Valuation of Confidentiality and Availability in a Personal Ransomware Attack Scenario

Freya Gassmann
Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau, Germany
freya.gassmann@rptu.de

Janina Beck
Boston Consulting Group
beck.janina@bcg.com

Nora Gourmelon
Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany
nora.gourmelon@fau.de

Zinaida Benenson
Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany
zinaida.benenson@fau.de

Abstract

To understand what is more valuable, availability or confidentiality of the data on a private computer, we conduct an online survey experiment with over 800 German participants assigned to one of the two scenarios: ransomware demanding payment for availability versus for confidentiality of their data. We find that 43.7% of respondents would pay for availability, whereas 38.6% would pay for confidentiality, this difference being not statistically significant. The amount of payment is higher for Confidentiality, this difference being statistically significant, but with small effect size. The probability of paying for young and elderly people is higher than for middle-aged ones, whereas sex, marital status and having children has no influence. Good backup quality and low income predict refusal to pay for availability, but not for confidentiality. In both scenarios, belief that the offenders will keep their promise and feeling scared predict payment, whereas belief that the payment is immoral and feeling strong negative emotions predict refusal to pay. Once the person decided to pay, the high emotional value of their files, as well as high social media usage predict higher payment value.

1 Introduction

Valuation of privacy has been an active research topic for decades. Valuation of confidentiality, although connected to this topic, has not received much attention yet. Finally, valuation of availability has become very pronounced in the last few years, with the threat of ransomware steadily growing. The question we are contemplating in this paper is:

> *What do people value more, availability or confidentiality of their data on a private computer?*

Although the above question is not immediately connected to ransomware, this threat provides a plausible scenario to investigate it. Ransomware threat has steadily grown in the last years, and the Joint Cybersecurity Advisory issued in 2021 by the UK, US and Australian authorities warns that this trend is going to continue [10]. This trend is corroborated by the German Federal Office of Criminal Investigation that chose ransomware as the focus of their annual 2021 report on the state of cybercrime in Germany [11]. In the recent years, the focus of attacks has shifted from individuals to companies and organizations, as these attacks showed to be more lucrative. Nevertheless, individuals are victimized as well, as criminals often deploy opportunistic strategies targeting any badly protected system [19]. For example, FBI's Internet Crime Complaint Center (IC3) received 2825 ransomware complaints from general public in 2023 [16]. In the past, most types of ransomware violated the availability of data on the attacked device to extort money from companies and individuals. However, as ransomware attacks has been getting more sophisticated, the criminals started using the so-called *double extortion* as a standard attack method [10, 11]: additionally to encrypting victim's data, they threaten to publish extracted data if the victim refuses to pay.

In the classical paper by Avizienis et al. [2, p. 13], availability is defined as "readiness for correct service [...] for authorized actions". Applying this definition to data on a private computer, availability means that the owner of the computer always has access to the data, and that other parties also have access when authorized by the owner. Confidentiality is defined as "the absence of unauthorized disclosure of information" [2, p. 13], meaning that the owner of the computer has full control over the disclosure of the data.

We note that in general, privacy is not the same as confidentiality [18]. Whereas information privacy is often (but not exclusively) considered as control over disclosure of personal information towards third parties [27], confidentiality is defined as restricting access to any kind of information (not necessarily personal) to authorized parties only [2]. We prefer using the term "confidentiality", because data stored on a personal device may be confidential, but not related to any person. When personal data is considered, however, privacy and confidentiality are especially closely related, such that related work on privacy valuation is highly relevant in our context.

Although extensive research has been conducted on the valuation of privacy (see, e.g., Wagner et al. [32] for an overview), and recently, several studies investigated private in-

dividuals' willingness to pay for availability in ransomware scenarios [14, 7, 8], there is no research that directly compares valuations of availability and confidentiality. In the following, we make first steps to investigate this research gap.

2 Background and Related Work

2.1 Valuation of Privacy

How much people value privacy of various data types has been a very active research field for decades [32]. Privacy valuation has been investigated in lab experiments, field experiments and surveys. Users are usually offered specific scenarios in which they are asked whether they would protect or sell their private information for a fixed amount of money, or asked to specify their own price. For example, Carrascal et al. [6] elicited users' willingness to sell their browsing information (such as uploaded photos, search terms or details of a financial transaction) and offline information (such as age, salary and address) in an online study using a specifically designed browser plugin.

Important notions in this research field are willingness-to-pay (WTP) and willingness-to-accept (WTA). Quite often, WTP for protecting private data is by many factors lower than WTA monetary compensation for selling the same data. For example, Grossklags and Acquisti [12] found in a lab experiment that WTA for selling personal information such as weight, performance in a quiz, vacation destination and number of sex partners is 4-5 times higher than WTP for protecting it. In another example, in an online survey, the participants were willing to sell access to their personal data to online companies for median \$80-100 (depending on whether this data included, e.g., name or health information), but their WTP had median of \$5 independently on data types [34]. Thus, valuation of privacy is highly dependent on the framing of the decision task (to protect or to sell), and to some extent on data type. Valuation of privacy is also heavily context-dependent aside of the WTP-WTA gap. It depends, for example, on the order of options presented to the participants [1] and on the saliency of privacy information [31]. This makes comparison of concrete privacy valuation amounts across different studies unreliable [32].

"Privacy" and "personal data" are usually operationalized by specific types of personal data that are relevant for online or offline privacy context (name, age, sex, address, salary, shopping and browsing behavior). Valuation of all data contained on a private device has not been investigated so far.

2.2 Data Ownership

Spiekermann and Korunovska [29] have investigated the concept of data ownership in a series of online field experiments, including two prestudies [3, 30]. They asked under which circumstances would people build a sense of ownership of their data and thus actively participate in the digital economics. The personal data they consider is the entire Face-

book profile of a user. Survey participants were presented with a scenario where Mark Zuckerberg sends them a message that he is "tired of business and intends to shut down the platform" [29, p. 66]. The scenario was designed to be as realistic as possible, e.g., the survey was designed to have the look and feel of Facebook to immerse the participants into the situation as much as possible. In five between-subjects experimental conditions, the participants are presented with different choices. In four conditions, WTP is elicited, and the fifth condition elicits WTA for comparison. The WTP conditions are organized as a 2x2 experiment with variables market awareness (yes/no) and data safeguarding method (data portability versus data download).

Market awareness is the most important variable from our point of view: In the market unaware condition, Mr. Zuckeberg says that he is going to delete all Facebook data, and participants can safeguard their data either by downloading it to their hard drive, or by transferring it to another social network site. The participants are asked how much they would pay to safeguard their data. Thus, in this condition WTP for availability of the Facebook profile data was elicited. In the market aware condition, Mr. Zuckerberg says that a "trustworthy third party" is interesting in buying users' Facebook profiles. By paying, the participants could still safeguard their data as above, and additionally could prevent their data from being sold. Thus, from our point of view, this condition elicited WTP for privacy (or confidentiality) as well as for availability of Facebook profile data. Whereas this condition made sense for the investigation by Spiekermann and Korunovska, it combines WTP for availability with WTP for confidentiality, such that we cannot draw reliable conclusions about WTP differences from this study.

In our study, we investigate how a variable similar to market awareness influences WTP. We call it "potential for misuse" (see Sec B.2.4): the participants are asked to rate their opinion on whether their data could be valuable for criminals or other persons with bad intentions. We also draw inspiration from the setup of the study by Spiekermann and Korunovska: We use a realistic scenario that shows a carefully designed ransom note and thus attempts to embed the participants into a ransomware experience to elicit WTP.

2.3 Availability and Data Exfiltration in the Ransomware Context

The idea of malicious software encrypting valuable data and demanding ransom dates back to the paper by Young and Yung on cryptovirology published in 1996 [35]. However, serious real-world attacks started to occur approximately 15 years later [36]. First ransomware variants attacked computers of private individuals, later moving to targeting businesses and governmental organizations. However, it seems that private individuals still suffer from ransomware. Thus, surveys conducted by security companies as well as by academic researchers in the last few years established the overall victimization rate of 16-18% in Germany, the UK and the USA [26, 24, 20, 28].

The study by Simoiu et al. [26] with a representative sample of the US population, and its replication with a representative sample of the German population by Ortloff et

al. [24] found that participants experience difficulties in distinguishing ransomware from other types of malware. Therefore, after asking their participants more details about the incidents, they corrected the victimization rates to lower percentages, depending on how strict were criteria for inclusion: 6-9% for the US, and 8-14% for Germany.

Willingness to pay for availability of data in case of a ransomware infection has been investigated by companies as well as by academic researchers. Thus, the IBM study [17] with US consumers found that 54% of participants would pay ransom to get their financial data back, with parents having higher WTP for photos than non-parents. Similarly, the Carbon Black [5] survey with a US sample found that 52% of participants would pay ransom, financial data and family photos being their most sensitive information. Median payments in both cases are under USD 100, but exact payment distributions are not presented.

Hernandez-Castro et al. [14] and Cartwright et al. [9, 7, 8] conducted a series of studies that elicited WTP and WTA for availability in different scenarios, and investigated factors related to WTP and WTA. Median WTP is around GBP 50-100, and median WTA is around GBP 400-700. The authors assume that this WTP-WTA gap is caused by WTA being an estimate not only of material, but also of psychological cost of losing files. Thus, people who reported to have backup exhibited higher WTA than people without backup, although the former would be able to restore their files without payment [9].

Factors related to WTP are not quite consistent across the studies, maybe due to differences in samples and in scenario framing. Thus, studies [9] and [8] were conducted with representative samples of the UK population, whereas Study 2 and 3 in [7] were conducted with non-representative Prolific samples. Moreover, although the technical report [9] and Study 1 from the workshop paper [7] seem to analyze the same data, results might differ due to different analysis techniques. Whereas the tobit regression in [7] includes all variables, [9] presents two linear regressions: one with the demographic variables only, and another with factors related to data storage and cyber security. Thus, having children has a high impact in [9], but no effect in [7]. Female users exhibit higher WTP in most of the studies, but sometimes sex does not have an effect (Studies 2 and 3 in [7]). Also the effects of age, marital status and occupation are different across the studies.

Furthermore, in [9] and [7], the WTP scenario is framed in terms of accidental data loss, whereas in [8] the scenario is framed in terms of ransomware. The latter study therefore takes the effects of unwillingness to pay the criminals and trust in criminals into account. Whereas in [8] less frequent backup is related to higher WTP, in Studies 2 and 3 in [7] higher backup frequency is related to higher WTP. The last result seems to be counter-intuitive. However, in the latter studies participants were asked to imagine that they do not have backup (irrespectively on whether they actually have it). We think that this might have influenced the answers, as people who have backup might value their files more than people who do not have backup. To summarize, WTP for availability seems to be consistent across the studies, but the factors related to it heavily depend on the presentation of the scenario.

Quite recently, Meurs et al. [22, 21] investigated factors influencing the intention to pay ransom, and the amount of ransom paid when the victim is an organization. They looked

at the real cases reported to the Dutch police and to an incident response company. In the first paper [22], they found that data exfiltration is a significant predictor of the decision to pay, as well as of the higher amount of the payment. In the consequent investigation [21] with a larger data set, they found that, although 40% of victims with data exfiltration threat paid ransom, as opposed to 25% of victims without data exfiltration, this difference became non-significant in the two-step regression analysis. However, the higher amount of ransom paid still remained statistically significant, with victims of double extortion paying 4.4 times more than victims of extortion without data exfiltration. It is not known, however, whether these results apply to the individuals. Moreover, they only studied cases where the data was encrypted, making it impossible to determine the influence of data exfiltration threat without encryption.

3 Hypotheses and Influencing Factors

3.1 Valuation of Availability versus Valuation of Confidentiality

As discussed in the previous section, valuations of privacy and availability are inherently context-dependent. If ransomware threatens availability, the victims will be able to instantly observe the consequences of this threat, as their files will not be available anymore. On the other hand, the consequences of a confidentiality threat are less immediate. In the moment of the incident, there are quite likely no consequences at all, as the data has not been released yet. It is likely that this psychological effect of immediate versus delayed consequences will lead to higher WTP for availability compared to WTP for confidentiality. Therefore, the corresponding hypotheses are as follows:

> H1: Higher number of victims will be willing to a pay a non-zero amount if the availability of their data is threatened than if the confidentiality of their data is threatened.

> H2: Payment amounts will be higher if the availability of data is threatened than if the confidentiality of data is threatened.

3.2 Factors Influencing WTP

To determine factors related to WTP, we rely on the results of previous academic and non-academic works discussed in Sections 2.2 and 2.3. We are interested in factors that make people pay or not pay, as well as in factors that influence the amount of non-zero payments. We assume that these factors are not the same. For example, we expect the existence of full and up-to-date backup to have a negative influence on willingness to pay for availability, but not on the amount paid. Nevertheless, when we introduce the factors, we do not make this distinction for brevity, but we will pay attention to it in the analysis.

We also chose not to formulate hypotheses, as the number of factors is very high. We prefer to do an exploratory regression analysis of factors, as this study in itself is exploratory, comparing valuation of availability with valuation of confidentiality for the first time.

3.2.1 Demographic Factors

We investigate the following demographic factors: age, sex, educational background, occupation, marital status, having children, income, IT background. As already mentioned in Section 2.3, different studies [9, 7, 8] have found an inconsistent evidence of the influence of these variables on WTP for availability, such that it should be further investigated.

3.2.2 Digital Factors

Digital factors are connected to the usage of the devices, and to the files stored on them. Here, the evidence from the previous studies is again inconclusive. For example, storing sensitive files and working files has an effect in [9], but not in [8]. Storing photos has an effect in [8], but not in [9]. Thus, we investigate how the storage of various types of files, such as private photos and videos, emails, calender, purchased software, personal notes, work and study materials, is related to WTP. Moreover, private computers are often shared with other people, especially with partners and family. Thus, private computers are likely to hold the files that are important to other people. This might influence WTP, as the loss of availability as well as the loss of confidentiality can have unpleasant social consequences, such as bad feelings within the family, loss of reputation or problems at work.

Surprisingly, Cartwright et al. [9] did not find a significant relation between the frequency of backup and WTP for availability. They found this relation in their later study [8], however. We assume that just asking about the frequency of backup is not enough, e.g., because it is not known whether all important data is backed up, and whether the user trusts that their backup is going to work if needed. Therefore, we assume that having no backup, or having backup of perceived low quality will positively influence WTP for availability, but not for confidentiality.

Further digital factors include security awareness, social media usage and the knowledge of cyber terms. These factors were found to have significant influence on the WTP by Cartwright et al. across almost all studies. Past experience with ransomware can also be relevant. Simoiu et al. [26] discovered that users who already experienced ransomware were less inclined to pay ransom for availability than people without such experience.

3.2.3 Psychological Factors

Cartwright et al. [8] consider several psychological factors that have influence on WTP, such as not being willing to pay criminals on principle, or trusting the criminals to return the files after the payment, or being willing to pay if the price is right. However, in their

study each participant is asked to choose only one of the possible reasons. We extend their work by considering these and further WTP factors for all participants. The victim would be motivated to pay if they think that the criminals will actually execute the actions they threaten to do, trust that the criminals will stop the attack after payment, and if they feel that they are able to conduct the payment. The latter is not self-evident, for example, if the ransom is demanded in Bitcoins or other cryptocurrencies. Some ransomware types provide tutorials for victims on how to make payment [13]. On the other hand, people who are strongly opposed to giving money to the criminals are likely not to pay.

Finally, we also assume that emotions felt in the scenario might influence the willingness to pay. However, the direction of these influences is not clear. For example, would frightened users tend to pay, or would they be so frightened that they give up? Thus, we consider the emotional state of the victim as an exploratory WTP factor for the first time.

4 Method

4.1 Scenario Framing

Our main research question asks what is more valuable for users, availability or confidentiality of their data on a private computer. Investigating this question using a ransomware-based scenario is not self-evident. For example, in a scenario involving criminals, people might be less inclined to pay than in a scenario involving a benign incident, because they consider the payment immoral. Fortunately, Hernandez-Castro et al. [15] found that there was no difference in WTP for availability between a ransomware-based and a benign scenario (accidental loss of files) in their survey. Thus, we assume that a ransomware-based scenario is a valid framing for answering our research question. Most importantly, whereas an accidental loss of all user data is easily imaginable (e.g., a crashed hard drive), accidental benign leak of all data from a private device seems to be unrealistic. Despite several brainstorming sessions and trials, we were unable to come up with a realistic scenario. Although accidental partial leak is possible (e.g., sending a wrong email attachment by mistake), we are interested in the valuation of all user data on a private PC.

We decided to elicit WTP and not WTA in our study, as we are less interested in the absolute amount of valuation (which would presumably differ for WTP and WTA), and more interested in whether there is a difference at all between valuations of availability and confidentiality. Furthermore, a ransomware scenario naturally lends itself to elicitation of WTP (how much would victims pay). Although Cartwright et al. [7] elicited WTA for availability in a scenario where participants were eligible for compensation after a ransomware incident, this scenario is less natural than the WTP scenario, and thus, we leave the investigation of the WTP-WTA gap to future work.

Another important question is how to frame the scenarios to ensure disjunct experimental conditions. As we outline in the previous sections, ransomware usually either threatens only availability, or adds to this threat an additional confidentiality threat. However, to

answer our research question we need two scenarios that threaten exclusively one of these security goals. That is, the Confidentiality scenario needs to be phrased in a way that makes sure that the availability of data is not affected, and vice versa. After extensive user tests (outlined in Section 4.2), we decided to use in the Confidentiality scenario the phrasing "Your computer can still be used as usual" and "The files on your computer are available and usable". The full phrasing of the scenario is presented in Appendix B.4.

Furthermore, for the availability scenario, two cases are possible, as Simoiu et al. [26] explain: The ransomware can either block access to the entire device, rendering it non-functional, or it can only block access to user files by encryption, leaving the functionality of the device unaffected. Fortunately, getting back the functionality of the infected device is always possible if the device is fully reset. Therefore, after the extensive user tests we decided to phrase the threat as following: "Your computer cannot currently be used as usual. The only way to make your computer usable again is to reset your computer completely. This will result in the loss of all files that were stored on the computer." The full phrasing of the scenario is presented in Appendix B.3.

4.2 Survey Construction

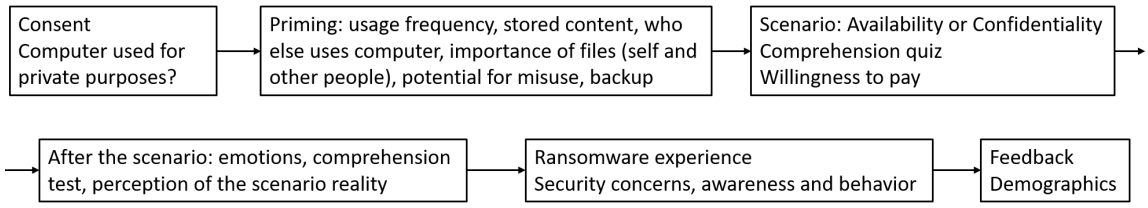

Figure 1: Overall structure of the survey

Following Spiekermann and Korunovska [29], we sought a realistic and understandable setting that would immerse the participants into the attack situation, and thus elicit answers that are as close to reality as possible. We developed the scenario as an online survey in German language, using multiple iterations.

Development Iterations The first version of the survey was reviewed by six usable security experts. Thereafter, the survey was tested in a laboratory setting with 22 non-expert users with diverse demographic characteristics. The users were encouraged to "think aloud" when they were answering the survey, indicating if something was not understandable, or seemed strange, unrealistic, or otherwise affected them in an adverse way. After every 3-5 tests we adjusted the survey according to the participants' comments. Next, the survey was tested again by five additional usable security experts. Finally, the survey was tested two times with 30 workers at the German crowdworking platform *clickworker.de*

and adjusted accordingly. Each worker could only participate in one test run, and test participants were later excluded from the actual run of the survey on the same platform. The most important changes and their reasons are presented below in the survey structure. The overall structure of the final survey is shown in Fig. 1, and the full survey is presented in Appendix B.

Consent & Computer After providing consent, the participants were asked whether they use a computer or a laptop for personal purposes. We decided to leave tablets and mobile phones to future work, because they may be used differently from the computers and store different files, which requires different wording of the survey. In order to enable better immersion in the ransomware scenarios later on, we asked the participants to fill in the survey using a computer or a laptop. We technically filtered out all users whose user agent did not correspond to allowed devices.

Priming The users were first asked questions about the files they store, how valuable and up-to-date are these files, whether these files might be important for other people, what would be the consequences of their loss or disclosure, including potential for misuse. We also asked several questions about backup: which files and system parts are backed up, on which data carriers, how often. The backup questions were especially often updated during the test runs, to make sure that all popular backup possibilities are included and understandable. All these questions were purposefully asked before the ransomware scenario, because we wanted to prime the participants on the value of their files and on the possibilities of recovery. The reason for the priming is that if the participants were under a real attack and had to think about payment, they would most likely consider all these factors. All participants were asked the same questions, independently of the scenario, to ensure that the difference between the experimental conditions is minimal.

Scenario & Quiz The first scenario that we created showed a ransom note for Availability or Confidentiality (see Fig. 2 and 3), and then asked about the payment amount. The notes were created using the actual wording of ransom notes of Chimera, Jigsaw and Petya ransomware (see Fig 7 in Appendix A). However, during the test runs we had to adapt the notes, such that they were better understandable to non-experts. For example, we dropped usage of the term "decryption key", and use "decryption program" instead. We also took special care to use approximately the same amount of words, and the same design and layout for both ransom notes to make sure that the experimental conditions are as close to each other as possible for both scenarios.

During the laboratory tests we encountered difficulties with understanding and credibility of the scenarios. Most participants believed that they could get rid of the ransom note if they restarted their computer, or asked a tech-savvy friend or relative for help. Moreover, as the note showed that they have 72 hours for the payment, they were sure

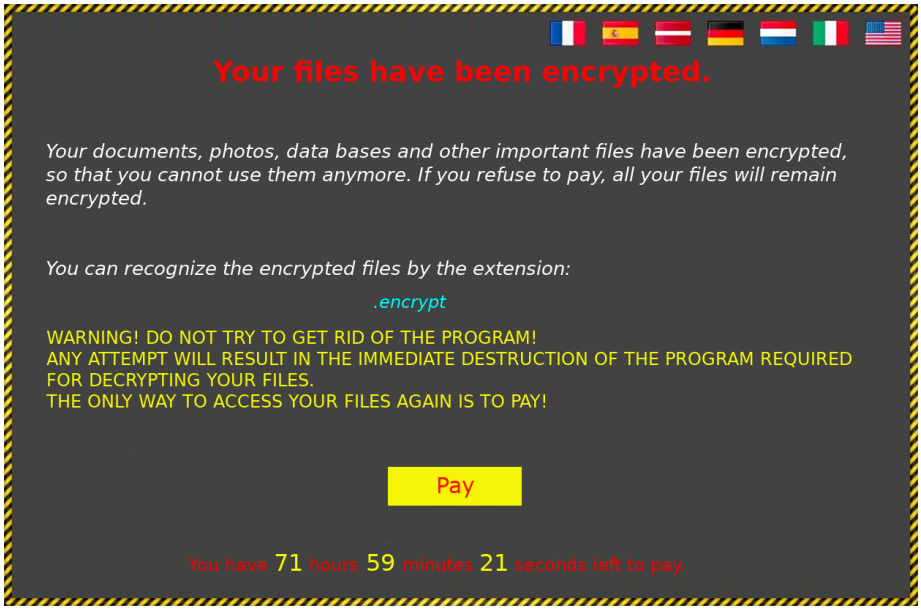

Figure 2: First ransom note for the Availability scenario, 72h left for making payment (translated into English)

that they would be able to solve the problem during this time. Although it is actually possible with some ransomware strains, our scenario represents a non-removable threat. Thus, we had to expand the scenario: We first show the ransom note with 72 hours remaining, and ask what users would do to solve this problem. Thereafter, we ask them to imagine that whatever they did was unsuccessful, and show them the ransom note for the second time, but this time there are only 15 minutes left for payment. We then ask them how much they would pay, provided that the payment can be made easily. The latter condition helps us to separate concerns about the payment method from the concerns about solving the main problem.

An important question is how to ask for payment. We started with asking people first whether they would pay (yes/no), and then if yes, how much. However, during the laboratory tests (see page 9), we noticed that in this case users tend to say "no" very quickly, as this is a socially desirable answer. Therefore, we decided to unbias this answer by directly asking about the payment amount. Further extensive user tests showed that if users do not want to pay, they enter "0" into the payment field.

During the tests we noticed that especially the Confidentiality scenario is very difficult to grasp, and participants often mistook it for the Availability scenario. We think that this happened because availability attacks are heavily present in the mass media. Therefore, we decided to introduce a quiz immediately after the scenarios, such that participants can

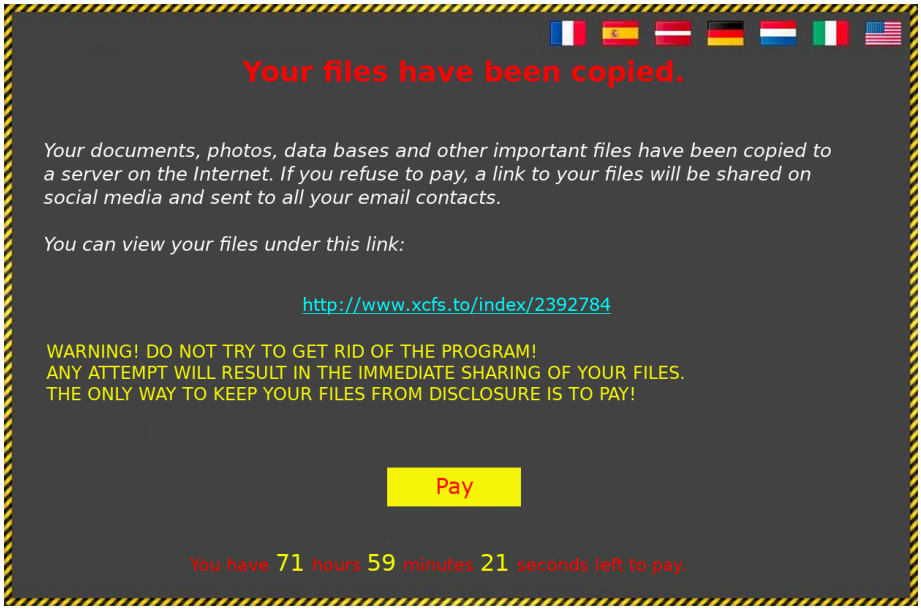

Figure 3: First ransom note for the Confidentiality scenario, 72h left for making payment (translated into English); the link points to a non-existing top-level domain (.to)

test their understanding. In case of incorrect answers, the scenario is explained again, and correct answers are shown. The structure of the scenario is shown in Fig. 4.

Emotions, Comprehension and Reality of the Scenario Emotions were asked immediately after scenario, to ensure that the users are still immersed into it, and measured using the German version [4] of the PANAS scale [33], where users rate how strongly they feel 20 various affects. Next, the participants filled out a comprehension test consisting of 7 items to be answered with "true", "false" or "don't know", for example: "In the scenario you dropped your computer and it broke." (false), or "In the scenario you were threatened with a disclosure of your files." (true for Confidentiality, false for Availability). The users were then asked whether they consider the scenario realistic and think that it could happen to them personally, whether they think that paying would be easy, and whether it would be immoral. Further, we asked whether the participants already experienced ransomware.

Security Concerns, Awareness and Behavior Next, the participants filled RSeBIS scale [25] to measure security behavior intentions. The German translation of RSeBIS was obtained directly from Morgner et al. [23] who used it in their survey on IoT security labels. The participants also answered questions by Cartwright et al. [9]: concern about data breaches, social media usage, and awareness of some cyber terms, such as doxing, identity theft or WannaCry. These questions were obtained directly from Cartwright et al.

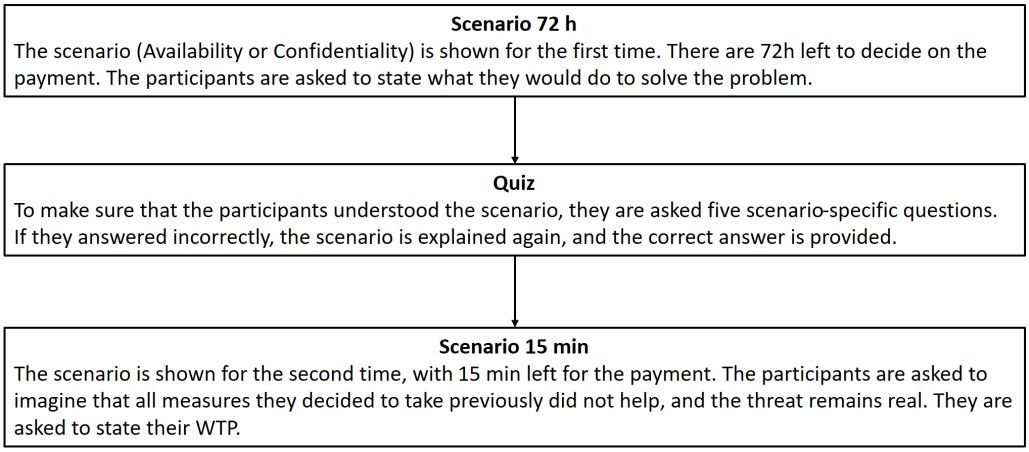

Figure 4: Structure of the scenarios; WTP = Willingess to Pay

They were translated into German independently by three research team members, who then discussed translation differences and agreed on the common version. This version was then translated back into English by a usable security researcher not involved in this research to verify that the translation semantically matches the original questions.

Quality Checks and Demographics Filling in the survey took 15-20 minutes in the trials, which is quite a long time, during which users might become distracted. Therefore, we asked some quality check questions, such as whether they were distracted, whether they understood the survey well, and took the task of determining their payment amount seriously. The participants were assured that answers to these questions would not have any negative consequences, and in particular will not influence the compensation of Clickworkers. We also added two attention tests, and the scenario comprehension test (but not the comprehension quiz) was used as a third attention test to exclude participants who gave answers of poor quality. Finally, we asked demographic questions: age, sex, education, occupation and income, marital status and whether they have children, and the IT background. The users also had the possibility to provide feedback, and were given contact information for further questions.

4.3 Ethics, Data Cleaning and Sample Description

The survey was approved by the data protection office of our university. The survey run at the server at our lab, and data access is restricted to the members of the project team. Our department does not have an ethical approval committee, but we ensured through the extensive user tests and expert reviews that the participants were not harmed. To

ensure a diverse user sample, we run the survey in two variants: on the German platform *clickworker.de*, and distributed the survey link at several German universities. Clickworkers received payment of 3 EUR for 20 min. The university sample was not compensated, as the participants were not registered. Although in similar cases participants are often offered a lottery (e.g., winning one of several 10 EUR online shop vouchers), we decided not to use this method in our study, because Bauer et al. [3] showed that the amount of compensation could influence WTP due to the psychological bias known as anchor effect. Not compensating the university sample is a compromise between the rigor of study design (as not to produce the anchor effect) and the ethical principles of sufficient compensation. In consequence, we assume that the university sample was motivated solely by their interest in the study subject, but the clickworkers had an additional monetary motivation. During the statistical analysis, we always looked at whether belonging to the particular set of participants (clickworkers or university) made a difference.

Overall, 1543 users (625 clickworkers and 918 university users) started the survey, and 1223 (604 clickworkers and 619 university users) finished it. The higher rate of non-completion among the university students is likely due to the fact that they were not compensated. Of them, 604 clickworkers and 608 university users provided WTP and took part in the comprehension test. 144 respondents who answered more than two questions incorrectly were excluded from further analysis. Answers of 234 users could not be used because they indicated that they were distracted during the study, or did not take the task of determining WTP seriously. One additional user was excluded because their WTP was 100,000, which we consider unrealistic for a private person. After that, no users remained who would be excluded because of the other two attention checks. Because people had to be removed for more than one reason, 857 respondents (454 clickworkers and 403 university users) remain for data analysis. The participation took 19.5 min on average.

We had to exclude a rather high percentage of participants (30%, 366 out of 1223). However, we believe that such rigorous data quality control is very important in our case. As we asked about a hypothetical situation in an immersive scenario, if people admit that they were distracted (and thus were possibly not able to remain immersed in the scenario) or did not take the determining their WTP seriously, they had to be excluded. There is also a difference in the number of excluded users between conditions. Thus, 203 out of 602 users (34%) were excluded in the Confidentiality condition, whereas 163 out of 621 users (26%) were excluded in the Availability condition. This difference is due to the fact that the Confidentiality scenario was more challenging to grasp, as we explain in Section 4.2 on page 11, and thus more users answered control questions wrongly. This difference is significant, but the effect size is very small ($\chi^2(1) = 8.1402, p < 0.05$, Cramer's V = -0.0816), which means that the difference is not relevant in terms of content.

Table 1 shows demographic data of the participants. As expected, the clickworker sample is older, contains more employees and fewer students, and has higher income than the university sample. Both samples are highly educated and over 20% of all participants have professional IT background. Overall, this means that the samples are not representative of

the German population. Additionally, 17% of respondents indicated that they experienced ransomware before, but none of them paid for their files. This victimization rate is consistent with the self-reported victimization rate of a representative German sample: 18,9%, although 2% of the sample reported that they paid ransom [24].

4.4 Data Analysis

Statistical analyses were performed using Stata SE 14.2 assuming a significance level of $p < 0.05$. Most variables were evaluated as an index, i.e., either by counting the number of "yes" answers (e.g., knowledge of the cyber terms, social media usage), or by averaging over individual items (e.g., backup quality, RSeBIS). To evaluate PANAS, we conducted a principal-component factor analysis with orthogonal Varimax rotation, as presented in Appendix C. We found four emotional factors, which we summarize under the following terms for better readability: Factor 1 with "afraid", factor 2 with "enthusiastic", factor 3 with "interested" and factor 4 with "hostile". We note that Factor 1 "afraid" seems to consist of negative weak (passive) affects, e.g., guilty, scared, ashamed. Three other factors mostly consist of strong (active) positive or negative affects: excited, alert, determined.

To evaluate hypotheses H1 and H2 that compare the number of non-zero payments and the amount of payments between the Availability and the Confidentiality scenarios, we use the χ^2-test and the two-sample Mann-Whitney rank-sum test, respectively.

To consider the factors for paying or not paying the ransom in both scenarios, logistic regression analyses were conducted on several models. Respondents who did not provide data concerning one of the considered variables had to be excluded from the analysis, resulting in 390 out of 458 (85%) participants for the Availability scenario and 351 out of 399 (88%) participants for the Confidentiality scenario. To consider the factors for the amount of payment (only including the non-zero payments), we run linear regressions on several models. The number of participants for the Availability scenario is 175, and for the Confidentiality scenario 138.

5 Results

5.1 H1 and H2: WTP for Availability versus WTP for Confidentiality

In the Availability scenario, 43.7% of respondents (200 out of 458) would pay a non-zero amount, whereas in the Confidentiality scenario, 38.6% (154 out of 399) would pay, see also Fig. 5. As there is no significant difference between the clickworkers and the university sample, we present cumulative results. Thus, a slightly higher percentage of participants would pay for Availability than for Confidentiality, as hypothesis H1 predicts. However, the value of $\chi^2(1) = 2.2623$ with $p > 0.05$ and Cramer's V $= 0.0514$ indicates that the scenario had no effect on paying for the data or not, and therefore, H1 is not supported.

		Clickworker		University		Total	
Sample size		454		403		857	
Gender	Female	265	58%	203	50%	468	55%
	Male	183	40%	193	48%	376	44%
	No answer	6	1%	7	2%	13	2%
Age	Mean age (sd)	39.2 (11.8)		25.7 (6.2)		32.9 (11.7)	
Vocational qualification	None	45	10%	142	35%	187	22%
	Vocational	184	41%	39	10%	223	26%
	Academic	215	47%	211	52%	426	50%
	No answer	10	2%	11	3%	21	2%
Occupation	Student	55	12%	302	75%	357	42%
	Employed	242	53%	71	18%	313	37%
	Self-employed	97	21%	1	0%	98	11%
	Other	49	11%	11	3%	60	7%
	No answer	11	2%	18	4%	29	4%
Income	none to 500	45	10%	122	30%	167	19%
	500 to 1100	63	14%	146	35%	209	24%
	1100 to 1700	87	19%	49	12%	136	16%
	1700 to 2600	107	24%	41	10%	148	17%
	2600 to 5000	86	19%	21	5%	107	12%
	No answer	66	15%	24	6%	90	11%
Marital status	Married or civil union	130	29%	37	9%	167	19%
	Living together but not married	94	21%	109	27%	203	24%
	Single	193	43%	241	60%	434	51%
	Other	24	5%	3	1%	27	3%
	No answer	13	3%	13	3%	26	3%
Children	Yes	130	29%	23	6%	153	18%
	No	312	69%	372	92%	684	80%
	No answer	12	3%	8	2%	20	2%
IT background	Yes	90	20%	114	28%	204	24%
	No	359	79%	285	70%	644	75%
	No answer	5	1%	4	1%	9	1%

Table 1: Demographic data of the participants; percentages may not always add up to 100% due to rounding errors.

Figure 5: Payments versus non-payments in the Availability and Confidentiality scenarios.

Hypothesis H2 states that the payment amount will be higher for Availability than for Confidentiality. Figure 6 shows the histograms of the natural logarithm of non-zero payments for both scenarios. Most participants would pay 50 EUR or less (median is 50 EUR in both scenarios), and the payment for Confidentiality is slightly higher than for Availability. As the amount that participants would pay is not normally distributed, a non-parametric test is used to compare the payment amounts. The two-sample Mann-Whitney rank-sum test indicates that the distributions of payments differ significantly ($z = 2.623, p < 0.01$). However, the hypothesis is not supported, as the effect shows into the "wrong" direction. The payment amounts for Confidentiality are significantly higher than for Availability, contrary to our intuition. However, the effect size is small ($r = 0.138$), which shows that the effect has low practical importance.

Considering the two samples (clickworkers versus university) separately, we can see a more differentiated picture. For clickworkers, the median payment for Availability is 50 EUR, for Confidentiality 30 EUR, and the difference is not statistically significant ($z = 0.626$, $p > 0.05$). For the university sample, the median payment for Availability is 50 EUR, whereas for Confidentiality it is 100 EUR, this difference being statistically significant with small effect size ($z = 2.735$, $p < 0.01$, $r = 0.201$). This means that the above statistically significant difference is due to the university sample.

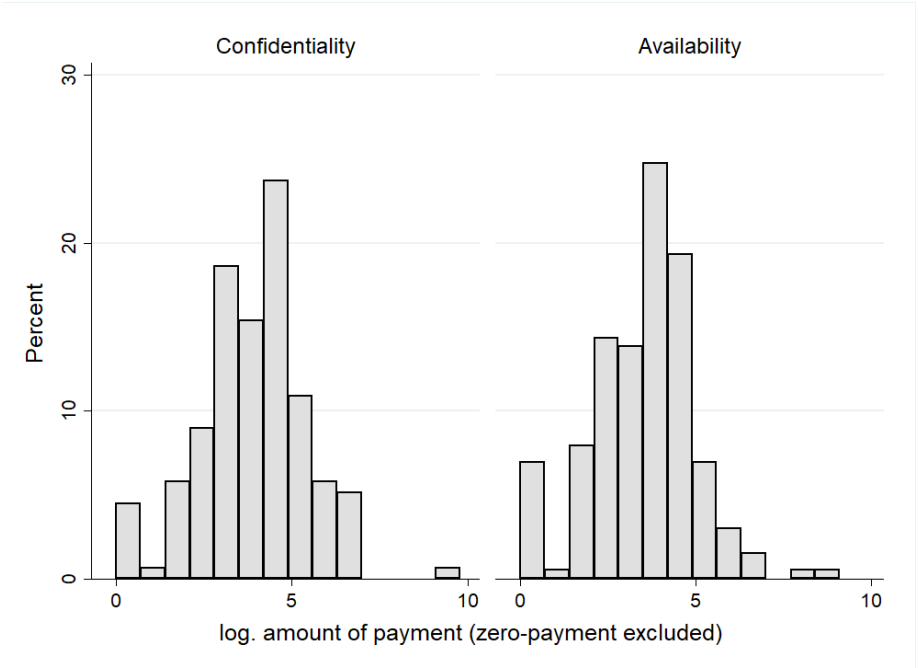

Figure 6: Histograms of the natural logarithm of Willingness To Pay (WTP) in the Availability and Confidentiality scenarios, including only non-zero payments.

5.2 Factors of Payment versus Non-Payment

We used logistic regressions to understand what drives decisions to pay or not to pay in the respective scenarios. The dependent variable is binary: "payment vs. no payment". Due to the high number of variables, we only present the most relevant regression models, see Table 2. For example, backup was found to be significant for Availability, but not for Confidentiality, which led to the inclusion of this factor into logistic regressions for both experimental conditions. On the other hand, models containing the following variables were tested, but are not presented, as the variables have no significant effect on payment in either condition: marital status, educational and vocational qualification, usage of the computer by other users, types of files stored, data breach concern, an index of protection measures, rating of files (sensitivity, emotional value and importance for self and for other people), potential for misuse of the files. We include some control variables, although they were not significant in either condition, such as sex and IT background.

Demographic Factors We show three models per condition. Avail-1 and Conf-1 consider demographic factors and expereince with ransomware. They have the lowest explanatory power, and most effects become weaker or stronger in further models that consider

additional variables and have more explanatory power. There is no significant effect of sex. We found a negative age effect and a positive squared effect of age in all models. This means that the effect is u-shaped: the probability of paying for young and for elderly people is higher than for middle-aged ones. Having children has an effect on payment for Confidentiality in the Conf-1 model that only considers demographic factors and has a low explanatory power. This effect disappears in further models.

A significant effect of income can be found in all Availability models: The higher the income, the more likely the participants would pay for getting back their files. However, there is no income effect for Confidentiality. People with IT background tend not to pay, although the effect is not significant. We found a positive effect for the clickworker sample (as opposed to students) in the model Avail-1. However, this effect becomes non-significant in Availability models with additional variables. The probability of paying is higher for respondents who had so far no experience with ransomware. This is not surprising, as although 17% of users reported ransomware experience in the past, none of them paid the criminals. This effect is significant only in the Conf-1 and Conf-2 models, though.

Digital Factors Respondents who said that they have a backup tend not to pay compared to those who said that they have partial backup in the Availability condition, but not in the Confidentiality condition. This corresponds to the expectation of the importance of backup to restore from an Availability incident. Also backup quality has this effect: the lower the quality, the more likely a person is to pay. However, this result is not presented here, because only people who have backup could be asked about its quality, which decreases the number of participants in the regression model from 390 to 373.

Users exhibiting higher security behavior intentions (higher RSeBIS score) tend not to pay for the availability of their data in Avail-2. However, this effect disappears in Avail-3 that accounts for the emotions felt in the scenario.

Respondents with a high social media usage are more likely to pay for Availability than those with a lower usage. This might be connected to the latent construct behind the social media usage: the time that the users spend on their digital life, and the quality of data they produce. This effect does not hold for Confidentiality, though, which is surprising, because the users were threatened that the link to their data will be distributed over social media if they refuse to pay.

Psychological Factors The judgment that the described threat is probable for the self has a significant positive effect on paying in all models. Also the belief that the criminals would keep their promise has a significant positive effect. The opinion that paying the offenders is immoral has a strong negative effect on paying. There is also, surprisingly, a negative effect of the perception that the payment is easy in the Availability scenario.

Models Avail-3 and Conf-3 include the extracted factors of the PANAS scale, which represent the emotions felt in the scenario. Frightened respondents are more likely to

pay, whereas Feeling hostile is negatively related to payment. Additionally, for Confidentiality, people who exhibit feelings from the factor "enthusiastic" are opposed to the payment. Overall, experiencing weak negative emotions leads to payment, whereas experiencing strong negative or positive emotions leads to non-payment. These models have the highest explanatory power, as their Pseudo R^2 is the highest among all considered models.

5.3 Factors for the Amount of Non-zero Payments

As explained in Sec. 4.4, we use linear regressions to determine factors influencing the amount of non-zero payment. The dependent variable "payment amount" is log-transformed. Again, we run analysis on several models and compare Availability and Confidentiality scenarios. Here, we only present two models per condition in Table 3: the one with the demographic variables only (PayAvail-1 and PayConf-1), and the one with additional variables (PayAvail-2 and PayConf-2).

Almost the same variables as in logistic regressions in Sec. 5.2 have no significant effect on the amount of payment in either condition: marital status, educational and vocational qualification, usage of the computer by other users, types of files stored, data breach concern, an index of protection measures, rating of files (sensitivity and importance for self and for other people), potential for misuse of the files. Therefore, we again do not include them into the presented models. In contrast to Sec. 5.2, the rating of stored files as having high emotional value, however, has an effect on the amount of payment. Therefore, this factor is included in the models PayAvail-2 and PayConf-2.

Demographic Factors Male participants pay a higher amount for Confidentiality in PayConf-1. This effect disappears in the model PayConf-2 with additional variables. Age is included into the regression models as an important demographic control variable, although it does not have any effect. Income has a strong negative effect in the Confidentiality scenario: In contrast to the group with the lowest income, the group with the second lowest income pays less, and this trend continues for the groups with the higher income. Thus, higher income in general means less payment for Confidentiality, apart from the reference group with the highest income. This trend cannot be observed in the payments for Availability. IT background has a strong negative effect in the Confidentiality scenario as well. Although Clickworker seem to be inclined to pay more for Confidentiality than the student sample, this effect disappears when additional variables are taken into account.

Digital Factors The existence of backup has no effect in Availability scenario anymore, which makes sense: Those who decide to pay in spite of having up-to-date backup will do this for other reasons than not being able to recover their files. This variable is not presented in the models. Higher social media use and storing files with high emotional value lead to higher amount of payment.

	Avail-1	Avail-2	Avail-3	Conf-1	Conf-2	Conf-3
Male	0.270 (1.17)	0.141 (0.53)	0.122 (0.43)	-0.242 (-0.96)	-0.148 (-0.51)	-0.394 (-1.25)
Age	-0.313***	-0.378***	-0.391***	-0.315***	-0.334***	-0.328 ***
	(-4.41)	(-4.53)	(-4.42)	(-3.96)	(-3.72)	(-3.41)
Age^2	0.0031***	0.0039***	0.0042***	0.0030**	0.0032**	0.0032**
	(3.64)	(3.89)	(3.88)	(3.18)	(2.98)	(2.81)
Children: Yes	0.258 (0.75)	0.278 (0.73)	0.339 (0.85)	0.882* (2.18)	0.817+ (1.80)	0.716 (1.49)
Income in EUR						
Less than 500	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.
500 to 1100	0.140 (0.44)	-0.0043 (-0.01)	0.209 (0.56)	0.252 (0.71)	0.170 (0.43)	0.262 (0.63)
1100 to 1700	0.894*	1.192**	1.453**	0.219	0.014	-0.089
	(2.26)	(2.63)	(3.00)	(0.51)	(0.03)	(-0.17)
1700 to 2600	0.667+ (1.66)	0.946* (2.11)	1.175* (2.43)	0.435 (1.00)	0.143 (0.30)	-0.014 (-0.03)
2600 to 5000	0.516 (1.17)	0.955+ (1.88)	1.019+ (1.90)	0.555 (1.10)	0.043 (0.07)	-0.089 (-0.14)
IT background	-0.515+ (-1.83)	-0.481 (-1.48)	-0.528 (-1.54)	-0.430 (-1.52)	-0.587+ (-1.80)	-0.666+ (-1.91)
Clickworker	0.651* (2.25)	0.491 (1.50)	0.401 (1.17)	0.535+ (1.75)	0.649+ (1.89)	0.658+ (1.81)
Ransomware exp.	Ref.	Ref.	Ref.	Ref.	Ref.	Ref.
No ransomware experience	0.585+ (1.91)	0.591 (1.64)	0.430 (1.13)	0.783* (2.29)	0.854* (2.25)	0.774+ (1.90)
Ransomware don't know	-0.177 (-0.22)	-0.168 (-0-20)	-0.172 (-0.20)	0	0	0
Backup: Yes		Ref.	Ref.		Ref	Ref.
Partial		0.740**	0.680*		0.216	-0.122
		(2.81)	(2.44)		(0.80)	(-0.41)
No		0.209 (0.32)	0.121 (0.18)		-1.114+ (-1.69)	-0.827 (-1.21)
RSeBIS		-0.032* (-2.39)	-0.021 (-1.48)		-0.015 (-1.05)	-0.002 (-0.08)
Social media		0.180**	0.160*		0.084	0.049
usage		(2.61)	(2.21)		(1.14)	(0.64)
Personal threat		0.257***	0.185*		0.237**	0.232*
probable		(3.24)	(2.18)		(2.72)	(2.48)
Offenders keep		0.358***	0.310***		0.387***	0.382 ***
their promise		(4.07)	(3.31)		(4.13)	(3.77)
Payment easy		-0.159* (-2.43)	-0.137* (-1.98)		0.072 (1.09)	0.105 (1.50)
Payment		-0.344***	-0.329***		-0.279***	-0.206*
immoral		(-3.67)	(-3.41)		(-3.30)	(-2.24)
Afraid			0.644***			0.434**
			(4.36)			(2.81)
Enthusiastic			-0.127			-0.410**
			(-0.91)			(-2.78)
Interested			0.185 (1.12)			-0.212 (-1.34)
Hostile			-0.336*			-0.487**
			(-2.53)			(-3.02)
Constant	4.974***	7.751***	7.611***	5.047***	5.747**	4.739*
	(4.12)	(4.42)	(4.09)	(3.67)	(3.26)	(2.54)
Observations	390	390	390	351	351	351
Pseudo R^2	0.095	0.243	0.295	0.094	0.225	0.282

Table 2: Logistic regressions in Availablity and Confidentiality scenarios, dependent variable no payment vs. payment; $^{+}p < 0.10,^{*} p < 0.05,^{**} p < 0.01,^{***} p < 0.001$; t statistics in parentheses (in the same line if the significance level in a line is at most *, otherwise in the line below for space reasons)

	PayAvail-1	PayAvail-2	PayConf-1	PayConf-2
Male	-0.220 (-0.88)	-0.441^{+} (-1.83)	0.607* (2.34)	0.252 (0.98)
Age	-0.0096 (-0.67)	-0.0054 (-0.39)	-0.015 (-1.08)	-0.0082 (-0.60)
Income in EUR (Ref. 2600 - 5000)				
Less than 500	0.126 (0.28)	0.452 (1.04)	-1.160* (-2.40)	-0.560 (-1.18)
500 to 1100	-0.179 (-0.39)	-0.021 (-0.05)	-1.675*** (-3.72)	-1.181** (-2.75)
1100 to 1700	0.080 (0.17)	0.382 (0.87)	-1.348** (-2.92)	-0.973* (-2.24)
1700 to 2600	-0.912* (-2.00)	-0.295 (-0.68)	-0.755^{+} (-1.70)	-0.385 (-0.92)
IT background	-0.167 (-0.58)	-0.312 (-1.09)	-1.156*** (-4.02)	-1.044*** (-3.80)
Clickworker	0.073 (0.24)	-0.168 (-0.56)	0.584* (1.99)	0.445 (1.61)
Social media usage		0.144* (2.36)		0.132* (2.18)
Emotional value		0.161* (2.02)		0.172* (2.30)
Payment immoral		-0.222** (-3.00)		-0.271*** (-3.74)
Payment easy		0.020 (0.32)		0.148* (2.50)
Afraid		0.365** (3.04)		0.021 (0.16)
Enthusiastic		0.024 (0.19)		0.033 (0.29)
Interested		-0.258^{+} (-1.84)		-0.203^{+} (-1.69)
Hostile		0.192 (1.53)		-0.0093 (-0.07)
Constant	4.149*** (6.69)	3.438*** (4.11)	5.649*** (9.35)	4.470*** (5.11)
Observations	175	175	138	138
R^2	0.080	0.255	0.231	0.417
Adjusted R^2	0.036	0.180	0.183	0.340

Table 3: Linear regressions in Availablity and Confidentiality scenarios, dependent variable is the log-transformed amount of non-zero payments; $^{+}p < 0.10,^{*}p < 0.05,^{**}p < 0.01,^{***}p < 0.001$; t statistics in parentheses

Emotional Factors Some factors that have significant effect on payment vs. non-payment, do not have significant effect on the amount of payment once the person decided to pay, and are therefore not presented in the models. Thus, the probability of the threat is not important anymore, as well as the perception that the offenders will keep their promise. People who consider paying criminals to be immoral not only decide not to pay with higher probability, but also pay less in case they decided to pay. The ease of payment has a positive effect on the amount of payment in the Confidentiality scenario.

Emotions from the PANAS scale do not have an effect in the Confidentiality scenario. However, in the Availability scenario, people who feel afraid pay more than people who do not experience emotions from this cluster.

Comparing the scenarios, we can see the more important role of income and easiness to pay in the Confidentiality scenario, and the less important role of emotions. There is also a difference in the explanatory power of the models. Although the Confidentiality models

are computed with less observations than the Availability models, the PayConf-2 explains more than one third of the variance in the independent variables ($R^2 = 0.417$, Adjusted $R^2 = 0.340$). This can be considered a quite good explanatory power that the Availability models do not reach.

6 Discussion

In this section, we first discuss our hypotheses and payment factors, and then consider the importance of the scenarios and the limitations of this study.

6.1 Willingness To Pay

We hypothesized that the WTP for Availability will be higher than for Confidentiality, and that the payment amounts will be higher for Availability. The reason for this would be the immediacy of the Availability threat. However, we were not able to support these hypotheses. Although 5% fewer people pay for Confidentiality than for Availability, this difference is not statistically significant. The median WTP for both threats is EUR 50, which corresponds to medians found in related work by Cartwright et al. [9, 7]. Moreover, the payment amounts for Confidentiality are slightly higher than for Availability. This result, although statistically significant, is of low practical value due to small effect size.

Furthermore, although we presented the threats in an immersive scenario, we still received the payment rates comparable to those of Cartwright et al., who just asked the questions on WTP in a plain manner. This shows that the elicitation of hypothetical WTP is difficult, and maybe the hypothetical WTA, as noticed by Cartwright et al. [9, 7], constitutes a more precise measurement for the valuation of the files.

6.2 Payment Factors in Two Stages

We found that factors driving the decision to pay (Table 2) are mostly different from the factors driving the amount of payment once the person decides to pay (Table 3). Thus, whereas age is highly significant for the decision to pay, with younger and older people more inclined to pay than the middle-aged, it does not play a role for the amount of payment. People with higher income are more likely to decide to pay for Availability, but again, the income does not influence the amount of payment for Availability. Also people with partial backup are more likely to decide to pay for Availability than people with full backup, but there is not effect on the amount of payment. Also the trust that criminals would keep their promise positively infleunces the decision to pay in both scenarios, but not the amount.

This result is new in the individual ransomware context, where most studies [9, 7] did not make this distinction, but ran tobit regressions on log(WTP+1). We decided against this approach, because the distribution of log(WTP+1) is not close to the normal distribution, which would be a condition for tobit and for linear regressions. On the other

hand, the distribution of the natural logarithm of the non-zero payments, as depicted in Fig. 6, is visually close to normal distribution, thus providing a better condition for linear regression. In the context of real ransomware attacks in organizations, Meurs et al. [21] also found that the factors differ between the decision to pay and the amount paid.

Furthermore, payment factors also differ for Availability versus for Confidentiality on both stages: the decision to pay and the amount of payment. Thus, higher income is positively related to decision to pay for Availability, but not for Confidentiality. Furthermore, the amount paid for Confidentiality even decreases with higher income, once the person decides to pay. There is no such effect for Availability. Social media use is a positive factor for the decision to pay for Availability, whereas there is no effect for Confidentiality. On the other hand, social media use and storage of files with high emotional value is positively connected to the amount of payment for both threats.

Our most important and novel factor for decision to pay is the emotional state of the victim. Frightened people are inclined to pay, whereas people who feel strong negative emotions do not pay in both scenarios. The regression models for payment vs. non-payment that include emotional factors have the greatest explanatory power for both, availability and confidentiality. The situation becomes different once the person decides to pay. Whereas the amount of payment for Availability is positively connected to feeling afraid, this effect is not present for Confidentiality, and other emotional states do not have an effect in both scenarios.

6.3 Payment Factors in Comparison to Related Work

As our study is the first to elicit WTP for Confidentiality, we cannot compare the latter results to previous work. However, we compare our results for Availability with the results of previous studies on Availability [9, 7, 8]. We could replicate the finding by Cartwright et al. that high social media usage is related to higher WTP for availability. We also corroborate the finding by Cartwright et al. from [8] that those who consider payment immoral have lower WTP rates.

Unfortunately, we were not able to find relation between data breach concern and WTP. Yet, Cartwright et al. found that those who are very concerned or not at all concerned about data breaches have a lower WTP than those who are fairly concerned (inverse u-shaped relation) in [7], whereas they report that higher data breach concern is related to higher payment decision rate in [8]. We also could not corroborate that females and people with children have higher WTP, and that storage of photos makes WTP higher. We were also not able to find an effect of the familiarity with cyber terms.

In Section 2.2, we discussed the importance of market awareness for data ownership in the work by Spiekermann and Korunovska [29], and assumed that in our scenario, the corresponding construct would be the potential for misuse of the files. Unfortunately, we were not able to find a relation between the WTP and the potential for misuse. In our case, the emotional state of the victim and the emotional value of files were more important.

6.4 Importance of Scenario

We find that both, the decision to pay as well as the amount of payment, are highly connected to factors related to the criminality of the scenario. Thus, people who find the payment of criminals immoral, are less willing to pay, and if they decide to pay, their amount of payment is lower. Furthermore, believing that personal threat is probable, and that the offenders will keep their promise, are very strong positive factors in the decision to pay. Overall, this means that the scenario quite likely played an important role in this study. We cannot compare it to a non-criminal scenario, and indeed, found it difficult to imagine a non-criminal scenario for the Confidentiality threat. Nevertheless, to better understand the valuation of Availability versus Confidentiality, a non-criminal scenario would be interesting. We note, however, that most Availability scenarios by Cartwright et al. [9, 7] consider a benign scenario for WTP, where the access to files was accidentally lost. If they consider a criminal scenario, they usually ask how willing the users will be to pay a fixed amount [8]. Thus, the issue of scenario requires further investigation.

6.5 Limitations

Although we designed our study with the utmost care, it has several limitations. Our sample is non-representative of the German population, over-representing females, younger people, students and academics. Moreover, 24% of the sample reported a professional IT background, which is too high for the general population. Furthermore, the clickworker sample was compensated, whereas the university sample was not. We explain the reason for this decision and possible consequences in detail in Section 4.3.

We also had a relatively low number of participants, despite the high recruitment effort, which makes our regression results fragile. For example, we removed all persons who provided no answer in the demographic data. If we took these persons into account, some of the regression factors that are not significant in the presented analyses would become significant at the $p < 0.05$ level, as we found out in the preliminary analysis. Nevertheless, because of the fragility of such results, we decided not to chase them.

We elicited WTP using an online hypothetical scenario, and thus, WTP stated in the scenario is likely to differ from the WTP in the real situation. We note, however, that there is no ethical possibility to conduct an experiment with a real ransomware attack. To complement our approach, one could look up real cases of individual ransomware reported to the police or to recovery companies, as Meurs et al. [22, 21] did for ransomware in organizations. In these real cases, however, some important variables will be missing, especially the emotional state, as also Meurs et al. observe in their studies.

7 Conclusion

In this work, we present the first comparative evaluation of Willingness To Pay (WTP) for Availability versus for Confidentiality and factors driving it. We find that different factors influence the decision to pay and the amount of payment once the person decided to pay. Moreover, these factors are different for Availability and Confidentiality. At the same time, the amount of payment does not differ much between conditions: the median of payment is 50 EUR for both, Availability and Confidentiality. Future work could consider different settings and cultural backgrounds, and also investigate the WTP-WTA gap. Most interesting would be to consider our research question without the co-influence of the criminal scenario.

References

[1] Alessandro Acquisti, Leslie K John, and George Loewenstein. What is privacy worth? *The Journal of Legal Studies*, 42(2):249–274, 2013.

[2] Algirdas Avizienis, J-C Laprie, Brian Randell, and Carl Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE transactions on dependable and secure computing*, 1(1):11–33, 2004.

[3] Christine Bauer, Jana Korunovska, and Sarah Spiekermann. On the value of information - what facebook users are willing to pay. In Ming-Hui Haung, Gabe Piccoli, and Vallabh Sambamurthy, editors, *European Conference on Information Systems (ECIS 2012)*. AIS Electronic Library, December 2012.

[4] B. Breyer and M. Bluemke. Deutsche version der positive and negative affect schedule PANAS (gesis panel). Technical report, Leibniz Institut für Sozialwissenschaften (GESIS), 2016.

[5] Carbon Black. Ransom-Aware, 2017.

[6] Juan Pablo Carrascal, Christopher Riederer, Vijay Erramilli, Mauro Cherubini, and Rodrigo De Oliveira. Your browsing behavior for a big mac: Economics of personal information online. In *Proceedings of the 22nd international conference on World Wide Web*, pages 189–200, 2013.

[7] Anna Cartwright, Edward Cartwright, and Lian Xue. The value of data: Estimating the value individuals put on access to their computer files. In *WEIS*, 2021.

[8] Anna Cartwright, Edward Cartwright, Lian Xue, and Julio Hernandez-Castro. An investigation of individual willingness to pay ransomware. *Journal of Financial Crime*, (ahead-of-print), 2022.

[9] Edward Cartwright, Anna Cartwright, and Lian Xue. Estimating the value of computer files using willingness to pay and willingness to accept. *Available at SSRN 3544951*, 2020.

[10] CISA, FBI, NSA and International Partners. Joint cybersecurity advisory: 2021 trends show increased globalized threat of ransomware, 2021.

[11] German Federal Office of Criminal Investigation. Cybercrime 2021 (in german), 2021. Last access: 2022-09-09.

[12] Jens Grossklags and Alessandro Acquisti. When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information. In *WEIS*, 2007.

[13] Lee Hadlington. Exploring the psychological mechanisms used in ransomware splash screens. De Montfort University, Contract research for SentinelOne, 2007.

[14] J Hernandez-Castro, A Cartwright, and Edward Cartwright. An economic analysis of ransomware and its welfare consequences. *Royal Society open science*, 7(3):190023, 2020.

[15] Julio Hernandez-Castro, Edward Cartwright, and Anna Stepanova. Economic analysis of ransomware. Technical report, University of Kent, 2017.

[16] Internet Crime Complaint Center (IC3). 2023 Internet Crime Report, 2023.

[17] Limor Kessem. Ransomware: How consumers and businesses value their data. IBM X-Force Research, 2016.

[18] Marc Langheinrich. Privacy in ubiquitous computing. In *Ubiquitous computing fundamentals*, pages 109–174. Chapman and Hall/CRC, 2018.

[19] Jamie MacColl, Pia Hüsch, Gareth Mott, James Sullivan, Jason RC Nurse, Sarah Turner, and Nandita Pattnaik. Ransomware: Victim insights on harms to individuals, organisations and society. 2024.

[20] Malwarebytes. Demographics of Cybercrime Report, 2021. Last access: 2022-09-09.

[21] Tom Meurs, Edward Cartwright, Anna Cartwright, Marianne Junger, Raphael Hoheisel, Erik Tews, and Abhishta Abhishta. Ransomware economics: A two-step approach to model ransom paid. In *APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 2023.

[22] Tom Meurs, Marianne Junger, Erik Tews, and Abhishta Abhishta. Ransomware: How attacker's effort, victim characteristics and context influence ransom requested, payment and financial loss. In *APWG Symposium on Electronic Crime Research (eCrime)*, pages 1–13. IEEE, 2022.

[23] Philipp Morgner, Christoph Mai, Nicole Koschate-Fischer, Felix Freiling, and Zinaida Benenson. Security update labels: establishing economic incentives for security patching of iot consumer products. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 429–446. IEEE, 2020.

[24] Anna-Marie Ortloff, Maike Vossen, and Christian Tiefenau. Replicating a study of ransomware in germany. In *European Symposium on Usable Security 2021*, pages 151–164, 2021.

[25] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. Self-confidence trumps knowledge: A cross-cultural study of security behavior. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 2202–2214. ACM, 2017.

[26] Camelia Simoiu, Joseph Bonneau, Christopher Gates, and Sharad Goel. "i was told to buy a software or lose my computer. i ignored it": A study of ransomware. In *Fifteenth symposium on usable privacy and security (SOUPS 2019)*, pages 155–174, 2019.

[27] H Jeff Smith, Tamara Dinev, and Heng Xu. Information privacy research: an interdisciplinary review. *MIS quarterly*, pages 989–1015, 2011.

[28] Sophos. The State of Consumer Home Cybersecurity 2021, 2021. Last access: 2022-09-09.

[29] Sarah Spiekermann and Jana Korunovska. Towards a value theory for personal data. *Journal of Information Technology*, 32(1):62–84, 2017.

[30] Sarah Spiekermann, Jana Korunovska, and Christine Bauer. Psychology of ownership and asset defense: Why people value their personal information beyond privacy. In Ming-Hui Haung, Gabe Piccoli, and Vallabh Sambamurthy, editors, *International Conference on Information Systems (ICIS 2012)*. AIS Electronic Library, December 2012.

[31] Janice Y Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. The effect of online privacy information on purchasing behavior: An experimental study. *Information systems research*, 22(2):254–268, 2011.

[32] Amina Wagner, Nora Wessels, Peter Buxmann, and Hanna Krasnova. Putting a price tag on personal information-a literature review. In *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018.

[33] David Watson, Lee Anna Clark, and Auke Tellegen. Development and validation of brief measures of positive and negative affect: the PANAS scales. *Journal of personality and social psychology*, 54(6):1063, 1988.

[34] Angela G Winegar and Cass R Sunstein. How much is data privacy worth? a preliminary investigation. *Journal of Consumer Policy*, 42(3):425–440, 2019.

[35] Adam Young and Moti Yung. Cryptovirology: Extortion-based security threats and countermeasures. In *Security and privacy, 1996. Proceedings., 1996 IEEE Symposium on*, pages 129–140, 1996.

[36] Adam L. Young and Moti Yung. Cryptovirology: The birth, neglect, and explosion of ransomware. *Communications of the ACM*, 60(7):24–26, 2017.

A Real Ransomware Notes

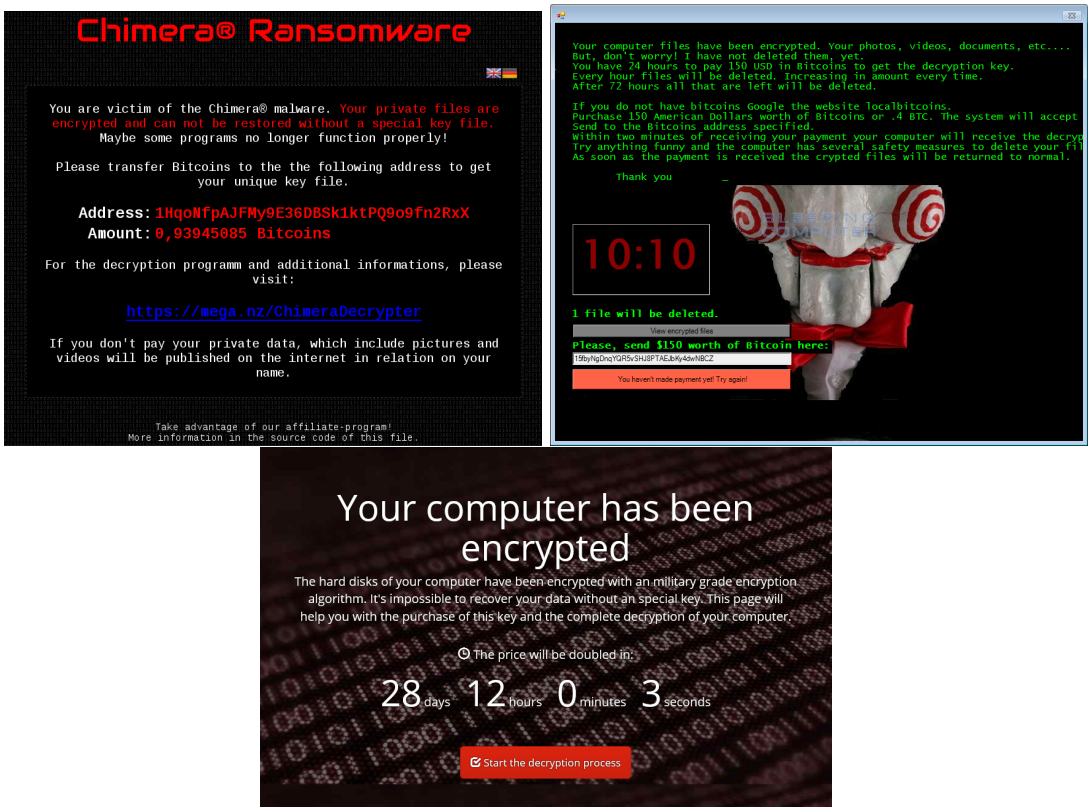

Figure 7: Ransom notes of the ransomware Chimera (to the left, includes a confidentiality threat at the bottom) and Jigsaw (to the right); darknet website of the Petya ransomware, personalized for each victim (at the bottom)

Ransom notes of Chimera, Jigsaw and Petya ransomware that were used to develop the ransom notes in our scenarios, are presented in Fig. 7.

B The survey

The survey was administered in German, and was translated into English for the publication purpose. Choice variants of some questions are presented in one line using "/" as delimiter for brevity.

B.1 Introductory Questions

- I hereby agree to participate in this survey. The goal of the survey is to collect data on private computer use. For further evaluation of the collected data, all information collected will be anonymized. (Yes/No)
- Do you use a computer (desktop computer or laptop) for private purposes? Mobile phones, smartphones and tablets do not count as computers.
  - Yes, I use one computer / Yes, I use multiple computers / No
- *(If only one computer used)* In the following, please refer to this computer.
- *(If multiple computers used)* In the following, please refer to the computer you are using the most.
- *(If no computer is used for private purposes, the survey ends)*
- What kind of computer do you have?
  - A desktop computer / A laptop that is not used outside the house / A laptop that is also used outside the house
- Please specify your operating system. If you have several operating systems on your computer, please select the one you use most frequently.
  - Windows / Mac / Linux / Don't know / Other: [text field]
- Click on '6' to indicate that you are reading this survey carefully. *(Attention test with possibilities to click 1, ..., 7)*

B.2 Priming before the Scenario

B.2.1 Computer Usage

- How often do you use your computer for private purposes?
  - Several times a day / Daily / Weekly / Monthly / Less Frequently
- What data is stored on your computer?

  - Private photos or videos
  - Music
  - Emails and email addresses
  - Health-related documents
  - Calender
  - Movies
  - Software that was purchased (Microsoft Office, games, ...)
  - Data on the Internet usage (visited websites, favorites, ...)
  - Passwords and access data
  - Work-related documents
  - Financial data and legal documents (contracts, insurances, tax documents, ...)
  - School/training/study materials
  - Personal notes (journal, ...)
  - Customer data (professional)
  - Other: [text field]

- Do other people besides yourself use your computer? Other people could be colleagues, friends or family. (Yes/No)

- *(If "Yes")* Please specify which people are using your computer.

  - Partner / Family members / Private contacts (friends, neighbours, ...) / Professional contacts (colleagues, customers, ...) / Other [text field]

- Are there any files on your computer that might be important to other people?

  - Yes / No / I don't know

- *(If "Yes")* For which persons could your files be important?

  - Partner / Family members / Private contacts (friends, neighbours, ...) / Professional contacts (colleagues, customers, ...) / Other [text field]

B.2.2 Backup Measures and Quality

- Do you have backup copies of your files? Backup copies can be copies of files on a USB flash drive, copies in the cloud, or on a hard drive.

  - Yes / Partially / No / Don't know

- Please indicate all backup measures you take and how often you do so.

  - Measure
    * additional data carrier (hard disk, usb-stick, RAID, DVD, ...)
    * Internet (Dropbox, GoogleDrive, Email to myself, iCloud, ...)
    * Own backup servery (NAS, Apple Time Capsule, ...)
    * Copies of the files on different PCs
  - What is secured? *(chosen for each of the above backup measures)*
    * Selected files / All user files / Complete system / Nothing
  - How often do you do this backup? *(chosen for each of the above backup measures)*
    * Permanently (on every change) / Daily or more often / Weekly or several times a week / Monthly or several times a month / Annually or less frequently / As needed (irregularly) / Never

- Do you perform any other backup of your files? If so, what do you back up? On which medium do you back up and how often? *open-ended*

- Please indicate to what extent you agree or disagree with the following statements: *(1= strongly disagree, 7= strongly agree)*

  - I have backup copies of all my important files.
  - My backup procedures work reliably.
  - I am sure that I can recover my important files if necessary.
  - I am sure that I can recover my important files with little effort if necessary.
  - My backup copies are up-to-date.

B.2.3 Importance and Sensitivity of Files

- Please indicate to what extent you agree or disagree with the following statements: *(1= strongly disagree, 7= strongly agree, randomized order)*

  - Many files on my computer are out of date. I consider them to be obsolete.
  - Some files on my computer are very useful. They should not be deleted.
  - Some files on my computer are important to me. I have to be able to access them at any time.
  - Some files on my computer are sensitive. They should not be disclosed to the public.
  - Many files on my computer are worthless to me. I do not need them anymore.
  - Some files on my computer are of high emotional value to me. I would be very upset if I lost them.

B.2.4 Potential for Misuse

- Please indicate to what extent you agree or disagree with the following statements. Other persons could be known (e.g. colleagues, friends, family) or unknown persons (e.g. criminals, curious third parties): *(1= strongly disagree, 7= strongly agree, randomized order)*
  - I think that other people might have an interest in my files.
  - I think that other people could abuse my data to obtain a financial benefit from my files.
  - I think that it could have negative consequences for me if other people had access to my files.
- Click on '4' to indicate that you are reading this survey carefully. *(Attention test with possibilities to click 1, ..., 7)*

B.3 Availability Scenario

- Please imagine: This message would appear on your computer. Please read all information in the following picture carefully.

  (First ransom note for Availability is shown, 72h left for making payment, see Fig. 2)

  The above message cannot be clicked away. You realize that the threat is real and that you cannot get rid of the program or the message. Your computer cannot currently be used as usual. The only way to make your computer usable again is to reset your computer completely. This will result in the loss of all files that were stored on the computer.

  What would you do in this situation? (*open-ended, asked for the purpose of making sure that the participants understand that the threat cannot be removed when the ransom note is shown for the second time, see below*)
- *(Quiz for the Availability scenario)* In the following we will test your understanding of the scenario by a quiz. If you answer a question incorrectly, the scenario and the correct answer will be explained to you. Decide which of the following statements apply to the scenario just described and which do not apply. *(True / False)*
  - In the scenario my files were encrypted. *(True)*
    - *(If the answer is "False")* Your answer is incorrect. Your files were encrypted and you cannot access them anymore.
  - In the scenario other people have access to my files. *(False)*
    - *(If the answer is "True")* Your answer is incorrect. Other people do not have access to your files.

  - In the scenario I cannot use my computer as usual and cannot access my files. *(True)*
    * *(If the answer is "False")* Your answer is incorrect. Your computer cannot be used anymore and you don't have access to your files. The only way to make your computer usable again is to reset your computer completely. This will result in the loss of all files that were stored on the computer.
  - Refusing to pay in the scenario will result in the permanent loss of my files, unless I have backup copies. *(True)*
    * *(If the answer is "False")* Your answer is incorrect. Not paying will result in the permanent loss of your files, if you don't have backup.
  - In the scenario my files were copied to a server on the Internet. *(False)*
    * *(If the answer is "True")* Your answer is incorrect. The files on your computer were encrypted, such that you cannot access them anymore. They were not copied to a server.

- *(Second ransom note for the Availability scenario is shown, 15 min left for making payment, see Fig. 8)* Please imagine: Any attempts to get rid of the program and the message did not work and you have less than 15 minutes left to pay. The files on your computer are encrypted and therefore you are no longer able to use it as usual. The payment is quick and easy to complete. What is the maximum amount you are willing to pay?

- Why did you choose this amount? Please justify your decision.

B.4 Confidentiality Scenario

- Please imagine: This message would appear on your computer. Please read all information in the following picture carefully.

  (First ransom note for Confidentiality is shown, 72h left for making payment, see Fig. 3)

  The above message cannot be clicked away. You realize that the threat is real and that you cannot get rid of the program or the message. Your computer can still be used as usual.

  What would you do in this situation? (*open-ended, asked for the purpose of making sure that the participants understand that the threat cannot be removed when the ransom note is shown for the second time, see below*)

- *(Quiz for the Confidentiality scenario)* In the following we will test your understanding of the scenario by a quiz. If you answer a question incorrectly, the scenario and

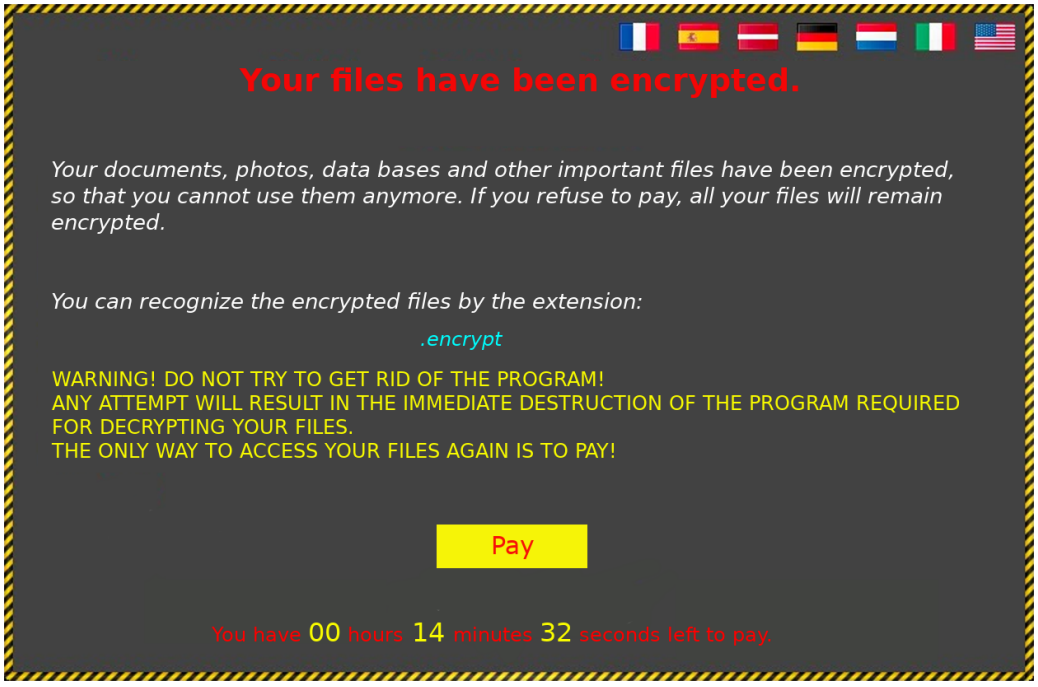

Figure 8: Second ransom note for the Availability scenario is shown, 15 min left for making payment

the correct answer will be explained to you. Decide which of the following statements apply to the scenario just described and which do not apply.

- In the scenario my files were copied to a server on the Internet. *(True)*
  - *(If the answer is "False")* Your answer is incorrect. Your files were copied to a server on the Internet. They can be accessed over a link. Currently only you and the extortioner has access to this link.
- In the scenario, my files were encrypted. *(False)*
  - *(If the answer is "True")* Your answer is incorrect. Your files were not encrypted, and you have full access to them.
- In the scenario, I can no longer use my computer as usual and can no longer access my files. *(False)*
  - *(If the answer is "True")* Your answer is incorrect. You can use your computer as usual and have full access to your files.
- Refusing to pay in the scenario will result in my contacts and strangers gaining access to my files. *(True)*

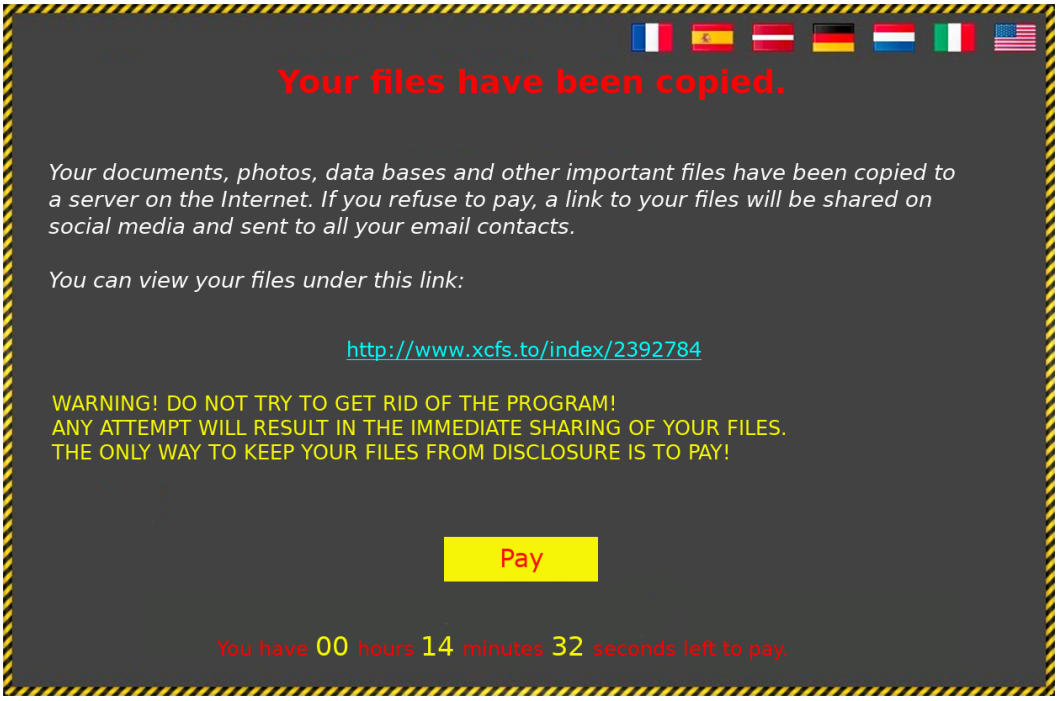

Figure 9: Second ransom note for the Confidentiality scenario is shown, 15 min left for making payment

  - ∗ *(If the answer is "False")* Your answer is incorrect. Refusing to pay will result in your contacts and strangers getting access to your files.
- – In the scenario other people have access to my files. *(True)*
  - ∗ *(If the answer is "False")* Your answer is incorrect. Currently you and the extortioners (that is, other people) have access to your files.

- *(Second ransom note for the Confidentiality scenario is shown, 15 min left for making payment, see Fig. 9)*

  Please imagine: Any attempts to get rid of the program and the message did not work and you have less than 15 minutes left to pay. The files on your computer are available and usable. The payment is quick and easy to complete. What is the maximum amount you are willing to pay?

- Why did you choose this amount? Please justify your decision.

B.5 After the Scenario

B.5.1 Emotions

- *(PANAS scale [33, 4] shown in randomized order; rated from 1= not at all to 5 = extremely)*

  Please state how you felt in the scenario. The following words describe different feelings and sensations. Read each word and then enter the intensity on the scale next to each word:

  distressed; upset; guilty; scared; ashamed; nervous; jittery; afraid; excited; proud; strong; enthusiastic; active; interested; inspired; alert; attentive; irritable; hostile; determined

B.5.2 Comprehension Test

Decide which of the following statements apply to the scenario described and which do not apply. *(True / False / Don't know, items shown in randomized order)*

- In the scenario you dropped your computer and it broke. *(False for both scenarios)*
- In the scenario you no longer had access to your files. *(True for Availability, false for Confidentiality)*
- In the scenario your files were encrypted. *(True for Availability, false for Confidentiality)*
- In the scenario your computer was no longer usable as usual. *(True for Availability, false for Confidentiality)*
- In the scenario your files were copied to a server on the Internet. *(True for Confidentiality, false for Availability)*
- In the scenario you received a link to a copy of your files. *(True for Confidentiality, false for Availability)*
- In the scenario you were threatened with a disclosure of your files. *(True for Confidentiality, false for Availability)*

B.5.3 Reality of the Scenario

- Please indicate to what extent you agree or disagree with the following statements: *(1= strongly disagree; 7 = strongly agree, shown in randomized order)*

  – I think the criminals will keep their promise if I pay.

- I consider the threat described to be likely to happen to me personally.
- I consider it immoral to pay the perpetrators money.
- I imagine the payment to be easy.
- I consider the threat described to be likely to happen in general.
- I think there might be a real threat similar to the scenario.

B.5.4 Ransomware Experience

- Have you ever been a victim of ransomware? Ransomware is software that confronts you (as in the scenario) with a certain threat and demands a ransom to resolve this threat.
  - Yes / No / Don't know
- *(If "Yes")* How long ago did your experience with ransomware take place? Please refer to your last experience with ransomware in the following.
  - Less than one year ago / Less than three years ago / Less than five years ago / 5 years ago or more / Don't know
- Did you pay to resolve the threat?
  - No / Don't remember. / Yes, I paid but I don't remember how much. / Yes, I paid about (in EUR): [text field]
- Has anyone helped you? *(multiple-choice)*
  - No / Don't remember. / Yes, relatives or friends / Yes, an expert / Other: [text field]
- What were the consequences of the incident? *(multiple-choice)*
  - I lost files. / I lost programs. / I bought a new device. / No consequences. / Don't know. / Other: [text field]

B.6 Security Concerns, Awareness and Behavior

- Do you take the following protective measures? *(Yes / No / Don't know)*
  - Antivirus / Firewall / Screen lock with password protection / Hard disk encryption
- *Refined Security Behavior Intentions Scale (RSeBIS) [25]*

- *Questions by Cartwright et al. [9], slightly adapted to German users (e.g., the usage of Xing is elicited, which is a German equivalent to LinkedIn)*
  - For the following question, by "data breach", we mean any occasion where sensitive, protected, or confidential data (e.g. personal identifying information, health records, credit card data) is compromised. This means that it may have been viewed, stolen, or used by someone who is not authorized to do so (e.g. someone outside of the company entrusted with the data). Overall how concerned, if at all, are you that your personal information may be subject to a data breach?
    * Very concerned / Fairly concerned / Not very concerned / Not concerned at all
  - Before taking this survey which, if any, of the following terms / phrases had you heard of?
    * Ransomware / Sexting / Crypto-currency / Online identity theft / WannaCry / CryptoLocker / Bitcoin / Cyber-bullying / Doxing (also known as Doxxing) / None of these
  - Have you used the following services within the last month:
    * Facebook / Twitter / LinkedIn / Xing / Google+ / Pinterest / Instagram / Facebook Messenger / WhatsApp / Skype / None of these

B.7 Feedback and Demographics

- Please give us honest feedback on the completion of this survey by answering the following questions. The feedback will not affect your compensation.
  - *(Yes / No)*
    * Were you distracted during the survey completion? (e.g. by TV, other people, ...)
    * Are there any reasons why your answers should not be used?
    * Did you take the task of determining the maximum amount you would pay in the scenario seriously?
  - *(rated from 1 = strongly disagree to 7 = strongly agree)*
    * I have answered the questions carefully.
    * I understood all the questions.
    * I was able to put myself into the scenario very well.
    * I could very well imagine how I would have felt in the scenario.
- Please enter your year of birth

  - 2004 / ... / 1918 / Not specified

- Please indicate your sex
  - Female / Male / Diverse / Not specified
- Please select your current occupation
  - Employee or civil servant / Self-employed / Pupil / Trainee / Student / Unemployed / Homemaker or on parental leave / Retired / Not specified / Other: [text field]
- What best describes your marital status?
  - Married or civil union / Living together but not married / Separated or divorced / Widowed / Single / Not specified
- Do you have children?
  - Yes / No / Not specified
- Please select your highest educational level:
  - Attending a school
  - No school certificate
  - Completion of secondary modern school
  - Secondary school certificate
  - Higher education entrance qualification (A-levels)
  - Not specified
  - Others: [text field]
- Please select your highest professional qualification:
  - No completed vocational qualification
  - Apprenticeship/vocational training
  - Professional qualification
  - Bachelor's degree
  - Master's degree, diploma, state examination, magister
  - PhD, doctoral degree
  - Not specified
  - Other: [text field]

- Are you working in computer science or a related field (work or studies):
  - Yes / No / Not specified
- For the evaluation of the results (in the scenario with the ransomware) your monthly net income is required. Please privide your monthly net income in EUR (approximately):
- Thank you very much for your participation! Is there anything else you would like to tell us? *(free text)*

C PANAS Analysis

We conduct a principal-component factor analysis with orthogonal Varimax rotation to check how many different factors are included and to aggregate the items to uncorrelated new variables. Four factors could be found. We summarize Factor 1 as "afraid" (the item with the highest factor loading), Factor 2 as "enthusiastic", Factor 3 as "interested" and Factor 4 as "hostile". Cronbach's alpha values are 0.89, 0.76, 0.70 and 0.59 (see Table 4).

Variable	Factor loading	Factor names	Cronbach's alpha
distressed	0,7474	Factor 1	0.89
upset	0,5818	afraid	
guilty	0,5766		
scared	0,7694		
ashamed	0,6883		
nervous	0,8316		
jittery	0,8108		
afraid	0,8502		
excited	0,7979	Factor 2	0.76
proud	0,705	enthusiastic	
strong	0,5014		
enthusiastic	0,8063		
active	0,6976	Factor 3	0.70
interested	0,754	interested	
inspired	0,4113		
alert	0,6891		
attentive	0,7077		
irritable	0,5729	Factor 4	0.59
hostile	0,7001	hostile	
determined	0,5585		

Table 4: Principal-component factor analysis of the PANAS scale