and extortion to reduce direct costs for consumers. The main reason is that the two types of cybercrime have the severest impact on the victims. Second, victims usually cannot refer to a third party, such as their bank, for help. In the words of the routine activity theory, both crimes lack a capable guardian who protects individual consumers (Yar, 2005). The recent increase in extortion with ransomware (e. g., Berr, 2017; August et al., 2017) may be added as a third reason to prioritize actions against it.

- **Country-specific efforts.** Our country-level results in Section 4.3.3 suggest that some countries are targeted more than others. We conjecture that infrastructure, language, and wealth play important roles. Therefore, larger and wealthier countries, such as the UK and Germany, need to devote comparably more money to law enforcement and consumer education.

- **Security incentives of e-commerce websites.** We find that concerned consumers tend to visit websites they already know and trust (Sections 5.3.3 and 5.5.4). In the context of online shopping such dynamics may be in favor of larger providers because a certain (perceived) level of cybercrime limits consumer choices and drives them towards well-known, trusted online brands. This subtle interaction is relevant for economic studies of online market structures aiming to inform policy makers, since the indirect beneficiaries of cybercrime may have few incentives to fight it alone or in joint efforts.

**Reducing the Societal Impact**

- **Importance of time-related costs.** Section 4.2.5 provides empirical evidence that time-related costs are a significant factor of victim losses and protection expenses. Efficient processes to report incidents, the provision of help, and clear instructions regarding effective protection measures can reduce a large part of the costs of cybercrime.

- **Facilitating online service use.** Perceived risk of cybercrime persistently increases the avoidance of online shopping, online banking, and unknown websites (Section 5.4.5). To facilitate online service use, policy makers can establish incentives, such as trustmarks, standards, or security certificates, to foster security investments and encourage clear communication by online service providers. In addition, campaigns to increase the digital literary of consumers can help to reduce avoidance (Section 5.5.4). The campaigns should ensure public awareness about cybercriminal threats, but most importantly, educate consumers to make informed decisions in the online environment.

### 7.2.2 Business Management

Our main implications for business management concern measures to increase use of technologies, similar to the former implication for policy making.

#### Increasing Adoption and Use

- **Increasing the confidence of consumers.** Our discussion in Section 5.5.4 demonstrates that online service providers can facilitate the use of their services by implementing clear and easy-to-use user interfaces to support the confidence of consumers. Another obvious action to reduce the perceived risk is to limit victimization by continuously improving defense measures. Most importantly, all actions need to be credibly communicated to ensure that the risk reduction is perceived by large parts of the population.

- **Improving customer communication.** We discuss in Section 6.4.2 that credit card issuers can limit the negative effects of fraud incidents through communication with the victims. An informative fraud dispute handling can reduce the magnitude of indirect losses after incidents of credit card fraud significantly. Information brochures, sent together with the new credit card, may be used to explain to customers what happened and how they can protect themselves while using the credit card.

## 7.3 Future Work

The title of this dissertation already indicates that we only provide a step towards a robust quantification of the societal impact of consumer-facing cybercrime. While we make substantial contributions in several directions, our studies have limitations; many aspects remained unstudied, raising suggestions for future research.

**Cost Estimation** We believe that the direct costs presented in this dissertation cover the central parts of the impact of consumer-facing cybercrime. However, we want to highlight other types of impact, which can benefit from a more robust measurement. This concerns opportunity costs and impact on life and health (Anderson, 1999). Many cybercriminals are smart people, who could contribute to society with positive innovations. Therefore, opportunity costs for their lost productivity may be very high, at least in some countries. Moreover, issues of life and health may become more important in the future, if computers and digital devices are increasingly linked to the physical world. Regardless of the types of costs, we encourage researchers to cooperate with industry and other organizations to advance methods and, more importantly, gain access to empirical data.

**Models of Online Service Avoidance** The limitations in our validation of the model of avoidance behavior suggest many opportunities for future research. The scales in the EB surveys led to the exclusion of the media awareness construct from the empirical analysis. We suggest defining a dedicated cybercrime awareness construct, possibly derived from the technical awareness construct that Dinev and Hu (2007) introduced, and testing the research model on primary data. Similar extensions concern the inclusion of original, positive TAM factors. As consumers consider benefits and risks during the adoption process, a complete model, including *Perceived Ease-of-use* and *Perceived Usefulness*, should be tested to assess the predictive power of our research model.

Another direction is the consideration of national differences. Several authors demonstrate the importance of cultural aspects when studying technology acceptance (e. g., Jarvenpaa et al., 1999; Im et al., 2011) and security behavior (e. g., Dinev et al., 2009). While we incorporate a longitudinal repetition, consumer reactions to cybercrime may also be compared between countries to gain a more comprehensive understanding of cultural differences.

A long-term goal must be the refinement and validation of models to predict cybercrime impact on online service avoidance and ultimately indirect cybercrime costs. Primary data should be collected at the societal level to evaluate these models. Such model would be extremely valuable for understanding the cybercrime problem and justifying expenses for countermeasures. In the best case, they can be validated with actual behavioral data.

**Prediction of Credit Card Avoidance** We believe that three directions for further work are most promising in the context of credit card avoidance. The first direction for future work follows from the limitations of our study, summarized in Section 6.4.1. The introduction of control groups, with ordinary credit card replacement and without credit card replacement, can underline our results. Moreover, conducting the survey on a rolling basis can provide stronger longitudinal evidence.

The second direction involves a refinement of our model for a more precise customer-relationship management. A cluster analysis could separate all victims into different customer segments, for example, high and low spenders or the mainly online versus offline users. Based on the clusters, more accurate predictions can be made for each group, and cost mitigation efforts can be focused on groups with the highest impact. This would require larger sample sizes, depending on the number of customer segments.

A third avenue for future work is the consideration of additional information about the incident in the model. The severity of the incident may be explicitly modeled by including additional costs of the victims, the time lost in dealing with the incident, or the money that was attempted to be stolen (as a ratio of the total revenues). Sophisticated modeling of the characteristics of the incident may further improve the predictive power of the model.

# Bibliography

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50(2), pp. 179–211.

Ajzen, I. (2015). Consumer Attitudes and Behavior: The Theory of Planned Behavior Applied to Food Consumption Decisions. *Rivista di Economia Agraria*, 70(2), pp. 121–138.

Ajzen, I. and Driver, B. L. (1992). Application of the Theory of Planned Behavior to Leisure Choice. *Journal of Leisure Research*, 24(3), pp. 207–224.

Ajzen, I. and Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behaviour.* Prentice-Hall, New Jersey, USA.

Alarcón-del Amo, M.-d.-C., Lorenzo-Romero, C., and Del Chiappa, G. (2014). Adoption of Social Networking Sites by Italian. *Information Systems and E-Business Management*, 12(2), pp. 165–187.

Alkaabi, A., Mohay, G., McCullagh, A., and Chantler, N. (2011). Dealing with the Problem of Cybercrime. In: Baggili, I., (ed.), *Digital Forensics and Cyber Crime*, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (vol. 53), pp. 1–18, Springer, Berlin, Heidelberg.

Alshalan, A. (2006). *Cyber-Crime Fear and Victimization: An Analysis of a National Survey.* Dissertation, Mississippi State University.

Altenhoven, T. (2017). Average Age of the Population Down to 44 Years and 3 Months in 2015. Press Release 197 Statistisches Bundesamt. URL: `www.destatis.de/EN/PressServices/Press/pr/2017/06/PE17_197_12411.html`.

Amichai-Hamburger, Y. and Hayat, Z. (2011). The Impact of the Internet on the Social Lives of Users: A Representative Sample from 13 Countries. *Computers in Human Behavior*, 27(1), pp. 585–589.

Anderson, C. L. and Agarwal, R. (2010). Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, 34(3), pp. 1–15.

Anderson, D. A. (1999). The Aggregate Burden of Crime. *The Journal of Law & Economics*, 42(2), pp. 611–642.

Anderson, D. A. (2012). The Cost of Crime. *Foundations and Trends in Microeconomics*, 7(3), pp. 209–265.

Anderson, J. C. and Gerbing, D. W. (1988). Structural Equation Modeling in Practice: A Review and Recommended Two-step Approach. *Psychological Bulletin*, 103(3), pp. 411–423.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Eeten, M. J. G., Levi, M., Moore, T., and Savage, S. (2013). Measuring the Cost of Cybercrime. In: Böhme, R., (ed.), *Economics of Information Security and Privacy*, pp. 265–300. Springer, Berlin, Germany.

Anderson, R., Böhme, R., Clayton, R., and Moore, T. (2008). Security Economics and the Internal

Market. *Study Commissioned by European Union Agency for Network and Information Security (ENISA)*. URL: www.enisa.europa.eu/publications/archive/economics-sec.

Arachchilage, N. A. G. and Love, S. (2014). Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective. *Computers in Human Behavior*, 38(0), pp. 304–312.

Arief, B. and Adzmi, M. A. B. (2015). Understanding Cybercrime from Its Stakeholders' Perspectives: Part 2 – Defenders and Victims. *IEEE Security & Privacy*, 13(2), pp. 84–88.

Arief, B., Adzmi, M. A. B., and Gross, T. (2015). Understanding Cybercrime from Its Stakeholders' Perspectives: Part 1 – Attackers. *IEEE Security & Privacy*, 13(1), pp. 71–76.

August, T., Dao, D., Laube, S., and Niculescu, M. (2017). Economics of Ransomware Attacks. In: *Proceedings of the Workshop on Information Systems and Economics (WISE)*, p. accepted, Seoul, Korea.

Bagozzi, R. P. (2007). The Legacy of the Technology Acceptance Model and a Proposal for a Paradigm Shift. *Journal of the Association for Information Systems*, 8(4), pp. 244–254.

Barn, R. and Barn, B. (2016). An Ontological Representation of a Taxonomy for Cybercrime. In: *Proceedings of the 24th European Conference on Information Systems (ECIS)*, Istanbul, Turkey.

Bates, D., Mächler, M., Bolker, B., and Walker, S. (2015). Fitting Linear Mixed-effects Models Using lme4. *Journal of Statistical Software*, 67(1), pp. 1–48.

Bauer, R. A. (1960). Consumer Behavior as Risk Taking. In: Hancock, R. S., (ed.), *Dynamic Marketing for a Changing World, Proceedings of the 43rd Conference of the American Marketing Association Chicago*, pp. 389–398.

Becker, G. S. (1976). *The Economic Approach to Human Behavior*. University of Chicago Press, Chicago, USA.

Benbasat, I. and Barki, H. (2007). Quo vadis TAM? *Journal of the Association for Information Systems*, 8(4), pp. 211–218.

Bentler, P. M. (1990). Comparative Fit Indexes in Structural Models. *Psychological Bulletin*, 107(2), pp. 238–46.

Bernal, J. L., Cummins, S., and Gasparrini, A. (2017). Interrupted Time Series Regression for the Evaluation of Public Health Interventions: A Tutorial. *International Journal of Epidemiology*, 46(1), pp. 348–355.

Berr, J. (2017). "WannaCry" Ransomware Attack Losses Could Reach $4 Billion. *CBS News*. URL: www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses.

Bidgoli, M. and Grossklags, J. (2016). End User Cybercrime Reporting: What We Know and What We Can Do to Improve it. In: *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, pp. 1–6.

Bilge, L., Sen, S., Balzarotti, D., Kirda, E., and Kruegel, C. (2014). Exposure: A Passive DNS Analysis Service to Detect and Report Malicious Domains. *ACM Transactions on Information System Security*, 16(4), pp. 1–28.

Blume, L. E. and Easley, D. (2008). Rationality. In: Durlauf, S. and Blume, L. E., (eds.), *The New Palgrave Dictionary of Economics*, pp. 856–901. Palgrave Macmillan, London, United Kingdom, 2nd edition.

Böhme, R., Laube, S., and Riek, M. (2018). A Fundamental Approach to Cyber Risk Analysis. *Variance*, 11(2), pp. in press.

Böhme, R. and Moore, T. (2012). How Do Consumers React to Cybercrime? In: *7th APWG eCrime Research Summit*, pp. 1–12, Las Croabas, Puerto Rico.

Bolker, B., Skaug, H., Magnusson, A., and Nielsen, A. (2012). Getting Started with the GlmmADMB Package. R Package Version: 0.8.3.3. URL: https://r-forge.r-project.org/scm/viewvc.php/*checkout*/pkg/inst/doc/glmmADMB.pdf?root=glmmadmb.

Box, G. E. P. and Pierce, D. A. (1970). Distribution of Residual Autocorrelations in Autoregressive-integrated Moving Average Time Series Models. *Journal of the American Statistical Association*, 65(332), pp. 1509–1526.

Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Crime, Media, and Popular Culture. Praeger, Santa Barbara, USA.

Brynjolfsson, E. (1996). The Contribution of Information Technology to Consumer Welfare. *Information Systems Research*, 7(3), pp. 281–300.

Brynjolfsson, E., Smith, M. D., and Hu, Y. J. (2003). Consumer Surplus in the Digital Economy: Estimating the Value of Increased Product Variety at Online Booksellers. *Management Science*, 49(11), pp. 1580–1596.

BSA (2015). EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace. Technical Report, Business Software Alliance, Washington, D.C., USA. URL: `http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf`.

Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., and Courtney, J. F. (2015). Assessing the Role of Security Education, Training, and Awareness on Insiders' Security-related Behavior: An Expectancy Theory Approach. In: *Proceedings of the 48th Hawaii International Conference on System Sciences (HICSS)*, pp. 3930–3940.

Burns, S. and Roberts, L. (2013). Applying the Theory of Planned Behaviour to Predicting Online Safety Behaviour. *Crime Prevention & Community Safety*, 15(1), pp. 48–64.

Byrne, B. M., Shavelson, R. J., and Muthén, B. (1989). Testing for Equivalence of Factor Covariance and Mean Structures: The Issue of Partial Measurement Invariance. *Psychological Bulletin*, 105(3), pp. 456–466.

Calhoun, C. (2002). *Dictionary of the Social Sciences*. Oxford University Press, Oxford, United Kingdom.

Canty, A. and Ripley, B. D. (2017). Boot: Bootstrap R (S-Plus) Functions. R Package Version: 1.3-19. URL: `https://cran.r-project.org/web/packages/boot/boot.pdf`.

Cardona, M., Kretschmer, T., and Strobel, T. (2013). ICT and Productivity: Conclusions from the Empirical Literature. *Information Econonomics and Policy*, 25(3), pp. 109–125.

Castells, M. (2008). The Network Society and Organizational Change. In: *Manuel Castells Interview: Conversations with History*, pp. 1–6. Institute of International Studies, University of California, Berkeley, USA.

Castells, M. (2009). *The Rise of the Network Society: The Information Age: Economy, Society, and Culture Volume I, 2nd Edition with a New Preface*. Wiley-Blackwell, New Jersey, USA.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, 9(1), pp. 70–104.

Cenfetelli, R. T. and Schwarz, A. (2011). Identifying and Testing the Inhibitors of Technology Usage Intentions. *Information Systems Research*, 22(4), pp. 808–823.

Chakravorti, S. (2003). Theory of Credit Card Networks: A Survey of the Literature. *Review of Network Economics*, 2(2), pp. 50–68.

Chang, M. K. (1998). Predicting Unethical Behavior: A Comparison of the Theory of Reasoned Action and the Theory of Planned Behavior. *Journal of Business Ethics*, 17(16), pp. 1825–1834.

Chang, M. K., Cheung, W., and Lai, V. S. (2005). Literature Derived Reference Models for the Adoption of Online Shopping. *Information & Management*, 42(4), pp. 543–559.

Chen, R. and He, F. (2003). Examination of Brand Knowledge, Perceived Risk and Consumers' Intention to Adopt an Online Retailer. *Total Quality Management & Business Excellence*, 14(6), pp. 677–693.

Chen, Y. and Zahedi, F. M. (2016). Individual's Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. *MIS Quarterly*, 40(1), pp. 205–222.

Cheney, J. S. (2010). Heartland Payment Systems: Lessons Learned from a Data Breach. FRB of Philadelphia - Payment Cards Center Discussion Paper No. 10-1. Available at SSRN: https://dx.doi.org/10.2139/ssrn.1540143.

Cheng, T. C. E., Lam, D. Y. C., and Yeung, A. C. L. (2006). Adoption of Internet Banking: An Empirical Study in Hong Kong. *Decision Support Systems*, 42(3), pp. 1558–1572.

Chiricos, T., Padgett, K., and Gertz, M. (2000). Fear, TV News, and the Reality of Crime. *Criminology*, 38(3), pp. 755–786.

Chiu, C.-M., Wang, E. T. G., Fang, Y.-H., and Huang, H.-Y. (2014). Understanding Customers' Repeat Purchase Intentions in B2C E-commerce: The Roles of Utilitarian Value, Hedonic Value and Perceived Risk. *Information Systems Journal*, 24(1), pp. 85–114.

Claar, C. L. and Johnson, J. (2012). Analyzing Home PC Security Adoption Behavior. *Journal of Computer Information Systems*, 52(4), pp. 20–29.

Clough, J. (2015). *Principles of Cybercrime.* Cambridge University Press, Cambridge, United Kingdom, 2nd edition.

Cohen, L. E. and Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4), pp. 588–608.

Council of Europe (2001). Convention on Cybercrime. ETS No. 185. Council of Europe. URL: www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

Council of Europe (2017). Chart of Signatures and Ratifications of Treaty 185. URL: www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

Craig, P., Cooper, C., Gunnell, D., Haw, S., Lawson, K., Macintyre, S., Ogilvie, D., Petticrew, M., Reeves, B., Sutton, M., and Thompson, S. (2012). Using Natural Experiments to Evaluate Population Health Interventions: New Medical Research Council Guidance. *Journal of Epidemiology Community Health*, pp. 1182–1186.

Cunningham, S. M. (1967). The Major Dimensions of Perceived Risk. In: Cox, D. F., (ed.), *Risk Taking Information Handling Consumer Behavior*, pp. 82–111. Harvard Business School Press, Boston, USA.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3), pp. 319–340.

Delignette-Muller, M. L. and Dutang, C. (2015). Fitdistrplus: An R Package for Fitting Distributions. *Journal of Statistical Software*, 64(4), pp. 1–34.

Denning, D. E. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In: Arquilla, J. and Ronfeldt, D., (eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy*, pp. 239–288. Rand Santa Monica, USA.

Destatis (2016). Datenreport 2016: Ein Sozialbericht für die Bundesrepublik Deutschland. Technical Report, Statistisches Bundesamt, Wiesbaden, Germany. URL: www.destatis.de/DE/Publikationen/Datenreport/Downloads/Datenreport2016.pdf.

Dinev, T., Goo, J., Hu, Q., and Nam, K. (2009). User Behaviour Towards Protective Information Technologies: The Role of National Cultural Differences. *Information Systems Journal*, 19(4), pp. 391–412.

Dinev, T. and Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention Toward Protective Information Technologies. *Journal of the Association for Information Systems*, 8(7), pp. 386–408.

Dolan, P., Loomes, G., Peasgood, T., and Tsuchiya, A. (2005). Estimating the Intangible Victim Costs of Violent Crime. *British Journal of Criminology*, 45(6), pp. 958–976.

Dolan, P. and Peasgood, T. (2007). Estimating the Economic and Social Costs of the Fear of Crime. *British Journal of Criminology*, 47(1), pp. 121–132.

Duan, N., Manning, W. G., Morris, C. N., and Newhouse, J. P. (1983). A Comparison of Alternative Models for the Demand for Medical Care. *Journal of Business & Economic Statistics*, 1(2), pp. 115–126.

Dutta, K. and Perry, J. (2006). A Tale of Tails: An Empirical Analysis of Loss Distribution Models for Estimating Operational Risk Capital. Federal Reserve Bank of Boston Working Paper. No. 6-13. Available at SSRN: `https://dx.doi.org/10.2139/ssrn.918880`.

EB77.2 (2012). Special Eurobarometer 390 Cyber Security. Wave EB77.2. European Commission. URL: `http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf`.

EB79.4 (2013). Special Eurobarometer 404 Cyber Security. Wave EB79.4. European Commission. URL: `http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf`.

EB82.2 (2015). Special Eurobarometer 423 Cyber Security. Wave EB82.2. European Commission. URL: `http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf`.

ECB (2014). Card Payments in Europe - A Renewed Focus on SEPA for Cards. Technical Report, European Central Bank. URL: `www.ecb.europa.eu/pub/pdf/other/cardpaymineu_renfoconsepaforcards201404en.pdf`.

ECC (2012). Der Internet-Zahlungsverkehr aus Sicht der Verbraucher in D-A-CH - Ergebnisse der Umfrage IZV11. Technical Report, E-Commerce-Center am IFH Köln, Köln, Germany. URL: `www.ifhshop.de/media/pdf/6e/83/7f/Der-Internet-Zahlungsverkehr-aus-Sicht-der-Verbraucher-in-D-A-CH_2013_Summary.pdf`.

Edwards, B., Hofmeyr, S., and Forrest, S. (2016). Hype and Heavy Tails: A Closer Look at Data Breaches. *Journal of Cybersecurity*, pp. 3–14.

Egelman, S., Cranor, L. F., and Hong, J. (2008). You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 1065–1074.

Emigh, A. (2006). The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond. *Journal of Digital Forensic Practice*, 1(3), pp. 245–260.

European Commission (2007). Towards a General Policy on the Fight Against Cyber Crime (SEC(2007) 641). European Commission. URL: `http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14560`.

European Commission (2015). Directive (EU) 2015/2366 of the European Parliament and of the Council of 25th November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and Repealing Directive 2007/64/EC. *Official Journal of the European Union.*

Europol (2017). Massive Blow to Criminal Dark Web Activities After Globally Coordinated Operation. *Europol Press Release.* URL: `www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation`.

Faqih, K. M. S. (2011). Integrating Perceived Risk and Trust with Technology Acceptance Model: An Empirical Assessment of Customers' Acceptance of Online Shopping in Jordan. In: *Research and Innovation in Information Systems (ICRIIS)*, pp. 1–5.

Farwell, J. P. and Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, 53(1), pp. 23–40.

Featherman, M. S. and Fuller, M. (2003). Applying TAM to E-Services Adoption: The Moderating Role of Perceived Risk. In: *Proceedings of the 36th Hawaii International Conference Systems Sciences (HICSS)*.

Featherman, M. S., Miyazaki, A. D., and Sprott, D. E. (2010). Reducing Online Privacy Risk to Facilitate E-service Adoption: The Influence of Perceived Ease of Use and Corporate Credibility. *Journal of Service Marketing*, 24(3), pp. 219–229.

Featherman, M. S. and Pavlou, P. (2003). Predicting E-services Adoption: A Perceived Risk Facets Perspective. *International Journal of Human-Computer Studies*, 59(4), pp. 451–474.

Ferraro, K. F. and LaGrange, R. (1987). The Measurement of Fear of Crime. *Sociological Inquiry*, 57(1), pp. 70–97.

Finney, S. J. and DiStefano, C. (2006). Non-normal and Categorical Data in Structural Equation Modeling. In: Hancock, G. R. and Mueller, R. O., (eds.), *Structural Equation Modeling a Second Course*, pp. 269–314. Greenwich: Information Age, Charlotte, USA.

Fishbein, M. and Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research.* Addison-Wesley Series in Social Psychology, Boston, USA.

Flatley, J. (2017). Crime in England and Wales: Year Ending Sept 2016. Technical Report, Office for National Statistics, London, United Kingdom. URL: `www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingsept2016`.

Florêncio, D. and Herley, C. (2013). Sex, Lies and Cyber-crime Surveys. In: Schneier, B., (ed.), *Economics of Information Security and Privacy III*, pp. 35–53. Springer, New York, USA.

Florêncio, D., Herley, C., and Shostack, A. (2014). FUD: A Plea for Intolerance. *Communication of the ACM*, 57(6), pp. 31–33.

Floyd, D. L., Prentice-Dunn, S., and Rogers, R. W. (2000). A Meta-analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, 30(2), pp. 407–429.

Fok, C. C., David, H., and James, A. (2015). Research Designs for Intervention Research with Small Samples II: Stepped Wedge and Interrupted Time-series Designs. *Prevention Science*, 16(7), pp. 967–977.

Fornell, C. and Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, 18(1), pp. 39–50.

Francesco Riccardi (2014). Il Salario Minimo Orario – Facile a Dirsi, Difficile a Farsi. *Avvenire.* URL: `www.avvenire.it/opinioni/pagine/salario-minimo-orario-difficile-a-farsi`.

Franklin, J., Perrig, A., Paxson, V., and Savage, S. (2007). An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants. In: *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS)*, pp. 375–388, New York, USA.

Gainey, R., Alper, M., and Chappell, A. T. (2010). Fear of Crime Revisited: Examining the Direct and Indirect Effects of Disorder, Risk Perception, and Social Capital. *American Journal of Criminal Justice*, 36(2), pp. 120–137.

Gartner (2017). Business Impact of Security Incidents and Evolving Regulations Driving Market Growth. *Gartner Press Release.* URL: `http://www.gartner.com/newsroom/id/3784965`.

Gefen, D., Karahanna, E., and Straub, D. W. (2003). Trust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly*, 27(1), pp. 51–90.

Gefen, D. and Straub, D. W. (2000). The Relative Importance of Perceived Ease of Use in IS Adoption: A Study of E-commerce Adoption. *Journal of the Association for Information Systems*, 1(1), pp. 1–30.

Gibson, W. (1987). *Burning Chrome.* Ace Books, New York, USA.

Gigerenzer, G. and Goldstein, D. G. (1996). Reasoning the Fast and Frugal Way: Models of Bounded Rationality. *Psychological Review*, 103(4), pp. 650–669.

Giovanis, A. N., Binioris, S., and Polychronopoulos, G. (2012). An Extension of TAM Model with IDT and Security/Privacy Risk in the Adoption of Internet Banking Services in Greece. *EuroMed Journal of Business*, 7(1), pp. 24–53.

Godin, G. and Kok, G. (1996). The Theory of Planned Behavior: A Review of its Applications to Health-related Behaviors. *American Journal of Health Promotion*, 11(2), pp. 87–98.

Goldman, R. (2017). What We Know and Don't Know About the International Cyberattack. *The New York Times*. URL: `www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html`.

Goodman, M. D. (1996). Why the Police Don't Care about Computer Crime. *Harvard Journal of Law & Technology*, 10(3), pp. 465–494.

Goodman, M. D. and Brenner, S. W. (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law and Information Technology*, 10(2), pp. 139–223.

Gordon, S. and Ford, R. (2006). On the Definition and Classification of Cybercrime. *Journal in Computer Virology*, 2(1), pp. 13–20.

Graves, J. T., Acquisti, A., and Christin, N. (2014). Should Payment Card Issuers Reissue Cards in Response to a Data Breach? In: *Workshop on the Economics of Information Security (WEIS)*, The Pennsylvania State University, State College, USA.

Hair, J. F. (2010). *Multivariate Data Analysis (7th Edition)*. Prentice-Hall, New Jersey, USA.

Hale, C. (1996). Fear of Crime: A Review of the Literature. *International Review of Victimology*, 4(2), pp. 79–150.

Hanafizadeh, P., Keating, B. W., and Khedmatgozar, H. R. (2013). A Systematic Review of Internet Banking Adoption. *Telematics and Informatics*, 31(3), pp. 492–510.

Hanus, B. and Wu, Y. A. (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*, 33(1), pp. 2–16.

Harrell, E. (2015). Victims of Identity Theft, 2014. Bureau of Justice Statistics (BJS). URL: `www.bjs.gov/index.cfm?ty=pbdetail&iid=5408`.

Harrell, E. and Langton, L. (2013). Victims of Identity Theft, 2012. Bureau of Justice Statistics (BJS). URL: `www.bjs.gov/index.cfm?ty=pbdetail&iid=4821`.

Heath, L. and Gilbert, K. (1996). Mass Media and Fear of Crime. *American Behavioral Scienctist*, 39(4), pp. 379–386.

Henry, S. and Einstadter, W. J. (2006). *Criminological Theory: An Analysis of its Underlying Assumptions*. Rowman & Littlefield Publishers, Lanham, USA.

Henseler, J., Ringle, C. M., and Sinkovics, R. R. (2009). The Use of Partial Least Squares Path Modeling in International Marketing. *New Challenges to International Marketing (Advances International Marketing Vol. 20)*, pp. 277–319.

Herley, C. (2009). So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In: *Proceedins of the 2009 Workshop on New Security Paradigms Workshop (NSPW)*, pp. 133–144, New York, USA.

Hernandez-Castro, J. and Boiten, E. (2014). Cybercrime Prevalence and Impact in the UK. *Computer Fraud & Security*, 2014(2), pp. 5–8.

Hoffmann, A. O. I. and Birnbrich, C. (2012). The Impact of Fraud Prevention on Bank-customer Relationships: An Empirical Investigation in Retail Banking. *International Journal of Bank Marketing*, 30(5), pp. 390–407.

Holt, T. J. and Bossler, A. M. (2008). Examining the Applicability of Lifestyle-routine Activities Theory for Cybercrime Victimization. *Deviant Behavior*, 30(1), pp. 1–25.

Holt, T. J. and Bossler, A. M. (2014). An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior*, 35(1), pp. 20–40.

Hsu, M.-H. and Chiu, C.-M. (2004). Internet Self-efficacy and Electronic Service Acceptance. *Decision Support Systems*, 38(3), pp. 369–381.

Hu, L.-t. and Bentler, P. M. (1999). Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria versus New Alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, 6(1), pp. 1–55.

Hunt, E. K. (2015). *History of Economic Thought: A Critical Perspective*. M. E. Sharpe, New York, USA.

Hunton, P. (2009). The Growing Phenomenon of Crime and the Internet: A Cybercrime Execution and Analysis Model. *Computer Law & Security Review*, 25(6), pp. 528–535.

Hyman, P. (2013). Cybercrime: It's Serious, but Exactly How Serious? *Communications of the ACM*, 56(3), pp. 18–20.

Ifinedo, P. (2012). Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers & Security*, 31(1), pp. 83–95.

Im, I., Hong, S., and Kang, M. S. (2011). An International Comparison of Technology Adoption. *Information & Management*, 48(1), pp. 1–8.

Inscoe, S. W. (2012). Global Consumers React to Rising Fraud: Beware Back of Wallet. Technical Report, Aite Group, Boston, USA. URL: `www.aciworldwide.com/-/media/files/collateral/trends/aci-aite-global-consumers-react-to-rising-fraud-1012.pdf`.

Inscoe, S. W. (2014). Global Consumers: Losing Confidence in the Battle Against Fraud. Technical Report, Aite Group, Boston, USA. URL: `www.aciworldwide.com/-/media/files/collateral/trends/2014-global-consumer-fraud-survey---part-1and-2.pdf`.

ITU (2017). ICT Facts and Figures 2017. Technical Report, Internet Telecommunication Union, Geneva, Switzerland. URL: `www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf`.

Jackson, J. (2011). Revisiting Risk Sensitivity in the Fear of Crime. *Journal of Research in Crime and Delinquency*, 48(4), pp. 513–537.

Jansson, K. (2007). *British Crime Survey – Measuring Crime for 25 years*. Home Office, London, United Kingdom.

Jarvenpaa, S. L., Tractinsky, N., and Saarinen, L. (1999). Consumer Trust in an Internet Store: A Cross-cultural Validation. *Journal of Computer-Mediated Communication*, 5(2), pp. 0–0.

Jiao, Y., Yang, J., and Xu, S. (2013). A Study of the Impact of Social Media Characteristics on Customer Adoption Intention of Social Media. In: *International Academic Workshop on Social Science (IAW-SC-13)*, pp. 1095–1099, Paris, France. Atlantis Press.

Johnston, A. C. and Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quaterly*, 34(3), pp. 549–566.

Juvonen, J. and Gross, E. F. (2008). Extending the School Grounds? – Bullying Experiences in Cyberspace. *Journal of School Health*, 78(9), pp. 496–505.

Kahn, C. M. and Liñares-Zegarra, J. M. (2016). Identity Theft and Consumer Payment Choice: Does Security Really Matter? *Journal of Financial Services Research*, 50(1), pp. 121–159.

Kahneman, D. (2003). Maps of Bounded Rationality: Psychology for Behavioral Economics. *The American Economic Review*, 93(5), pp. 1449–1475.

Kahneman, D. and Tversky, A. (1979). Prospect Theory: An Analysis of Decision Under Risk. *Econometrica: Journal of the Econometric Society*, 47(2), pp. 263–291.

Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G. M., Paxson, V., and Savage, S. (2008). Spamalytics: An Empirical Analysis of Spam Marketing Conversion. In: *Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS)*, pp. 3–14.

Kehr, F. and Kowatsch, T. (2015). Quantitative Longitudinal Research: A Review of IS Literature, and a Set of Methodological Guidelines. In: *Proceedings of the 23th European Conference on Information Systems (ECIS)*, Münster, Germany.

Kerr, O. S. (2003). Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *NYU Law Review*, 78(5), pp. 1596–1668.

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., and Kirda, E. (2015). Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. In: Almgren, M., Gulisano, V., and Maggi, F., (eds.), *Detection of Intrusions and Malware, and Vulnerability Assessment: 12th International Conference, DIMVA 2015, Milan, Italy, July 9-10, 2015, Proceedings*, pp. 3–24. Springer International Publishing, New York, USA.

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review*, 30(4), pp. 470–486.

Kline, R. B. (2010). *Principles and Practice of Structural Equation Modeling, Third Edition.* Methodology in the Social Sciences. Guilford Publications.

Knieff, B. (2016). Global Consumer Card Fraud: Where Card Fraud Is Coming From. Technical Report, Aite Group, Boston, USA. URL: `www.aciworldwide.com/-/media/files/collateral/trends/2016-global-consumer-card-fraud-where-card-fraud-is-coming-from.pdf`.

Koops, B.-J. and Leenes, R. (2006). Identity Theft, Identity Fraud and/or Identity-related Crime. *Datenschutz und Datensicherheit*, 30(9), pp. 553–556.

Kosse, A. (2013). Do Newspaper Articles on Card Fraud Affect Debit Card Usage? *Journal of Banking & Finance*, 37(12), pp. 5382–5391.

Krasnova, H., Günther, O., Spiekermann, S., and Koroleva, K. (2009). Privacy Concerns and Identity in Online Social Networks. *Identity in the Information Society*, 2(1), pp. 39–63.

Krebs, B. (2014a). Home Depot: Hackers Stole 53M Email Addresses. *Krebs on Security.* URL: `https://krebsonsecurity.com/2014/11/home-depot-hackers-stole-53m-email-addreses`.

Krebs, B. (2014b). The Target Breach, By the Numbers. *Krebs on Security.* URL: `https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers`.

Krebs, B. (2017). Breach at Equifax May Impact 143M Americans. *Krebs on Security.* URL: `https://krebsonsecurity.com/2017/09/breach-at-equifax-may-impact-143m-americans`.

Kumar, N., Mohan, K., and Holowczak, R. (2008). Locking the Door but Leaving the Computer Vulnerable: Factors Inhibiting Home Users' Adoption of Software Firewalls. *Decision Support Systems*, 46(1), pp. 254–264.

Kuznetsova, A., Brockhoff, P. B., and Christensen, R. H. B. (2015). Package "lmerTest". R Package Version: 2.0. URL: `https://cran.r-project.org/web/packages/lmerTest/index.html`.

Kwon, O. and Wen, Y. (2010). An Empirical Study of the Factors Affecting Social Network Service Use. *Computers in Human Behavior*, 26(2), pp. 254–263.

Kwon, W.-S. and Lennon, S. J. (2009). What Induces Online Loyalty? Online versus Offline Brand Images. *Journal of Business Research*, 62(5), pp. 557–564.

Laube, S. and Böhme, R. (2016). The Economics of Mandatory Security Breach Reporting to Authorities. *Journal of Cybersecurity*, 2(1), pp. 29–41.

Lauritsen, J. L. and Rezey, M. L. (2013). Measuring the Prevalence of Crime with the National Crime Victimization Survey. Bureau of Justice Statistics (BJS). URL: `https://www.bjs.gov/content/pub/pdf/mpcncvs.pdf`.

Law, J. (2015). *A Dictionary of Law.* Oxford University Press, Oxford, United Kingdom.

Lazarus, R. S. (1966). *Psychological Stress and the Coping Process.* McGraw-Hill, New York, USA.

Lee, M.-C. (2009). Factors Influencing the Adoption of Internet Banking: An Integration of TAM and TPB with Perceived Risk and Perceived Benefit. *Electronic Commerce Research and Applications*, 8(3), pp. 130–141.

Lee, Y. and Kozar, K. A. (2008). An Empirical Investigation of Anti-spyware Software Adoption: A Multitheoretical Perspective. *Information and Management*, 45(2), pp. 109–119.

Lee, Y. and Larsen, K. R. (2009). Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-malware Software. *European Journal of Information Systems*, 18(2), pp. 177–187.

Legris, P., Ingham, J., and Collerette, P. (2003). Why Do People Use Information Technology? A Critical Review of the Technology Acceptance Model. *Information & Management*, 40(3), pp. 191–204.

Lessig, L. (1998). The New Chicago School. *The Journal of Legal Studies*, 27(S2), pp. 661–691.

Levchenko, K., Pitsillidis, A., Chachra, N., Enright, B., Félegyházi, M., Grier, C., Halvorson, T., Kanich, C., Kreibich, C., Liu, H., McCoy, D., Weaver, N., Paxson, V., Voelker, G. M., and Savage, S. (2011). Click Trajectories: End-to-end Analysis of the Spam Value Chain. In: *IEEE Symposium on Security and Privacy (SP)*, pp. 431–446.

Levi, M. (2017). Assessing the Trends, Scale and Nature of Economic Cybercrimes: Overview and Issues. *Crime, Law and Social Change*, 67(1), pp. 3–20.

Levi, M. and Burrows, J. (2008). Measuring the Impact of Fraud in the UK: A Conceptual and Empirical Journey. *The British Journal of Criminology*, 48(3), pp. 293–318.

Levi, M., Doig, A., Gundur, R., Wall, D., and Williams, M. (2017). Cyberfraud and the Implications for Effective Risk-based Responses: Themes from UK Research. *Crime, Law and Social Change*, 67(1), pp. 77–96.

Li, Y.-H. and Huang, J.-W. (2009). Applying Theory of Perceived Risk and Technology Acceptance Model in the Online Shopping Channel. *World Academy of Science, Engineering and Technology*, 53(4), pp. 816–822.

Liang, H. and Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, 33(1), pp. 71–90.

Liang, H. and Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, 11(7), pp. 394–413.

Lim, N. (2003). Consumers' Perceived Risk: Sources versus Consequences. *Electronic Commerce Research and Applications*, 2(3), pp. 216–228.

Lin, H.-F. (2006). Understanding Behavioral Intention to Participate in Virtual Communities. *CyberPsychology & Behavior*, 9(5), pp. 540–547.

Lin, K.-Y. and Lu, H.-P. (2011). Why People Use Social Networking Sites: An Empirical Study Integrating Network Externalities and Motivation Theory. *Computers in Human Behavior*, 27(3), pp. 1152–1161.

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 22(3), pp. 365–404.

Liska, A. E. and Baccaglini, W. (1990). Feeling Safe by Comparison: Crime in the Newspaper. *Social Problems*, 37(3), pp. 360–374.

Liska, A. E., Sanchirico, A., and Reed, M. D. (1988). Fear of Crime and Constrained Behavior Specifying and Estimating a Reciprocal Effects Model. *Social Forces*, 66(3), pp. 827–837.

Loewenstein, G. F., Weber, E. U., Hsee, C. K., and Welch, N. (2001). Risk as Feelings. *Psychological Bulletin*, 127(2), pp. 267–286.

Lynn, W. J. (2010). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, 89(5), pp. 97–108.

Mackey, R. (2010). "Operation Payback" Attacks Target MasterCard and PayPal Sites to Avenge WikiLeaks. *The New York Times*. URL: https://thelede.blogs.nytimes.com/2010/12/08/operation-payback-targets-mastercard-and-paypal-sites-to-avenge-wikileaks.

Madden, T. J., Ellen, P. S., and Ajzen, I. (1992). A Comparison of the Theory of Planned Behavior and the Theory of Reasoned Action. *Personality and Social Psychology Bulletin*, 18(1), pp. 3–9.

Martins, C., Oliveira, T., and Popovič, A. (2014). Understanding the Internet Banking Adoption: A Unified Theory of Acceptance and Use of Technology and Perceived Risk Application. *International Journal of Information Management*, 34(1), pp. 1–13.

McAfee and CSIS (2014). Net Losses: Estimating the Global Cost of Cybercrime. Technical Report, McAfee and Center for Strategic and International Studies, Washington, D.C., USA. URL: www.mcafee.com/de/resources/reports/rp-economic-impact-cybercrime2.pdf.

McCoy, D., Pitsillidis, A., Grant, J., Weaver, N., Kreibich, C., Krebs, B., Voelker, G., Savage, S., and Levchenko, K. (2012). Pharmaleaks: Understanding the Business of Online Pharmaceutical Affiliate Programs. In: *USENIX Security 12*, pp. 1–16.

McGarrell, E. F., Giacomazzi, A. L., and Thurman, Q. C. (1997). Neighborhood Disorder, Integration, and the Fear of Crime. *Justice Quarterly*, 14(3), pp. 479–500.

McGuire, M. and Dowling, S. (2013). Cyber Crime: A Review of the Evidence. Technical Report, UK Home Office. URL: www.justiceacademy.org/iShare/Library-UK/horr75-chap1.pdf.

McKnight, D. H., Choudhury, V., and Kacmar, C. (2002). The Impact of Initial Consumer Trust on Intentions to Transact with a Web Site: A Trust Building Model. *Journal of Strategic Information Systems*, 11(3-4), pp. 297–323.

Meade, A. W., Johnson, E. C., and Braddy, P. W. (2008). Power and Sensitivity of Alternative Fit Indices in Tests of Measurement Invariance. *Journal of Applied Psychology*, 93(3), pp. 568–592.

Merton, R. K. (1968). The Matthew Effect in Science. *Science*, 159(3810), pp. 56–63.

Metzger, M. J. (2006). Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. *Journal of Computer-Mediated Communication*, 9(4), pp. 0–0.

Meyer, B. D. (1995). Natural and Quasi-experiments in Economics. *Journal of Business & Economic Statistics*, 13(2), pp. 151–161.

Milan, S. (2013). WikiLeaks, Anonymous, and the Exercise of Individuality: Protesting in the Cloud. In: Brevini, B., Hintz, A., and McCurdy, P., (eds.), *Beyond WikiLeaks*, pp. 191–208. Palgrave Macmillan, London, United Kingdom.

Millsap, R. E. and Yun-Tein, J. (2004). Assessing Factorial Invariance in Ordered-categorical Measures. *Multivariate Behavior Research*, 39(3), pp. 479–515.

Milne, S., Orbell, S., and Sheeran, P. (2002). Combining Motivational and Volitional Interventions to Promote Exercise Participation: Protection Motivation Theory and Implementation Intentions. *British Journal of Health Psychology*, 7(2), pp. 163–184.

Min, Y. and Agresti, A. (2002). Modeling Nonnegative Data with Clumping at Zero: A Survey. *Journal of the Iranian Statistical Society*, 1(1), pp. 7–33.

Modic, D. and Anderson, R. (2015). It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud. *IEEE Security & Privacy*, 13(5), pp. 99–103.

Montazemi, A. R. and Saremi, H. Q. (2013). Factors Affecting Internet Banking Pre-usage Expectation Formation. pp. 4666–4675.

Moore, R. (2010). *Cybercrime: Investigating High-technology Computer Crime*. Elsevier Science, Amsterdam, Netherlands.

Moore, T., Clayton, R., and Anderson, R. (2009). The Economics of Online Crime. *Journal of Economic Perspectives*, 23(3), pp. 3–20.

Morgan, S. (2016). Hackerpocalypse: A Cybercrime Revelation. Technical Report, Cybersecurity Ventures, Menlo Park, USA. URL: `https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016`.

Mulilis, J.-P. and Lippa, R. (1990). Behavioral Change in Earthquake Preparedness Due to Negative Threat Appeals: A Test of Protection Motivation Theory. *Journal of Applied Social Psychology*, 20(8), pp. 619–638.

Muthen, B., Du Toit, S. H. C., and Spisic, D. (1997). Robust Inference Using Weighted Least Squares and Quadratic Estimating Equations in Latent Variable Modeling with Categorical and Continuous Outcomes. *Psychometrika*, 75.

Nakagawa, S. and Schielzeth, H. (2013). A General and Simple Method for Obtaining R2 from Generalized Linear Mixed-effects Models. *Methods in Ecology and Evolution*, 4(2), pp. 133–142.

NCA (2016). Cyber Crime Assessment 2016. Technical Report, National Crime Agency – Strategic Cyber Industry Group, London, United Kingdom. URL: `www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file`.

Ng, B.-Y., Kankanhalli, A., and Xu, Y. C. (2009). Studying Users' Computer Security Behavior: A Health Belief Perspective. *Decision Support Systems*, 46(4), pp. 815–825.

OECD (2014). Long-term Baseline Projections, No. 95. Technical Report, Organisation for Economic Co-operation and Development, Paris, France. URL: `http://dx.doi.org/10.1787/data-00690-en`.

Pavlou, P. A. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce*, 7(3), pp. 69–103.

Pavlou, P. A. and Fygenson, M. (2006). Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior. *MIS Quarterly*, pp. 115–143.

Pechmann, C., Zhao, G., Goldberg, M. E., and Reibling, E. T. (2003). What to Convey in Antismoking Advertisements for Adolescents: The Use of Protection Motivation Theory to Identify Effective Message Themes. *Journal of Marketing*, 67(2), pp. 1–18.

Pinho, J. C. M. R. and Soares, A. M. (2011). Examining the Technology Acceptance Model in the Adoption of Social Networks. *Journal of Research in Interactive Marketing*, 5(2/3), pp. 116–129.

Ponemon Institute (2015). 2015 Cost of Cyber Crime Study: Global. Technical Report, Ponemon Institute, Traverse City, USA. URL: `www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report`.

Pratt, T. C., Holtfreter, K., and Reisig, M. D. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency*, 47(3), pp. 267–296.

PwC (2015). Global State of Information Security Survey. Technical Report, PricewaterhouseCoopers LLP, New York, USA. URL: `www.pwccn.com/en/services/risk-assurance/publications/the-global-state-of-information-security-survey-2016-turnaround-and-transformation-in-cybersecurity.html`.

Rader, N. E., May, D. C., and Goodrum, S. (2007). An Empirical Assessment of the "Threat of Victimization": Considering Fear of Crime, Perceived Risk, Avoidance, and Defensive Behaviors. *Sociological Spectrum*, 27(5), pp. 475–505.

Rand, M. (2006). The National Crime Victimization Survey: 34 Years of Measuring Crime in the United States. *Statistical Journal of the United Nations Economic Commission for Europe*, 23(4), pp. 289–301.

Recker, J. (2016). Reasoning about Discontinuance of Information System Use. *Journal of Information Technology Theory and Application*, 17(1), pp. 41–66.

Reyns, B. W. (2013). Online Routines and Identity Theft Victimization. *Journal of Research in Crime and Delinquency*, 50(2), pp. 216–238.

Rieckmann, J. and Kraus, M. (2015). Tatort Internet: Kriminalität verursacht Bürgern Schäden in Milliardenhöhe. *DIW Wochenbericht*, 82(12), pp. 295–301.

Riek, M., Böhme, R., and Moore, T. (2016). Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transactions on Dependable and Secure Computing*, 13(2), pp. 261–273.

Riffai, M. M. M. A., Grant, K., and Edgar, D. (2012). Big TAM in Oman: Exploring the Promise of On-line Banking, Its Adoption by Customers and the Challenges of Banking in Oman. *International Journal of Information Management*, 32(3), pp. 239–250.

Ringle, C. M., Sarstedt, M., and Straub, D. W. (2012). A Critical Look at the Use of PLS-SEM in MIS Quarterly. *MIS Quarterly*, 36(1), pp. iii–xiv.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *Journal Psychological*, 91(1), pp. 93–114.

Rogers, R. W. (1983). Cognitive and Physiological Process in Fear Appeals and Attitudes Change: A Revised Theory of Protection Motivation. In: Cacioppo, J. T. and Petty, R., (eds.), *Social Psychophysiology*, pp. 153–177. Guilford Press, New York, USA.

Rosenfeld, R. and Weisburd, D. (2016). Explaining Recent Crime Trends: Introduction to the Special Issue. *Journal of Quantitative Criminology*, 32(3), pp. 329–334.

Rosenstock, I. M. (1974). Historical Origins of the Health Belief Model. *Health Education Monographs*, 2(4), pp. 328–335.

Ryan, J. J. and Jefferson, T. I. (2003). The Use, Misuse, and Abuse of Statistics in Information Security Research. In: *Proceedings of the 2003 ASEM National Conference*, St. Louis, USA.

Saban, K. A., McGivern, E., and Saykiewicz, J. N. (2002). A Critical Look at the Impact of Cybercrime on Consumer Internet Behavior. *Journal of Marketing Theory and Practice*, 10(2), pp. 29–37.

Schulten, T. (2015). WSI Minimum Wage Database. Wirtschafts- und Sozialwissenschaftliches Institut (WSI) in der Hans-Böckler-Stiftung. URL: `www.boeckler.de/pdf/ta_mwdb_v0115.pdf`.

Schumacker, R. E. and Lomax, R. G. (2004). *A Beginner's Guide to Structural Equation Modeling*. Lawrence Erlbaum Associates, Mahwah, USA.

Scott, J. (2008). *Rational Choice Theory*, pp. 126–138. SAGE Publications, Thousand Oaks, USA.

Scrucca, L. (2004). An R Package for Quality Control Charting and Statistical Process Control. *R News*, 4(1), pp. 11–17.

Shapiro, C. and Varian, H. R. (1998). *Information Rules: A Strategic Guide to the Network Economy*. Harvard Business School Press, Boston, USA.

Shin, D.-H. (2010). The Effects of Trust, Security and Privacy in Social Networking: A Security-based Approach to Understand the Pattern of Adoption. *Interacting with Computers*, 22(5), pp. 428–438.

Shin, D.-H. and Kim, W.-Y. (2008). Applying the Technology Acceptance Model and Flow Theory to Cyworld User Behavior: Implication of the Web 2.0 User Acceptance. *CyberPsychology & Behavior*, 11(3), pp. 378–382.

Shropshire, J., Warkentin, M., and Sharma, S. (2015). Personality, Attitudes, and Intentions: Predicting Initial Adoption of Information Security Behavior. *Computers & Security*, 49(0), pp. 177–191.

Simon, H. A. (1957). *Models of Man: Social and Rational; Mathematical Essays on Rational Human Behavior in Society Setting.* Wiley, New York, USA.

Singer, J. D. and Willett, J. B. (2003). *Applied Longitudinal Data Analysis: Modeling Change and Event Occurrence.* Oxford University Press, New York, USA.

Skogan, W. G. (1987). The Impact of Victimization on Fear. *Crime & Delinquency*, 33(1), pp. 135–154.

Slovic, P. and Peters, E. (2006). Risk Perception and Affect. *Current Directions in Psychological Science*, 15(6), pp. 322–325.

Smart Card Alliance (2015). The True Cost of Data Breaches in the Payments Industry. Technical Report, Smart Card Alliance, New Jersey, USA. URL: `www.emv-connection.com/downloads/2015/03/The-Cost-of-Data-Breaches.pdf`.

Smith, A. (1827). *An Inquiry into the Nature and Causes of the Wealth of Nations.* Printed at the University Press for T. Nelson and P. Brown, Harvard, USA.

Smith, A. D. (2004). Cybercriminal Impacts on Online Business and Consumer Confidence. *Online Information Review*, 28(3), pp. 224–234.

Somanchi, S. and Telang, R. (2017). Impact of Security Events and Fraudulent Transactions on Customer Loyalty: A Field Study. In: *Workshop on the Economics of Information Security (WEIS)*, University of California, San Diego, USA.

Sommestad, T., Karlzén, H., and Hallberg, J. (2015). A Meta-analysis of Studies on Protection Motivation Theory and Information Security Behaviour. *International Journal of Information Security and Privacy*, 9(1), pp. 26–46.

Srisawang, S., Thongmak, M., and Ngarmyarn, A. (2015). Factors Affecting Computer Crime Protection Behavior. In: *Proceedings of the 19th Pacific Asia Conference on Information Systems (PACIS)*, Marina Bay Sands, Singapore.

Stanton, J. (2015). Payment Card Data Breaches: How Does the Consumer Respond? Technical Report, Lightspeed Research, Warren, USA.

Steel, D. G. and McLaren, C. (2008). *Design and Analysis of Repeated Surveys.* Centre for Statistical and Survey Methodology, Wollongong, Australia.

Steiger, J. H. (1990). Structural Model Evaluation and Modification: An Interval Estimation Approach. *Multivariate Behavioral Research*, 25(2), pp. 173–180.

Steiger, J. H. (2007). Understanding the Limitations of Global Fit Assessment in Structural Equation Modeling. *Personality and Individual Differences*, 42(5), pp. 893–898.

Straub, D., Boudreau, M.-C., and Gefen, D. (2004). Validation Guidelines for IS Positivist Research. *The Communications of the Association for Information Systems*, 13(1), pp. 380–427.

Suh, B. and Han, I. (2003). Effect of Trust on Customer Acceptance of Internet Banking. *Electronic Commerce Research and Applications*, 1(3), pp. 247–263.

Sullivan, R. J. (2010). The Changing Nature of US Card Payment Fraud: Industry and Public Policy Options. *Economic Review – Federal Reserve Bank of Kansas City*, 95(2), pp. 101–133.

Symantec (2012). 2012 Norton Cybercrime Report. Technical Report, Symantec Corporation, Mountain View, USA. URL: `http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf`.

Symantec (2013). 2013 Norton Report. Technical Report, Symantec Corporation, Mountain View, USA. URL: `www.symantec.com/content/en/us/about/presskits/b-norton-report-2013-infographic.en-us.pdf`.

Symantec (2016a). Norton Cybersecurity Insights Report. Technical Report, Symantec Corporation, Mountain View, USA. URL: `http://us.norton.com/cyber-security-insights`.

Symantec (2016b). Security Response: Trojan.Zbot. Technical Report, Symantec Corporation, Mountain View, USA. URL: `www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99`.

Tajalizadehkhoob, S., Gañán, C., Noroozian, A., and Van Eeten, M. (2017). The Role of Hosting Providers in Fighting Command and Control Infrastructure of Financial Malware. In: *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS)*, pp. 575–586.

Tan, S. J. (1999). Strategies for Reducing Consumers' Risk Aversion in Internet Shopping. *Journal of Consumer Marketing*, 16(2), pp. 163–180.

Taylor, A. H. and May, S. (1996). Threat and Coping Appraisal as Determinants of Compliance with Sports Injury Rehabilitation: An Application of Protection Motivation Theory. *Journal of Sports Sciences*, 14(6), pp. 471–482.

Thomas, K., McCoy, D., Grier, C., Kolcz, A., and Paxson, V. (2013). Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse. In: *USENIX Security 13*, pp. 195–210.

Tourangeau, R. and Bradburn, N. M. (2010). *The Psychology of Survey Response*, pp. 315–346. Emerald Group Publishing Limited Bingley, United Kingdom.

Tryon, W. W. (1982). A Simplified Time-series Analysis for Evaluating Treatment Interventions. *Journal of Applied Behavior Aanalysis*, 15(3), pp. 423–429.

Tsai, H.-y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., and Cotten, S. R. (2016). Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective. *Computers & Security*, 59(0), pp. 138–150.

Tucker, L. R. and Lewis, C. (1973). A Reliability Coefficient for Maximum Likelihood Factor Analysis. *Psychometrika*, 38(1), pp. 1–10.

Turel, O. (2015). Quitting the Use of a Habituated Hedonic Information System: A Theoretical Model and Empirical Examination of Facebook Users. *European Journal of Information Systems*, 24(4), pp. 431–446.

Tyler, T. R. (1984). Assessing the Risk of Crime Victimization: The Integration of Personal Victimization Experience and Socially Transmitted Information. *Journal of Social Issues*, 40(1), pp. 27–38.

UNODC-UNECE (2009). Manual on Victimization Surveys. United Nations Office on Drugs and Crime – United Nations Economic Commission for Europe. URL: `www.unodc.org/documents/data-and-analysis/Crime-statistics/Manual_on_Victimization_surveys_2009_web.pdf`.

Urbach, N. and Ahlemann, F. (2010). Structural Equation Modeling in Information Systems Research Using Partial Least Squares. *Journal of Information Technology Theory and Application*, 11(2), pp. 5–40.

Van Dijk, J. (2015). The Case for Survey-based Comparative Measures of Crime. *European Journal of Criminology*, 12(4), pp. 437–456.

Vasiu, I. and Vasiu, L. (2015). Riders on the Storm: An Analysis of Credit Card Fraud Cases. *Suffolk Journal of Trial & Appellate Advocacy*, pp. 184–217.

Venkatesh, V. (2000). Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model. *Information Systems Research*, 11(4), pp. 342–365.

Venkatesh, V. and Bala, H. (2008). Technology Acceptance Model 3 and a Research Agenda on Interventions. *Decision Sciences*, 39(2), pp. 273–315.

Venkatesh, V. and Davis, F. D. (1996). A Model of the Antecedents of Perceived Ease of Use: Development and Test. *Decision Science*, 27(3), pp. 451–481.

Venkatesh, V. and Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, 46(2), pp. 186–204.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 27(3), pp. 425–478.

Viega, J. (2012). Ten Years on, How are We Doing? (Spoiler Alert: We Have no Clue). *IEEE Security & Privacy*, 6(10), pp. 13–16.

Visser, M., Scholte, M., and Scheepers, P. (2013). Fear of Crime and Feelings of Unsafety in European Countries: Macro and Micro Explanations in Cross-national Perspective. *The Sociological Quarterly*, 54(2), pp. 278–301.

Vroom, V. H. (1964). *Work and Motivation.* Wiley, New York, USA.

Wahlberg, A. A. F. and Sjoberg, L. (2000). Risk Perception and the Media. *Journal of Risk Research*, 3(1), pp. 31–50.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age.* Crime and Society. Wiley, New York, USA.

Wall, D. S. (2015). The Internet as a Conduit for Criminal Activity. In: Pattavina, A., (ed.), *Information Technology and the Criminal Justice System*, pp. 77–98. SAGE Publications, Thousand Oaks, USA.

Wang, Y.-S., Wang, Y.-M., Lin, H.-H., and Tang, T.-I. (2003). Determinants of User Acceptance of Internet Banking: An Empirical Study. *International Journal of Service Industry Management*, 14(5), pp. 501–519.

West, B. T., Welch, K. B., and Galecki, A. T. (2014). *Linear Mixed Models: A Practical Guide Using Statistical Software, Second Edition.* Taylor & Francis, Abingdon, United Kingdom.

West, J. and Bhattacharya, M. (2016). Intelligent Financial Fraud Detection: A Comprehensive Review. *Computers & Security*, 57(0), pp. 47–66.

Wheatley, S., Maillart, T., and Sornette, D. (2016). The Extreme Risk of Personal Data Breaches and the Erosion of Privacy. *The European Physical Journal*, 89(1), pp. 1–12.

Wickramasekera, N., Wright, J., Elsey, H., Murray, J., and Tubeuf, S. (2015). Cost of Crime: A Systematic Review. *Journal of Criminal Justice*, 43(3), pp. 218–228.

Wiener, N. (1948). *Cybernetics: Control and Communication in the Animal and the Machine.* MIT Press, Cambridge, USA.

Wiener, N. (1961). *Cybernetics or Control and Communication in the Animal and the Machine.* MIT Press, Cambridge, USA.

Williams, M. L. (2016). Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. *The British Journal of Criminology*, 56(1), pp. 21–48.

Winkfield, M. A., Parrish, J. L., and Tejay, G. (2017). Information Systems Security Leadership: An Empirical Study of Behavioral Influences. In: *Proceedings of the 23rd Americas Conference on Information Systems (AMCIS)*, Boston, USA.

Wittebrood, K. and Junger, M. (2002). Trends in Violent Crime: A Comparison Between Police Statistics and Victimization Surveys. *Social Indicators Research*, 59(2), pp. 153–173.

Wittek, R. (2013). Rational Choice Theory. In: *Theory in Social and Cultural Anthropology: An Encyclopedia*, pp. 686–689. SAGE Publications, Thousand Oaks, USA.

Wittes, B., Poplin, C., Jurecic, Q., and Spera, C. (2016). Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault. Center for Technology at Brookings. URL: `www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf`.

Wogalter, M. S. (2006). Communication-human Information Processing (C-HIP) Model. In: Wogalter, M. S., (ed.), *Handbook of Warnings*, pp. 51–61. Lawrence Erlbaum Associates, Mahwah, USA.

Xiao-Hua, Z. and Tu, W. (1999). Comparison of Several Independent Population Means When Their Samples Contain Log-normal and Possibly Zero Observations. *Biometrics*, 55(2), pp. 645–651.

Yar, M. (2005). The Novelty of "Cybercrime". *European Journal of Criminology*, 2(4), pp. 407–427.

Young, A. L. and Yung, M. (2017). Cryptovirology: The Birth, Neglect, and Explosion of Ransomware. *Communications of the ACM*, 60(7), pp. 24–26.

Yousafzai, S. Y., Foxall, G. R., and Pallister, J. G. (2007). Technology Acceptance: A Meta-analysis of the TAM: Part 1. *Journal Modeling Management*, 2(3), pp. 251–280.

Yu, C.-Y. and Muthén, B. (2002). Evaluation of Model Fit Indices for Latent Variable Models with Categorical and Continuous Outcomes. In: *Paper Presented at the Annual Meeting of the American Educational Research Association*, New Orleans, USA.

Zhou, L., Dai, L., and Zhang, D. (2007). Online Shopping Acceptance Model – A Critical Survey of Consumer Factors in Online Shopping. *Journal Electronic Commerce Research*, 8(1), pp. 41–62.

# Appendix A

# Estimation of Direct Costs

## A.1 Data Collection

### A.1.1 Proxy for Online Shopping Fraud

Initial descriptive statistics suggest that the wording for online shopping fraud (OSF; see Table 4.1) could have been too general, as the victimization rate for this type of cybercrime is significantly higher compared to all other types of cybercrime and other surveys. An explanation for this could be that respondents who have experienced inconveniences when shopping online, which were not necessarily caused by fraud (e. g., products not being of the quality they had expected, or delivery problems), were also classified as cybercrime. The issue has also been reported by Viega (2012).

To mitigate the problem we have developed a proxy logic to approximate a more realistic extent of OSF victimization. We use detailed questions on the criminal case to identify respondents that have been victims of OSF among the ones that were originally identified. According to our proxy a respondent is victim of OSF if:

1. He or she is only victim of OSF or the severest incident he or she reported is OSF.
2. He or she lost money due to the incident.
3. He or she was *not* able to recover all losses.

Using the proxy variable significantly reduces the number of OSF cases in the data set from 2 052 respondents who answered *Yes* to the original question to 551 who meet all three conditions of the proxy logic. Table A.1 shows the relative effects by country.

**Table A.1:** Incident rates of online shopping fraud by country

| | DE | EE | IT | NL | PL | UK |
|---|---|---|---|---|---|---|
| Original OSF definition | 36.89 % | 30.46 % | 17.24 % | 29.43 % | 36.02 % | 43.31 % |
| Proxy definition | 8.40 % | 9.12 % | 5.00 % | 10.27 % | 9.69 % | 9.01 % |
| *For comparison:* EB82.2 (2015) | 13 % | 13 % | 11 % | 16 % | 19 % | 16 % |

The proxy logic and the incident rates provide confidence that the selected respondents are indeed victims of OSF. As our incidents rate for OSF is smaller than in the comparable Eurobarometer survey (EB82.2, 2015) in all six countries, we believe that our proxy is still on the conservative side and rather underestimates the real victimization rate.

### A.1.2 Sample Demographics

Table A.2 reports the demographics of the full sample ($n$) and the subgroup of victims ($v$) for each of the six surveyed countries. It comprises gender, age, and area of living.

**Table A.2:** Sample demographics by country

| Variable | DE | | EE | | IT | | NL | | PL | | UK | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $v$ | $n$ | $v$ | $n$ | $v$ | $n$ | $v$ | $n$ | $v$ | $n$ | $v$ | $n$ |
| Gender | | | | | | | | | | | | |
| Male | 53 % | 58 % | 47 % | 58 % | 53 % | 57 % | 51 % | 47 % | 46 % | 48 % | 50 % | 49 % |
| Female | 47 % | 42 % | 53 % | 42 % | 47 % | 43 % | 49 % | 53 % | 54 % | 52 % | 50 % | 51 % |
| Age | | | | | | | | | | | | |
| 18-20 | 5 % | 6 % | 7 % | 4 % | 6 % | 8 % | 5 % | 5 % | 7 % | 4 % | 7 % | 6 % |
| 21-30 | 20 % | 18 % | 23 % | 30 % | 21 % | 24 % | 18 % | 25 % | 28 % | 33 % | 20 % | 20 % |
| 31-40 | 19 % | 25 % | 19 % | 24 % | 23 % | 16 % | 17 % | 21 % | 26 % | 33 % | 17 % | 19 % |
| 41-50 | 24 % | 21 % | 22 % | 24 % | 25 % | 22 % | 21 % | 22 % | 19 % | 15 % | 18 % | 19 % |
| 51-60 | 19 % | 21 % | 17 % | 14 % | 16 % | 18 % | 18 % | 12 % | 14 % | 10 % | 18 % | 19 % |
| 61-70 | 7 % | 6 % | 9 % | 3 % | 8 % | 10 % | 13 % | 9 % | 5 % | 3 % | 12 % | 9 % |
| 70+ | 5 % | 4 % | 3 % | 1 % | 1 % | 1 % | 8 % | 4 % | 1 % | 1 % | 5 % | 5 % |
| Area of living | | | | | | | | | | | | |
| Big city | 19 % | 20 % | 54 % | 59 % | 16 % | 17 % | 27 % | 32 % | 28 % | 27 % | 13 % | 12 % |
| Suburbs | 17 % | 14 % | 5 % | 8 % | 8 % | 7 % | 18 % | 18 % | 11 % | 10 % | 19 % | 22 % |
| Town | 34 % | 37 % | 22 % | 18 % | 35 % | 34 % | 24 % | 25 % | 31 % | 39 % | 39 % | 38 % |
| Village | 25 % | 23 % | 16 % | 12 % | 37 % | 36 % | 27 % | 22 % | 23 % | 21 % | 20 % | 17 % |
| Countrys. | 4 % | 6 % | 3 % | 2 % | 4 % | 6 % | 3 % | 3 % | 7 % | 4 % | 6 % | 8 % |
| Other | 0 % | 0 % | 0 % | 1 % | 0 % | 0 % | 1 % | 0 % | 0 % | 0 % | 1 % | 0 % |

### A.1.3 Cybercrime Victims with Monetary Losses

Table A.3 reports all incidents with monetary losses broken down by type of cybercrime and country. It contains all cases with point estimates of monetary losses $> 0$ €, which were used to estimate parameters of the conditional loss distributions. The probability of losses $\hat{q}$ is also reported. Table A.3 illustrates that the data set only very few cases with monetary losses for some types of cybercrime.

**Table A.3:** Cybercrime incidents with monetary losses by country and type

| Cybercrime | Proportion $\hat{q}$ | DE | EE | IT | NL | PL | UK | Total |
|---|---|---|---|---|---|---|---|---|
| IDT wrt. OB | 33.7 % | 1 | 6 | 1 | 2 | 2 | 10 | 22 |
| IDT wrt. BC | 34.3 % | 6 | 18 | 18 | 12 | 2 | 13 | 69 |
| IDT wrt. PP | 24.1 % | 2 | 2 | 1 | 2 | 0 | 5 | 12 |
| OS fraud | 91.0 % | 73 | 95 | 48 | 102 | 92 | 78 | 488 |
| IDT wrt. OS | 17.9 % | 3 | 1 | 5 | 1 | 2 | 5 | 17 |
| Extortion | 13.7 % | 3 | 2 | 1 | 1 | 4 | 3 | 14 |
| Scams | 45.2 % | 18 | 18 | 14 | 11 | 13 | 16 | 90 |
| Total | | 106 | 142 | 88 | 131 | 115 | 130 | 712 |

## A.2 Description of Variables

Table A.4 provides an overview of all variables we use to model the costs of consumer-facing cybercrime together with a description and, where applicable, a reference to the definition of the variable. The minimum wage per country $\hat{\alpha}_j$ is the only external data source not collected in the survey.

**Table A.4:** Description of variables

| Variable | Description | Definition |
|---|---|---|
| $i$ | Type of cybercrime | |
| $j$ | Country | |
| $v$ | Number of cybercrime victims | |
| $v_l$ | Number of cybercrime victims with monetary losses | |
| $n$ | Number of respondents | |
| $n_s$ | Number of respondents with protection expenses | |
| $\hat{\alpha}_j$ | Time conversion factor: Minimum wage per country $j$ | |
| **Conditions** | | |
| $\hat{q}_i$, $\hat{q}_j$ | Probability of losses $M_i$ per crime $i$ and expenses $C_j$ per country $j$ | |
| $\hat{p}_i$ | Probability of victimization per type of crime $i$ | |
| **Conditional estimates** of monetary loss $M_i$ and protection expenses $C_j$ | | |
| $\bar{y}$, $\bar{m}_i$, $\bar{c}_j$ | Empirical mean | |
| $\tilde{y}$, $\tilde{m}_i$, $\tilde{c}_j$ | Empirical median | |
| $\mu_i$, $\mu_j$ | Distribution-based mean (log normal distribution) | |
| $\rho_i$, $\rho_j$ | Distribution-based median (log normal distribution) | |
| **Unconditional indicators** of monetary loss $M_i$ and protection expenses $C_j$ | | |
| ELI | Expected value indicator | Eq.: 4.3 |
| AMLI | Adjusted median indicator | Eq.: 4.4 |
| HLI | Harmonized loss indicator | Eq.: 4.5 |
| UCM | Unconditional empirical mean (also for $T_i$ and $S_j$) | |
| **Aggregate estimates** using the harmonized loss indicator (HLI) | | |
| $\mathcal{P}_j$ | Protection expenses per country $j$ | Eq.: 4.6 |
| $\mathcal{L}_i$ | Cybercrime losses per type of crime $i$ | Eq.: 4.6 |
| $\mathcal{L}_j$ | Cybercrime losses per country $j$ | Eq.: 4.7 |
| **Aggregate estimates** using unconditional sample mean (UCM) | | |
| $\mathcal{P}'_j$ | Protection expenses per country $j$ | |
| $\mathcal{L}'_i$ | Cybercrime losses per type of crime $i$ | |
| $\mathcal{L}'_j$ | Cybercrime losses per country $j$ | |

## A.3 Cost Estimation

### A.3.1 Distribution of Initial Monetary Losses

Table A.5 shows the parameter estimates for the distributions of initial monetary losses $g_{i,\hat{\theta}}$, the number of point estimates $n_i$ used for the distribution fitting, and AIC and BIC scores for each type of cybercrime $i$. Distributions are fitted using a weighted maximum likelihood method of the R-package "fitdistrplus" Delignette-Muller and Dutang (2015). Note, that the lower bounds of the rate parameter of the gamma distribution $\hat{\theta_{i,2}}$ are fixed to 0.005, to avoid unsuccessful termination of the maximum likelihood estimation. Accordingly, these bounds are rounded to 0 in Table A.5.

**Table A.5:** Parameter estimates for initial cybercrime losses

| | | Lognormal distribution | | | |
|---|---|---|---|---|---|
| Cyber crime | $n_i$ | $\hat{\theta_{i,1}}(sd)$ | $\hat{\theta_{i,2}}(sd)$ | AIC | BIC |
| IDT wrt. OB | 22 | 6.14 (.485) | 1.85 (.343) | 242 | 244 |
| IDT wrt. BC | 69 | 5.8 (.269) | 1.81 (.190) | 708 | 712 |
| IDT wrt. PP | 12 | 6.19 (.668) | 2.1 (.473) | 169 | 170 |
| OS fraud | 488 | 3.98 (.60) | 1.34 (.42) | 5685 | 5694 |
| IDT wrt. OS | 17 | 4.94 (.434) | 1.53 (.307) | 172 | 174 |
| Extortion | 14 | 4.31 (.574) | 1.84 (.406) | 135 | 136 |
| Scams | 90 | 5.29 (.207) | 1.66 (.146) | 928 | 933 |
| | | Gamma distribution | | | |
| Cyber crime | $n_i$ | $\hat{\theta_1}(sd)$ | $\hat{\theta_2}(sd)$ | AIC | BIC |
| IDT wrt. OB | 22 | 2.82 (.871) | 0 (.2) | 436 | 438 |
| IDT wrt. BC | 69 | 2.12 (.379) | 0 (.1) | 961 | 965 |
| IDT wrt. PP | 12 | 2.92 (1.94) | 0 (.2) | 288 | 289 |
| OS fraud | 488 | 0.53 (.26) | 0 (.) | 5981 | 5990 |
| IDT wrt. OS | 17 | 1.14 (.390) | 0 (.2) | 191 | 192 |
| Extortion | 14 | 0.63 (.220) | 0 (.1) | 132 | 133 |
| Scams | 90 | 1.45 (.219) | 0 (.1) | 1358 | 1363 |
| | | Weibull distribution | | | |
| Cyber crime | $n_i$ | $\hat{\theta_1}(sd)$ | $\hat{\theta_2}(sd)$ | AIC | BIC |
| IDT wrt. OB | 22 | 0.56 (.109) | 1170.8 (576.457) | 244 | 246 |
| IDT wrt. BC | 69 | 0.62 (.71) | 796.27 (201.141) | 709 | 713 |
| IDT wrt. PP | 12 | 0.58 (.146) | 1317.02 (762.114) | 168 | 169 |
| OS fraud | 488 | 0.65 (.19) | 107.34 (7.817) | 5855 | 5863 |
| IDT wrt. OS | 17 | 0.64 (.136) | 310.39 (146.177) | 175 | 176 |
| Extortion | 14 | 0.75 (.189) | 167.82 (73.220) | 132 | 133 |
| Scams | 90 | 0.55 (.46) | 468.42 (113.924) | 947 | 952 |
| | | Normal distribution | | | |
| Cyber crime | $n_i$ | $\hat{\theta_1}(sd)$ | $\hat{\theta_2}(sd)$ | AIC | BIC |
| IDT wrt. OB | 22 | 1087.52 (.485) | 767.39 (.343) | 288 | 290 |
| IDT wrt. BC | 69 | 275.96 (.269) | 195.19 (.190) | 810 | 814 |
| IDT wrt. PP | 12 | 1017.27 (.668) | 719.98 (.473) | 191 | 192 |
| OS fraud | 488 | 29.24 (.60) | 20.68 (.42) | 7891 | 7900 |
| IDT wrt. OS | 17 | 196.77 (.434) | 139.13 (.307) | 201 | 203 |
| Extortion | 14 | 72.35 (.574) | 51.17 (.406) | 146 | 147 |
| Scams | 90 | 494.3 (.207) | 348.32 (.146) | 1247 | 1252 |

Based on cybercrime victims who reported point estimates of monetary losses ($v' = 712$)

In addition to the parameter estimates Figure A.4 – Figure A.5 illustrate the empirical and fitted distributions of initial monetary losses for each type of cybercrime. The left part of each figure shows a histogram of the initial losses, with breaks according to the categorical intervals, and the fitted candidate loss distributions. The right part of each figure shows a Q–Q plot of the four candidate loss distributions on the log scale. The histograms are truncated at losses of 1200 € for a better visualization, the Q–Q plots show all data points.

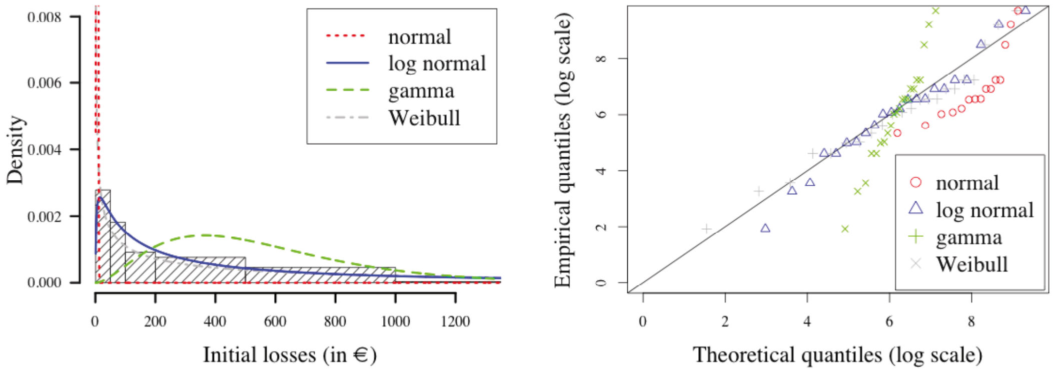


**Figure A.1:** Initial losses from IDT wrt. online banking; Left: Histogram and candidate loss distributions, Right: Q–Q plot of candidate loss distributions on log scale

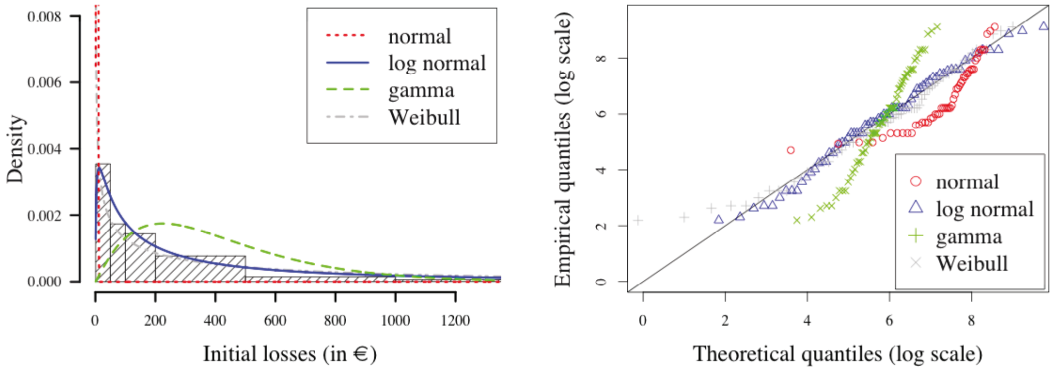


**Figure A.2:** Initial losses from IDT wrt. bank cards; Left: Histogram and candidate loss distributions, Right: Q–Q plot of candidate loss distributions on log scale

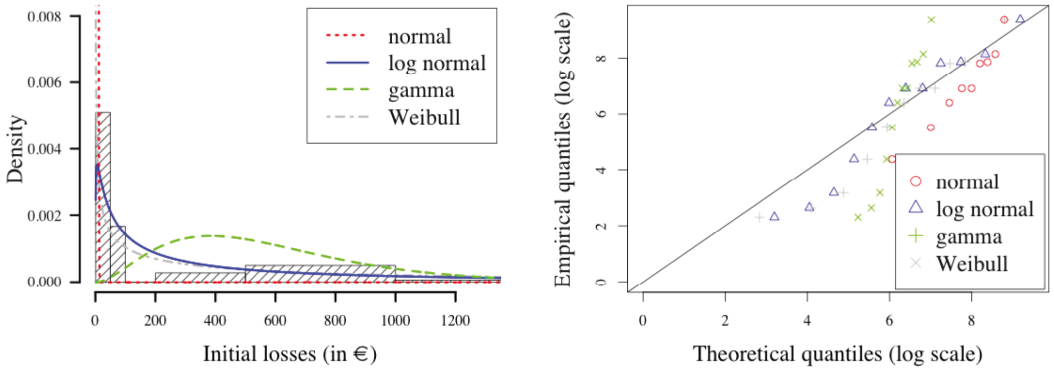


**Figure A.3:** Initial losses from IDT wrt. PayPal; Left: Histogram and candidate loss distributions, Right: Q–Q plot of candidate loss distributions on log scale

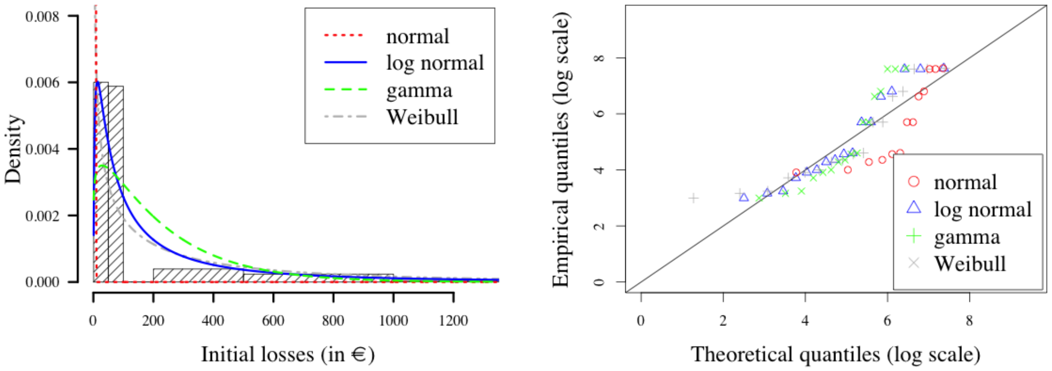


**Figure A.4:** Initial losses from IDT wrt. online shopping; Left: Histogram and candidate loss distributions, Right: Q–Q plot of candidate loss distributions on log scale

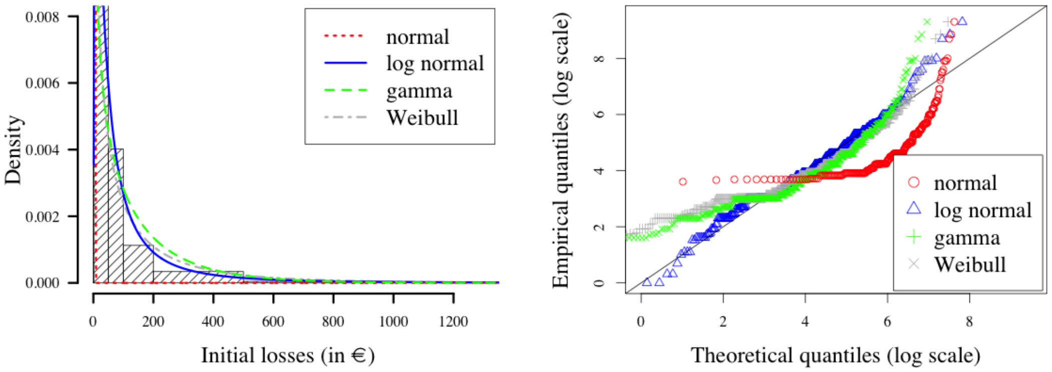


**Figure A.5:** Initial losses from online shopping fraud; Left: Histogram and candidate loss distributions, Right: Q–Q plot of candidate loss distributions on log scale

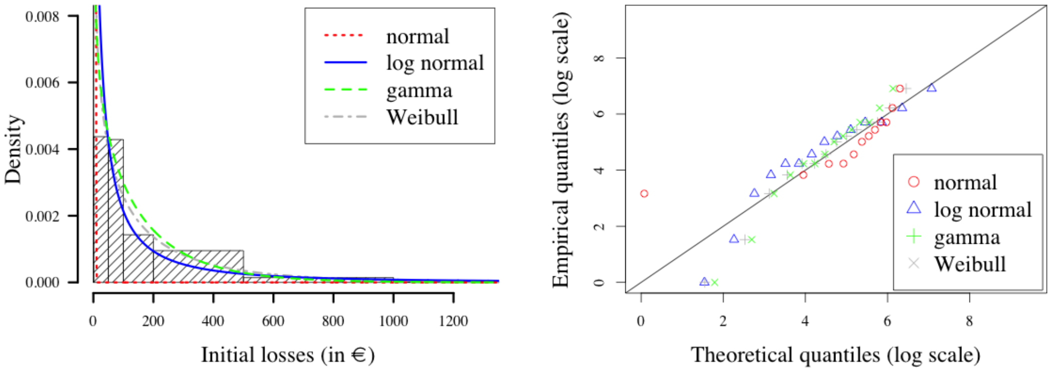


**Figure A.6:** Initial losses from extortion; Left: Histogram and candidate loss distributions, Right: Q–Q plot of candidate loss distributions on log scale

### A.3.2 Distribution of Out-of-pocket Losses

Table A.6 shows the parameter estimates for the distributions $g_{i,\hat{\theta}}$ of the out-of-pocket losses, the number of point estimates $n_i$, and AIC and BIC scores for each type of cybercrime $i$. All distributions have been fitted using a weighted maximum likelihood method in the R-package "fitdistrplus" Delignette-Muller and Dutang (2015). Note, that the lower bounds of the rate parameter of the gamma distribution $\hat{\theta_{i,2}}$ are fixed to 0.005, to avoid unsuccessful termination of the maximum likelihood estimation. Accordingly, these bounds are rounded to 0 in Table A.5. We do not illustrate empirical and theoretical distributions of the out-of-pocket losses, with histograms and Q–Q plots for each type of cybercrime, as they are very similar to the initial losses.

**Table A.6:** Parameter estimates for out-of-pocket cybercrime losses

| | | Lognormal distribution | | | |
|---|---|---|---|---|---|
| Cyber crime | $n_i$ | $\hat{\theta_{i,1}}(sd)$ | $\hat{\theta_{i,2}}(sd)$ | AIC | BIC |
| IDT wrt. OB | 11 | 5.81 (.734) | 1.96 (.519) | 117 | 117 |
| IDT wrt. BC | 36 | 5.14 (.370) | 1.8 (.261) | 343 | 346 |
| IDT wrt. PP | 6 | 5.31 (1.162) | 2.49 (.822) | 74 | 74 |
| OS fraud | 481 | 3.73 (.62) | 1.38 (.44) | 5408 | 5416 |
| IDT wrt. OS | 10 | 4.53 (.601) | 1.63 (.426) | 98 | 99 |
| Extortion | 13 | 4.16 (.567) | 1.78 (.401) | 125 | 126 |
| Scams | 82 | 5.22 (.217) | 1.66 (.154) | 833 | 837 |
| | | Gamma distribution | | | |
| Cyber crime | $n_i$ | $\hat{\theta_{i,1}}(sd)$ | $\hat{\theta_{i,2}}(sd)$ | AIC | BIC |
| IDT wrt. OB | 11 | 2.15 (.965) | 0 (.2) | 195 | 196 |
| IDT wrt. BC | 36 | 1.31 (.323) | 0 (.1) | 409 | 412 |
| IDT wrt. PP | 6 | 1.48 (.828) | 0 (.3) | 95 | 95 |
| OS fraud | 481 | 0.54 (.28) | 0 (.) | 5666 | 5674 |
| IDT wrt. OS | 10 | 0.89 (.393) | 0 (.3) | 106 | 106 |
| Extortion | 13 | 0.69 (.258) | 0 (.2) | 122 | 123 |
| Scams | 82 | 1.38 (.218) | 0 (.1) | 1197 | 1202 |
| | | Weibull distribution | | | |
| Cyber crime | $n_i$ | $\hat{\theta_{i,1}}(sd)$ | $\hat{\theta_{i,2}}(sd)$ | AIC | BIC |
| IDT wrt. OB | 11 | 0.54 (.148) | 886.31 (657.33) | 117 | 118 |
| IDT wrt. BC | 36 | 0.61 (.91) | 407.68 (146.314) | 344 | 347 |
| IDT wrt. PP | 6 | 0.55 (.214) | 626.1 (555.70) | 73 | 73 |
| OS fraud | 481 | 0.66 (.20) | 84.59 (6.150) | 5549 | 5558 |
| IDT wrt. OS | 10 | 0.61 (.169) | 216.62 (139.264) | 100 | 100 |
| Extortion | 13 | 0.81 (.215) | 138.55 (56.827) | 122 | 123 |
| Scams | 82 | 0.55 (.49) | 433.43 (110.704) | 850 | 855 |
| | | Normal distribution | | | |
| Cyber crime | $n_i$ | $\hat{\theta_{i,1}}(sd)$ | $\hat{\theta_{i,2}}(sd)$ | AIC | BIC |
| IDT wrt. OB | 11 | 1250.5 (.734) | 883.01 (.519) | 140 | 141 |
| IDT wrt. BC | 36 | 316.05 (.370) | 223.44 (.261) | 419 | 422 |
| IDT wrt. PP | 6 | 503 (1.162) | 355.6 (.822) | 81 | 81 |
| OS fraud | 481 | 24.47 (.62) | 17.3 (.44) | 7624 | 7632 |
| IDT wrt. OS | 10 | 202.93 (.601) | 143.62 (.426) | 117 | 118 |
| Extortion | 13 | 48.16 (.567) | 34.07 (.401) | 131 | 132 |
| Scams | 82 | 512.42 (.217) | 362.33 (.154) | 1129 | 1134 |

Based on cybercrime victims with point estimates of monetary losses ($v'' = 639$)

### A.3.3 Distribution of Protection Expenses

Table A.7 shows the parameter estimates for the expenses for protection measures $g_{\hat{\theta}}$ along with the number of point estimates $n_j$ and the relative goodness-of-fit indicators AIC and BIC for country $j$. All distributions have been fitted using a weighted maximum likelihood method in the R-package "fitdistrplus" Delignette-Muller and Dutang (2015).

**Table A.7:** Parameter estimates for the protection expenses by country

| | | Lognormal distribution | | | |
|---|---|---|---|---|---|
| Country | $n_j$ | $\hat{\theta}_{j,1}(sd)$ | $\hat{\theta}_{j,2}(sd)$ | AIC | BIC |
| Germany | 597 | 5.05 (.34) | 0.82 (.24) | 7457 | 7466 |
| Estonia | 173 | 4.51 (.81) | 1.05 (.57) | 2020 | 2027 |
| Italy | 452 | 4.77 (.46) | 0.97 (.33) | 5502 | 5510 |
| the Netherlands | 476 | 5.1 (.39) | 0.85 (.28) | 6033 | 6041 |
| Poland | 628 | 4.4 (.41) | 1.02 (.29) | 7311 | 7320 |
| United Kingdom | 609 | 5.21 (.34) | 0.84 (.24) | 7862 | 7871 |
| | | Gamma distribution | | | |
| Country | $n_j$ | $\hat{\theta}_{j,1}(sd)$ | $\hat{\theta}_{j,2}(sd)$ | AIC | BIC |
| Germany | 597 | 1.52 (.78) | 0.01 (.) | 7572 | 7581 |
| Estonia | 173 | 1.27 (.122) | 0.01 (.1) | 2006 | 2012 |
| Italy | 452 | 1.17 (.67) | 0.01 (.) | 5580 | 5589 |
| the Netherlands | 476 | 1.72 (.99) | 0.01 (.1) | 6016 | 6024 |
| Poland | 628 | 1.34 (.67) | 0.01 (.1) | 7258 | 7266 |
| United Kingdom | 609 | 1.56 (.78) | 0.01 (.) | 7928 | 7937 |
| | | Weibull distribution | | | |
| Country | $n_j$ | $\hat{\theta}_{j,1}(sd)$ | $\hat{\theta}_{j,2}(sd)$ | AIC | BIC |
| Germany | 597 | 1.1 (.29) | 233.64 (9.238) | 7617 | 7625 |
| Estonia | 173 | 1.09 (.60) | 146.4 (10.921) | 2009 | 2015 |
| Italy | 452 | 0.99 (.32) | 191.18 (9.676) | 5587 | 5595 |
| the Netherlands | 476 | 1.33 (.45) | 246.92 (9.31) | 6028 | 6037 |
| Poland | 628 | 1.11 (.32) | 129.6 (4.932) | 7275 | 7284 |
| United Kingdom | 609 | 1.18 (.33) | 279.1 (10.160) | 7960 | 7969 |
| | | Normal distribution | | | |
| Country | $n_j$ | $\hat{\theta}_{j,1}(sd)$ | $\hat{\theta}_{j,2}(sd)$ | AIC | BIC |
| Germany | 597 | 13.21 (.34) | 9.34 (.24) | 8561 | 8570 |
| Estonia | 173 | 12.37 (.81) | 8.75 (.57) | 2196 | 2203 |
| Italy | 452 | 14.39 (.46) | 10.18 (.33) | 6370 | 6378 |
| the Netherlands | 476 | 8.53 (.39) | 6.03 (.28) | 6297 | 6305 |
| Poland | 628 | 5.38 (.41) | 3.81 (.29) | 7915 | 7924 |
| United Kingdom | 609 | 11.18 (.34) | 7.9 (.24) | 8565 | 8574 |

Based on the all consumers who spend money on protection software ($s' = 2\,935$)

In addition to the parameter estimates Figure A.7 – Figure A.12 illustrate the empirical and fitted distributions of protection expenses for each country. The histograms are truncated at losses of 1200 € for a better visualization, the Q–Q plots show all data points.

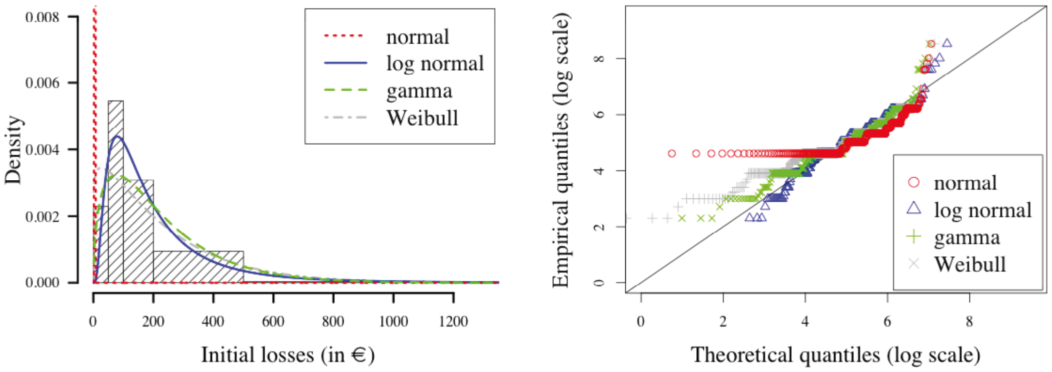


**Figure A.7:** Protection expenses of German consumers; Left: Histogram and candidate cost distributions, Right: Q–Q plot of candidate cost distributions on log scale

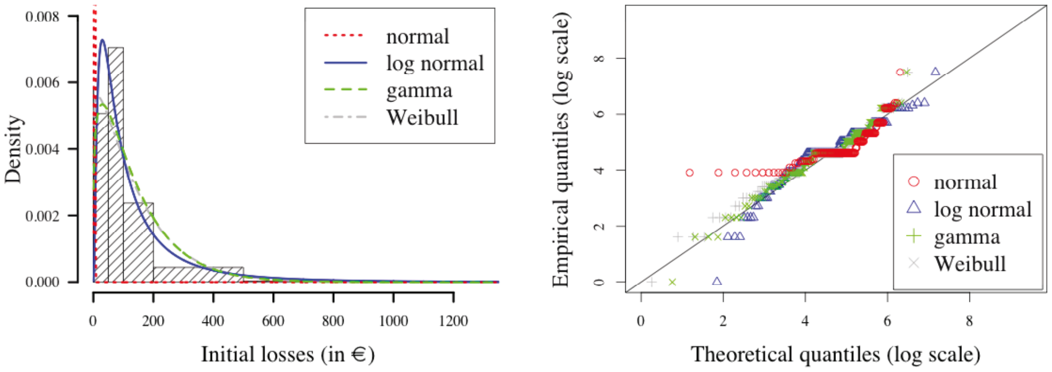


**Figure A.8:** Protection expenses of Estonian consumers; Left: Histogram and candidate cost distributions, Right: Q–Q plot of candidate cost distributions on log scale

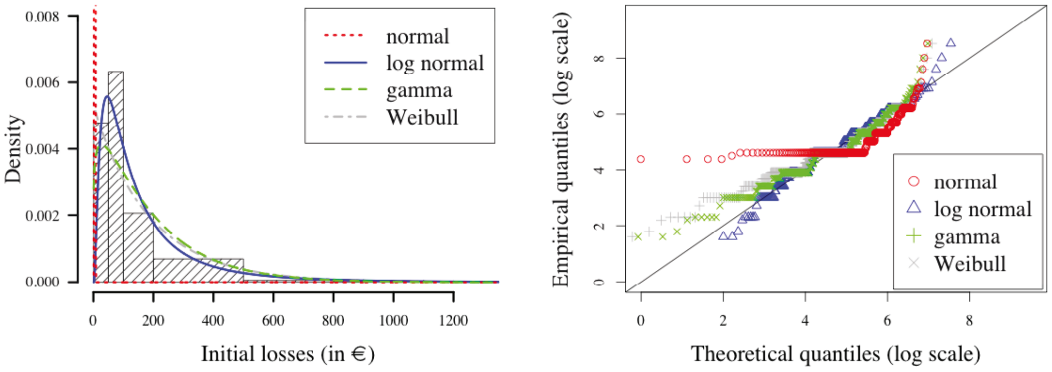


**Figure A.9:** Protection expenses of Italian consumers; Left: Histogram and candidate cost distributions, Right: Q–Q plot of candidate cost distributions on log scale

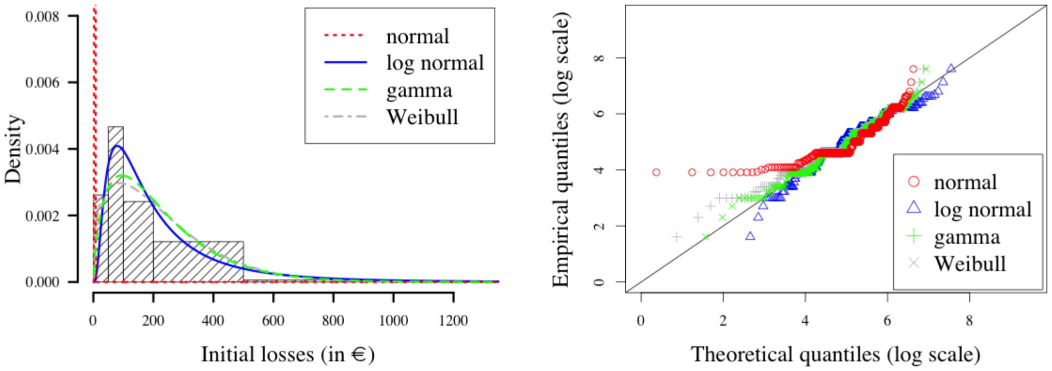


**Figure A.10:** Protection expenses of Dutch consumers; Left: Histogram and candidate cost distributions, Right: Q–Q plot of candidate cost distributions on log scale

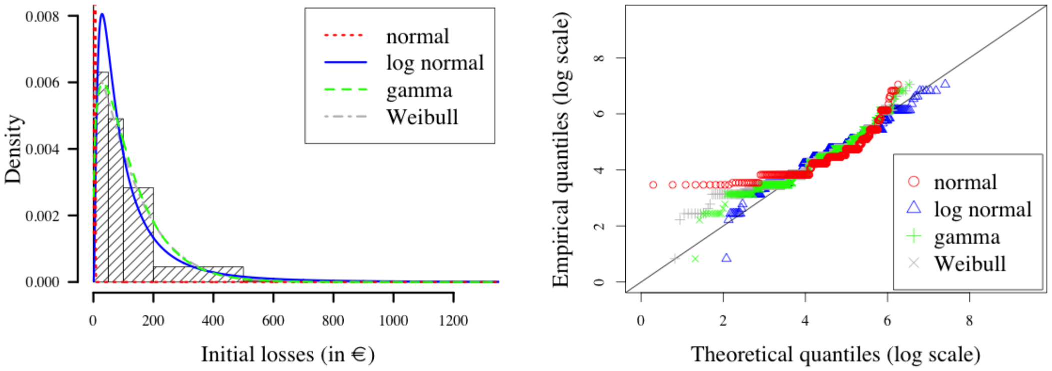


**Figure A.11:** Protection expenses of Polish consumers; Left: Histogram and candidate cost distributions, Right: Q–Q plot of candidate cost distributions on log scale

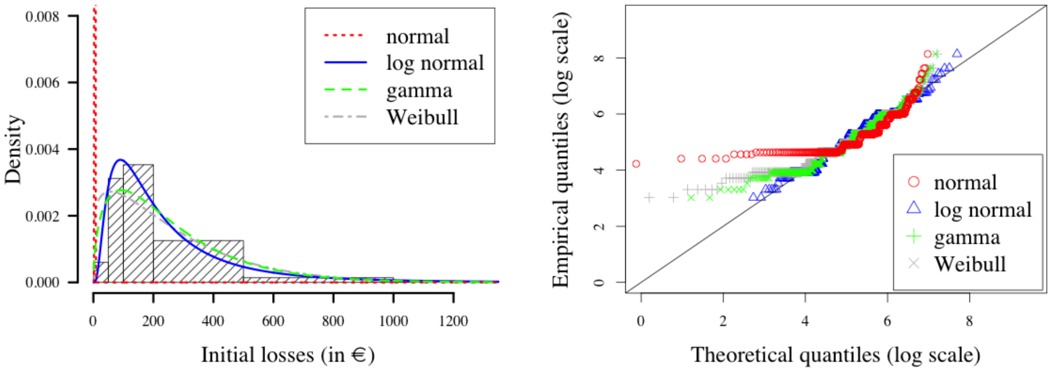


**Figure A.12:** Protection expenses of consumers in the UK; Left: Histogram and candidate cost distributions, Right: Q–Q plot of candidate cost distributions on log scale

### A.3.4 Mean-based Cost Estimates

Table A.8 compares cost estimates based on the harmonized loss indicator with pure mean-based estimates for cybercrime losses $\mathcal{L}$ and protection expenses $\mathcal{P}$. Each cell represents the estimated costs for each Internet user (older than 18) over a time period of five years in €. Cybercrime losses are based on initial monetary losses HLI or sample mean respectively, assuming that victim compensation is payed for by all customers through higher service fees.

Table A.8 shows the large difference between the two estimation approaches for cybercrime losses $\mathcal{L}$. The mean reports losses about four times larger than the harmonized loss indicator in all countries. For protection expenses the difference is smaller. Mean-based estimates are about 1.5 times larger than the harmonized estimates in all countries.

**Table A.8:** Aggregate cost estimates by country

| Country | Cyber crime losses $\mathcal{L}$ in € | | Protection expenses $\mathcal{P}$ in € | |
|---|---|---|---|---|
| | HLI | UCM | HLI | UCM |
| Germany | 39.07<br>[35:47] | 96.66<br>[74:129] | 262.94<br>[253:279] | 299.92<br>[289:316] |
| Estonia | 12.93<br>[12:16] | 42.10<br>[32:55] | 46.93<br>[44:51] | 56.80<br>[54:61] |
| Italy | 19.92<br>[18:24] | 52.92<br>[40:70] | 164.81<br>[156:176] | 199.14<br>[190:211] |
| the Netherlands | 26.25<br>[24:31] | 63.61<br>[50:81] | 251.42<br>[235:267] | 280.94<br>[265:297] |
| Poland | 15.41<br>[14:20] | 52.27<br>[38:73] | 89.51<br>[87:93] | 115.04<br>[112:119] |
| United Kingdom | 42.45<br>[38:54] | 112.81<br>[84:153] | 225.23<br>[217:241] | 270.42<br>[262:286] |

# Appendix B

# Quantitative Evidence of Indirect Impact

## B.1 Confirmatory Factor Analysis

**Reduced model** This section reports additional tables used in the CFA analyses. Table B.1 shows factor loadings of the CFA analysis for the baseline model. The results are based on the EB data for the year 2012.

**Table B.1:** Baseline model: standardized factor loadings

| **Latent variable** | **Indicator** | **Loading** | **SE** | **Z-Score** | $\boldsymbol{R^2}$ |
|---|---|---|---|---|---|
| Cybercrime Experience | exp1 | $0.671^{***}$ | 0.037 | 18.29 | 0.450 |
| | exp2 | $0.661^{***}$ | 0.027 | 24.64 | 0.437 |
| | exp3 | $0.707^{***}$ | 0.023 | 30.43 | 0.500 |
| | exp4 | $0.671^{***}$ | 0.036 | 18.65 | 0.450 |
| | exp5 | $0.721^{***}$ | 0.037 | 19.42 | 0.520 |
| Media Awareness | ma1 | $0.082^{***}$ | 0.015 | 5.35 | 0.007 |
| | ma2 | $0.560^{***}$ | 0.040 | 13.92 | 0.314 |
| | ma3 | $0.738^{***}$ | 0.026 | 28.43 | 0.545 |
| | ma4 | $0.809^{***}$ | 0.021 | 38.71 | 0.654 |
| Perceived Cybercrime Risk | pcr1 | $0.822^{***}$ | 0.007 | 113.32 | 0.676 |
| | pcr2 | $0.820^{***}$ | 0.008 | 101.31 | 0.672 |
| | pcr3 | $0.806^{***}$ | 0.010 | 77.13 | 0.650 |
| | pcr4 | $0.801^{***}$ | 0.009 | 86.22 | 0.642 |
| | pcr5 | $0.822^{***}$ | 0.007 | 124.51 | 0.676 |
| | pcr6 | $0.795^{***}$ | 0.007 | 120.15 | 0.632 |

Model fit: N=17 773; $\chi^2(df)$=460(159); RMSEA=.010 (.009 – .011), TLI=.968, CFI=.957.

Table B.2 reports scores for reliability and validity as well as between-construct correlations for the baseline model. The results are based on the EB data for the year 2012.

**Table B.2:** Baseline model: reliability and discriminant validity

| | **CR** | **AVE** | **MA** | **EXP** | **PCR** | **avS** | **avB** | **avN** | **pbA** | **pbP** | **pbS** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| MA | 0.66 | 0.38 | **.616** | (.023) | (.040) | (.036) | (.028) | (.025) | (.030) | (.025) | (.035) |
| EXP | 0.82 | 0.47 | $.235^{***}$ | **.686** | (.021) | (.045) | (.033) | (.012) | (.023) | (.025) | (.036) |
| PCR | 0.92 | 0.66 | .018 | $.266^{***}$ | **.812** | (.019) | (.017) | (.028) | (.029) | (.015) | (.029) |
| avS | - | - | .033 | .061 | $.170^{***}$ | - | (.035) | (.032) | (.025) | (.021) | (.028) |
| avB | - | - | .017 | $.173^{***}$ | $.127^{***}$ | $.577^{***}$ | - | (.050) | (.027) | (.017) | (.033) |
| avN | - | - | $.312^{***}$ | $.153^{***}$ | $.092^{***}$ | $.305^{***}$ | $.297^{***}$ | - | (.046) | (.046) | (.038) |
| pbA | - | - | $.329^{***}$ | $.318^{***}$ | $.066^{*}$ | .011 | $.072^{**}$ | $.450^{***}$ | - | (.025) | (.043) |
| pbP | - | - | $.357^{***}$ | $.183^{***}$ | $.047^{**}$ | $-.027$ | .010 | $.414^{***}$ | $.557^{***}$ | - | (.033) |
| pbS | - | - | $.368^{***}$ | $.082^{*}$ | .006 | $-.026$ | $-.038$ | $.453^{***}$ | $.427^{***}$ | $.532^{***}$ | - |

Lower-left: between construct correlations; Diagonal: $\sqrt{\text{AVE}}$; Upper-right: SE's of the correlations. Media Awareness (MA), Cybercrime Experience (EXP), Perceived Cybercrime Risk (PCR), Avoidance Intention (AV): Online shopping (avS), Online banking (avB), Online social networking (avN), Protection Behavior (PB): Anti-virus (pbA), Different passwords (pbP), Changed security settings (pbS).

**Improved Measurement Model** Table B.3 reports scores for reliability and validity as well as between-construct correlations for the improved measurement model. The results are based on the latest EB data for the year 2014.

**Table B.3:** Improved measurement model (14'): reliability and discriminant validity

| **Constructs** | | | | **Correlations (lower-left)** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Year | Name | CR | AVE | EXP | PCR | avS | avB | avN | avU | pbA | pbS | pbP |
| 14' | Exp | 0.86 | 0.56 | **0.748** | (0.033) | (0.039) | (0.029) | (0.027) | (0.018) | (0.019) | (0.015) | (0.034) |
| | Con | 0.91 | 0.67 | $0.281^{***}$ | **0.819** | (0.024) | (0.024) | (0.026) | (0.016) | (0.023) | (0.032) | (0.028) |
| | avS | - | - | 0.038 | $0.149^{***}$ | - | (0.023) | (0.040) | (0.034) | (0.052) | (0.033) | (0.042) |
| | avB | - | - | $0.083^{**}$ | $0.145^{***}$ | $0.557^{***}$ | - | (0.039) | (0.021) | (0.026) | (0.032) | (0.024) |
| | avN | - | - | 0.037 | $0.047^{\dagger}$ | $0.347^{***}$ | $0.284^{***}$ | - | (0.021) | (0.028) | (0.029) | (0.042) |
| | avU | - | - | $-0.023$ | $0.137^{***}$ | $0.221^{***}$ | $0.209^{***}$ | $0.307^{***}$ | - | (0.022) | (0.018) | (0.024) |
| | pbA | - | - | $0.222^{***}$ | $0.044^{\dagger}$ | $0.098^{\dagger}$ | $0.056^{*}$ | $0.391^{***}$ | $0.175^{***}$ | - | (0.029) | (0.027) |
| | pbP | - | - | $0.096^{***}$ | 0.044 | $0.100^{**}$ | $0.068^{*}$ | $0.396^{***}$ | $0.219^{***}$ | $0.507^{***}$ | - | (0.029) |
| | pbS | - | - | $-0.040$ | 0.022 | $0.154^{***}$ | $0.092^{***}$ | $0.454^{***}$ | $0.357^{***}$ | $0.394^{***}$ | $0.455^{***}$ | - |

Upper-right: SE's of the correlations; Diagonal: $\sqrt{\text{AVE}}$. Cybercrime Experience (EXP), Perceived Cybercrime Risk (PCR), Avoidance Intention (AV): Online shopping (avS), Online banking (avB), Online social networking (avN), Protection Behavior (PB): Anti-virus (pbA), Different passwords (pbP), Changed security settings (pbS)

## B.2 Structural Models

Table B.4 reports the path coefficients and fit indexes for all models of *Avoidance Intention*.

**Table B.4:** Structural models: path coefficients and fit indexes

| | Path coefficients | | | | Model fit | | | |
|---|---|---|---|---|---|---|---|---|
| Year | EXP→PCR | PCR→AV | $\text{EXP}\xrightarrow{\text{PCR}}\text{AV}$ | EXP→AV | $\chi^2$ (*df*) | RMSEA (90 CI) | CFI | TLI |
| Online shopping (AvS) | | | | | | | | |
| 2012 | 0.258$^{***}$<br>(0.020) | 0.167$^{***}$<br>(0.020) | 0.043$^{***}$<br>(0.006) | 0.020<br>(0.044) | 139 (51) | .010 (.008–.012) | .993 | .991 |
| 2013 | 0.223$^{***}$<br>(0.020) | 0.189$^{***}$<br>(0.016) | 0.042$^{***}$<br>(0.007) | −0.051<br>(0.039) | 145 (51) | .010 (.008–.012) | .989 | .986 |
| 2014 | 0.243$^{***}$<br>(0.034) | 0.133$^{***}$<br>(0.026) | 0.032$^{***}$<br>(0.007) | 0.017<br>(0.031) | 92 (51) | .007 (.004–.009) | .994 | .993 |
| 2014’ | 0.283$^{***}$<br>(0.034) | 0.148$^{***}$<br>(0.024) | 0.042$^{***}$<br>(0.009) | −0.003<br>(0.044) | 97 (42) | .008 (.006–.010) | .991 | .988 |
| Online banking (AvB) | | | | | | | | |
| 2012 | 0.258$^{***}$<br>(0.020) | 0.093$^{***}$<br>(0.023) | 0.024$^{***}$<br>(0.005) | 0.142$^{***}$<br>(0.034) | 143 (51) | .010 (.008–.012) | .993 | .990 |
| 2013 | 0.223$^{***}$<br>(0.020) | 0.173$^{***}$<br>(0.036) | 0.039$^{***}$<br>(0.008) | 0.108<br>(0.067) | 159 (51) | .011 (.009–.013) | .987 | .983 |
| 2014 | 0.243$^{***}$<br>(0.034) | 0.140$^{***}$<br>(0.023) | 0.034$^{***}$<br>(0.0070) | −0.011<br>(0.026) | 98 (51) | .007 (.005–.009) | .994 | .992 |
| 2014’ | 0.282$^{***}$<br>(0.033) | 0.135$^{***}$<br>(0.020) | 0.038$^{***}$<br>(0.007) | 0.032<br>(0.033) | 100 (42) | .009 (.006–.011) | .990 | .987 |
| Online social networking (AvN) | | | | | | | | |
| 2012 | 0.260$^{***}$<br>(0.020) | 0.061$^{*}$<br>(0.027) | 0.021$^{*}$<br>(0.010) | 0.121$^{***}$<br>(0.011) | 202 (51) | .013 (.011–.015) | .988 | .985 |
| 2013 | 0.225$^{***}$<br>(0.020) | 0.054<br>(0.033) | 0.012<br>(0.008) | 0.226$^{***}$<br>(0.030) | 169 (51) | .011 (.009–.013) | .986 | .982 |
| 2014 | 0.244$^{***}$<br>(0.035) | −0.022<br>(0.033) | −0.005<br>(0.008) | 0.161$^{***}$<br>(0.030) | 127 (51) | .009 (.007–.011) | .990 | .987 |
| 2014’ | 0.282$^{***}$<br>(0.033) | 0.047<br>(0.027) | 0.013<br>(0.008) | 0.017<br>(0.028) | 116 (42) | .010 (.008–.012) | .988 | .984 |
| Unknown websites (AvU) | | | | | | | | |
| 2012 | 0.258$^{***}$<br>(0.020) | 0.145$^{***}$<br>(0.025) | 0.037$^{***}$<br>(0.008) | −0.040<br>(0.027) | 140 (51) | .010 (.008–.012) | .993 | .991 |
| 2013 | 0.223$^{***}$<br>(0.020) | 0.125$^{***}$<br>(0.015) | 0.028$^{***}$<br>(0.008) | −0.042<br>(0.023) | 164 (51) | .011 (.009–.013) | .987 | .984 |
| 2014 | 0.244$^{***}$<br>(0.034) | 0.116$^{***}$<br>(0.014) | 0.028$^{***}$<br>(0.006) | −0.001<br>(0.017) | 126 (51) | .009 (.007–.011) | .990 | .987 |
| 2014’ | 0.283$^{***}$<br>(0.033) | 0.157$^{***}$<br>(0.017) | 0.051$^{***}$<br>(0.008) | −0.066$^{**}$<br>(0.022) | 92 (42) | .008 (.006–.010) | .991 | .989 |

Cybercrime Experience (EXP), Perc. Cybercrime Risk (PCR), Avoidance Intention (AV); Improved model: 2014’

## B.3 Descriptive Statistics Separated by User Confidence

**Table B.5:** Descriptive statistics of indicators for 2012 (separated by *User Confidence*)

| ID | Latent variable (scale)/ indicator | Answers | | |
|---|---|---|---|---|
| | Group of users | All* | Confident | Unconfident |
| | Number of respondents (normalized weights) | 18 605 | 4 972 | 2 196 |
| **EXP** | **Cybercrime Experience (Ordinal)** | | | |
| "How often have you experienced or been victim of . . . ?" – At least occasionally | | | | |
| exp1 | Identity theft | 8.22 % | 9.18 % | 4.81 % |
| exp2 | Receiving spam emails (or phone calls) | 38.25 % | 52.94 % | 20.54 % |
| exp3 | Online shopping fraud | 12.52 % | 16.47 % | 6.24 % |
| exp4 | Encountering illegal content | 15.38 % | 18.89 % | 9.47 % |
| exp6 | Unavailable online services (due to cyber-attacks) | 12.87 % | 16.42 % | 5.98 % |
| **MA** | **Media Awareness (Binary)** | | | |
| "In the last year have you heard about cybercrime from . . . ?" – Yes | | | | |
| ma1 | Television | 67.14 % | 69.81 % | 65.62 % |
| ma2 | Radio | 23.09 % | 30.02 % | 16.83 % |
| ma3 | Newspaper | 33.56 % | 41.51 % | 21.19 % |
| ma4 | Internet | 34.54 % | 49.10 % | 17.34 % |
| **PCR** | **Perceived Cybercrime Risk (Ordinal)** | | | |
| "How concerned are you personally about becoming a victim of . . . ?" – At least fairly | | | | |
| pcr1 | Identity theft | 61.77 % | 54.12 % | 67.03 % |
| pcr2 | Receiving spam emails (or phone calls) | 48.39 % | 37.98 % | 55.86 % |
| pcr3 | Online shopping fraud | 49.30 % | 44.05 % | 50.29 % |
| pcr4 | Encountering child pornography | 51.03 % | 44.60 % | 59.63 % |
| pcr5 | Encountering content of racial hatred | 41.03 % | 32.91 % | 50.37 % |
| pcr6 | Unavailable online services (due to cyber-attacks) | 43.07 % | 39.07 % | 42.86 % |
| **AV** | **(Behavioral) Avoidance Intention (Binary)** | | | |
| "Has concern about security issues made you change the way you use the Internet?" – Yes | | | | |
| avS | I'm less likely to do online shopping | 17.85 % | 11.42 % | 27.25 % |
| avB | I'm less likely to do online banking | 14.67 % | 9.05 % | 24.38 % |
| avN | I'm less likely to publish personal information online | 37.04 % | 39.36 % | 29.84 % |

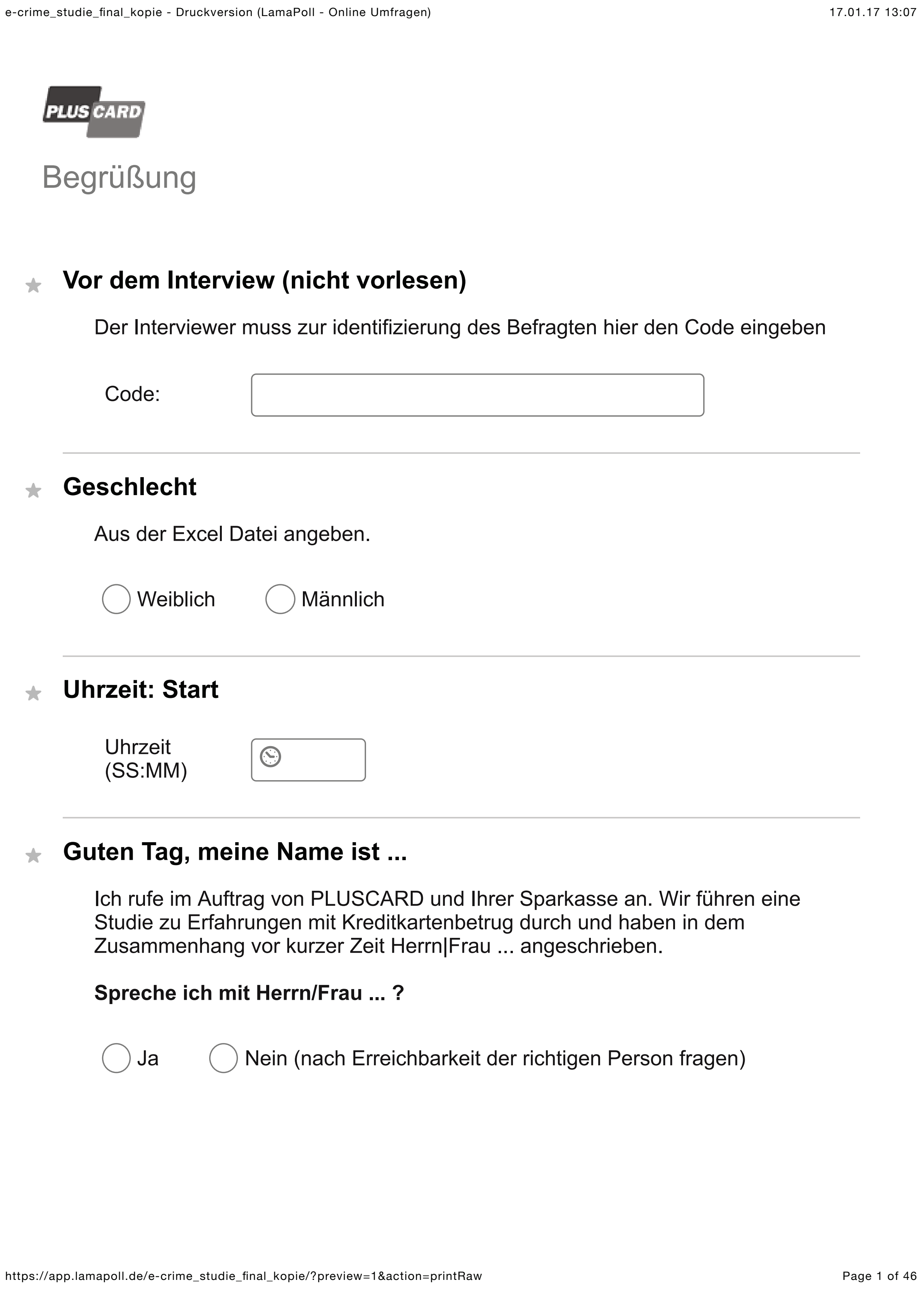
*EU Internet users above the age of 15.

# Appendix C

# Case Study: Credit Card Fraud

## C.1 Data Collection

### C.1.1 Questionnaire



PLUS CARD

## Begrüßung

### ★ Vor dem Interview (nicht vorlesen)

Der Interviewer muss zur identifizierung des Befragten hier den Code eingeben

Code:

### ★ Geschlecht

Aus der Excel Datei angeben.

○ Weiblich ○ Männlich

### ★ Uhrzeit: Start

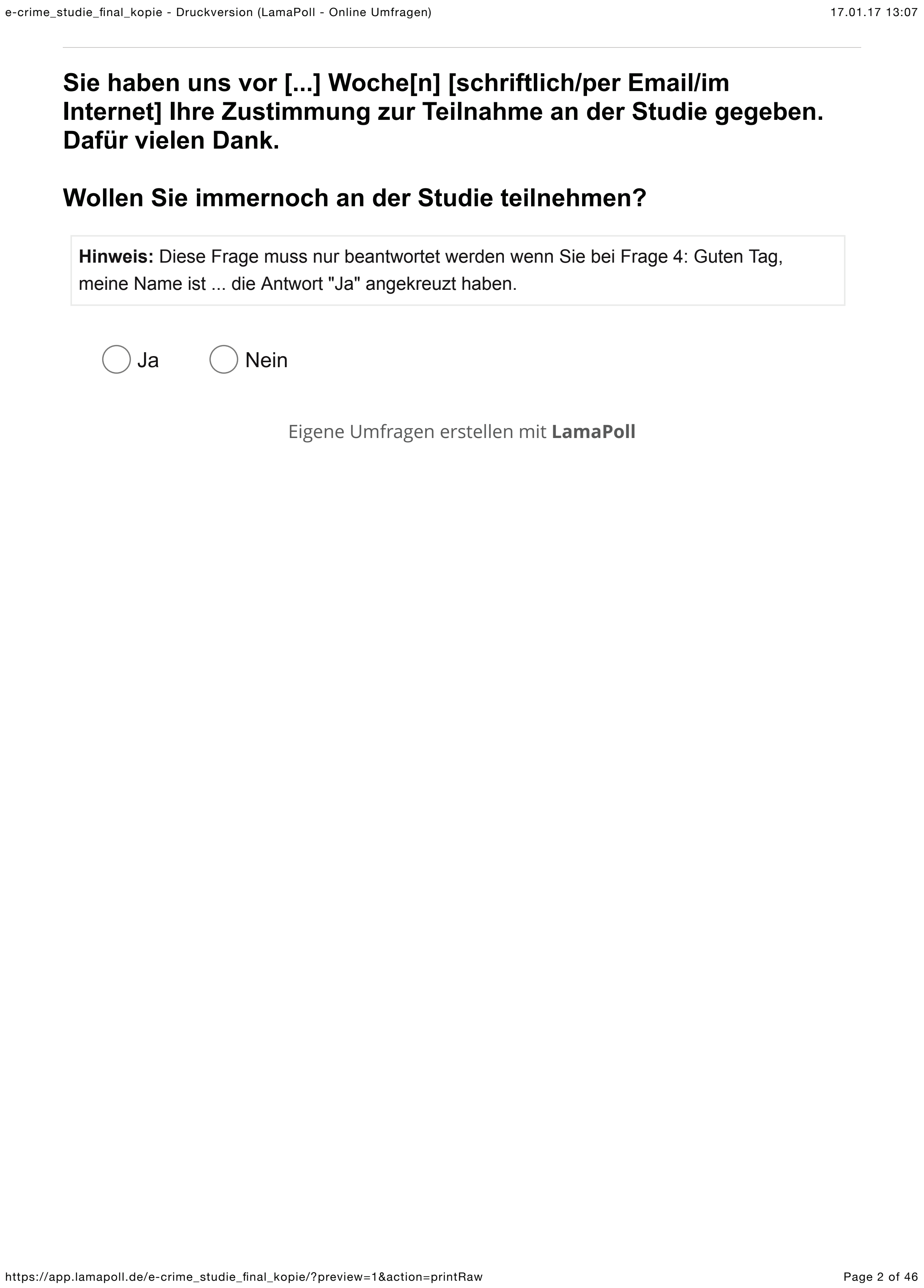
Uhrzeit (SS:MM)

### ★ Guten Tag, meine Name ist ...

Ich rufe im Auftrag von PLUSCARD und Ihrer Sparkasse an. Wir führen eine Studie zu Erfahrungen mit Kreditkartenbetrug durch und haben in dem Zusammenhang vor kurzer Zeit Herrn|Frau ... angeschrieben.

**Spreche ich mit Herrn/Frau ... ?**

○ Ja ○ Nein (nach Erreichbarkeit der richtigen Person fragen)



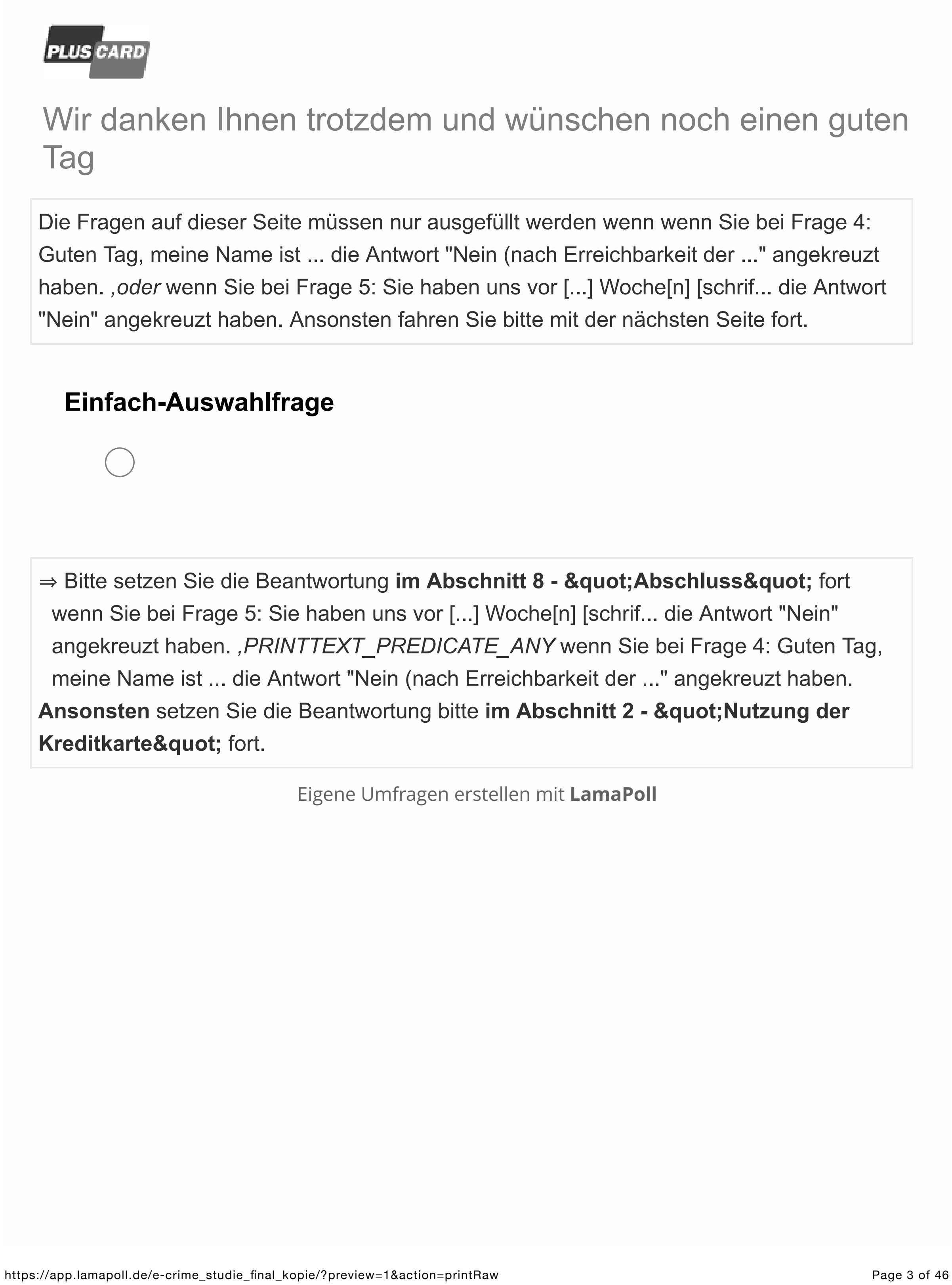
**Sie haben uns vor [...] Woche[n] [schriftlich/per Email/im Internet] Ihre Zustimmung zur Teilnahme an der Studie gegeben. Dafür vielen Dank.**

**Wollen Sie immernoch an der Studie teilnehmen?**

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 4: Guten Tag, meine Name ist ... die Antwort "Ja" angekreuzt haben.

○ Ja ○ Nein

Eigene Umfragen erstellen mit **LamaPoll**



PLUS CARD

# Wir danken Ihnen trotzdem und wünschen noch einen guten Tag

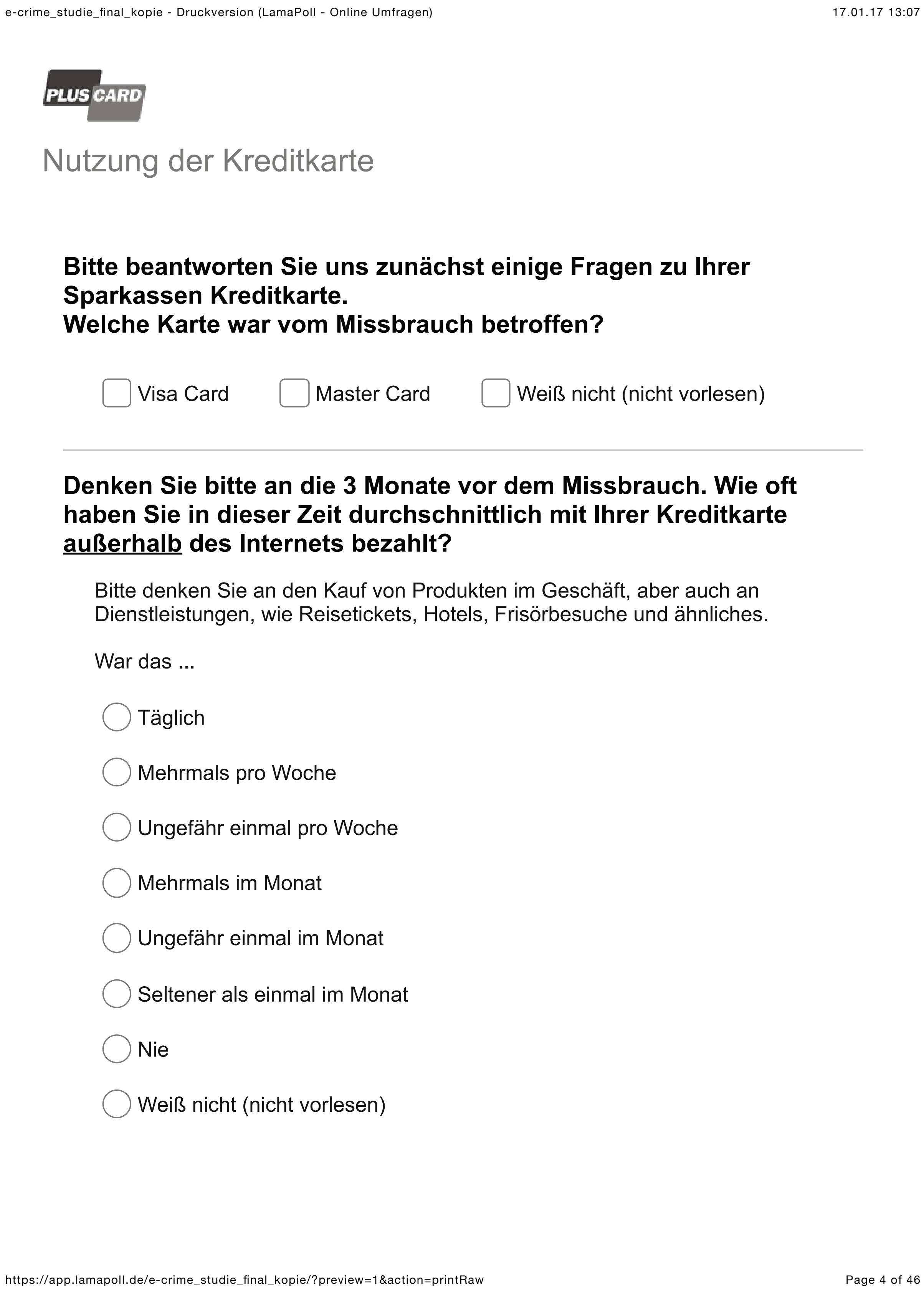
Die Fragen auf dieser Seite müssen nur ausgefüllt werden wenn wenn Sie bei Frage 4: Guten Tag, meine Name ist ... die Antwort "Nein (nach Erreichbarkeit der ..." angekreuzt haben. *,oder* wenn Sie bei Frage 5: Sie haben uns vor [...] Woche[n] [schrif... die Antwort "Nein" angekreuzt haben. Ansonsten fahren Sie bitte mit der nächsten Seite fort.

## Einfach-Auswahlfrage

○

⇒ Bitte setzen Sie die Beantwortung **im Abschnitt 8 - &quot;Abschluss&quot;** fort wenn Sie bei Frage 5: Sie haben uns vor [...] Woche[n] [schrif... die Antwort "Nein" angekreuzt haben. *,PRINTTEXT_PREDICATE_ANY* wenn Sie bei Frage 4: Guten Tag, meine Name ist ... die Antwort "Nein (nach Erreichbarkeit der ..." angekreuzt haben.
**Ansonsten** setzen Sie die Beantwortung bitte **im Abschnitt 2 - &quot;Nutzung der Kreditkarte&quot;** fort.

Eigene Umfragen erstellen mit **LamaPoll**



## Nutzung der Kreditkarte

**Bitte beantworten Sie uns zunächst einige Fragen zu Ihrer Sparkassen Kreditkarte.**
**Welche Karte war vom Missbrauch betroffen?**

□ Visa Card □ Master Card □ Weiß nicht (nicht vorlesen)

**Denken Sie bitte an die 3 Monate vor dem Missbrauch. Wie oft haben Sie in dieser Zeit durchschnittlich mit Ihrer Kreditkarte außerhalb des Internets bezahlt?**

Bitte denken Sie an den Kauf von Produkten im Geschäft, aber auch an Dienstleistungen, wie Reisetickets, Hotels, Frisörbesuche und ähnliches.

War das ...

○ Täglich

○ Mehrmals pro Woche

○ Ungefähr einmal pro Woche

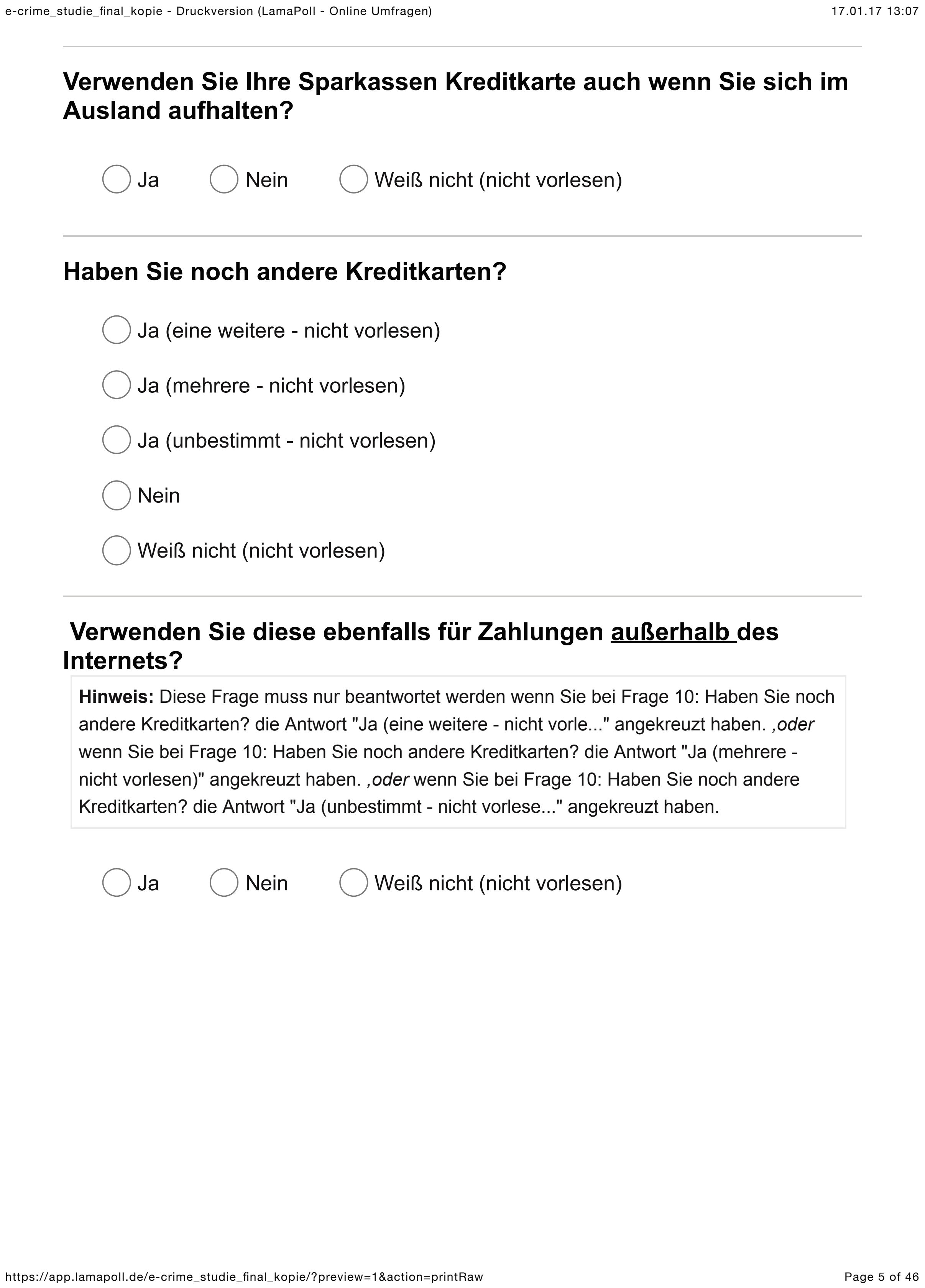
○ Mehrmals im Monat

○ Ungefähr einmal im Monat

○ Seltener als einmal im Monat

○ Nie

○ Weiß nicht (nicht vorlesen)



**Verwenden Sie Ihre Sparkassen Kreditkarte auch wenn Sie sich im Ausland aufhalten?**

○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)

**Haben Sie noch andere Kreditkarten?**

○ Ja (eine weitere - nicht vorlesen)

○ Ja (mehrere - nicht vorlesen)

○ Ja (unbestimmt - nicht vorlesen)

○ Nein

○ Weiß nicht (nicht vorlesen)

**Verwenden Sie diese ebenfalls für Zahlungen außerhalb des Internets?**

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 10: Haben Sie noch andere Kreditkarten? die Antwort "Ja (eine weitere - nicht vorle..." angekreuzt haben. *,oder* wenn Sie bei Frage 10: Haben Sie noch andere Kreditkarten? die Antwort "Ja (mehrere - nicht vorlesen)" angekreuzt haben. *,oder* wenn Sie bei Frage 10: Haben Sie noch andere Kreditkarten? die Antwort "Ja (unbestimmt - nicht vorlese..." angekreuzt haben.

○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)

### Welches Zahlungsmittel verwenden Sie hauptsächlich für Zahlungen außerhalb des Internets?

Bei Unsicherheit erinnern. Bitte denken Sie an den Kauf von Produkten im Geschäft, aber auch an Dienstleistungen, wie Reisetickets, Hotels, Frisörbesuche und ähnliches.

○ Ihre Sparkassen-Kreditkarte

○ Andere Kreditkarten

○ Eine EC-Karte

○ Bargeld

○ Ein anderes Zahlungsmittel (nicht vorlesen)

○ Weiß nicht (nicht vorlesen)

### Und welches Zahlungsmittel verwenden Sie hauptsächlich wenn Sie sich im Ausland aufhalten?

Bei Unsicherheit erinnern. Bitte denken Sie an den Kauf von Produkten im Geschäft, aber auch an Dienstleistungen, wie Reisetickets, Hotels, Frisörbesuche und ähnliches.

○ Ihre Sparkassen-Kreditkarte

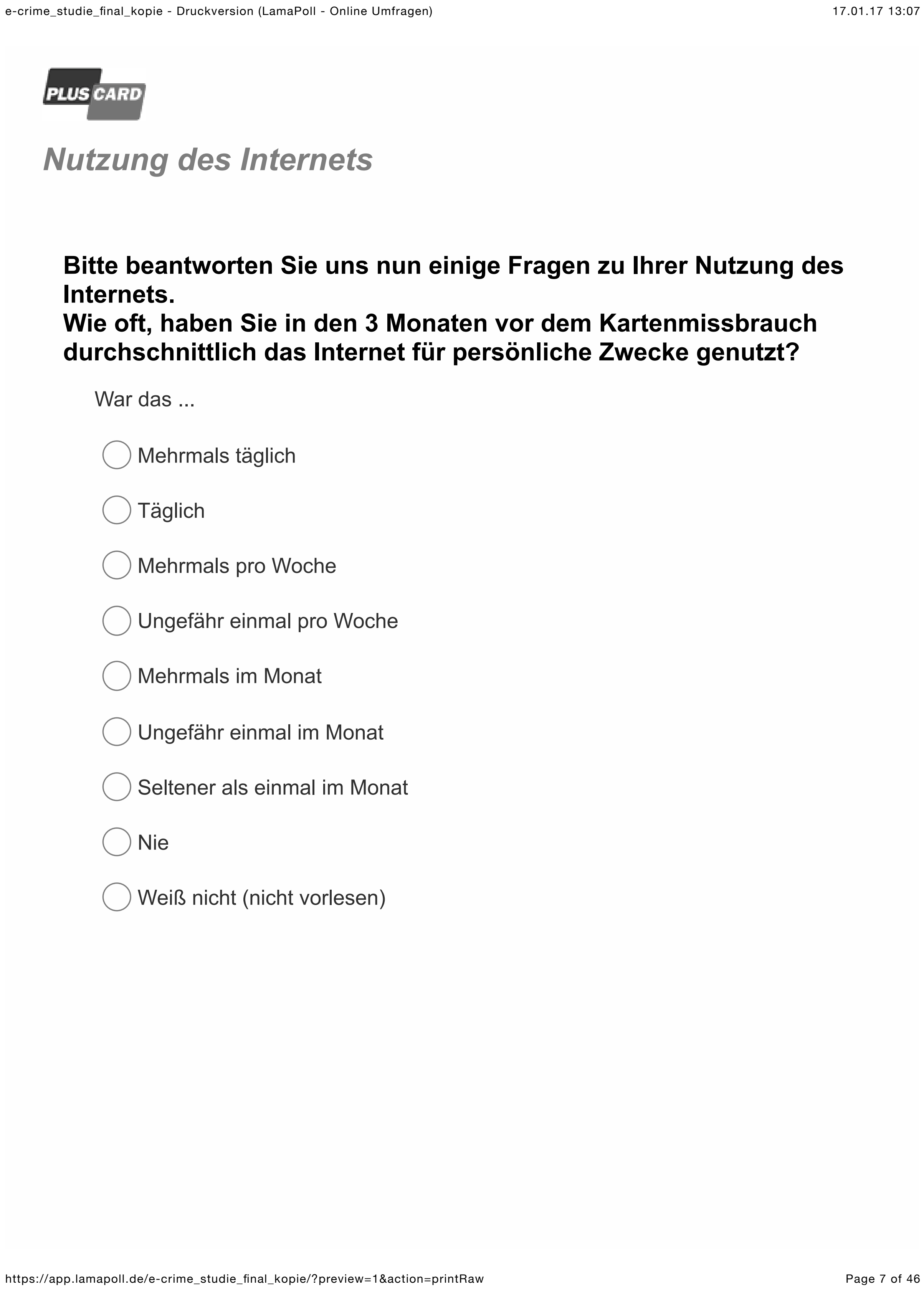
○ Andere Kreditkarten

○ Eine EC-Karte

○ Bargeld

○ Ein anderes Zahlungsmittel (nicht vorlesen)

○ Weiß nicht (nicht vorlesen)



e-crime_studie_final_kopie - Druckversion (LamaPoll - Online Umfragen) 17.01.17 13:07

## Nutzung des Internets

**Bitte beantworten Sie uns nun einige Fragen zu Ihrer Nutzung des Internets.**
**Wie oft, haben Sie in den 3 Monaten vor dem Kartenmissbrauch durchschnittlich das Internet für persönliche Zwecke genutzt?**

War das ...

○ Mehrmals täglich

○ Täglich

○ Mehrmals pro Woche

○ Ungefähr einmal pro Woche

○ Mehrmals im Monat

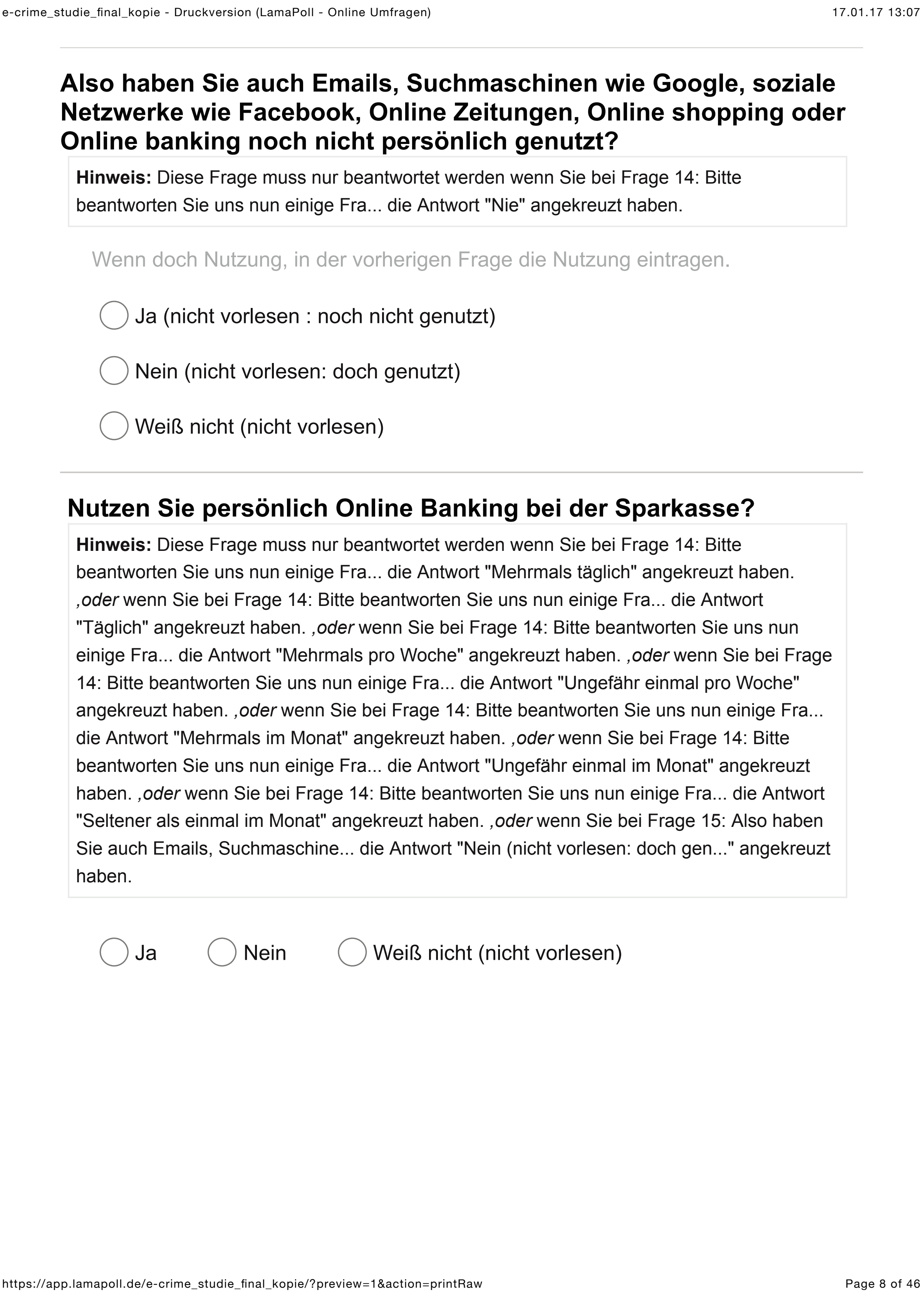
○ Ungefähr einmal im Monat

○ Seltener als einmal im Monat

○ Nie

○ Weiß nicht (nicht vorlesen)

https://app.lamapoll.de/e-crime_studie_final_kopie/?preview=1&action=printRaw Page 7 of 46



## Also haben Sie auch Emails, Suchmaschinen wie Google, soziale Netzwerke wie Facebook, Online Zeitungen, Online shopping oder Online banking noch nicht persönlich genutzt?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 14: Bitte beantworten Sie uns nun einige Fra... die Antwort "Nie" angekreuzt haben.

Wenn doch Nutzung, in der vorherigen Frage die Nutzung eintragen.

○ Ja (nicht vorlesen : noch nicht genutzt)

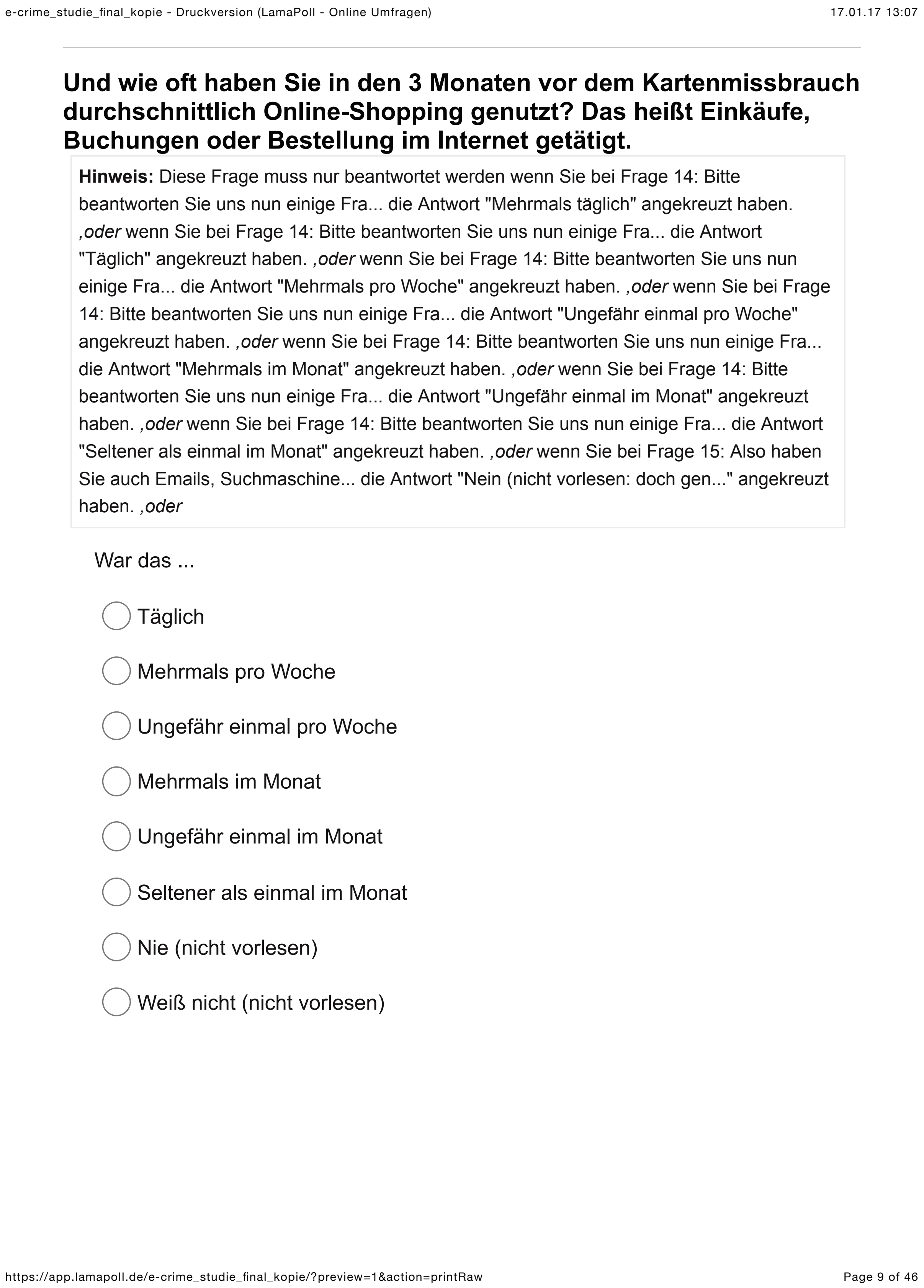
○ Nein (nicht vorlesen: doch genutzt)

○ Weiß nicht (nicht vorlesen)

## Nutzen Sie persönlich Online Banking bei der Sparkasse?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 14: Bitte beantworten Sie uns nun einige Fra... die Antwort "Mehrmals täglich" angekreuzt haben. *,oder* wenn Sie bei Frage 14: Bitte beantworten Sie uns nun einige Fra... die Antwort "Täglich" angekreuzt haben. *,oder* wenn Sie bei Frage 14: Bitte beantworten Sie uns nun einige Fra... die Antwort "Mehrmals pro Woche" angekreuzt haben. *,oder* wenn Sie bei Frage 14: Bitte beantworten Sie uns nun einige Fra... die Antwort "Ungefähr einmal pro Woche" angekreuzt haben. *,oder* wenn Sie bei Frage 14: Bitte beantworten Sie uns nun einige Fra... die Antwort "Mehrmals im Monat" angekreuzt haben. *,oder* wenn Sie bei Frage 14: Bitte beantworten Sie uns nun einige Fra... die Antwort "Ungefähr einmal im Monat" angekreuzt haben. *,oder* wenn Sie bei Frage 14: Bitte beantworten Sie uns nun einige Fra... die Antwort "Seltener als einmal im Monat" angekreuzt haben. *,oder* wenn Sie bei Frage 15: Also haben Sie auch Emails, Suchmaschine... die Antwort "Nein (nicht vorlesen: doch gen..." angekreuzt haben.

○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)



**Und wie oft haben Sie in den 3 Monaten vor dem Kartenmissbrauch durchschnittlich Online-Shopping genutzt? Das heißt Einkäufe, Buchungen oder Bestellung im Internet getätigt.**

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 14: Bitte beantworten Sie uns nun einige Fra... die Antwort "Mehrmals täglich" angekreuzt haben. *,oder* wenn Sie bei Frage 14: Bitte beantworten Sie uns nun einige Fra... die Antwort "Täglich" angekreuzt haben. *,oder* wenn Sie bei Frage 14: Bitte beantworten Sie uns nun einige Fra... die Antwort "Mehrmals pro Woche" angekreuzt haben. *,oder* wenn Sie bei Frage 14: Bitte beantworten Sie uns nun einige Fra... die Antwort "Ungefähr einmal pro Woche" angekreuzt haben. *,oder* wenn Sie bei Frage 14: Bitte beantworten Sie uns nun einige Fra... die Antwort "Mehrmals im Monat" angekreuzt haben. *,oder* wenn Sie bei Frage 14: Bitte beantworten Sie uns nun einige Fra... die Antwort "Ungefähr einmal im Monat" angekreuzt haben. *,oder* wenn Sie bei Frage 14: Bitte beantworten Sie uns nun einige Fra... die Antwort "Seltener als einmal im Monat" angekreuzt haben. *,oder* wenn Sie bei Frage 15: Also haben Sie auch Emails, Suchmaschine... die Antwort "Nein (nicht vorlesen: doch gen..." angekreuzt haben. *,oder*

War das ...

○ Täglich

○ Mehrmals pro Woche

○ Ungefähr einmal pro Woche

○ Mehrmals im Monat

○ Ungefähr einmal im Monat

○ Seltener als einmal im Monat

○ Nie (nicht vorlesen)

○ Weiß nicht (nicht vorlesen)

## Treffen die folgenden Fragen zum Online-Shopping auf Sie zu?

### *Kaufen Sie Produkte und Dienstleistungen bei Online-Shops, von denen Sie vorher noch nichts gehört haben?*

○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)

### *Bestellen Sie nur bei Online-Shops, die von Ihnen bevorzugte Zahlungsarten anbieten?*

Bei Nachfrage. Hauptfrage: Treffen die folgenden Fragen zum Online-Shopping auf Sie zu?

○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)

### *Haben Sie schon auf Produkte oder Dienstleistungen komplett verzichtet, weil die von Ihnen bevorzugte Zahlungsart nicht angeboten wurde?*

Bei Nachfrage. Hauptfrage: Treffen die folgenden Fragen zum Online-Shopping auf Sie zu?

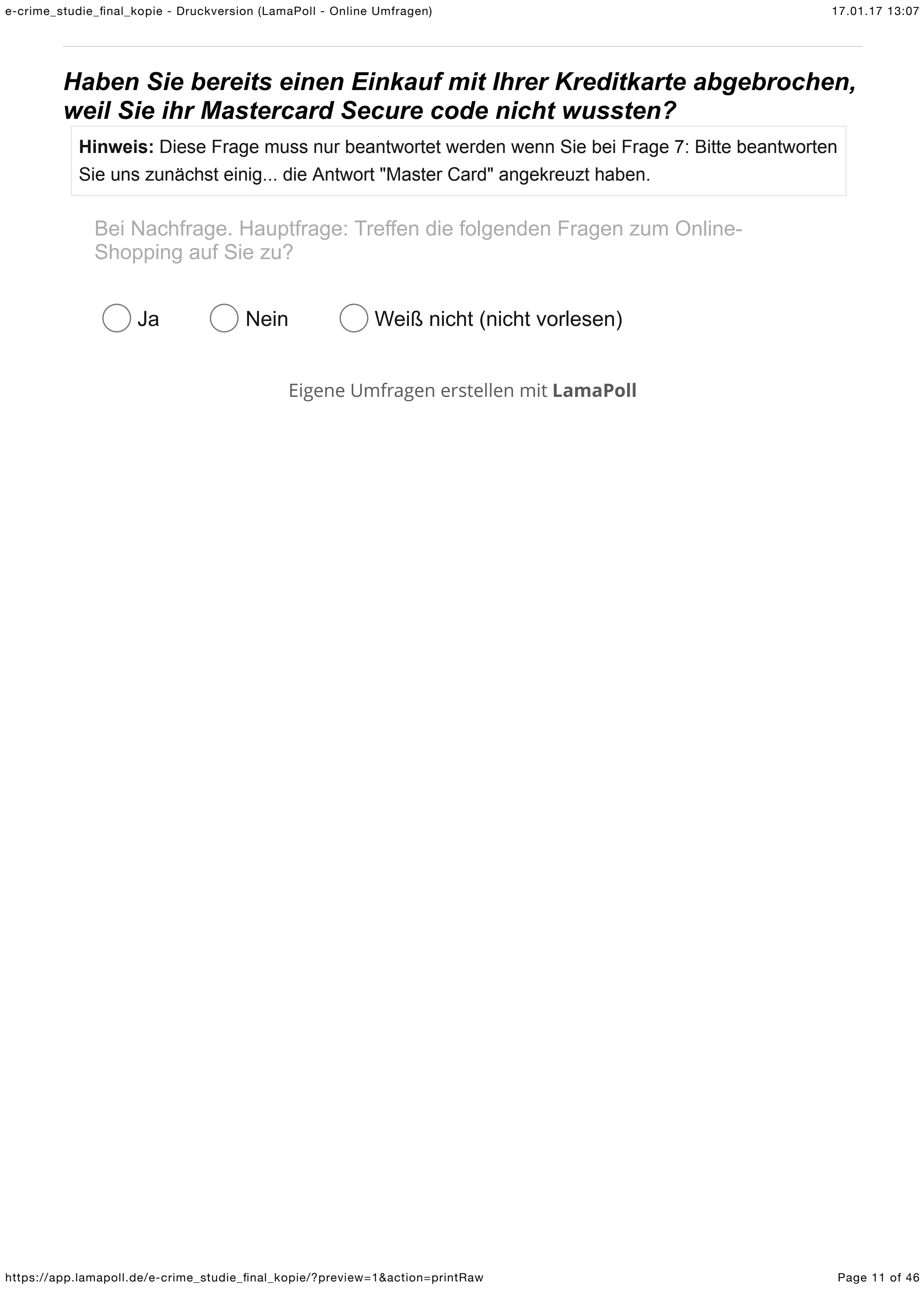
○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)

### *Haben Sie bereits einen Einkauf mit Ihrer Kreditkarte abgebrochen, weil Sie ihr Verified by Visa Passwort nicht wussten?*

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 7: Bitte beantworten Sie uns zunächst einig... die Antwort "Visa Card" angekreuzt haben.

Bei Nachfrage. Hauptfrage: Treffen die folgenden Fragen zum Online-Shopping auf Sie zu?

○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)



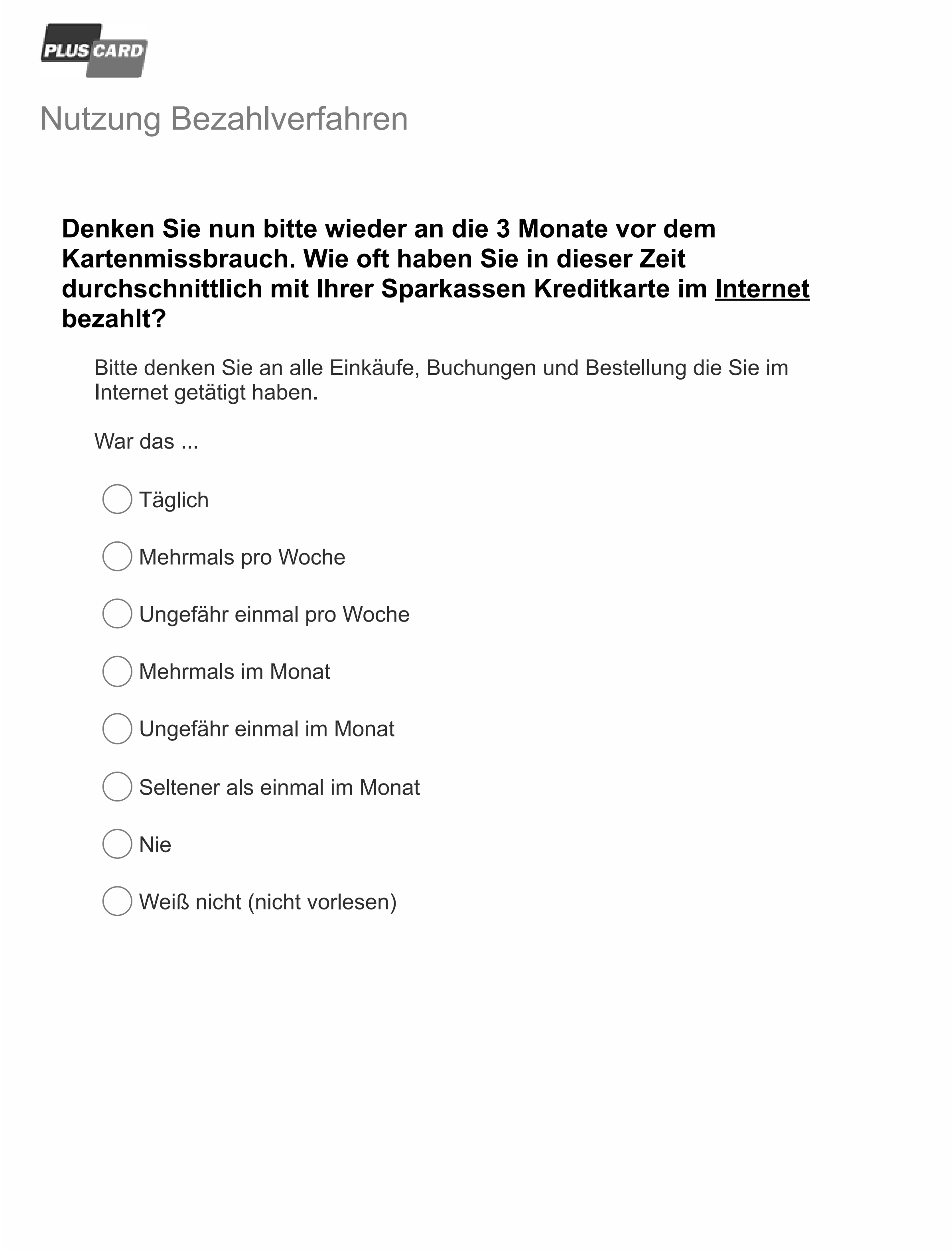
***Haben Sie bereits einen Einkauf mit Ihrer Kreditkarte abgebrochen, weil Sie ihr Mastercard Secure code nicht wussten?***

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 7: Bitte beantworten Sie uns zunächst einig... die Antwort "Master Card" angekreuzt haben.

Bei Nachfrage. Hauptfrage: Treffen die folgenden Fragen zum Online-Shopping auf Sie zu?

○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)

Eigene Umfragen erstellen mit **LamaPoll**



PLUS CARD

## Nutzung Bezahlverfahren

**Denken Sie nun bitte wieder an die 3 Monate vor dem Kartenmissbrauch. Wie oft haben Sie in dieser Zeit durchschnittlich mit Ihrer Sparkassen Kreditkarte im Internet bezahlt?**

Bitte denken Sie an alle Einkäufe, Buchungen und Bestellung die Sie im Internet getätigt haben.

War das ...

○ Täglich

○ Mehrmals pro Woche

○ Ungefähr einmal pro Woche

○ Mehrmals im Monat

○ Ungefähr einmal im Monat

○ Seltener als einmal im Monat

○ Nie

○ Weiß nicht (nicht vorlesen)

**Online-Shops bieten neben der Kreditkarte verschiedene Zahlungsarten an. Welche der folgenden klassischen Zahlungsarten haben Sie im Internet schon genutzt?**
**Bitte antworten Sie mit *"Ja, schon genutzt"*, *"Nein, noch nicht genutzt"* oder "*Kenne ich nicht*".**

### Bezahlung per Rechnung

○ Ja, schon genutzt

○ Nein, noch nicht genutzt

○ Kenne ich nicht

○ Weiß nicht (nicht vorlesen)

### Lastschriftverfahren

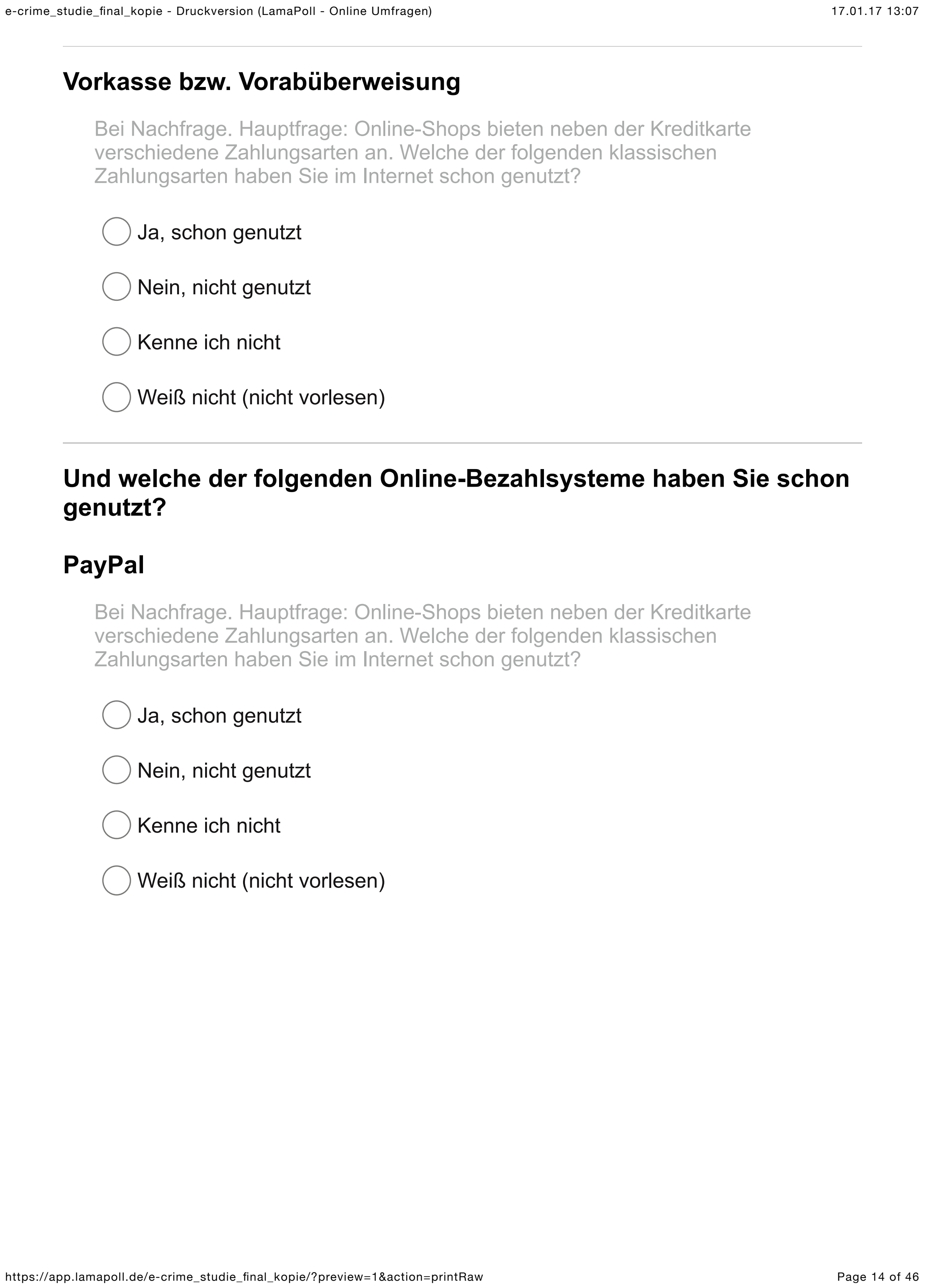
Bei Nachfrage. Hauptfrage: Online-Shops bieten neben der Kreditkarte verschiedene Zahlungsarten an. Welche der folgenden klassischen Zahlungsarten haben Sie im Internet schon genutzt?

○ Ja, schon genutzt

○ Nein, nicht genutzt

○ Kenne ich nicht

○ Weiß nicht (nicht vorlesen)



## Vorkasse bzw. Vorabüberweisung

Bei Nachfrage. Hauptfrage: Online-Shops bieten neben der Kreditkarte verschiedene Zahlungsarten an. Welche der folgenden klassischen Zahlungsarten haben Sie im Internet schon genutzt?

○ Ja, schon genutzt

○ Nein, nicht genutzt

○ Kenne ich nicht

○ Weiß nicht (nicht vorlesen)

## Und welche der folgenden Online-Bezahlsysteme haben Sie schon genutzt?

## PayPal

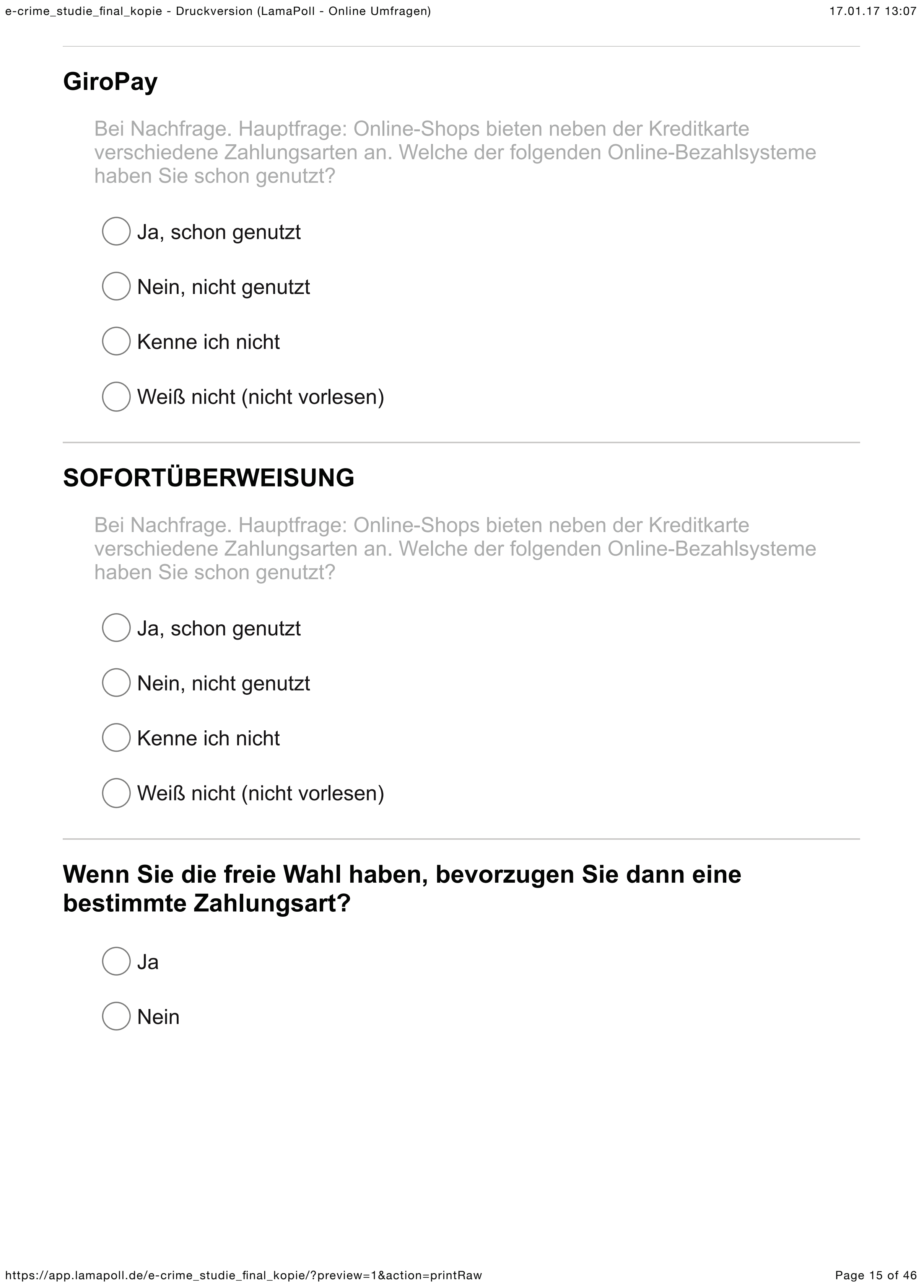
Bei Nachfrage. Hauptfrage: Online-Shops bieten neben der Kreditkarte verschiedene Zahlungsarten an. Welche der folgenden klassischen Zahlungsarten haben Sie im Internet schon genutzt?

○ Ja, schon genutzt

○ Nein, nicht genutzt

○ Kenne ich nicht

○ Weiß nicht (nicht vorlesen)



## GiroPay

Bei Nachfrage. Hauptfrage: Online-Shops bieten neben der Kreditkarte verschiedene Zahlungsarten an. Welche der folgenden Online-Bezahlsysteme haben Sie schon genutzt?

○ Ja, schon genutzt

○ Nein, nicht genutzt

○ Kenne ich nicht

○ Weiß nicht (nicht vorlesen)

## SOFORTÜBERWEISUNG

Bei Nachfrage. Hauptfrage: Online-Shops bieten neben der Kreditkarte verschiedene Zahlungsarten an. Welche der folgenden Online-Bezahlsysteme haben Sie schon genutzt?

○ Ja, schon genutzt

○ Nein, nicht genutzt

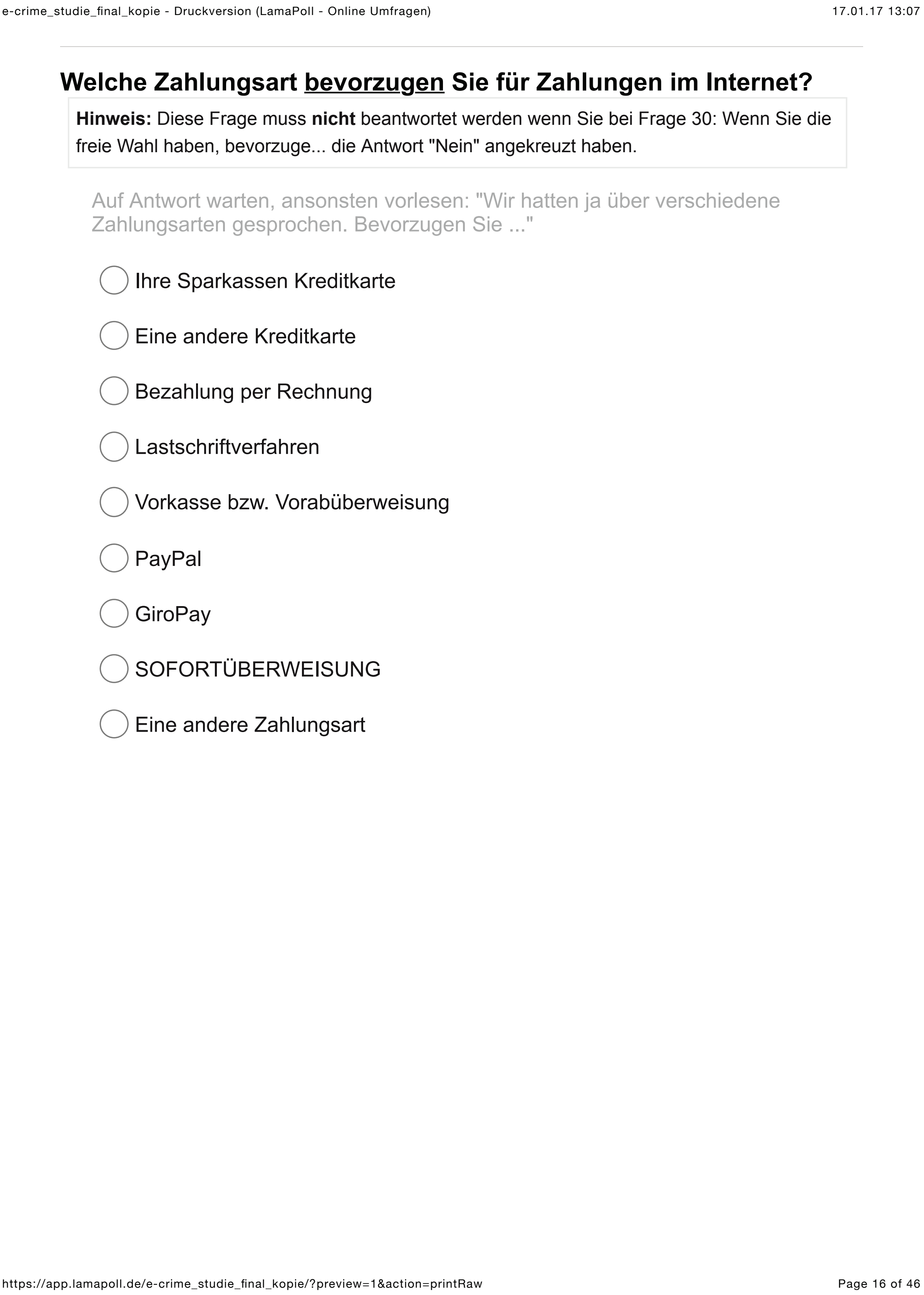
○ Kenne ich nicht

○ Weiß nicht (nicht vorlesen)

## Wenn Sie die freie Wahl haben, bevorzugen Sie dann eine bestimmte Zahlungsart?

○ Ja

○ Nein



## Welche Zahlungsart bevorzugen Sie für Zahlungen im Internet?

**Hinweis:** Diese Frage muss **nicht** beantwortet werden wenn Sie bei Frage 30: Wenn Sie die freie Wahl haben, bevorzuge... die Antwort "Nein" angekreuzt haben.

Auf Antwort warten, ansonsten vorlesen: "Wir hatten ja über verschiedene Zahlungsarten gesprochen. Bevorzugen Sie ..."

○ Ihre Sparkassen Kreditkarte

○ Eine andere Kreditkarte

○ Bezahlung per Rechnung

○ Lastschriftverfahren

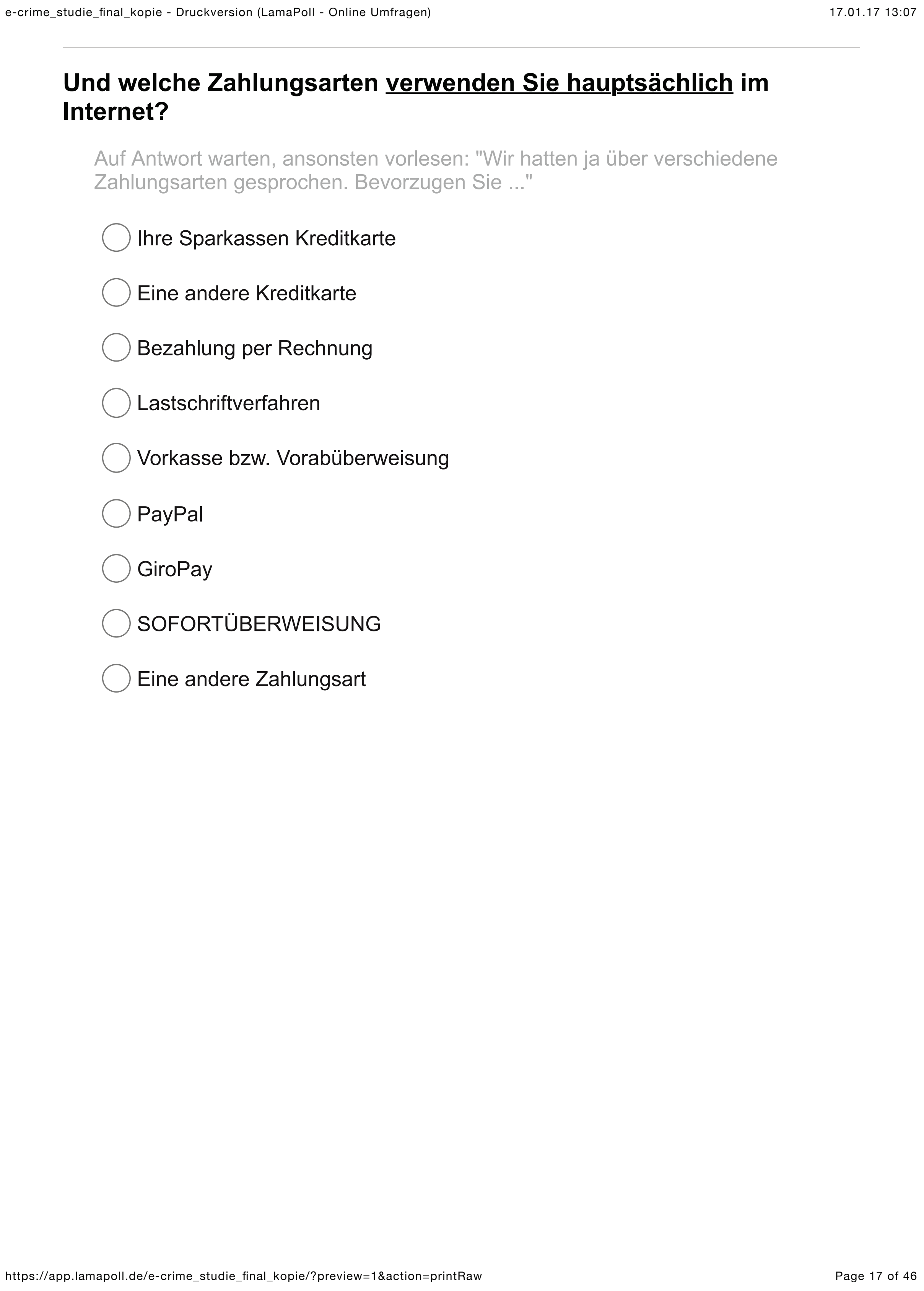
○ Vorkasse bzw. Vorabüberweisung

○ PayPal

○ GiroPay

○ SOFORTÜBERWEISUNG

○ Eine andere Zahlungsart



## Und welche Zahlungsarten verwenden Sie hauptsächlich im Internet?

Auf Antwort warten, ansonsten vorlesen: "Wir hatten ja über verschiedene Zahlungsarten gesprochen. Bevorzugen Sie ..."

○ Ihre Sparkassen Kreditkarte

○ Eine andere Kreditkarte

○ Bezahlung per Rechnung

○ Lastschriftverfahren

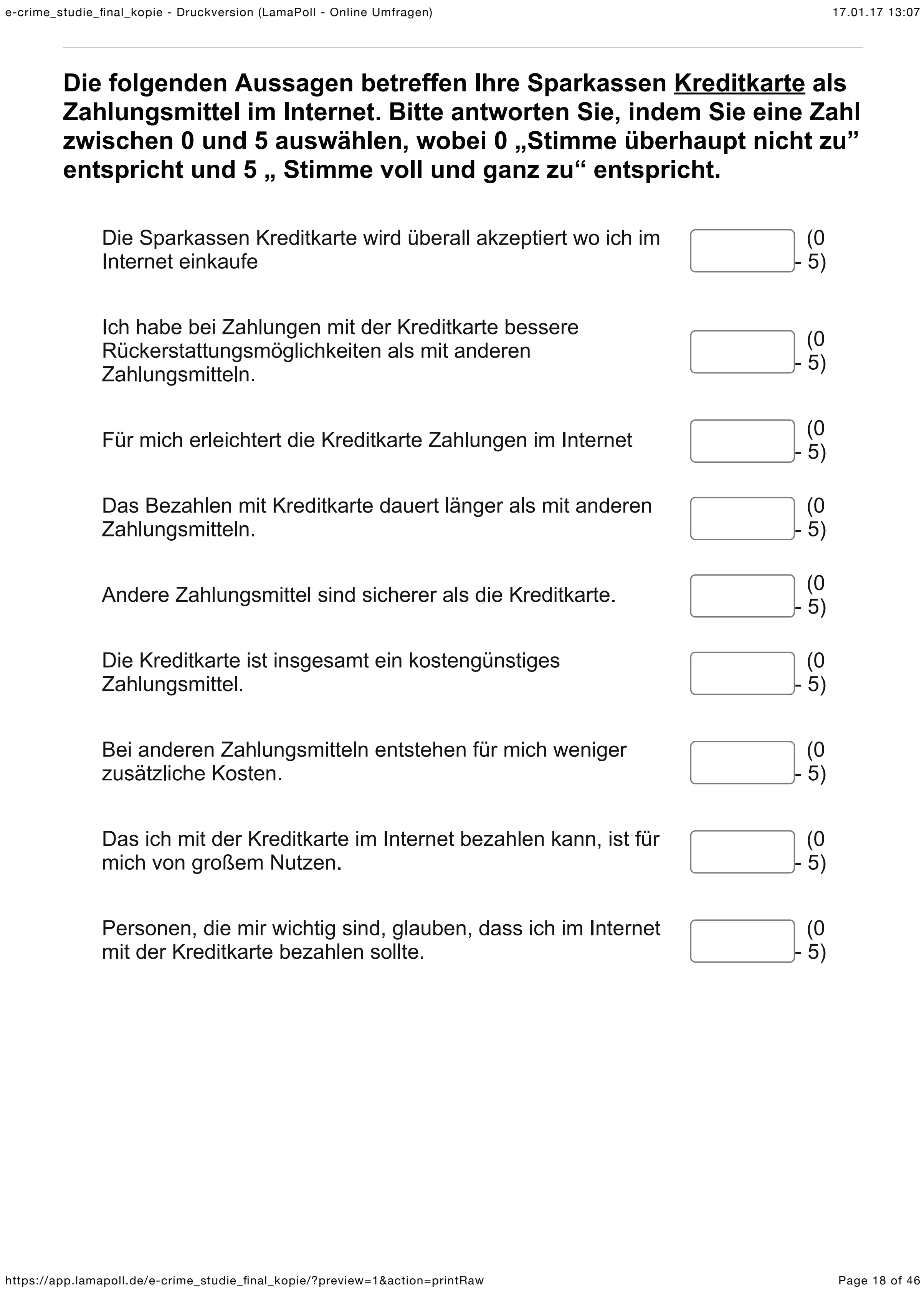
○ Vorkasse bzw. Vorabüberweisung

○ PayPal

○ GiroPay

○ SOFORTÜBERWEISUNG

○ Eine andere Zahlungsart



**Die folgenden Aussagen betreffen Ihre Sparkassen Kreditkarte als Zahlungsmittel im Internet. Bitte antworten Sie, indem Sie eine Zahl zwischen 0 und 5 auswählen, wobei 0 „Stimme überhaupt nicht zu” entspricht und 5 „ Stimme voll und ganz zu“ entspricht.**

Die Sparkassen Kreditkarte wird überall akzeptiert wo ich im Internet einkaufe □ (0 - 5)

Ich habe bei Zahlungen mit der Kreditkarte bessere Rückerstattungsmöglichkeiten als mit anderen Zahlungsmitteln. □ (0 - 5)

Für mich erleichtert die Kreditkarte Zahlungen im Internet □ (0 - 5)

Das Bezahlen mit Kreditkarte dauert länger als mit anderen Zahlungsmitteln. □ (0 - 5)

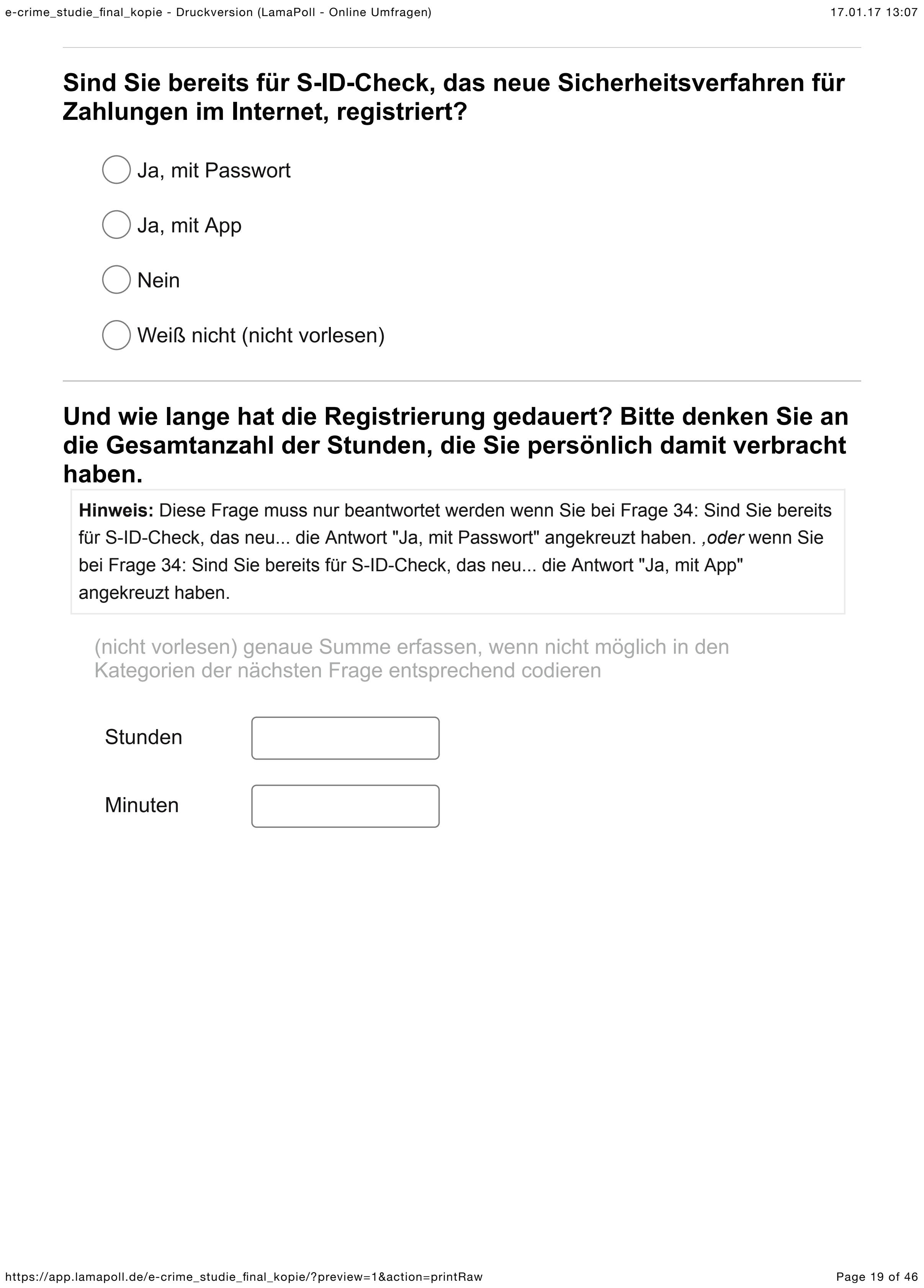
Andere Zahlungsmittel sind sicherer als die Kreditkarte. □ (0 - 5)

Die Kreditkarte ist insgesamt ein kostengünstiges Zahlungsmittel. □ (0 - 5)

Bei anderen Zahlungsmitteln entstehen für mich weniger zusätzliche Kosten. □ (0 - 5)

Das ich mit der Kreditkarte im Internet bezahlen kann, ist für mich von großem Nutzen. □ (0 - 5)

Personen, die mir wichtig sind, glauben, dass ich im Internet mit der Kreditkarte bezahlen sollte. □ (0 - 5)



## Sind Sie bereits für S-ID-Check, das neue Sicherheitsverfahren für Zahlungen im Internet, registriert?

○ Ja, mit Passwort

○ Ja, mit App

○ Nein

○ Weiß nicht (nicht vorlesen)

## Und wie lange hat die Registrierung gedauert? Bitte denken Sie an die Gesamtanzahl der Stunden, die Sie persönlich damit verbracht haben.

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 34: Sind Sie bereits für S-ID-Check, das neu... die Antwort "Ja, mit Passwort" angekreuzt haben. *,oder* wenn Sie bei Frage 34: Sind Sie bereits für S-ID-Check, das neu... die Antwort "Ja, mit App" angekreuzt haben.

(nicht vorlesen) genaue Summe erfassen, wenn nicht möglich in den Kategorien der nächsten Frage entsprechend codieren

Stunden □

Minuten □

## Können Sie den Zeitaufwand in eine der folgenden Kategorien einordnen?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 34: Sind Sie bereits für S-ID-Check, das neu... die Antwort "Ja, mit Passwort" angekreuzt haben. *,oder* wenn Sie bei Frage 34: Sind Sie bereits für S-ID-Check, das neu... die Antwort "Ja, mit App" angekreuzt haben.

(falls keine genaue Zeit bekannt)

○ Weniger als 5 Minuten

○ 5 Minuten bis weniger als 15 Minuten

○ 15 Minuten bis weniger als 30 Minuten

○ 30 Minuten bis weniger als 1 Stunde

○ 1 Stunde bis weniger als 2 Stunden

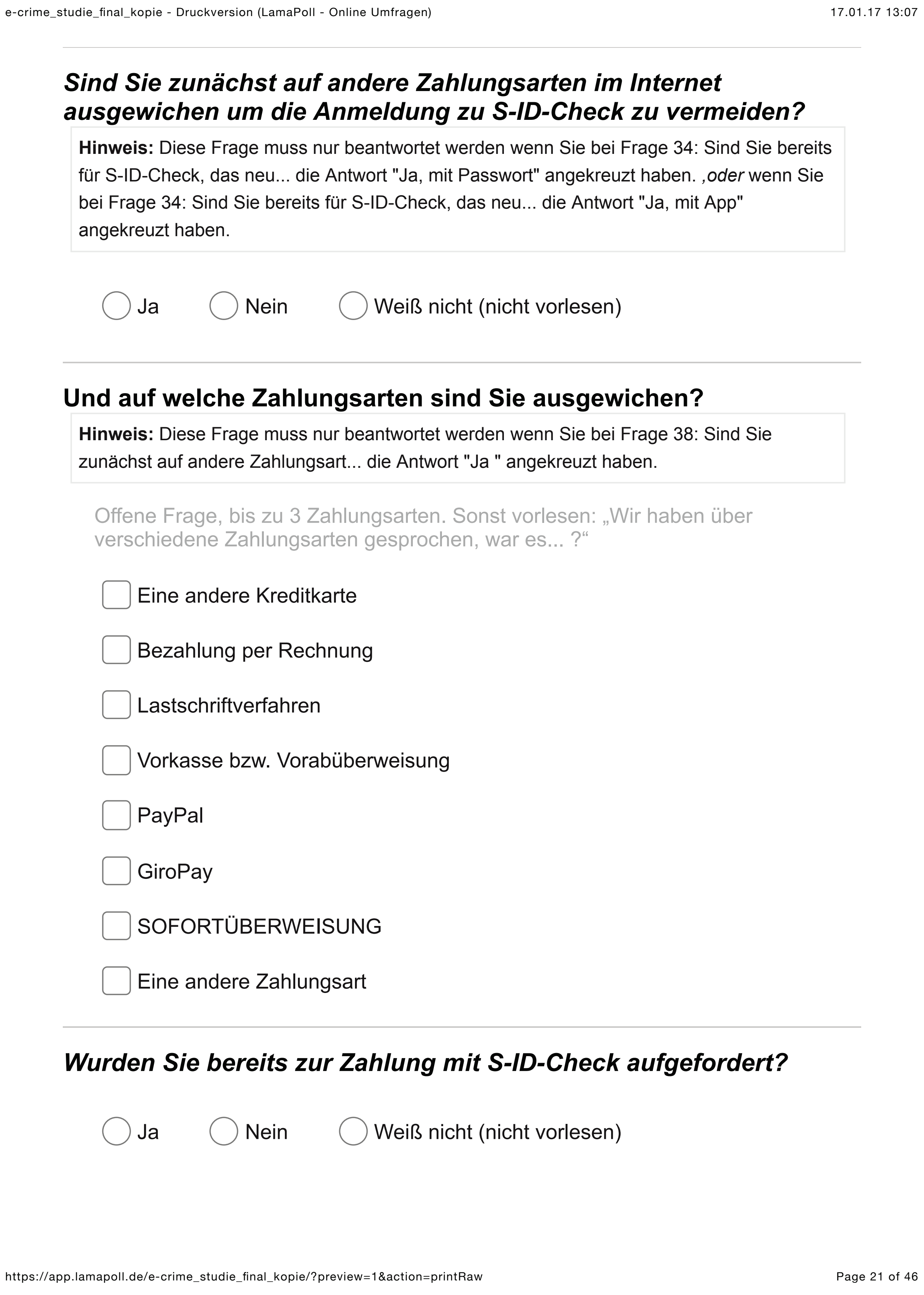
○ 2 Stunden oder mehr

○ Weiß nicht (nicht vorlesen)

## Fanden Sie die Anmeldung zu S-ID-Check war problemlos?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 34: Sind Sie bereits für S-ID-Check, das neu... die Antwort "Ja, mit Passwort" angekreuzt haben. *,oder* wenn Sie bei Frage 34: Sind Sie bereits für S-ID-Check, das neu... die Antwort "Ja, mit App" angekreuzt haben.

○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)



## *Sind Sie zunächst auf andere Zahlungsarten im Internet ausgewichen um die Anmeldung zu S-ID-Check zu vermeiden?*

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 34: Sind Sie bereits für S-ID-Check, das neu... die Antwort "Ja, mit Passwort" angekreuzt haben. *,oder* wenn Sie bei Frage 34: Sind Sie bereits für S-ID-Check, das neu... die Antwort "Ja, mit App" angekreuzt haben.

○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)

## Und auf welche Zahlungsarten sind Sie ausgewichen?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 38: Sind Sie zunächst auf andere Zahlungsart... die Antwort "Ja " angekreuzt haben.

Offene Frage, bis zu 3 Zahlungsarten. Sonst vorlesen: „Wir haben über verschiedene Zahlungsarten gesprochen, war es... ?“

□ Eine andere Kreditkarte

□ Bezahlung per Rechnung

□ Lastschriftverfahren

□ Vorkasse bzw. Vorabüberweisung

□ PayPal

□ GiroPay

□ SOFORTÜBERWEISUNG

□ Eine andere Zahlungsart

## *Wurden Sie bereits zur Zahlung mit S-ID-Check aufgefordert?*

○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)

## *Würden Sie sagen S-ID-Check macht das Bezahlen im Internet unnötig kompliziert?*

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 34: Sind Sie bereits für S-ID-Check, das neu... die Antwort "Ja, mit Passwort" angekreuzt haben. *,oder* wenn Sie bei Frage 34: Sind Sie bereits für S-ID-Check, das neu... die Antwort "Ja, mit App" angekreuzt haben.

○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)

## Und warum haben Sie sich bisher nicht für S-ID-Check registriert?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 34: Sind Sie bereits für S-ID-Check, das neu... die Antwort "Nein" angekreuzt haben.

**Offene Frage!** Auf Antwort warten und zuordnen. Wenn keine Antwort, dann nachfragen

□ Keine Möglichkeit

□ Bisher nicht nötig

□ Zu schwierig

□ Kein Handy oder Smartphone

□ Halte es für unsicher

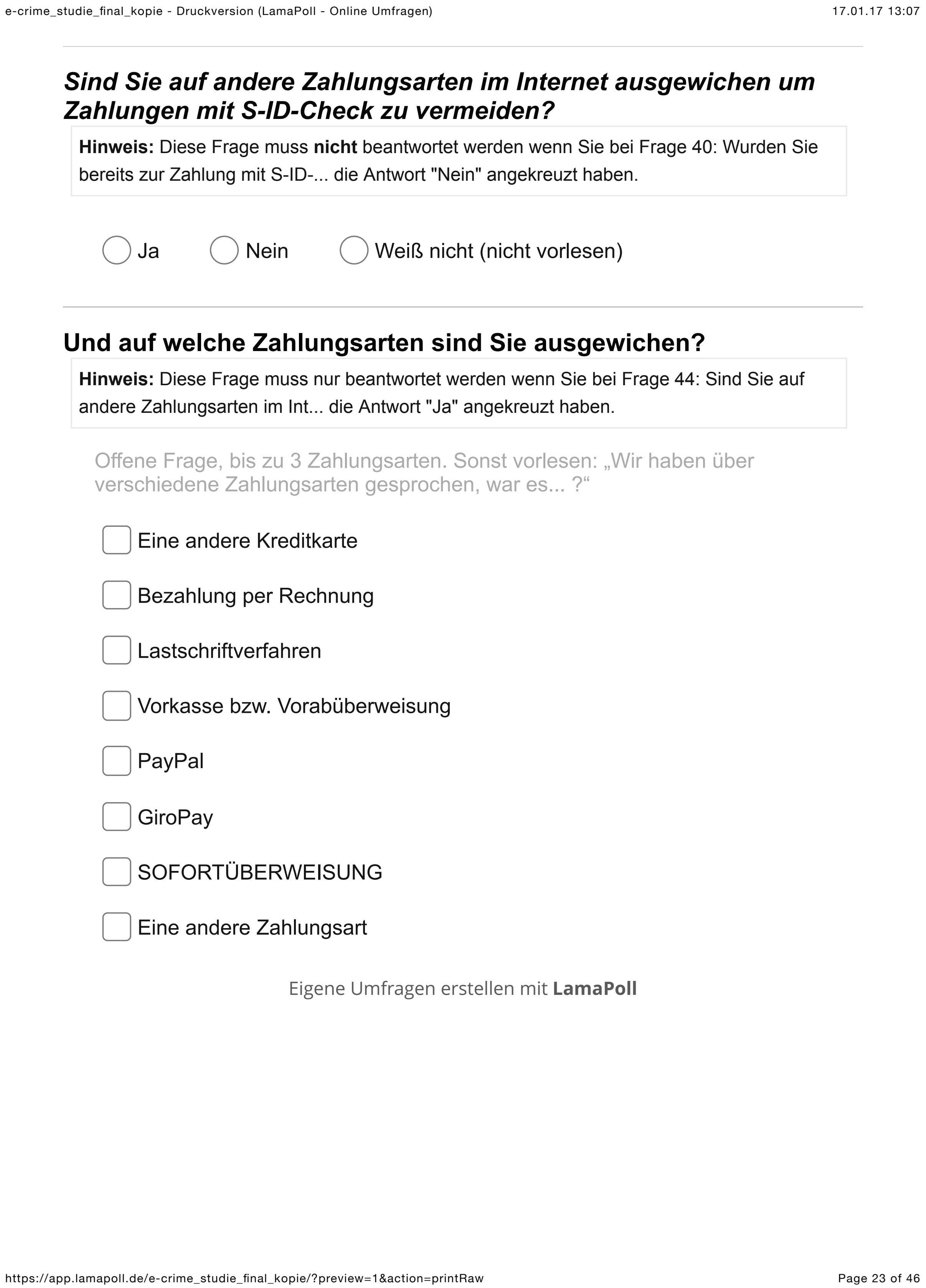
□ Bringt nichts

□ Weiß nicht (nicht vorlesen)

## *Nutzen Sie ihre Kreditkarte nicht mehr im Internet um die Registrierung zu S-ID-Check zu vermeiden?*

**Hinweis:** Diese Frage muss **nicht** beantwortet werden wenn Sie bei Frage 40: Wurden Sie bereits zur Zahlung mit S-ID-... die Antwort "Nein" angekreuzt haben.

○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)



## *Sind Sie auf andere Zahlungsarten im Internet ausgewichen um Zahlungen mit S-ID-Check zu vermeiden?*

**Hinweis:** Diese Frage muss **nicht** beantwortet werden wenn Sie bei Frage 40: Wurden Sie bereits zur Zahlung mit S-ID-... die Antwort "Nein" angekreuzt haben.

○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)

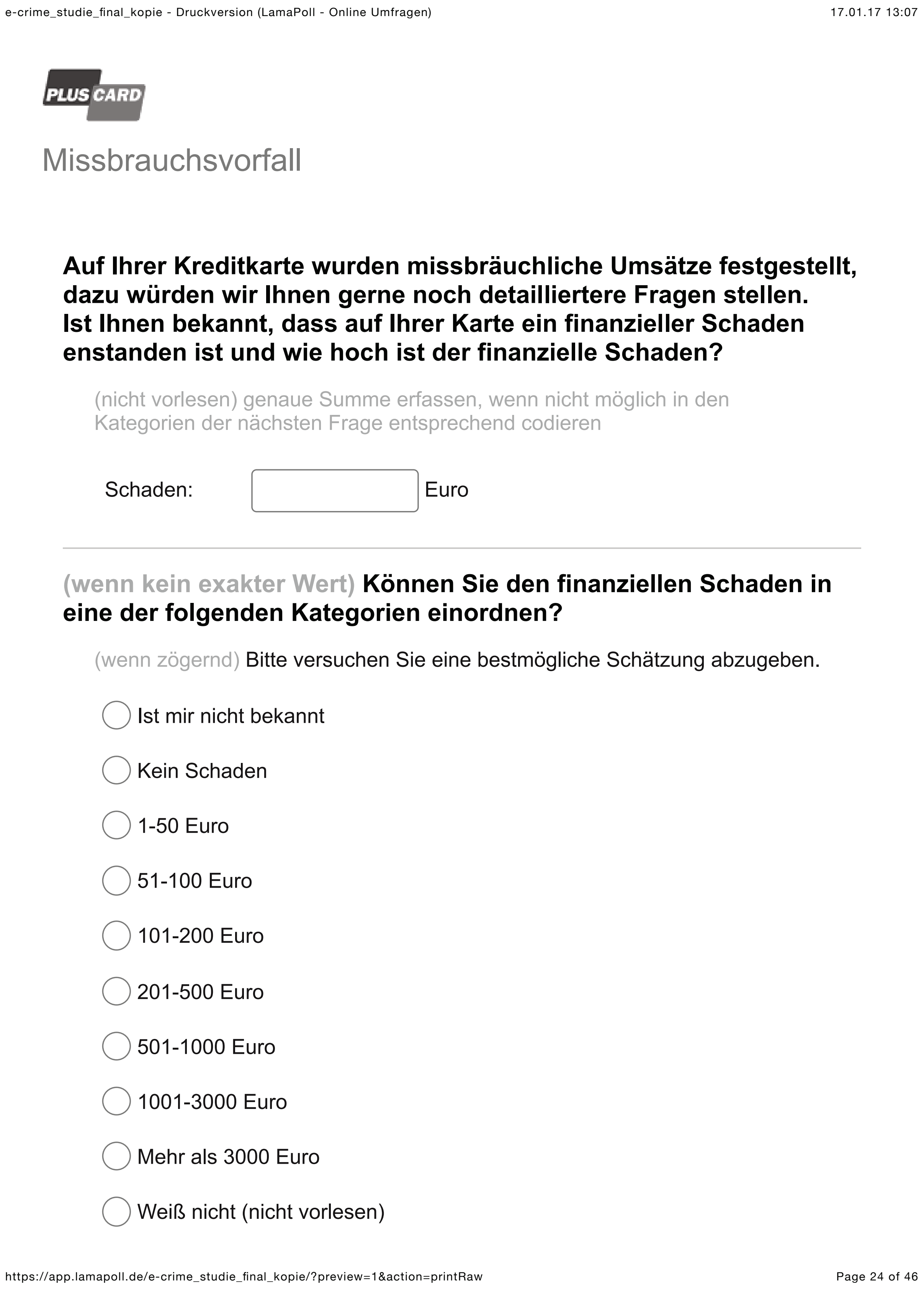
## Und auf welche Zahlungsarten sind Sie ausgewichen?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 44: Sind Sie auf andere Zahlungsarten im Int... die Antwort "Ja" angekreuzt haben.

Offene Frage, bis zu 3 Zahlungsarten. Sonst vorlesen: „Wir haben über verschiedene Zahlungsarten gesprochen, war es... ?“

- □ Eine andere Kreditkarte
- □ Bezahlung per Rechnung
- □ Lastschriftverfahren
- □ Vorkasse bzw. Vorabüberweisung
- □ PayPal
- □ GiroPay
- □ SOFORTÜBERWEISUNG
- □ Eine andere Zahlungsart

Eigene Umfragen erstellen mit **LamaPoll**



PLUS CARD

## Missbrauchsvorfall

**Auf Ihrer Kreditkarte wurden missbräuchliche Umsätze festgestellt, dazu würden wir Ihnen gerne noch detailliertere Fragen stellen.
Ist Ihnen bekannt, dass auf Ihrer Karte ein finanzieller Schaden enstanden ist und wie hoch ist der finanzielle Schaden?**

(nicht vorlesen) genaue Summe erfassen, wenn nicht möglich in den Kategorien der nächsten Frage entsprechend codieren

Schaden: ________ Euro

---

(wenn kein exakter Wert) **Können Sie den finanziellen Schaden in eine der folgenden Kategorien einordnen?**

(wenn zögernd) Bitte versuchen Sie eine bestmögliche Schätzung abzugeben.

○ Ist mir nicht bekannt

○ Kein Schaden

○ 1-50 Euro

○ 51-100 Euro

○ 101-200 Euro

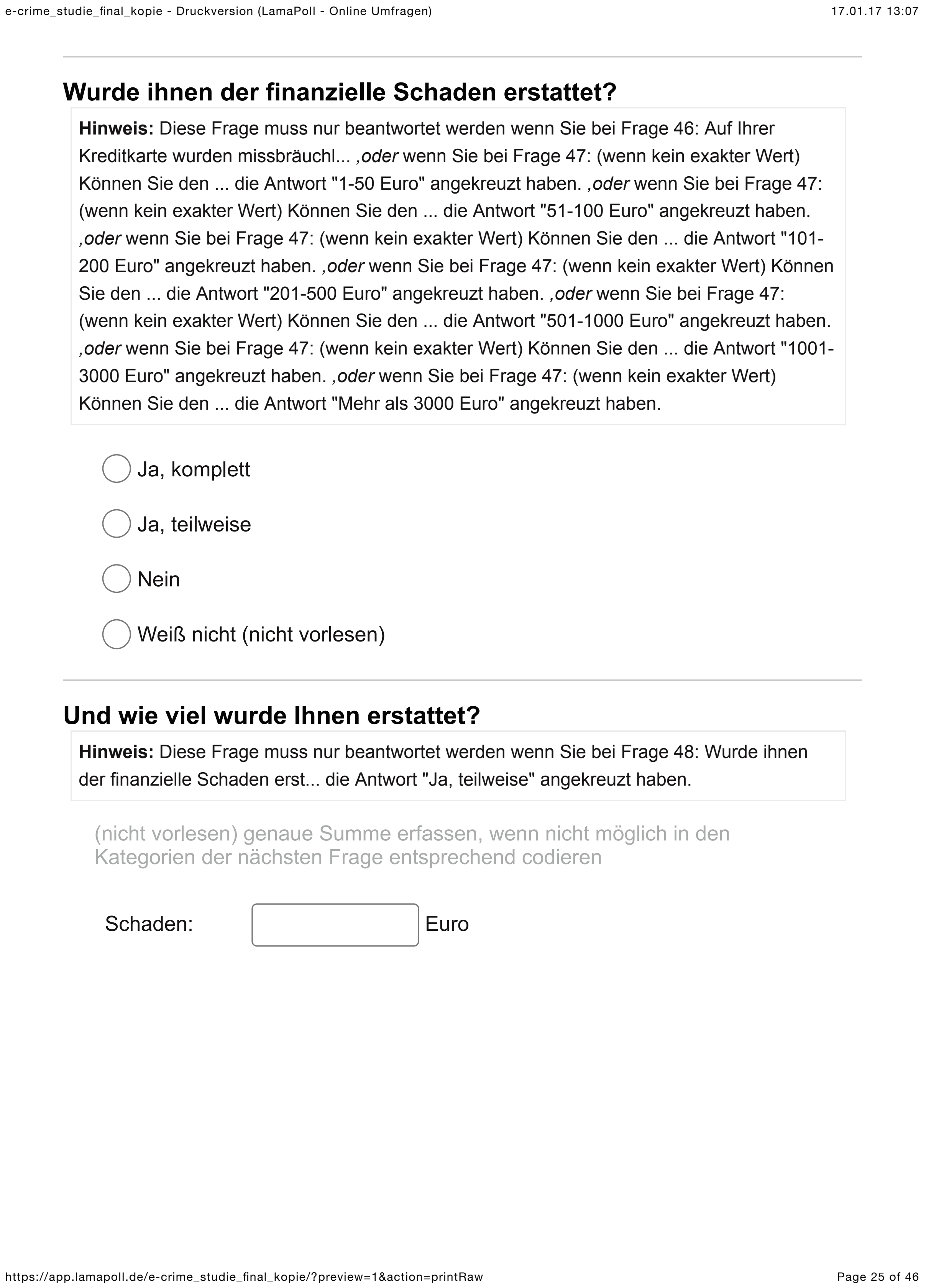
○ 201-500 Euro

○ 501-1000 Euro

○ 1001-3000 Euro

○ Mehr als 3000 Euro

○ Weiß nicht (nicht vorlesen)



## Wurde ihnen der finanzielle Schaden erstattet?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 46: Auf Ihrer Kreditkarte wurden missbräuchl... *,oder* wenn Sie bei Frage 47: (wenn kein exakter Wert) Können Sie den ... die Antwort "1-50 Euro" angekreuzt haben. *,oder* wenn Sie bei Frage 47: (wenn kein exakter Wert) Können Sie den ... die Antwort "51-100 Euro" angekreuzt haben. *,oder* wenn Sie bei Frage 47: (wenn kein exakter Wert) Können Sie den ... die Antwort "101-200 Euro" angekreuzt haben. *,oder* wenn Sie bei Frage 47: (wenn kein exakter Wert) Können Sie den ... die Antwort "201-500 Euro" angekreuzt haben. *,oder* wenn Sie bei Frage 47: (wenn kein exakter Wert) Können Sie den ... die Antwort "501-1000 Euro" angekreuzt haben. *,oder* wenn Sie bei Frage 47: (wenn kein exakter Wert) Können Sie den ... die Antwort "1001-3000 Euro" angekreuzt haben. *,oder* wenn Sie bei Frage 47: (wenn kein exakter Wert) Können Sie den ... die Antwort "Mehr als 3000 Euro" angekreuzt haben.

○ Ja, komplett

○ Ja, teilweise

○ Nein

○ Weiß nicht (nicht vorlesen)

## Und wie viel wurde Ihnen erstattet?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 48: Wurde ihnen der finanzielle Schaden erst... die Antwort "Ja, teilweise" angekreuzt haben.

(nicht vorlesen) genaue Summe erfassen, wenn nicht möglich in den Kategorien der nächsten Frage entsprechend codieren

Schaden: ☐ Euro

## (wenn kein exakter Wert) Können Sie die Erstattung in eine der folgenden Kategorien einordnen?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 48: Wurde ihnen der finanzielle Schaden erst... die Antwort "Ja, teilweise" angekreuzt haben.

(wenn zögernd) Bitte versuchen Sie eine bestmögliche Schätzung abzugeben.

○ Ist mir nicht bekannt

○ Kein Schaden

○ 1-50 Euro

○ 51-100 Euro

○ 101-200 Euro

○ 201-500 Euro

○ 501-1000 Euro

○ 1001-3000 Euro

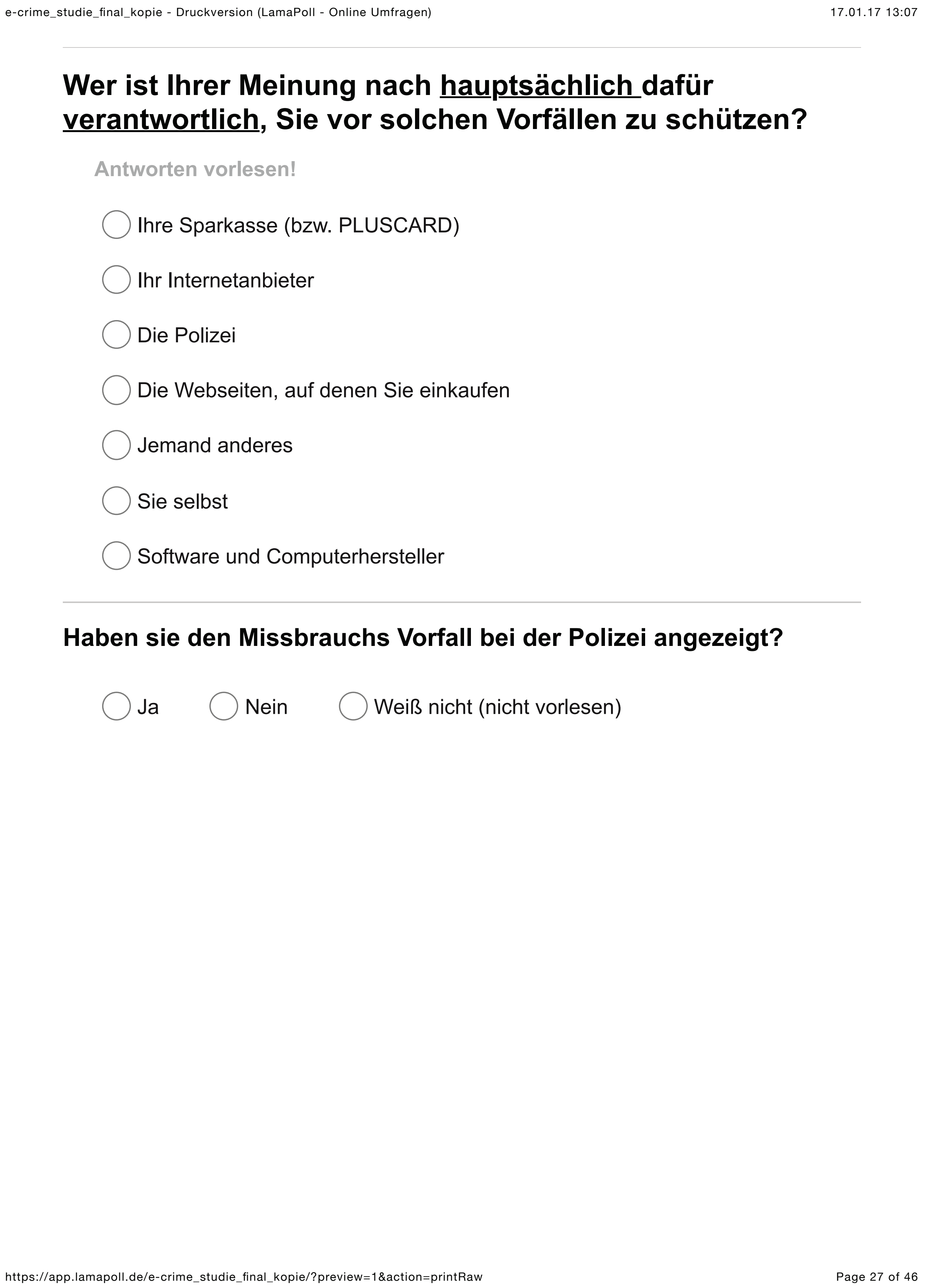
○ Mehr als 3000 Euro

○ Weiß nicht (nicht vorlesen)

## Befinden Sie sich noch im Reklamationsprozess?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 48: Wurde ihnen der finanzielle Schaden erst... die Antwort "Nein" angekreuzt haben.

○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)



## Wer ist Ihrer Meinung nach hauptsächlich dafür verantwortlich, Sie vor solchen Vorfällen zu schützen?

Antworten vorlesen!

○ Ihre Sparkasse (bzw. PLUSCARD)

○ Ihr Internetanbieter

○ Die Polizei

○ Die Webseiten, auf denen Sie einkaufen

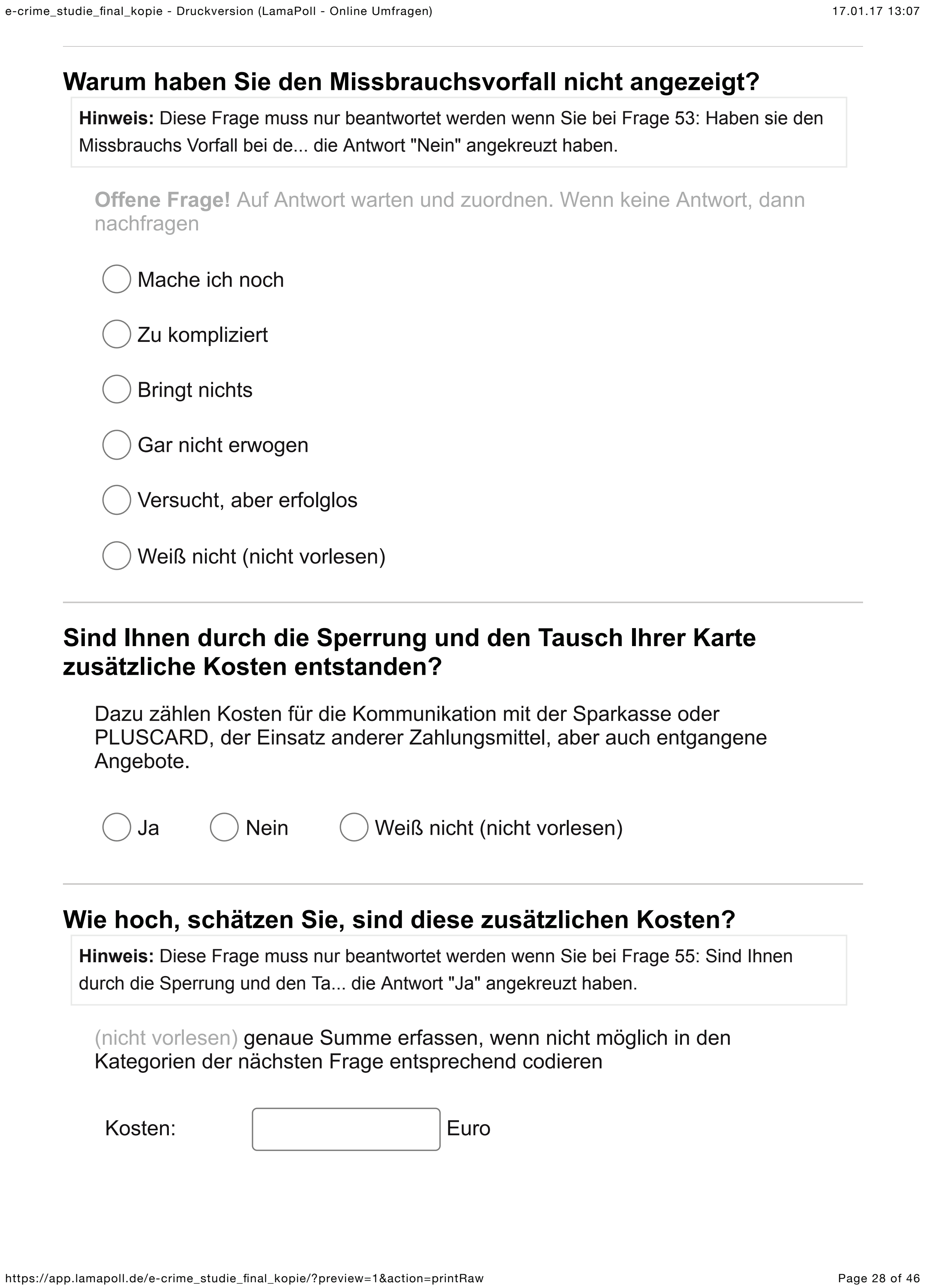
○ Jemand anderes

○ Sie selbst

○ Software und Computerhersteller

## Haben sie den Missbrauchs Vorfall bei der Polizei angezeigt?

○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)



## Warum haben Sie den Missbrauchsvorfall nicht angezeigt?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 53: Haben sie den Missbrauchs Vorfall bei de... die Antwort "Nein" angekreuzt haben.

**Offene Frage!** Auf Antwort warten und zuordnen. Wenn keine Antwort, dann nachfragen

○ Mache ich noch

○ Zu kompliziert

○ Bringt nichts

○ Gar nicht erwogen

○ Versucht, aber erfolglos

○ Weiß nicht (nicht vorlesen)

## Sind Ihnen durch die Sperrung und den Tausch Ihrer Karte zusätzliche Kosten entstanden?

Dazu zählen Kosten für die Kommunikation mit der Sparkasse oder PLUSCARD, der Einsatz anderer Zahlungsmittel, aber auch entgangene Angebote.

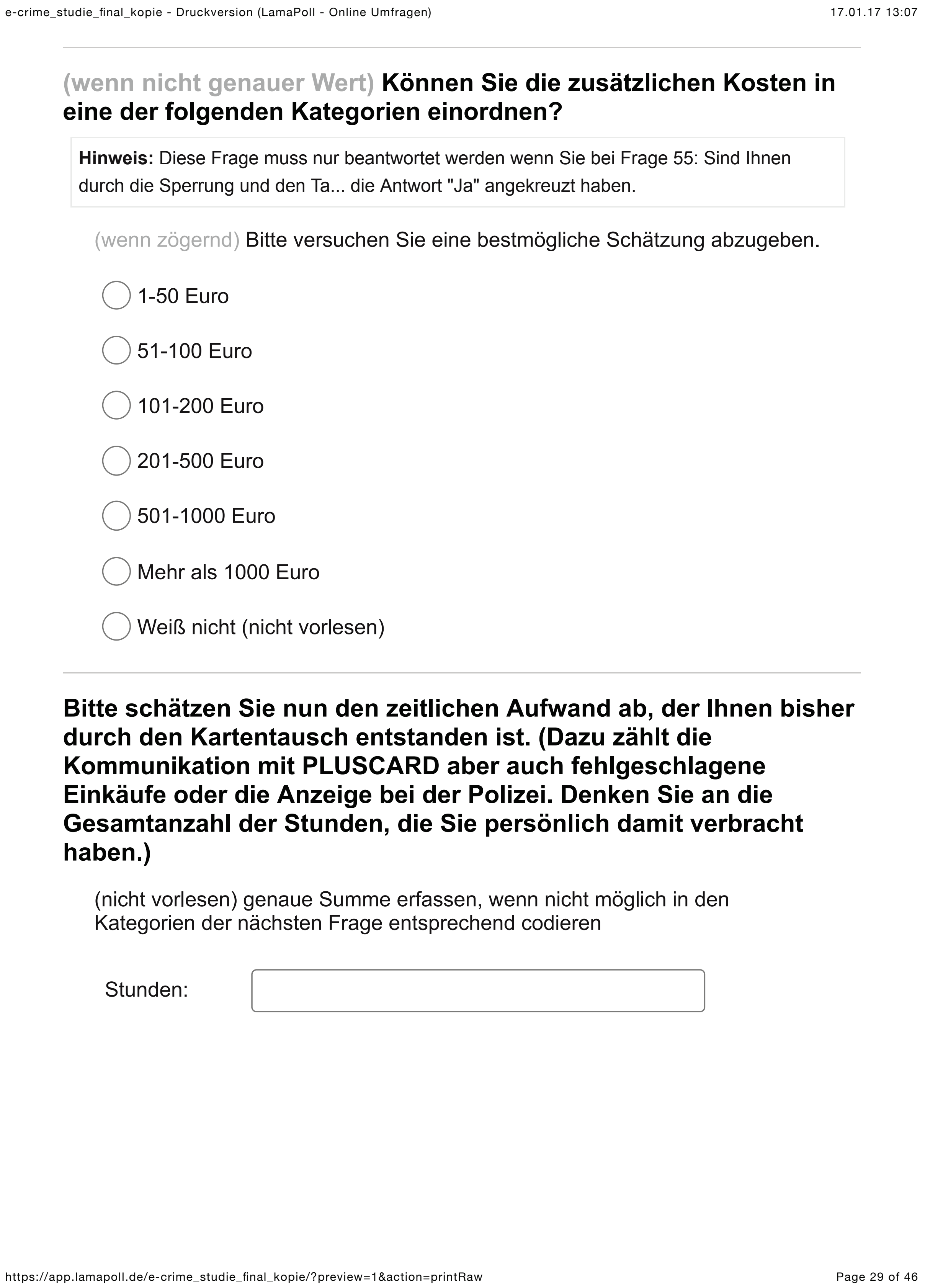
○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)

## Wie hoch, schätzen Sie, sind diese zusätzlichen Kosten?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 55: Sind Ihnen durch die Sperrung und den Ta... die Antwort "Ja" angekreuzt haben.

(nicht vorlesen) genaue Summe erfassen, wenn nicht möglich in den Kategorien der nächsten Frage entsprechend codieren

Kosten: ____ Euro



**(wenn nicht genauer Wert) Können Sie die zusätzlichen Kosten in eine der folgenden Kategorien einordnen?**

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 55: Sind Ihnen durch die Sperrung und den Ta... die Antwort "Ja" angekreuzt haben.

(wenn zögernd) Bitte versuchen Sie eine bestmögliche Schätzung abzugeben.

○ 1-50 Euro

○ 51-100 Euro

○ 101-200 Euro

○ 201-500 Euro

○ 501-1000 Euro

○ Mehr als 1000 Euro

○ Weiß nicht (nicht vorlesen)

**Bitte schätzen Sie nun den zeitlichen Aufwand ab, der Ihnen bisher durch den Kartentausch entstanden ist. (Dazu zählt die Kommunikation mit PLUSCARD aber auch fehlgeschlagene Einkäufe oder die Anzeige bei der Polizei. Denken Sie an die Gesamtanzahl der Stunden, die Sie persönlich damit verbracht haben.)**

(nicht vorlesen) genaue Summe erfassen, wenn nicht möglich in den Kategorien der nächsten Frage entsprechend codieren

Stunden: ▭

### (wenn kein exakter Wert) Können Sie den Zeitaufwand in eine der folgenden Kategorien einordnen?

(wenn zögernd) Bitte versuchen Sie eine bestmögliche Schätzung abzugeben.

○ Keine Zeit

○ Weniger als 1 Stunde

○ 1 bis weniger als 10 Stunden

○ 10 bis weniger als 20 Stunden

○ 20 bis weniger als 40 Stunden

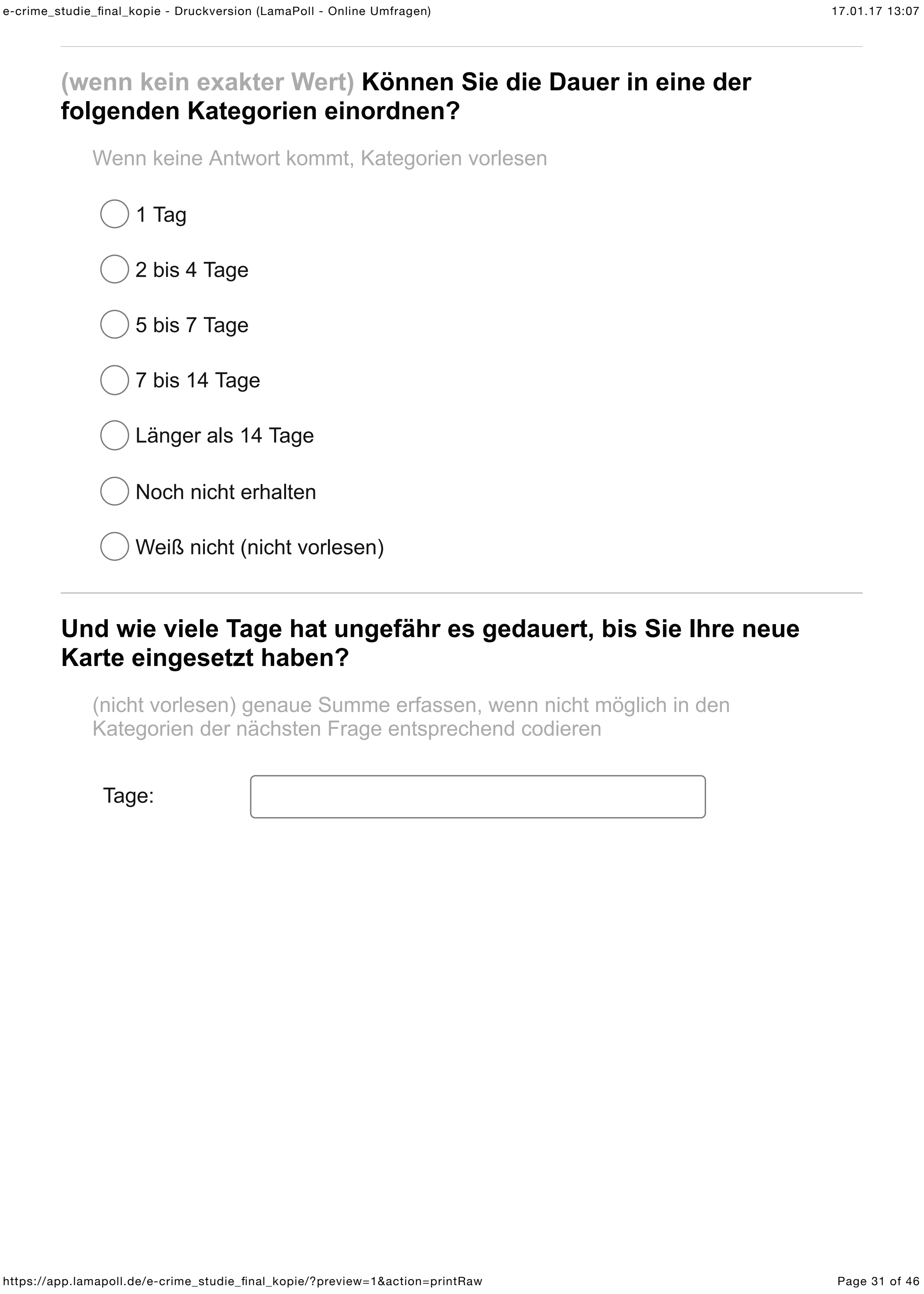
○ 40 Stunden oder mehr

○ Weiß nicht (nicht vorlesen)

### Und wie viele Tage hat es ungefähr gedauert, bis Sie nach der Sperrung Ihre neue Karte erhalten haben?

(nicht vorlesen) genaue Summe erfassen, wenn nicht möglich in den Kategorien der nächsten Frage entsprechend codieren

Tage: ______



### (wenn kein exakter Wert) Können Sie die Dauer in eine der folgenden Kategorien einordnen?

Wenn keine Antwort kommt, Kategorien vorlesen

○ 1 Tag

○ 2 bis 4 Tage

○ 5 bis 7 Tage

○ 7 bis 14 Tage

○ Länger als 14 Tage

○ Noch nicht erhalten

○ Weiß nicht (nicht vorlesen)

### Und wie viele Tage hat ungefähr es gedauert, bis Sie Ihre neue Karte eingesetzt haben?

(nicht vorlesen) genaue Summe erfassen, wenn nicht möglich in den Kategorien der nächsten Frage entsprechend codieren

Tage: □

## Können Sie die Dauer in eine der folgenden Kategorien einordnen?

Wenn keine Antwort kommt, Kategorien vorlesen

○ 1 Tag

○ 2 bis 4 Tage

○ 5 bis 7 Tage

○ 7 bis 14 Tage

○ Länger als 14 Tage

○ Noch nicht eingesetzt

○ Weiß nicht (nicht vorlesen)

## Wie haben Sie seit dem Kartenmissbrauch Ihre neue Kreditkarte im Gegensatz zu Ihrer alten Karte genutzt?

Bitte denken Sie an alle Zahlungen im und außerhalb des Internets

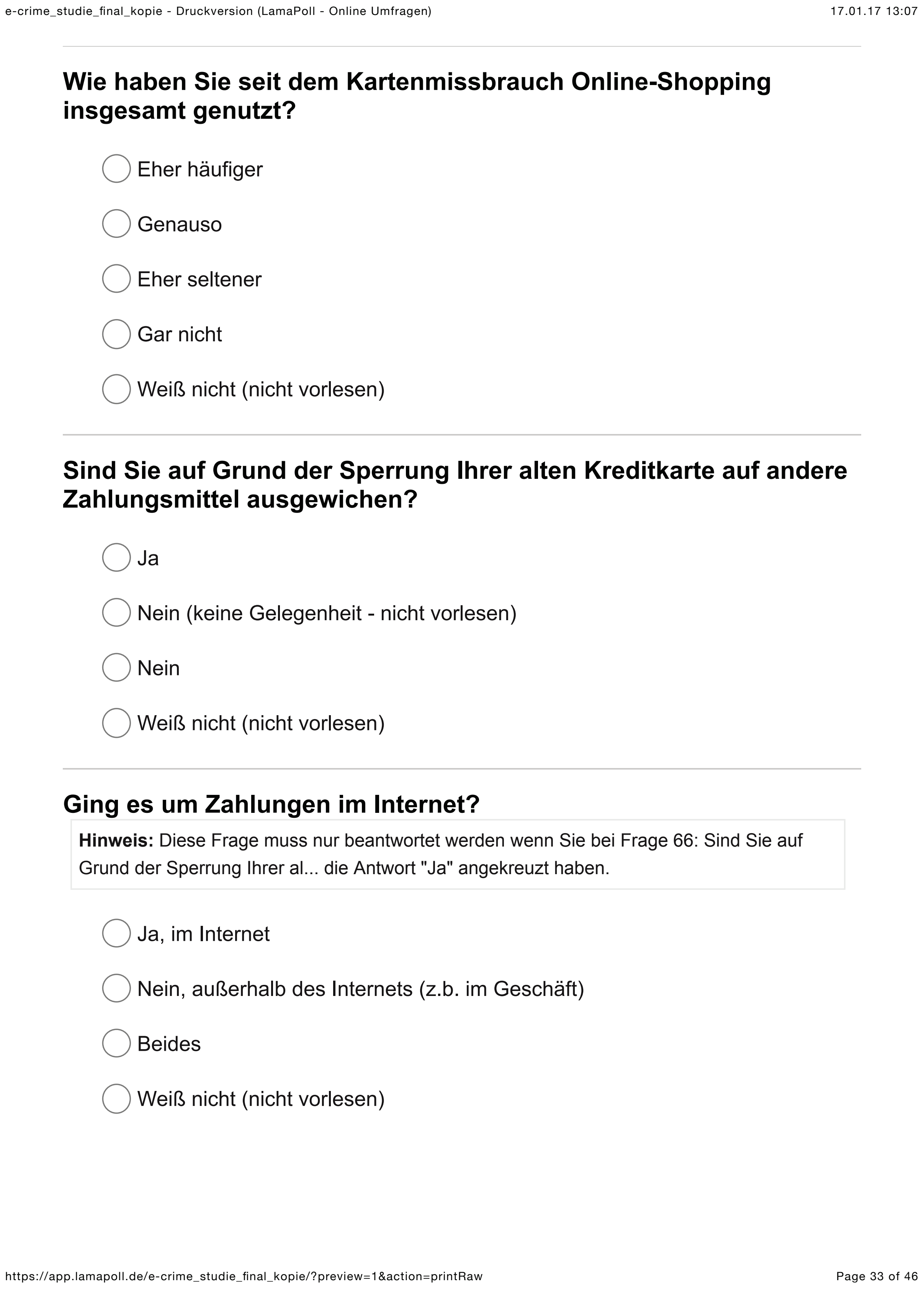
○ Eher häufiger

○ Genauso

○ Eher seltener

○ Gar nicht

○ Weiß nicht (nicht vorlesen)



## Wie haben Sie seit dem Kartenmissbrauch Online-Shopping insgesamt genutzt?

○ Eher häufiger

○ Genauso

○ Eher seltener

○ Gar nicht

○ Weiß nicht (nicht vorlesen)

## Sind Sie auf Grund der Sperrung Ihrer alten Kreditkarte auf andere Zahlungsmittel ausgewichen?

○ Ja

○ Nein (keine Gelegenheit - nicht vorlesen)

○ Nein

○ Weiß nicht (nicht vorlesen)

## Ging es um Zahlungen im Internet?

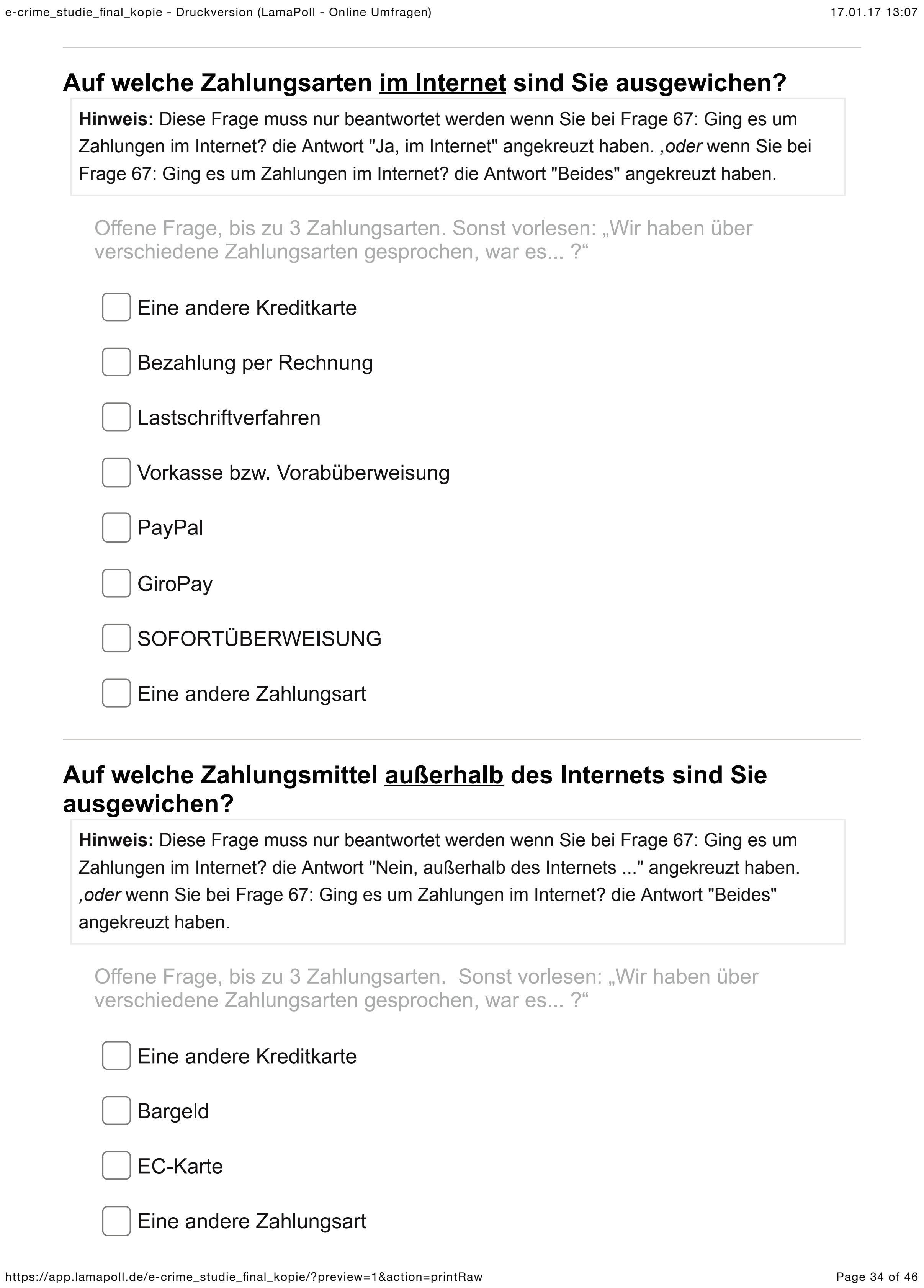
**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 66: Sind Sie auf Grund der Sperrung Ihrer al... die Antwort "Ja" angekreuzt haben.

○ Ja, im Internet

○ Nein, außerhalb des Internets (z.b. im Geschäft)

○ Beides

○ Weiß nicht (nicht vorlesen)



## Auf welche Zahlungsarten <u>im Internet</u> sind Sie ausgewichen?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 67: Ging es um Zahlungen im Internet? die Antwort "Ja, im Internet" angekreuzt haben. *,oder* wenn Sie bei Frage 67: Ging es um Zahlungen im Internet? die Antwort "Beides" angekreuzt haben.

Offene Frage, bis zu 3 Zahlungsarten. Sonst vorlesen: „Wir haben über verschiedene Zahlungsarten gesprochen, war es... ?“

□ Eine andere Kreditkarte

□ Bezahlung per Rechnung

□ Lastschriftverfahren

□ Vorkasse bzw. Vorabüberweisung

□ PayPal

□ GiroPay

□ SOFORTÜBERWEISUNG

□ Eine andere Zahlungsart

## Auf welche Zahlungsmittel <u>außerhalb</u> des Internets sind Sie ausgewichen?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 67: Ging es um Zahlungen im Internet? die Antwort "Nein, außerhalb des Internets ..." angekreuzt haben. *,oder* wenn Sie bei Frage 67: Ging es um Zahlungen im Internet? die Antwort "Beides" angekreuzt haben.

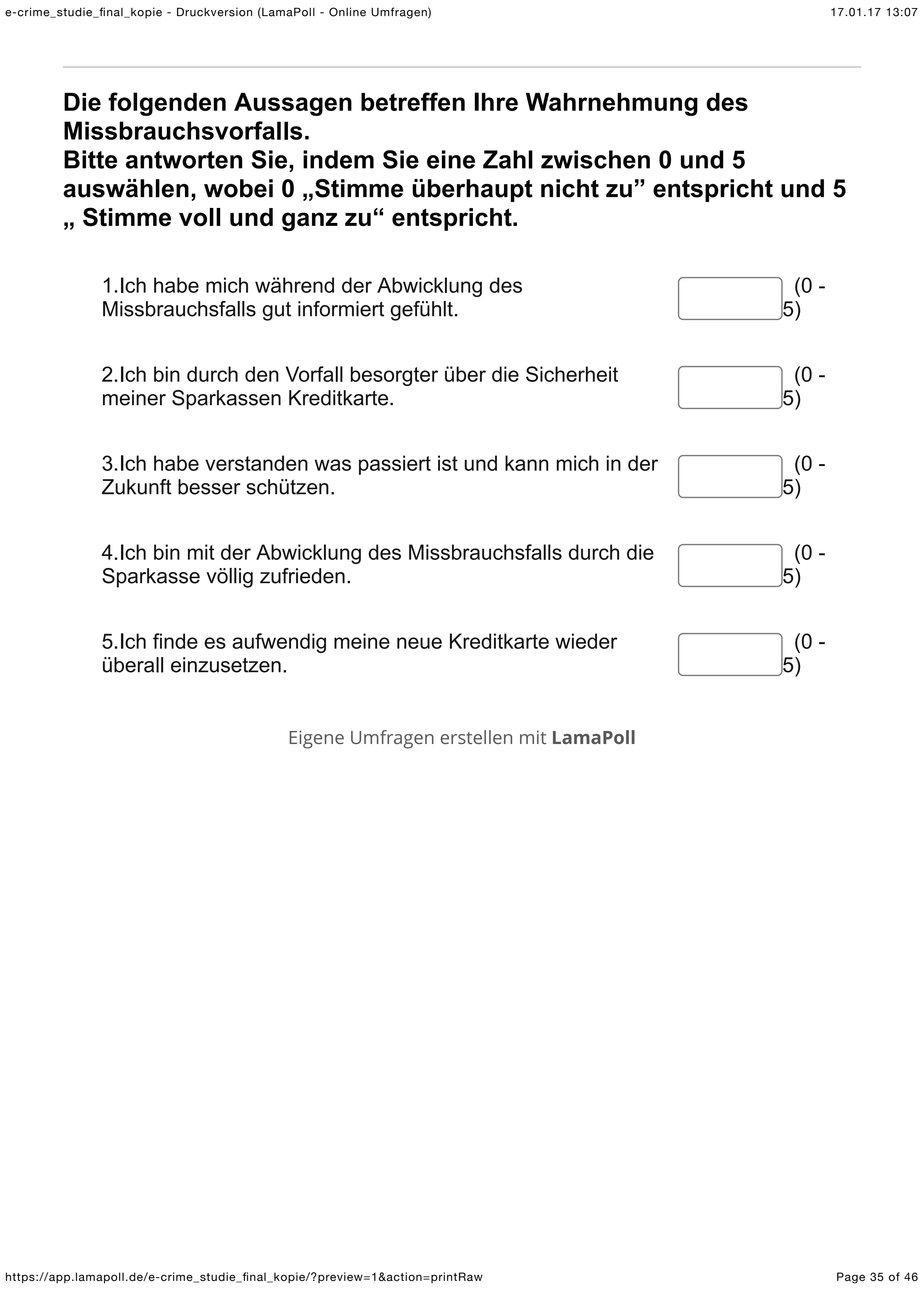
Offene Frage, bis zu 3 Zahlungsarten. Sonst vorlesen: „Wir haben über verschiedene Zahlungsarten gesprochen, war es... ?“

□ Eine andere Kreditkarte

□ Bargeld

□ EC-Karte

□ Eine andere Zahlungsart



**Die folgenden Aussagen betreffen Ihre Wahrnehmung des Missbrauchsvorfalls.
Bitte antworten Sie, indem Sie eine Zahl zwischen 0 und 5 auswählen, wobei 0 „Stimme überhaupt nicht zu” entspricht und 5 „ Stimme voll und ganz zu“ entspricht.**

1.Ich habe mich während der Abwicklung des Missbrauchsfalls gut informiert gefühlt. □ (0 - 5)

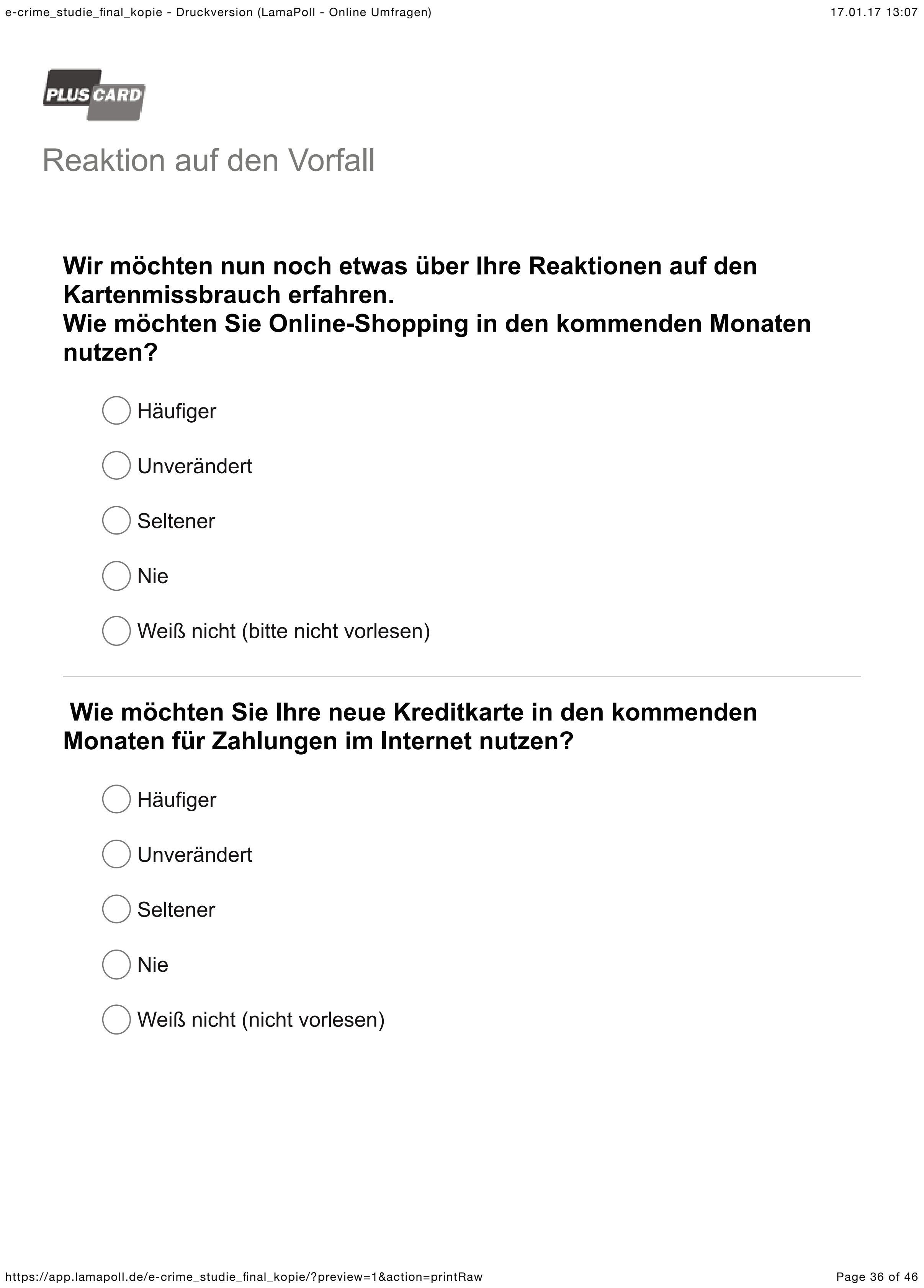
2.Ich bin durch den Vorfall besorgter über die Sicherheit meiner Sparkassen Kreditkarte. □ (0 - 5)

3.Ich habe verstanden was passiert ist und kann mich in der Zukunft besser schützen. □ (0 - 5)

4.Ich bin mit der Abwicklung des Missbrauchsfalls durch die Sparkasse völlig zufrieden. □ (0 - 5)

5.Ich finde es aufwendig meine neue Kreditkarte wieder überall einzusetzen. □ (0 - 5)

Eigene Umfragen erstellen mit **LamaPoll**



PLUS CARD

## Reaktion auf den Vorfall

**Wir möchten nun noch etwas über Ihre Reaktionen auf den Kartenmissbrauch erfahren.**
**Wie möchten Sie Online-Shopping in den kommenden Monaten nutzen?**

○ Häufiger

○ Unverändert

○ Seltener

○ Nie

○ Weiß nicht (bitte nicht vorlesen)

---

**Wie möchten Sie Ihre neue Kreditkarte in den kommenden Monaten für Zahlungen im Internet nutzen?**

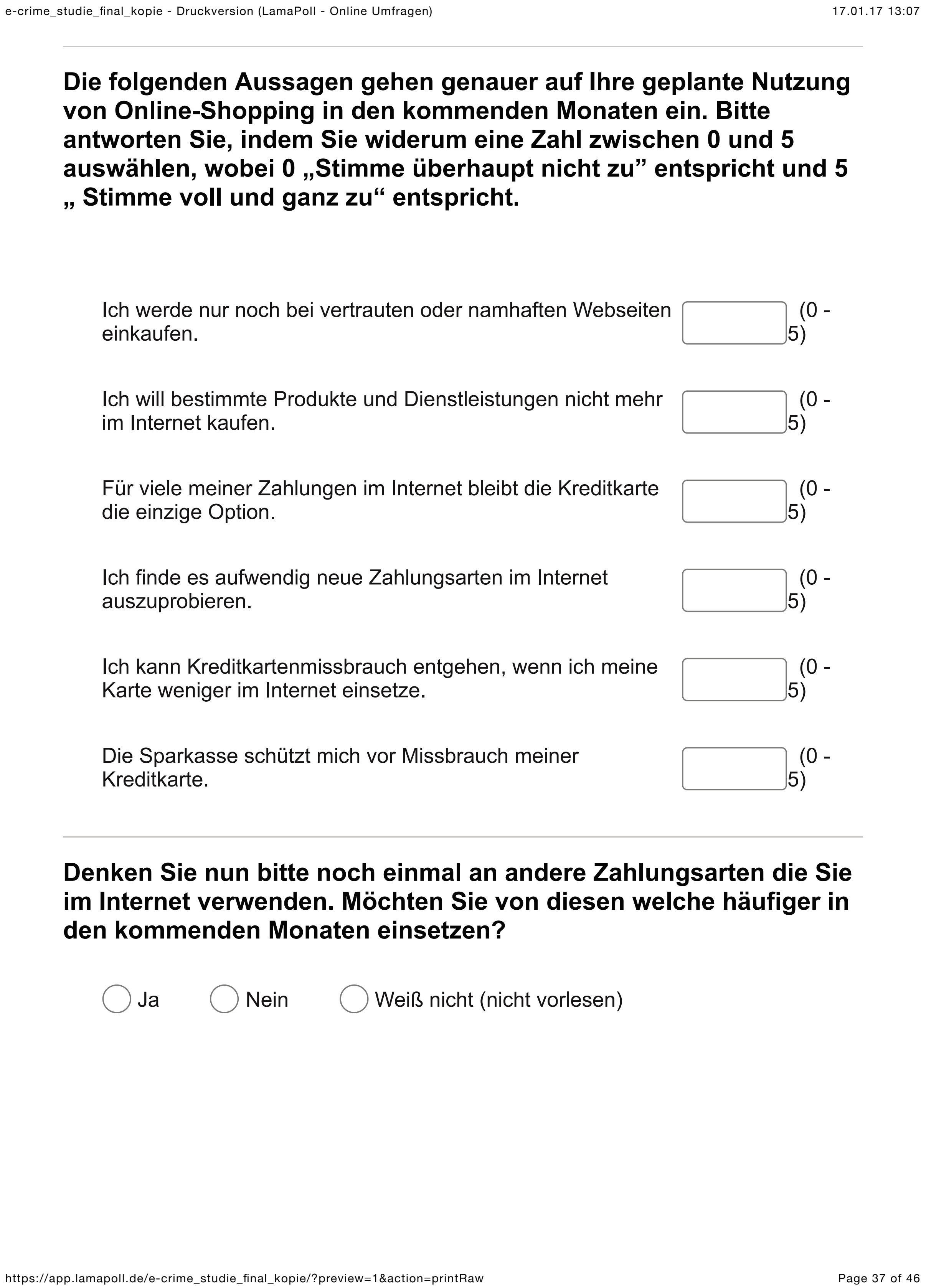
○ Häufiger

○ Unverändert

○ Seltener

○ Nie

○ Weiß nicht (nicht vorlesen)



**Die folgenden Aussagen gehen genauer auf Ihre geplante Nutzung von Online-Shopping in den kommenden Monaten ein. Bitte antworten Sie, indem Sie widerum eine Zahl zwischen 0 und 5 auswählen, wobei 0 „Stimme überhaupt nicht zu” entspricht und 5 „ Stimme voll und ganz zu“ entspricht.**

Ich werde nur noch bei vertrauten oder namhaften Webseiten einkaufen. ☐ (0 - 5)

Ich will bestimmte Produkte und Dienstleistungen nicht mehr im Internet kaufen. ☐ (0 - 5)

Für viele meiner Zahlungen im Internet bleibt die Kreditkarte die einzige Option. ☐ (0 - 5)

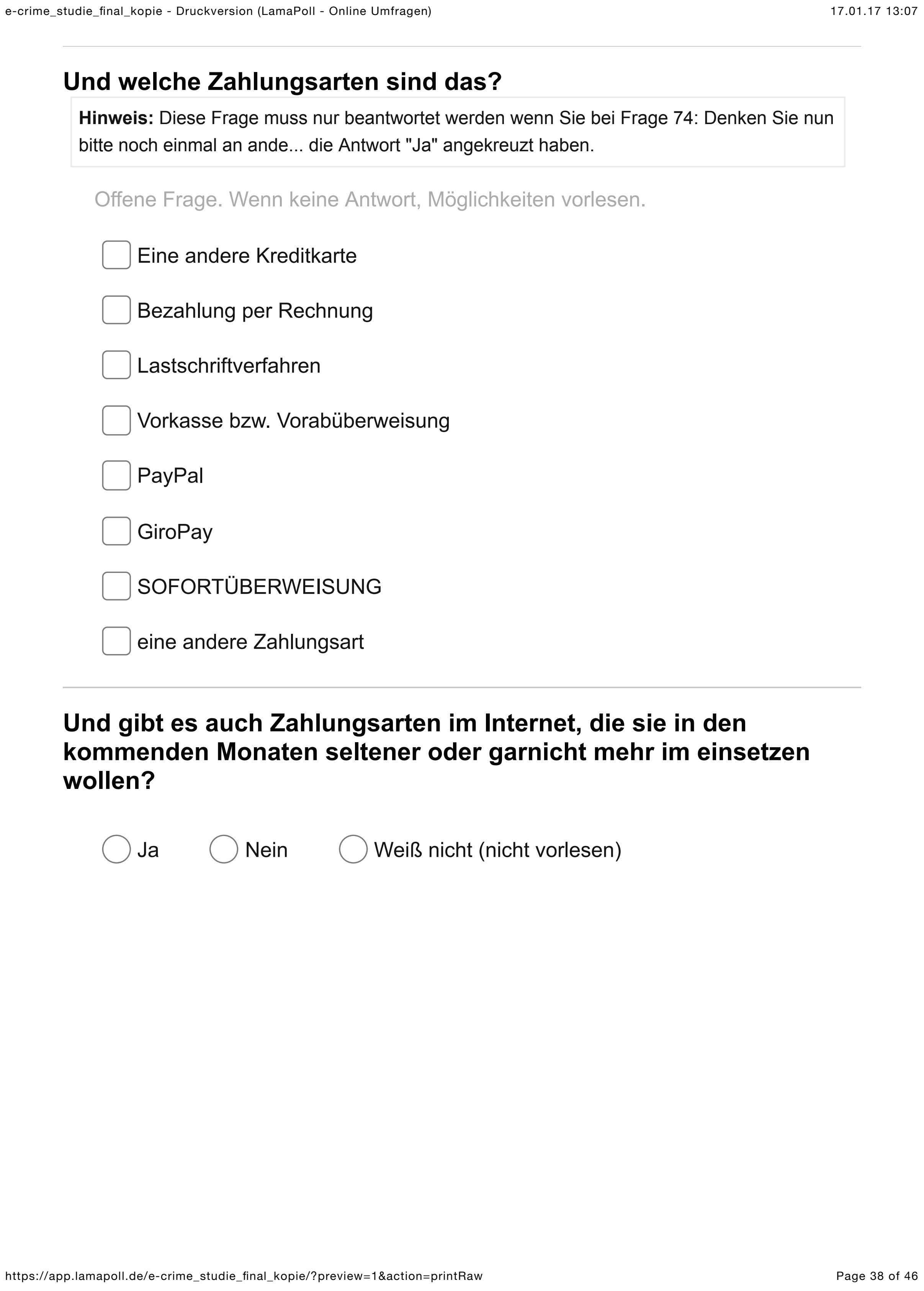
Ich finde es aufwendig neue Zahlungsarten im Internet auszuprobieren. ☐ (0 - 5)

Ich kann Kreditkartenmissbrauch entgehen, wenn ich meine Karte weniger im Internet einsetze. ☐ (0 - 5)

Die Sparkasse schützt mich vor Missbrauch meiner Kreditkarte. ☐ (0 - 5)

**Denken Sie nun bitte noch einmal an andere Zahlungsarten die Sie im Internet verwenden. Möchten Sie von diesen welche häufiger in den kommenden Monaten einsetzen?**

○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)



## Und welche Zahlungsarten sind das?

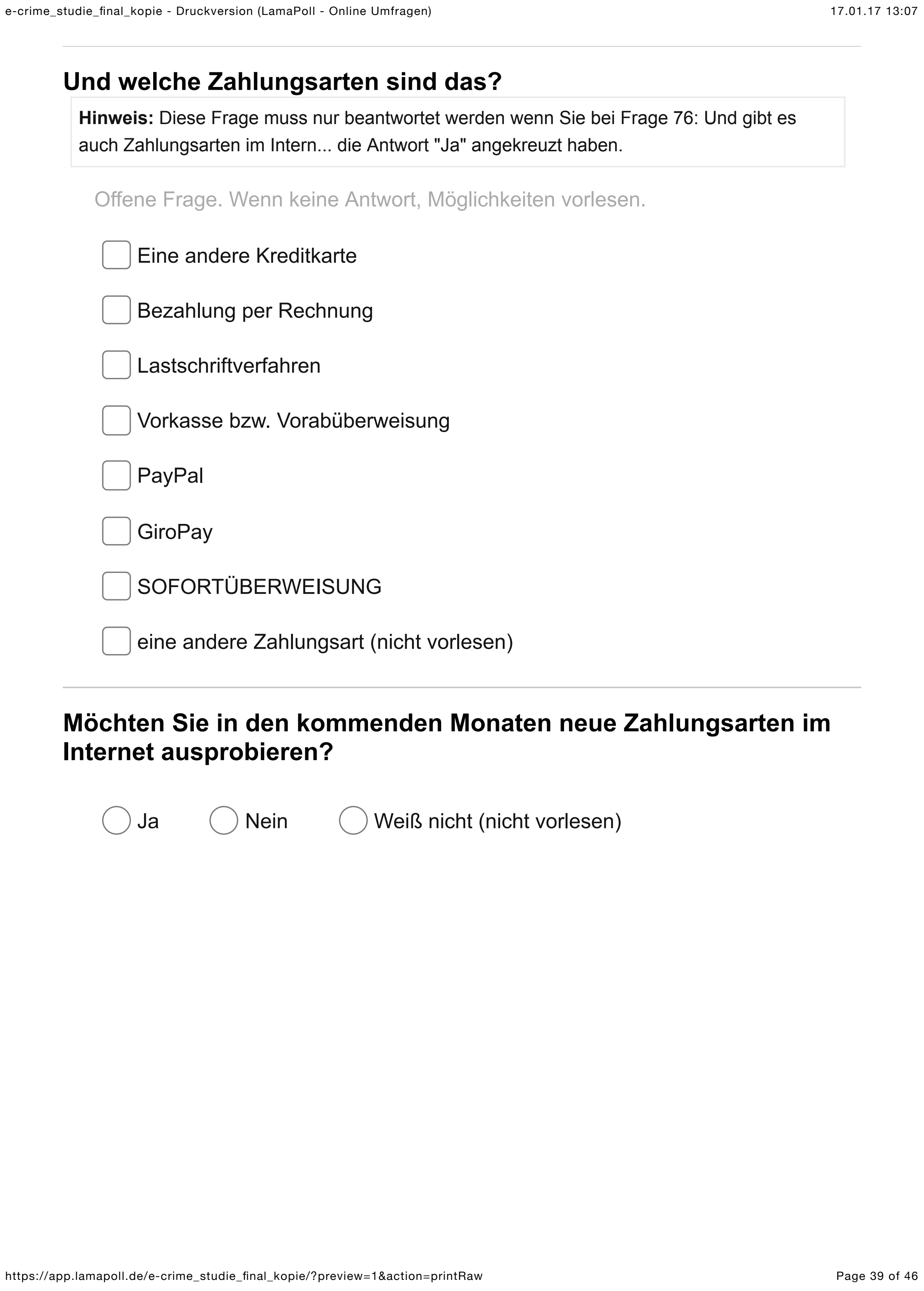
**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 74: Denken Sie nun bitte noch einmal an ande... die Antwort "Ja" angekreuzt haben.

Offene Frage. Wenn keine Antwort, Möglichkeiten vorlesen.

- □ Eine andere Kreditkarte
- □ Bezahlung per Rechnung
- □ Lastschriftverfahren
- □ Vorkasse bzw. Vorabüberweisung
- □ PayPal
- □ GiroPay
- □ SOFORTÜBERWEISUNG
- □ eine andere Zahlungsart

## Und gibt es auch Zahlungsarten im Internet, die sie in den kommenden Monaten seltener oder garnicht mehr im einsetzen wollen?

○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)



## Und welche Zahlungsarten sind das?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 76: Und gibt es auch Zahlungsarten im Intern... die Antwort "Ja" angekreuzt haben.

Offene Frage. Wenn keine Antwort, Möglichkeiten vorlesen.

- □ Eine andere Kreditkarte
- □ Bezahlung per Rechnung
- □ Lastschriftverfahren
- □ Vorkasse bzw. Vorabüberweisung
- □ PayPal
- □ GiroPay
- □ SOFORTÜBERWEISUNG
- □ eine andere Zahlungsart (nicht vorlesen)

## Möchten Sie in den kommenden Monaten neue Zahlungsarten im Internet ausprobieren?

○ Ja ○ Nein ○ Weiß nicht (nicht vorlesen)

## Und welche Zahlungsarten sind das?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 78: Möchten Sie in den kommenden Monaten neu... die Antwort "Ja " angekreuzt haben.

Offene Frage. Wenn keine Antwort, Möglichkeiten vorlesen.

□ Eine andere Kreditkarte

□ Bezahlung per Rechnung

□ Lastschriftverfahren

□ Vorkasse bzw. Vorabüberweisung

□ PayPal

□ GiroPay

□ SOFORTÜBERWEISUNG

□ eine andere Zahlungsart (nicht vorlesen)

## Denken Sie nun bitte noch einmal an Zahlungen außerhalb des Internets. Wie wollen Sie Ihre neue Kreditkarte bei Zahlungen in den kommenden Monaten nutzen?

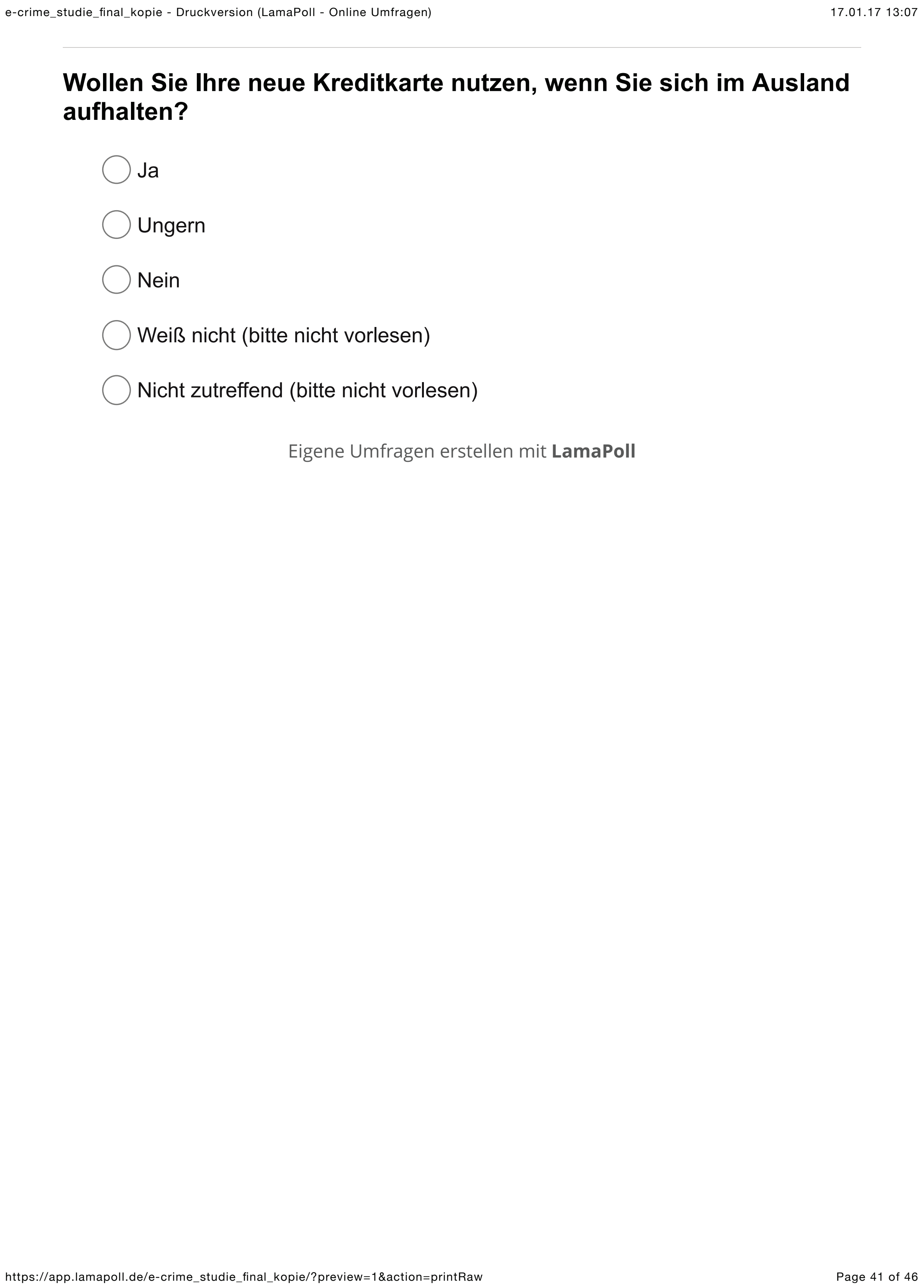
○ Häufiger

○ Unverändert

○ Seltener

○ Nie

○ Weiß nicht (nicht vorlesen)



## Wollen Sie Ihre neue Kreditkarte nutzen, wenn Sie sich im Ausland aufhalten?

○ Ja

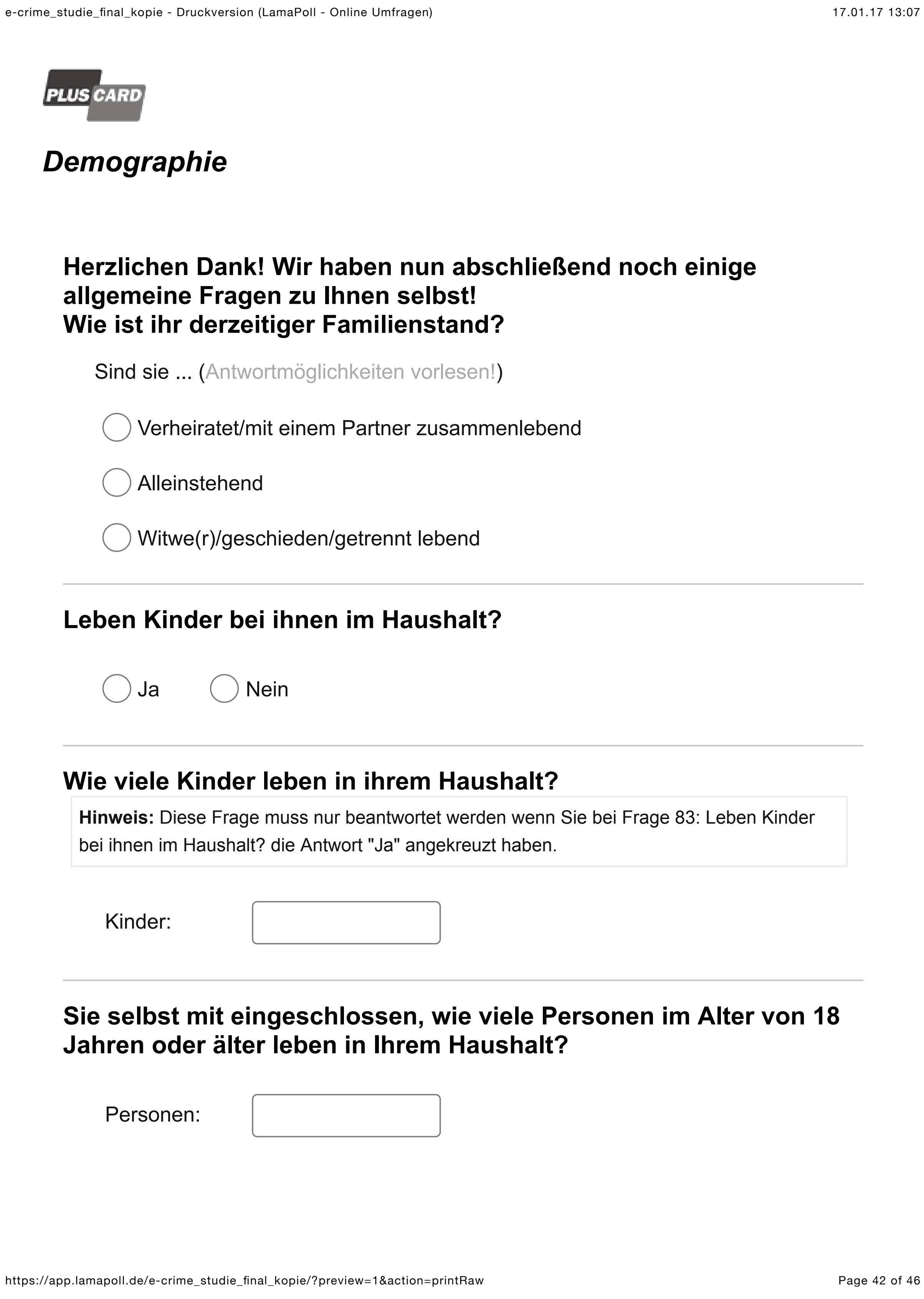
○ Ungern

○ Nein

○ Weiß nicht (bitte nicht vorlesen)

○ Nicht zutreffend (bitte nicht vorlesen)

Eigene Umfragen erstellen mit **LamaPoll**



## Demographie

### Herzlichen Dank! Wir haben nun abschließend noch einige allgemeine Fragen zu Ihnen selbst!
### Wie ist ihr derzeitiger Familienstand?

Sind sie ... (Antwortmöglichkeiten vorlesen!)

○ Verheiratet/mit einem Partner zusammenlebend

○ Alleinstehend

○ Witwe(r)/geschieden/getrennt lebend

### Leben Kinder bei ihnen im Haushalt?

○ Ja ○ Nein

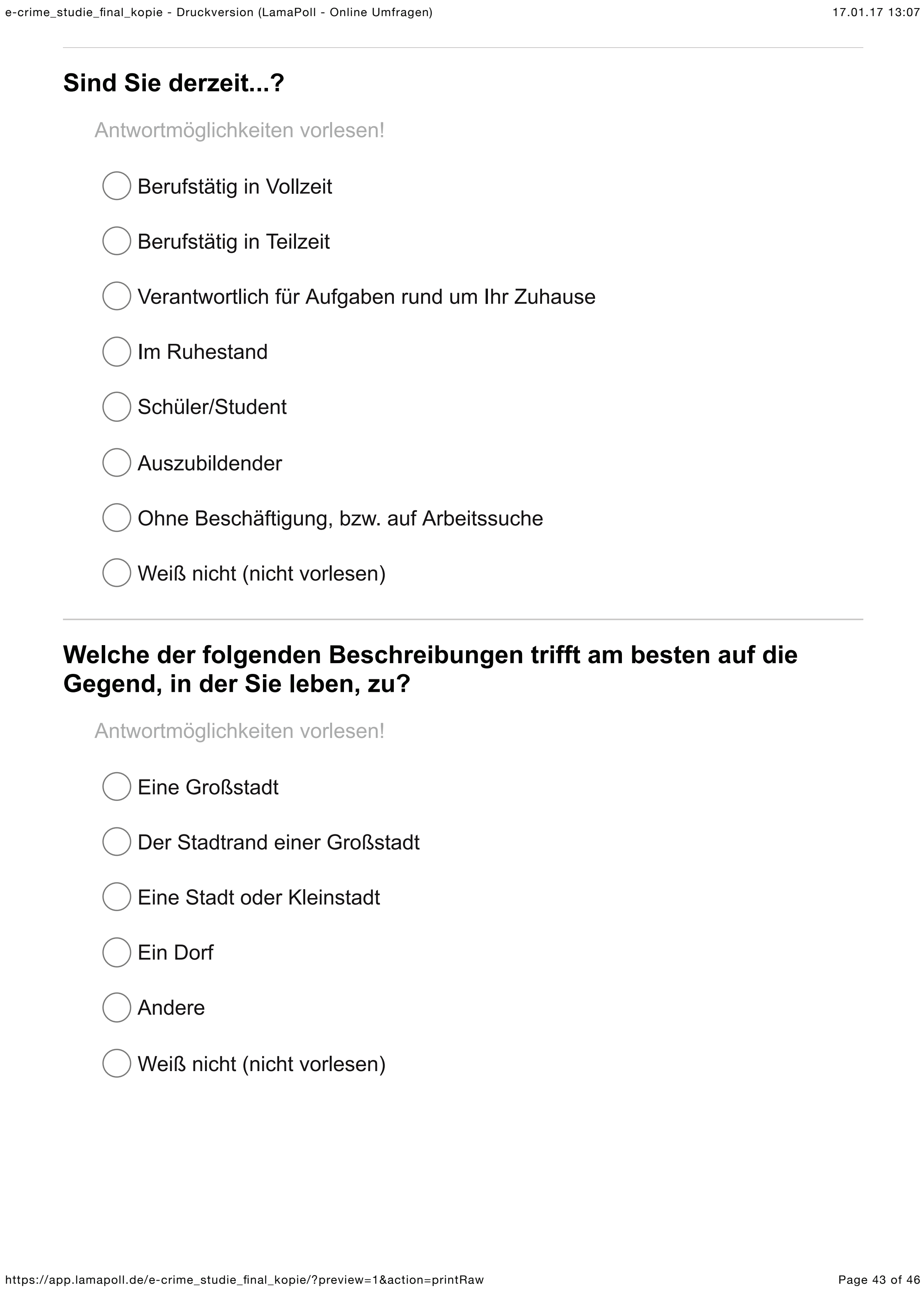
### Wie viele Kinder leben in ihrem Haushalt?

**Hinweis:** Diese Frage muss nur beantwortet werden wenn Sie bei Frage 83: Leben Kinder bei ihnen im Haushalt? die Antwort "Ja" angekreuzt haben.

Kinder:

### Sie selbst mit eingeschlossen, wie viele Personen im Alter von 18 Jahren oder älter leben in Ihrem Haushalt?

Personen:



## Sind Sie derzeit...?

Antwortmöglichkeiten vorlesen!

○ Berufstätig in Vollzeit

○ Berufstätig in Teilzeit

○ Verantwortlich für Aufgaben rund um Ihr Zuhause

○ Im Ruhestand

○ Schüler/Student

○ Auszubildender

○ Ohne Beschäftigung, bzw. auf Arbeitssuche

○ Weiß nicht (nicht vorlesen)

## Welche der folgenden Beschreibungen trifft am besten auf die Gegend, in der Sie leben, zu?

Antwortmöglichkeiten vorlesen!

○ Eine Großstadt

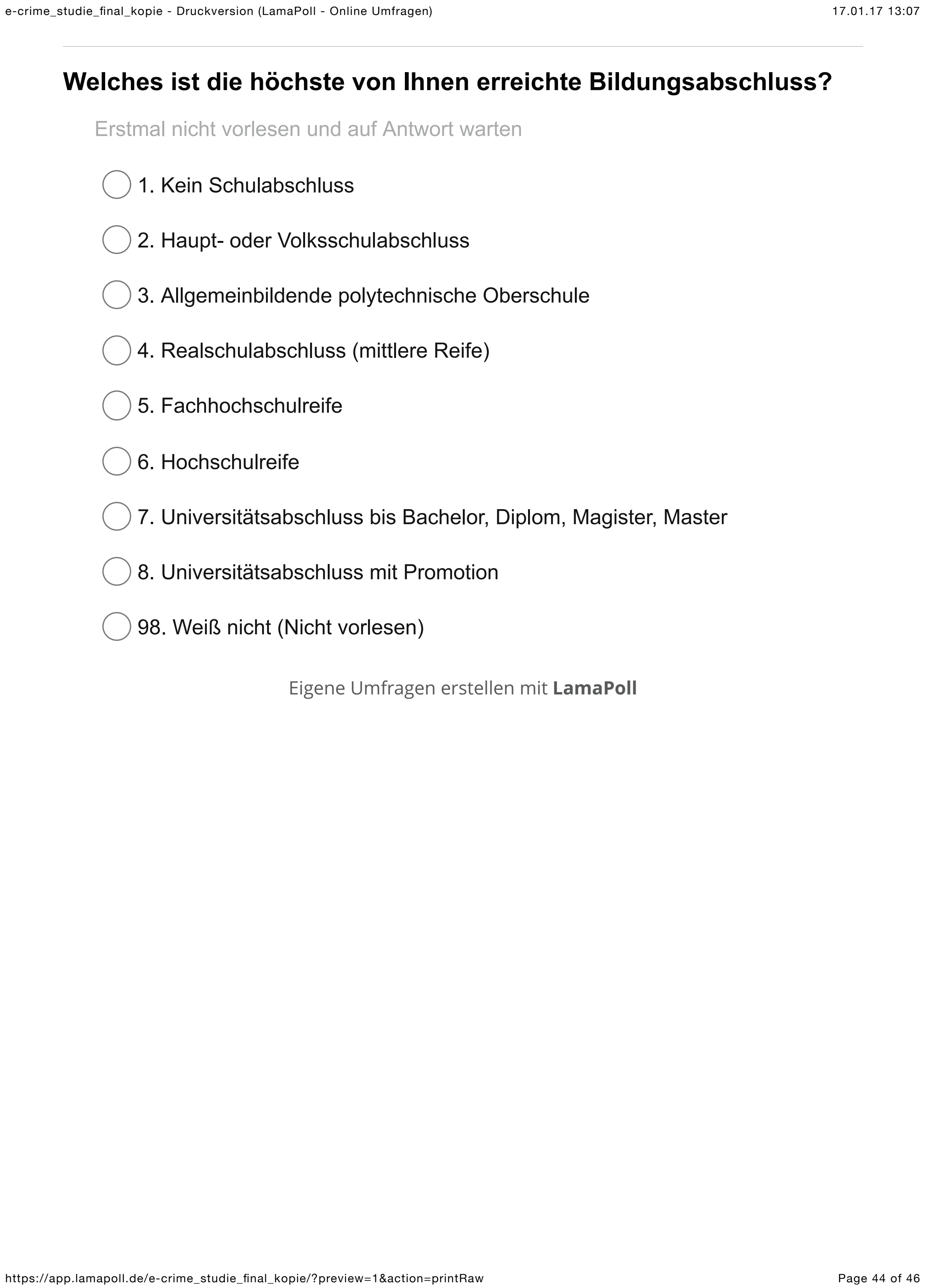
○ Der Stadtrand einer Großstadt

○ Eine Stadt oder Kleinstadt

○ Ein Dorf

○ Andere

○ Weiß nicht (nicht vorlesen)



### Welches ist die höchste von Ihnen erreichte Bildungsabschluss?

Erstmal nicht vorlesen und auf Antwort warten

○ 1. Kein Schulabschluss

○ 2. Haupt- oder Volksschulabschluss

○ 3. Allgemeinbildende polytechnische Oberschule

○ 4. Realschulabschluss (mittlere Reife)

○ 5. Fachhochschulreife

○ 6. Hochschulreife

○ 7. Universitätsabschluss bis Bachelor, Diplom, Magister, Master

○ 8. Universitätsabschluss mit Promotion

○ 98. Weiß nicht (Nicht vorlesen)

Eigene Umfragen erstellen mit **LamaPoll**

### C.1.2 Descriptive Statistics

**Self-reported Behavior** Table C.1 reports *self-reported* statistics regarding the use of the Internet and online shopping, as well as the credit card for Internet and offline payments.

**Table C.1:** Self-reported statistics: average use three month before the incident

| | | Monthly (M.) | | | Weekly (W.) | | Daily (D.) | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Never | <M. | M. | >M. | W. | >W. | D. | >D. | DK | NA |
| On average, how often have you used the Internet for personal purposes during the three months before the incident ? | | | | | | | | | | |
| use.internet | 0.0 % | 2.5 % | 5.0 % | 6.2 % | 5.0 % | 21.2 % | 22.5 % | 36.2 % | 1.2 % | 0.0 % |
| On average, how often have you used online shopping during the three months before the incident ? | | | | | | | | | | |
| use.oshopping | 5.0 % | 7.5 % | 18.8 % | 33.8 % | 16.2 % | 13.8 % | 2.5 % | 0.0 % | 1.2 % | 1.2 % |
| On average, how often have you paid with your credit card outside of the Internet during the three months before the incident ? | | | | | | | | | | |
| use.cc_offline | 30.0 % | 13.8 % | 6.2 % | 18.8 % | 17.5 % | 11.2 % | 0.0 % | 0.0 % | 2.5 % | 0.0 % |
| On average, how often have you paid with your credit card on the Internet during the three months before the incident ? | | | | | | | | | | |
| use.cc_internet | 13.8 % | 15.0 % | 30.0 % | 23.8 % | 8.8 % | 5.0 % | 1.2 % | 0.0 % | 2.5 % | 0.0 % |

**Table C.2:** Choice of payment method offline

| | **Credit card** | **Cash** | **Debit card** | **Other CC** | **Multiple** | **DK** | **NA** |
|---|---|---|---|---|---|---|---|
| Which payment method do you mainly use outside of the Internet ? | | | | | | | |
| main_pay.offline | 8.8 % | 22.5 % | 32.5 % | 0.0 % | 36.2 % | 0.0 % | 0.0 % |
| Which payment method do you mainly use when you are abroad ? | | | | | | | |
| main_pay.abroad | 40.0 % | 30.0 % | 8.8 % | 3.8 % | 15.0 % | 2.5 % | 0.0 % |

**Table C.3:** Internet payment preference and use

| | CC | Invoice | Direct debit | Prepay | PayPal | Giropay | SofortUe | Other CC | Other | NA |
|---|---|---|---|---|---|---|---|---|---|---|
| Which payment method do you prefer for payments on the Internet ? | | | | | | | | | | |
| pref_pay.Int | 16.2 % | 31.2 % | 10.0 % | 0.0 % | 35.0 % | 1.2 % | 1.2 % | 1.2 % | 1.2 % | 2.5 % |
| Which payment method do you mainly use for payments on the Internet ? | | | | | | | | | | |
| main_pay.Int | 32.5 % | 23.8 % | 10.0 % | 2.5 % | 27.5 % | 0.0 % | 2.5 % | 0.0 % | 0.0 % | 1.2 % |

Credit card (CC), Sofort Überweisung (SofortUe)

**Table C.4:** Attitudes towards online shopping

| **(Abbreviated) statement** | **No** | **Yes** | **DK** | **NA** |
|---|---|---|---|---|
| Only buy from online shops which offer preferred payment methods | 27.5 % | 71.2 % | 1.2 % | 0.0 % |
| Renounced products because preferred payment method not offered | 55.0 % | 37.5 % | 3.8 % | 3.8 % |
| Buy from online shops you have never heard of before | 63.7 % | 36.2 % | 0.0 % | 0.0 % |
| Canceled a payment because did not know 3D-Secure* password | 21.2 % | 76.2 % | 2.5 % | 0.0 % |

*Conditional questions adjust 3D-Secure for credit card type, i. e., *Verified by Visa* or *Mastercard Secure*

## C.2 Model Selection

**Table C.5:** Correlation matrix for predictors in the full combined model

| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
|---|---|---|---|---|---|---|---|---|---|---|
| 1) *incident* | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2) *well informed* | 0 | 1 | 0.65 | 0.3 | -0.12 | 0.07 | 0.03 | 0.06 | -0.05 | -0.11 |
| 3) *satisfied process* | 0 | **0.65** | 1 | 0.43 | -0.07 | 0.12 | 0.03 | 0.03 | -0.14 | -0.05 |
| 4) *bank prot. fraud* | 0 | 0.3 | 0.43 | 1 | -0.19 | -0.11 | 0.23 | 0.06 | 0.12 | 0.18 |
| 5) *less secure* | 0 | -0.12 | -0.07 | **-0.19** | 1 | 0.11 | 0.01 | 0.36 | 0.09 | -0.16 |
| 6) *o. paym. cheaper* | 0 | 0.07 | 0.12 | -0.11 | 0.11 | 1 | -0.51 | 0.07 | 0.06 | -0.08 |
| 7) *inexpensive* | 0 | 0.03 | 0.03 | 0.23 | 0.01 | **-0.51** | 1 | -0.01 | 0 | 0.2 |
| 8) *can avoid fraud* | 0 | 0.06 | 0.03 | 0.06 | 0.36 | 0.07 | -0.01 | 1 | -0.02 | -0.03 |
| 9) *card only option* | 0 | -0.05 | -0.14 | 0.12 | 0.09 | 0.06 | 0 | -0.02 | 1 | 0.29 |
| 10) *overall useful* | 0 | -0.11 | -0.05 | 0.18 | -0.16 | -0.08 | 0.2 | -0.03 | 0.29 | 1 |

**Table C.6:** Approximation of bootstrap p-values

| **Variable** | **Estimate** | **Bound at $\alpha$-level** | | | |
|---|---|---|---|---|---|
| | | 0.001 ($^{***}$) | 0.01 ($^{**}$) | 0.05 ($^{*}$) | 0.1 ($^{\dagger}$) |
| (Intercept) | 2.735 | -0.109 | 0.5 | 1.195 | 1.476 |
| newCC1 | -2.283 | -1.092 | -1.388 | -1.648 | -1.796 |
| *well informed* | -0.271 | 0.088 | 0.017 | -0.074 | -0.111 |
| *can avoid fraud* | 0.011 | -0.219 | -0.15 | -0.107 | -0.081 |
| *card only option* | 0.179 | -0.034 | 0.017 | 0.064 | 0.091 |
| *less secure* | -0.231 | 0.021 | -0.045 | -0.1 | -0.129 |
| *inexpensive* | 0.175 | -0.056 | 0.002 | 0.052 | 0.078 |
| newCC1:inc.good_info | 0.442 | 0.246 | 0.293 | 0.34 | 0.361 |
| newCC1:osInt.avoid_fraud | -0.087 | 0.026 | -0.002 | -0.028 | -0.041 |

# Appendix D

# Curriculum Vitae

Intentionally left blank.