Master Thesis

Stories of Cybervictims

“Exploration of Cyber Victimology through Victims’ Narrations to Design for Digital Resilience”

Siegen 27.02.2020

First Corrector: Prof. Dr. Gunnar Stevens
Second Corrector: Univ.- Prof. Volker Wulf

Surname, name: Alizadeh, Fatemeh
Address: 
Tel.Nr.: 
E-Mail: Fatemeh.alizadeh@student.uni-siegen.de
Matr.-Nr.: 
Term:
Executive Summary

Within the framework of this master thesis, we applied the episodic narrative interview approach to conducting interviews with 14 individuals who experienced cybercrime victimization recently. Our goal was to provide a deeper insight into understanding cyber victims and their coping strategies for moving from prevention techniques towards digital resilience. Therefore, we used victims’ narration to separate and analyze their experiences of cyber victimization in three sequential episodes namely before, during and after the incident.

By using a three-stage thematic analysis and based on the grounded theory, we proposed a new victimization theory to move beyond victims’ blaming and acknowledge the role of skilled offenders and highly complex social engineering techniques. According to our denial theory, a certain amount of delay between when the victim perceives the first clue and when they perceive the crime, in which victims take a passive role depends on the ambiguity of the clues for the victim and the frequency of receiving them. Therefore, cyber victims are normal technology users who were affected by a specific crime tailored to them. By addressing and categorizing cyber victims’ coping strategies, we suggest low costs risk exposures to vaccinate the society against cyber victimization and build resilience rather than unrealistic trials to prevent cybercrime through digital bulletproof vests, which do not exist.

In the future, we to apply more participatory techniques in which cyber victims can take a more active role and contribute to discovering new design-based implications and opportunities.
# Table of Contents

Table of Figures .................................................................................................................. VI

Table Of Tables ................................................................................................................. VII

Table Of Annexes ............................................................................................................... VIII

1 Introduction ...................................................................................................................... 5

2 Background & Related Work ............................................................................................ 8
   2.1 Victimology & Cyber victimology .............................................................................. 8
   2.2 Victims’ Precipitation & Typologies ......................................................................... 9
      2.2.1 Lifestyle Exposure Theory ............................................................................... 11
      2.2.2 Routine Activities Theory .............................................................................. 12
      2.2.3 Low Self-control Theory ............................................................................... 12
      2.2.4 Big five Personality Traits Model .................................................................... 12
      2.2.5 Space Transition Theory ............................................................................... 13
      2.2.6 Why victim blaming happens? ......................................................................... 14

3 State of the Art ................................................................................................................... 15
   3.1 Fraud ....................................................................................................................... 15
   3.2 Identity theft ........................................................................................................... 17
   3.3 Hacking .................................................................................................................. 18
   3.4 Phishing ................................................................................................................ 18
   3.5 Malware Attack ..................................................................................................... 19
   3.6 Victim-centered research and design .................................................................... 20
   3.7 Digital security and digital resilience ................................................................... 2

4. Methodology ..................................................................................................................... 22
   4.1 Research method .................................................................................................... 22
   4.2 Scope of investigation ............................................................................................ 25
### 5. Results

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 First story of the victims: Tell me what happened</td>
<td>28</td>
</tr>
<tr>
<td>5.1.1 Cyber fraud</td>
<td>28</td>
</tr>
<tr>
<td>5.1.2 Identity Theft</td>
<td>3</td>
</tr>
<tr>
<td>5.1.3 Hacking</td>
<td>39</td>
</tr>
<tr>
<td>5.1.4 Phishing</td>
<td>42</td>
</tr>
<tr>
<td>5.1.5 Malware attack</td>
<td>43</td>
</tr>
<tr>
<td>5.2 Before the Incident</td>
<td>44</td>
</tr>
<tr>
<td>5.2.1 Victims’ Profession, Knowledge &amp; Online behaviour</td>
<td>44</td>
</tr>
<tr>
<td>5.2.2 Exploited vulnerability</td>
<td>48</td>
</tr>
<tr>
<td>5.2.3 Are victims’ past experiences related?</td>
<td>50</td>
</tr>
<tr>
<td>5.3 Denial Phase: Not Accepting yourself as a victim of cybercrime</td>
<td>51</td>
</tr>
<tr>
<td>5.3.1 How denying starts?</td>
<td>52</td>
</tr>
<tr>
<td>5.3.2 Why denying continues?</td>
<td>54</td>
</tr>
<tr>
<td>5.3.3 How denying ends?</td>
<td>56</td>
</tr>
<tr>
<td>5.3.4 What are the consequences?</td>
<td>58</td>
</tr>
<tr>
<td>5.3.5 The theory of denial</td>
<td>60</td>
</tr>
<tr>
<td>5.4 During the incident</td>
<td>60</td>
</tr>
<tr>
<td>5.4.1 Victims’ action</td>
<td>60</td>
</tr>
<tr>
<td>5.4.2 Support</td>
<td>64</td>
</tr>
<tr>
<td>5.4.3 Emotional Analysis</td>
<td>67</td>
</tr>
<tr>
<td>5.4.4 Victims’ Assumptions: Did victims know what went wrong?</td>
<td>69</td>
</tr>
<tr>
<td>5.4.5 Victims’ Expectations</td>
<td>72</td>
</tr>
<tr>
<td>5.5 After the Incident</td>
<td>73</td>
</tr>
<tr>
<td>5.5.1 Long-lasting Effects: What remains with the victims?</td>
<td>74</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>5.5.2 Online behavioral changes</td>
<td>80</td>
</tr>
<tr>
<td>5.5.3 Costs</td>
<td>83</td>
</tr>
<tr>
<td>5.5.4 Regrets</td>
<td>83</td>
</tr>
<tr>
<td>5.6 Support suggestions: Do victims really want to have a passive role in the cycle?</td>
<td>84</td>
</tr>
<tr>
<td>5.7 Coping strategies: Damage control &amp; recovery</td>
<td>89</td>
</tr>
<tr>
<td>5.7.1 Draw positive results from the negative experience</td>
<td>89</td>
</tr>
<tr>
<td>5.7.2 Denying the costs</td>
<td>90</td>
</tr>
<tr>
<td>5.7.3 Commonality</td>
<td>91</td>
</tr>
<tr>
<td>5.7.4 Humor</td>
<td>91</td>
</tr>
<tr>
<td>5.7.5 Social recognition</td>
<td>92</td>
</tr>
<tr>
<td>5.7.6 Deliberate confrontation</td>
<td>92</td>
</tr>
<tr>
<td>5.8 Blaming &amp; Shaming: Who is responsible of a crime?</td>
<td>93</td>
</tr>
<tr>
<td>6. Discussion &amp; Conclusion</td>
<td>96</td>
</tr>
<tr>
<td>6.1 Victim, survivor or normal users?</td>
<td>96</td>
</tr>
<tr>
<td>6.2 Why victims’ stories matter? Reflection on our method regarding the research question</td>
<td>97</td>
</tr>
<tr>
<td>6.3 Towards designing for digital resilience</td>
<td>98</td>
</tr>
<tr>
<td>6.4 Limitations and future work</td>
<td>98</td>
</tr>
<tr>
<td>References</td>
<td>00</td>
</tr>
<tr>
<td>Confirmation</td>
<td>106</td>
</tr>
<tr>
<td>Appendix</td>
<td>107</td>
</tr>
</tbody>
</table>
Table of Figures

Figure 1: Comparison of victims' categorization based on the level of responsibilities ..................10
Figure 2: The big five personality traits .........................................................................................13
Figure 3: Change in victims’ behavior as a result of the fraud .........................................................16
Figure 4: Characteristics of potential phishing victims .................................................................... 9
Figure 5: The nested approach to an episodic narrative interview and its process .................. 23
Figure 6: Warning of the eBay for the bidders .................................................................................. 29
Figure 7: Landing page of the wish, to be able to see the prices users need to log in .................. 36
Figure 8: Facebook bot for the case of hacking .................................................................................. 37
Figure 9: GitHub repository, settings and features .......................................................................... 41
Table of Tables

Table 1: Participants’ demographic information and characteristics of cases ........................................ 24
Table 2: Victims’ background: before the incident ................................................................................. 45
Table 3: Previous offline and online experiences of the victims ............................................................ 51
Table 4: Victims’ reaction during the incident ....................................................................................... 60
Table 5: Victims consequences after the incident ................................................................................ 73
Table 6: Communication of the victims ............................................................................................... 93
Table Of Annexes

Appendix 1: Consent from .......................................................... 107

Appendix 2: Interview guideline ................................................... 108
1 Introduction

With the advent of “cyberspace” and the growth of internet domination in every aspect of our lives, a huge risk of cybercrime occurrence affects every internet user [21]. In 2017, the German digital ICT industry association bitkom found that every second German internet user had become a victim of cybercrime during the 12 months before the survey and every second case involved a financial loss [8]. As shutting down cyber systems in an open developed nation for the fear of definite threats is not an option in today’s world, to mitigate with cybercrime and maintain open and yet secure cyberspace, a national user resilience is needed [96]. However, to date, cyber safety strategies are focused on protective measures and minimizing the users’ exposure risk to cyber threats and privacy breaches instead [98]. Given that even with the best security strategies we are all bound to get hit sooner or later [122], a shift in this emphasis to strategies promoting digital literacy and cyber resilience is demanded [98]. To investigate digital resilience, as the ability to deal with negative online experiences and recover from inevitable digital attacks, and consider it in the user experience design process, an in-depth exploration of the current victims’ mitigation techniques and their needs for further adaptions is needed [122].

Previous researchers have argued a lack of a universally accepted definition of cybercrime [21, 38, 103]. Gercke started by discussing to dimensions of cybercrime, in a broader sense (computer-related crimes) covers any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network and in a narrow sense (computer crime) covers any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them. [100]. However, the European Commission describes cybercrime as:

“Criminal acts that are committed online by using electronic communications networks and information systems [22].”

And divides it into 3 main categories, including:

1. Crimes specific to the Internet, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts).
2. Online fraud and forgery. Large-scale fraud can be committed online through instruments such as identity theft, phishing, spam, and malicious code.
3. Illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism, and xenophobia [22].”
As Halder and Jainshakar discussed [62], these categories suggest an evolved definition of cybercrime from a machine-centered phenomenon to human-related experience. An adaptation of this definition to the new millennium as he introduces is as follows:

“Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim to cause physical or mental harm to the victim directly or indirectly, using modern telecommunication technologies [21].”

The recent shift of cybercrime definition to the victimization perspective reveals the important role of users’ experience in the field of cybersecurity [62]. Additionally, the rules governing cyberspace are different from those of the real world, therefore the consequences of the victimization in cyberspace evoke different responses depending on victims’ characteristics, characteristics of the incident and the past-victimization experience [118]. Moreover, previous studies have claimed that adults in the age group (18-64) are the least researched target group in terms of cybervictimizations [98]. Given the inevitable risk of cybervictimation more in-depth research in this regard is urgently needed.

The Lack of a universal understanding of cybercrime and therefore cyber victimization makes the decision whether the unlucky users should be regarded as cybercrime victims remain to a huge extent a matter of their own perception and interpretation of the negative experience. Given the limited available research concerning cybervictimization especially with regard to digital immigrants [74], an investigation of the adult victims’ perspective and the role of their experiences in building resilience seems to be necessary. To contribute to this investigation, we set the following goals as our research focus in this work:

1. Indicating the dimensions of the negative experiences
2. Understanding the hidden aspects of cybervictimization from the victims’ perspective
3. Conceptualization of mitigation techniques and coping strategies
4. Investigating the positive and negative consequences of cybercrime
5. Interpretation of the victims’ support suggestions for design implications
6. Contribution to the shift from digital prevention to digital resilience

To gain an in-depth understanding of traditional victimology and theoretical research background for understanding the victims, we firstly review the existing research in this field and discuss the possible adoption of these theories to the domain of cyber victimology in chapter 2.

---

1 Crimes committed over the Internet
We then continue with exploring state of the art with regard to mitigation and coping techniques specifically within the scope of this interview-based research i.e. the four main domain of cyber fraud, identity theft, hacking and malware attack and explain the recent works related to the design aspects of human computer interaction for the victim. We then finish chapter 3 with a review of the data collection and analysis techniques and their respective background.

Chapter 4 covers an in-depth description of the episodic narrative interview method and set up, participants’ sampling and data analysis technique. Moreover, in this chapter, the code-set and its evolution during the 3-stage analytic strategy will be explained step by step.

The results and findings of interviews and the categorization of different aspects explored together with the new phenomena, which were discovered during the interview session by applying grounded theory and their dimension will be covered in chapter 5.

In chapter 6 we will discuss the results and compare and contrast them against the state of the art and related works to indicate our unique contribution to the field of cyber victimology and possible design implications for future work and research projects in the area of human computer interaction. Finally, we explain the limitations and challenges of this work and finish the report with a brief conclusion in chapter 7.
2 Background & Related Work

Although the rules governing cyberspace are quite different when compared to the crimes happening in the physical space [74], many researches have applied the findings and theories from the traditional victimology to cybercrime victimization and argued the interrelation of specific factors within cyber and traditional crime e.g. the fear of cybercrime exceeds the fear of traditional crime [21, 41, 45, 60, 74, 80, 81, 119]. In order to study the dimensions of cyber-victimology and the social reactions and impact of it, it is necessary to take a look at the relevant research studies and theories in traditional victimology and compare and contrast them with cyber victimization based on the previous studies. Therefore, in this chapter we aim at introducing the term “cyber victimology” in relation to traditional victimology, comparing victims and cyber-victims typologies and the underlying theories on victims precipitation, and providing an overview on the previous studies on usable security and user-centered design.

2.1 Victimology & Cyber victimology

The term *victim* with the Latin origin (*victima*), anciently refers to “an animal offered as a sacrifice”. Today, this word is commonly used for someone or something that is harmed by some act or circumstances [88]. A crime victim is an individual who is harmed by an illegal act and victimization is an asymmetrical interpersonal relationship between the offenders and their victims that is abusive, painful, destructive, parasitical, and unfair [55, 88].

Victimology is the scientific study of the physical, emotional and financial harm people suffer from through illegal activities [55] i.e. victimologists investigate how victims experience physical, psychological, social and economic hardships, their life-transforming injuries, healing process and the effectiveness of the assistance and support they are provided with. Adrew Karmen suggests the following step-by-step guideline for a victimological research process [55]:

1. Identify, define and describe the problem: The extent of physical injuries, emotional damage, economic costs, plus any social consequences.
2. Measure the true dimensions of the problem: Incident rate, lifetime likelihoods, characteristics of the typical victims, need assessment.
3. Investigate how victims are handled: evaluation of help provided by the criminal justice and social service system.
4. Gather evidence to test: cast doubts on common sense and sort out myths from realities.
According to the dictionary, cyber-victimization refers to the process of victimizing others through the use of information and communication technologies. Cyber-victims can be governments, organizations or individuals [109]. Cyber-victimology as the study of cyber behaviour and victimization to understand the characteristics of victims, crime patterns and crime trends, is of great importance and relevance for developing preventing strategies and user-awareness programs [74]. Due to the variety of factors affecting cyber-victimization when compared with the traditional victimization and the high dependency of the investigation on the tape of cyber-crime occurred, Debra Littlejohn introduces various aspects, which should be considered in the investigation process of a cyber-crime by different parties [74, 88]. She introduces the following steps for conducting investigation [88]:

1. Acquisition: the process of gathering information and evidence.
2. Authentication: the process of ensuring that the acquired evidence is the same as the data that was originally seized.
3. Analysis: the process of examining and evaluating information.

As a necessary part of the acquisition process, Littlejohn introduced an interview with the affected people to collect a wealth of information for a successful investigation [88], which created the basis of our work.

2.2 Victims’ Precipitation & Typologies

Since the emergence of victimology, victims’ contribution to their misfortune, which is known as “victim blame” [88] has gained significant attention in theorizing victimization and classification of the victims’ typologies [68]. The origin of the term “victims’ precipitation” is grounded in two classic criminological studies on homicide and rape, carried out by Wolfgang and Amir respectively [4, 68, 117]. Wolfgang defined victims’ precipitation as when the violence was initiated by the victims [117]. And Amir focused on the criminals’ interpretation of the victims’ behaviour rather than the behaviour itself [68]. However, the underlying assumption in both studies can be explained as victims’ behaviour is the activator of the criminals’ passive state [31]. Franklin & Franklin explicate this idea in the following example:

“A woman who walks alone toward her car on an enlightened street at night causes her own rape as surely as the man who precipitates his car theft by accidentally leaving his car keys in the car ignition” [31, 68].

Therefore, many early victimologists have established victims’ typologies based on the degree of victims’ guilt and responsibility [1]. One of the first victimologists, who introduced the term “born victims” against “born criminals” and classified victims into 13 categories according to the psychological, social, and biological risk factors, was von Hentig [10, 11]. He assigned these 13 categories to the level of
victims’ responsibility ranging from no to high responsibility [4]. Following von Hentig’s idea of the active role of the victim in the victimization process, Mendelsohn, known as the “father of victimology”, introduced two different victim topologies [20]. The first typology categorizes victims based on the level of their guilt. These 6 categories ranged from completely innocent to completely guilty (imaginary victims who fabricate a crime based on personal motivations [18, 20]). And the second broader typology categorized victims into 5 five categories (victims of criminals, victims of one’s self, victims of anti-social behaviour, victims of technology and natural environment) according to the type of crime they suffered from [19, 20]. Schafer [20, 25] classified victims based on the “functional responsibility” (The responsibility of the victims to actively prevent their own victimization from occurring) rather than risk factors. Figure 1 shows Moriarty’s comparison between these 3 approaches [20].

To be able to frame the risk factors and gain a broader understanding of the incidents, several researchers have presented theoretical perspectives with 2 different focuses (on the offender and on the victim) [19, 40]. But there is no consensus on the applicability of these theories to the cyber-victimization [60]. The “transformationists”, who believe in cybercrime as a novel phenomenon by virtue of the new space within that it is configured, state the need for the development of new criminological theories [60]. For example, Meško has argued the necessity of different responses to the consequences of cyber-victimization depending on: (1) the victim’s characteristics, (2) characteristics of the incident, and (3) characteristics of the post-victimisation experience [74, 118]. In this regard, Debra Littlejohn has also introduced the following categorization of the cybercrime victims [88]:

![Table comparing victims' categorization based on the level of responsibilities](image)

**Figure 1: Comparison of victims’ categorization based on the level of responsibilities**
1. People who are new to the Net
2. People who are naturally naive
3. People who are disabled and disadvantaged
4. The desperate, who are greedy, are lonely or have other emotional needs
5. Pseudo-victims who report having been victimized but actually were not
6. People who are simply unlucky enough to be in the wrong place at the wrong time

On the other hand, the “continuists”, who simply consider cybercrime as “new wine in old bottles.” argue for applicability of the existing victimization theories e.g. RAT [60]. Following both perspectives, Jaishankar argued that the victims of cybercrime are not more unique than the victims of conventional crime. He also believed the contribution of cyber-victims to the occurrence of the incident by the creation of a trap for themselves was the reason for the negative consequences of the crime such as shame and self-hatred [62]. However, by taking a transformationists’ perspective, he also introduced a new theory within the realm cyberspace known as “Space transition theory” [76].

In the following, the traditional theories applicable to the cyberspace and the new cybercrime theories and their relevance for cyber victimization will be discussed in detail.

**2.2.1 Lifestyle Exposure Theory**

Lifestyle exposure theory (LET) states that the risk of experiencing crime varies across society given the demographic differences of individuals and how individuals are structurally situated (e.g., age, class, gender, race) [19, 66, 72]. Here, lifestyle is defined as "routine daily activities, both vocational activities (work, school, keeping house, etc.) and leisure activities [66, 104]. For example a young bachelor is likely at greater risk of experiencing a crime because of the more active lifestyle that exposes him to potential offenders [19].

LET is also applicable to cybercrime victimization [19]. Reyns et al. successfully applied LET in their study on cyberstalking victimization and found that greater target attractiveness (e.g., risky online behaviours), when considered separately, are correlated to experiencing cyberstalking [19, 79]. Scholars stated that LET is very similar to the routine activities theory (RAT) [17, 19, 60]. Similar studies (e.g. Choi [17]), often utilize the broader perspective of LET referred to as RAT, to show that risky online behaviour is important for assessing the risk of victimization both offline and online crime [19].
2 Background & Related Work

2.2.2 Routine Activities Theory

As an extension of LET, Routine Activities Theory (RAT) focuses on the spatial and temporal order of the criminal events and asserts that a criminal act occurs when a motivated offender comes into contact with a suitable target in the absence of a capable guardian that could potentially prevent the offender from committing the crime (convergence of 3 factors in time and space)[19, 72]. Several studies have applied RAT and LRAT (lifestyle & routine activities theory applied together) successfully to investigate the risk of cyber victimization and revealed that routine activities of one’s computer usage put one at the risk of becoming a cyber victim [17, 45, 60, 66, 72, 80, 119].

2.2.3 Low Self-control Theory

Low self-control (LSC) theory, also known as “self-control theory” or as the “general theory of crime,” is a general explanation of why individuals engage in crime regardless of the type of incident or surrounding cultural background [19, 42]. According to the theory, individuals engage in criminal activity because of their inability to resist the opportunity for immediate and easy gratification that it provides [19, 42, 72]. This individual level of cybercrime is established in childhood between the age of 8-10 [42, 72].

LSC has been applied to various types of crime, both online and offline [19, 107]. Gottfredson & Hirschi argued the uniqueness of LSC, in that it is an alleged universal explanation for crime engagement and Schreck successfully utilized LSC to explain and predict the risk of victimization [19, 42, 90, 107]. Several studies have shown that individuals with lower levels of self-control are at increased risk to become a victim of some types of cybercrime, because at least some degree of victim cooperation is necessary for a successful noncontact crime, for example, fraud and cybercrime (e.g. Buzzell et al.) [10, 16, 46, 102, 107]. In accordance with this line of reasoning, Bossler & Holt also used self-control theory to explain several forms of cybercrime victimization and showed that individuals with low levels of self-control were more likely to pray for authorized access to their computer files and on-line harassment [10].

2.2.4 Big five Personality Traits Model

The Big Five personality traits, also known as the five-factor model (FFM) is a grouping for personality traits and suggests five broad dimensions commonly to describe the human personality and psyche [83]. Figure 2 shows these five personality traits [7]:
Following the low self-control theory and both conceptual and empirical overlap of the traits conscientiousness and agreeableness with self-control [52, 101], several scholars have investigated the association between Big Five personality traits with traditional and cyber victimization [25, 77, 107, 114].

Traditional crime investigators showed the three personality traits (i.e., conscientiousness, emotional stability, and openness to experience) are significantly related to the victimization of traditional crime [25, 77, 107, 114]. Van de Weijer & Leukfeldt studied a sample of Dutch individuals and showed that the level of conscientiousness, emotional stability and openness to experience were significantly related to victimization risk of cybercrime, while no significant relationship was found with agreeableness [107]. A comparison between cybercrime victims and traditional crime victims showed that only those with higher scores on emotional stability were less likely to become a victim of cybercrime than traditional crime [107].

### 2.2.5 Space Transition Theory

The Space transition theory was introduced by Jaishankar to explain the phenomena of cybercrimes. This theory argues that, people behave differently when they move from one space to another. Although the focus of this theory is on criminology and the causation of crimes in cyberspace, this theory addressed some specific characteristics of cyberspace and human behaviour in this area [76]:

1. Different statuses and positions of people in cyberspace.
2. Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace.
3. Behaviour of offenders in cyberspace is likely to be imported to Physical space which, in physical space may be exported to cyberspace as well.
4. The dynamic spatio-temporal nature of cyberspace provides the chance to escape.
5. The conflict of Norms and Values of Physical Space with the Norms and Values of cyberspace may lead to cyber-crimes.

2.2.6 Why victim blaming happens?

There are several possible reasons for blaming the victim, here are some reasons, which Moriarty [68] addresses in her book:

1. Just world belief: Individuals who strongly hold to a just world belief (the world is largely a safe and fair place to live in) more likely blame the victim [51]. In other words, bad things do not happen to good people [51, 68]. This belief allows for a false sense of security [68].
2. Victim blaming (and also self-blaming) perspectives allow for the idea of victim prevention, which gives people a false sense of empowerment and being in control of their lives [67, 68].
3. Victim blaming is easier than answering questions about the motivations of offenders and shift the attention from the criminologists’ inability to prevent the crime from happening [68].
3 State of the Art

As Meško argues there are still no in-depth international cyber victimization studies and the studies are mostly fragmented pilot projects relating to specific groups of respondents and on the specific type of cybercrime [74]. Therefore, within the scope of this project, we firstly provide an overview of the scholars on the 5 types of cybercrimes, our victims have suffered from. We also take a look at the integration of security precautions in the design process, state of the art in designing user-centered secure systems and concept of digital resilience against digital security.

3.1 Fraud

Definition: Online fraud is defined as “the experience of an individual who has responded to a dishonest invitation, request, notification or offer on the internet by providing money or personal information which has led to the financial or non-financial loss or impact of any kind” [97]. The new technological changes had a significant impact in providing opportunities for targeting potential victims [15, 97]. Given the large scale of cyber fraud victimization specially in countries with high densities of internet access, several studies have investigated cyber fraud victimization and its impacts [15, 20, 73, 82, 93, 97, 102]. However, most of the prior research in this area has been conducted through victims’ surveys and analysis of official administrative databases and little studies have involved in-depth interviews with the victims about their experiences and their needs [97].

Understanding victims: Van Wilsem [102] tried to explain why some groups are more vulnerable to cyber fraud than others. He found out that low self-control plays an important role in being more vulnerable. He also introduced some prevention precaution (e.g. auction sites refuse sellers with negative feedback records) but mentioned that the prevention possibilities are not probably helpful for people with low self-control, who will probably neglect them.

Victims’ blaming: In an interview with 85 seniors Cross et al. [73] have examined the extent and validity of the greed discourse (victims are responsible for their victimization through their decision to respond to a fraudulent email out of perceived greed or not) against cyber fraud victims and concluded that there is disjuncture between the perceived greed of the victim and the reality of individuals become victim of cyber fraud and that the current discourse does not take the level of complexity and sophistication of fraudulent approaches into account.

Coping: In another study Cross [20] has looked into cyber fraud victims coping strategies and introduced humour as a defence mechanism that allowed the victims to distance themselves from the possibility of their vulnerability to fraudulent attempts.
Impact: In their book “Cyber Frauds Scams and their victims”, Button & Cross have summarized and categorized the impact of cyber fraud from these studies into the following groups [15]:

1. Physical and mental health impact (heart conditions, high blood pressure, depression, skin conditions, a catalyst for a more rapid decline in physical health)
2. Financial impact
3. Physiological impact (anger, stress, upset, ridicule and embarrassment)
4. Impact on the relationship
5. Suicide (attempts and ideation)
6. Damaged reputation
7. Fear of violence and other negative consequences
8. Change in behaviour (being more cautious, loss of trust, rudeness, agoraphobia, living more frugally)

Figure 3 shows the behavioural changes in the cyber fraud victims from the study conducted by Button et al [14].

<table>
<thead>
<tr>
<th>Type of change reported</th>
<th>Number</th>
<th>Per cent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No change reported</td>
<td>190</td>
<td>25.5%</td>
</tr>
<tr>
<td>A lot more cautious with regard to investments/purchases generally</td>
<td>164</td>
<td>22.0%</td>
</tr>
<tr>
<td>A lot more careful in response to approach to invest, especially by phone</td>
<td>111</td>
<td>14.9%</td>
</tr>
<tr>
<td>More careful in using credit card, especially online</td>
<td>102</td>
<td>13.7%</td>
</tr>
<tr>
<td>Specific preventative action taken to avoid future frauds</td>
<td>97</td>
<td>13.0%</td>
</tr>
<tr>
<td>Behavioural change such as frequent anger, loss of trust, addiction to junk mail, agoraphobia, rudeness</td>
<td>86</td>
<td>11.5%</td>
</tr>
<tr>
<td>Increased awareness of fraud context and greater security</td>
<td>28</td>
<td>3.8%</td>
</tr>
<tr>
<td>Loss of money has meant living more frugally (usually in retirement)</td>
<td>8</td>
<td>1.1%</td>
</tr>
<tr>
<td>Total changes reported by victims</td>
<td>586</td>
<td></td>
</tr>
<tr>
<td>Total victims reporting changes in behaviour</td>
<td>555</td>
<td>74.5%</td>
</tr>
<tr>
<td>Total number of telephone interviews</td>
<td>745</td>
<td></td>
</tr>
</tbody>
</table>

*Figure 3: Change in victims’ behavior as a result of the fraud*

Victims’ needs: To address fraud victims needs and requirements Cross et al. have conducted in-depth interviews with 80 victims and introduced the following results as [97]:

1. to be listened to and treated with respect and dignity rather than blamed.
2. to receive an acknowledgement that a crime has been committed.
3. to have access to clear channels of reporting and be directed to appropriate agencies quickly and simply
4. to have access to agency staff who are trained in dealing with victims of fraud.
5. to be openly and honestly supported by friends and relatives.
6. to know what support services are available, how and where these can be accessed.
7. to have access to trained professional support that addresses not only the consequences of financial victimisation, but also the factors that precipitate such victimisation.

They also mentioned the following points as preventive measures suggested by victims [97]:
1. the provision of advice and information about the risks of online fraud and how to avoid it
2. the promotion of clear prevention messages that are consistent across agencies

To conclude, although previous studies have explained cyber fraud victims’ needs and expectations, as well as the dimensions of the impacts and victims’ blaming, they do not offer practical results for user experience designers and designers. Moreover, as the results and conclusion address different parties involved, it is not clear who will be responsible for or can contribute to responding to these needs and requirements.

### 3.2 Identity theft

Definition: Identity theft is defined as a crime in which a person’s identifying information (e.g., driver’s license, credit card, or Social Security number) is stolen [19, 71]. Studies show that each year one of the twenty-five adults across western societies becomes victims of identity theft and this number is on the rise [19, 81]. Cyberspace provides new possibilities for obtaining identity information and increase the scale of the problem [19, 81]. However, there are few studies, which have reported the impacts and experiences of victims of cyber-identity theft.

Understanding victims: Anderson examined the relationship between demographic factors and becoming the victim of identity theft and discovered for people with higher income, for younger people and for women the risk of experiencing identity theft is higher. She also introduced some preventing measures like monitoring accounts and placing mail in secure mailboxes [6].

Impact: Identity theft does not end with the occurrence of the crime and the possible financial costs related to it [19]. Therefore, researchers have addressed the amount of time and effort spent by victims to reclaim their identities, the change in consumer habits (purchasing less online), the fear of cyber identity theft and the additional sense of victimization and psychological trauma, as the additional impacts of the cyber identity theft [5, 19, 81].

Coping: Lai et al. examined the applicability of both conventional coping and technological coping to cope with identity theft and showed that both coping strategies are effective in this context [58]. Additionally, they introduced some implications for practice including: (1) practitioners need to stress the important role of an individual consumer’s learning in the conventional context and those individual consumers can apply this knowledge to the electronic commerce context, (2) practitioners need to
provide sufficient technical and computer training for individuals to develop stronger self-efficacy, (3) when an individual's self-efficacy is questionable, the individual should be encouraged to seek help from the social network [58].

3.3 Hacking

Definition: activities involved in attempting or gaining unauthorised access to IT systems [1, 19, 44]. Because of the intrigue around the topic (several different sub-groups including white, dark, and grey hat hackers\(^2\)) it is difficult to ascertain broader social aspects of this phenomenon and most of the studies investigated the offenders rather than hacking victims perspective [1, 115].

Understanding victims: In a study on hacking victims, Van Wilsem has examined the applicability of traditional cybercrime theories and found out, that the likelihood of becoming a victim of hacking attack increases with the low self-control of the individuals [115]. They also examined the relationship of the victimization risk with the demographic characteristics of the victims [115].

Impact and coping: Unfortunately, the impact of the hacking on the victims has not gained much attention from the previous scholars [44]. In his study on the hacking and harassment victims, Van Wilsem discovered hacking victims were much more likely to experience online harassment compared with non-victims of hacking [115]. With regard to the coping strategies, Van de Weijer et al. showed that hacking victims do not usually report the cases to the police [108].

3.4 Phishing

Definition: Phishing is a form of social engineering attack in which phishers trick the victim to fraudulently obtain private information [23, 63]. Phishing attacks have been on the rise in the past few years [2, 23]. Therefore, several studies have been conducted on phishing attack victims and designing a user-centric approach to the traditional technology-centric designs for phishing prevention [23].

Understanding victims: Darwish et al. demonstrated the relationship between users’ demographic and personality traits with the likelihood to fall for a phishing attack. Figure 4 shows their results on the characteristics of their impact on the risk of getting phished [23]. Vishwanath et al. studied the influencing factors on phishing victimization more specifically and discovered some specific factors like the more emails one receives, the more likely they are being deceived [105].

\(^2\) White hat or ethical hackers infiltrate a system to find weaknesses in security systems without causing any damage, black hat hackers penetrate computer systems with the specific purpose of causing damage or accessing unauthorized information, and grey hat hackers seek opportunities to exploit systems to obtain a monetary reward and may cause malicious damage [1].
Impact: The impacts of phishing on victims have not received much attention from scholars and were mainly introduced besides focus on some other aspects, for example, Parrish et al. state monetary damages, indirect costs, and opportunity costs in their research on the relationship between the big five personality traits and phishing victimization [75].

Coping: It can be concluded that a simulated phishing attack together with embedded training can contribute towards cultivating users’ phishing resistance as this approach reduces the user’s risk of becoming a victim to any future phishing attack [50].

Prevention and design: Unlike other cybercrimes that can be mitigated primarily through the use of technology, phishing needs intervention on the human level as well [75]. Therefore, several HCI research techniques have used to design user-centered anti-phishing training and education systems [39, 50, 56, 57]. Apart from prevention, the resilience of the users to phishing attacks after using a training system has also been investigated and the positive effects of the training have been proved [50].

### 3.5 Malware Attack

Definition: Malware is defined as a digital “workforce” that automates various functions (capturing sensitive information without victims’ knowledge). Therefore, they are used by criminals to assist them in committing the crime [19].

Understanding victims: Bossler and Holt examined the data from college students to show how individual characteristics are related to malware victimization [9, 19]. Besides the Ngo and Paternoster also indicated that daily activities on the Internet make malware victimization possible [19].

Impact: The Pew Internet and American Life survey showed that malware cause high costs for removal and high tangible and intangible costs for individuals [19].

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Highly Susceptible</th>
<th>Less Susceptible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>18-24 years old or less</td>
<td>25 years old or more</td>
</tr>
<tr>
<td>Gender</td>
<td>Female</td>
<td>Male</td>
</tr>
<tr>
<td>Anti-phishing Training</td>
<td>No training</td>
<td>Anti-Phishing trained</td>
</tr>
<tr>
<td>Education</td>
<td>Humanities</td>
<td>Computer Science</td>
</tr>
<tr>
<td>Training Delivery Method</td>
<td>Non-embedded</td>
<td>Embedded</td>
</tr>
<tr>
<td>Personality</td>
<td>Agreeableness</td>
<td>Consciousness</td>
</tr>
<tr>
<td>Internet Usage Behavior</td>
<td>E-commerce &amp; Online Banking</td>
<td>E-mails and simple browsing</td>
</tr>
</tbody>
</table>

Figure 4: characteristics of potential phishing victims
3.6 Victim-centered research and design

For most criminologists, victimization surveys are the standard method in crime measurement [15]. However, some researchers argued the necessity of speaking with victims to gather holistic data on victims’ experiences and needs [97]. Littlejohn and Franklin went even further and defined interviewing as an important step in a successful investigation of cybercrime for providing essential information about the incidents [30, 88].

In 1975, Saltzer & Schoeder introduced the need for “psychological acceptability” in security feedback mechanisms [33, 43, 85, 120]. Psychological acceptability suggests that users will only then be able to use mechanisms correctly (with a minimal chance of making mistakes) when the design and interface match their mental model [43]. Therefore, ease of use and cognitive load have become part of the discussion of security mechanisms and the term user-centered security, as an approach to security that places the user at the centre of security development, has been defined [91, 120]. In the literature user-centered security has taken three stands: usefulness and activity, trust, and privacy and the control of personal information [91]. However, some researchers have even gone further and taken a more extreme view and suggested that the security systems must be redesigned from the beginning with usability in mind by collaboration between the human-computer interaction and security research communities [92].

Sasse and Flechias viewed secure systems as socio-technical systems, therefore they aim was not just to improve the usability of security mechanisms for individual users, but to improve the effectiveness of security understanding the social factors [87]. Other researchers also argued the importance of social factors to guide the design of the cultural meanings of activities and facilitation for the adoption of secure mechanisms by understanding the social context behind users’ decisions [34, 91]. The socio-technical stand has been used in designing of different security mechanisms (e.g. encryption, password sharing, smartphone security) [91, 106]. Thus, information security has been treated as a multidisciplinary field, bringing together expertise from computer science, engineering, social sciences, and many other disciplines [70].

Moreover, some scholars have criticized the user-centered security and design approaches for their focus on users’ security rather than their real feeling of being secured in the interaction [64, 65]. The incapability of design in establishing and maintaining users’ trust and accountability will lead to the reluctance of the users to use the system in their everyday affairs [32, 91]. D’Hertefelt mentioned:

“The feeling of security experienced by a user of an interactive system is determined by the user’s feeling of control of the interactive system [78]“.
Given the importance of social factors and maintaining users’ trust in designing users’ interaction with the system, the necessity of specific attention of HCI practitioners towards the experiences of cyber-victims becomes clear. However, only a few studies have investigated the experiences of the victims through their narrations previously [65, 97]. Furthermore, some types of cyber-victims (e.g. hacking victims) have been neglected more than others (e.g. phishing) [44]. Considering the successful results of previous research by using users’ narrations in investigating users’ experiences with security issues and more specifically cybercrime, and the commonality of these negative experiences, there is a significant need for further research in this area [65, 97].

3.7 Digital security and digital resilience

Traditionally, cyber safety has focused on external protections (e.g. control technologies) [98]. But the problem is that the means of protection are not bulletproof [84]. To close this gap, digital resilience emphasizes internal protections (e.g. self-regulation and digital literacy3). Digital resilience is defined as the ability to deal with negative experiences online or offline. These techniques try to enable users to react and respond effectively to harmful online experiences [98].

Third et al. that resilience can only improve through exposure to risks and stressful situations [98]. They also mentioned the importance of translating these risks and exposure into meaningful knowledge and understanding, which can be used in the future possible negative experiences [98]. Following this idea, Jansson and Solms [50] simulated phishing attacks together with embedded training for cultivating users’ resistance towards ‘phishing attacks’. Some other researchers also used training methods and asserted their positive effect on improving participants’ ability to detect phishing [57, 94]. However, achieving and maintaining resilience towards different types of cybercrime through training the users by exposure to cyber threats and training systems seems to be too demanding and unrealistic. Since technology offers enhancement of peoples’ personal and business lives, which far outweigh the security risks, we must find new approaches to implement resilience, as the only variation we know to achieve digital security and do not suffer from the negative effects of cyber threats [122]. By investigating stories of cyber-victims, this work aims at discovering new opportunities for the realization of resilience in today’s digital world.

---

3 The competence and understanding people need to have to use technology effectively and critically [12].
4. Methodology

To clarify our approach in the data acquisition and analysis, in this section we will explain the research methodology in 4 phases including describing the research method, defining scope of investigation, participants’ sampling, data analysis technique (based on Floersch et al. qualitative social work [29]), and eventually generating design implications by using Sas et al. design research [86].

4.1 Research method

Previous studies have revealed the power of victims’ stories in revealing the dimensions of cybercrime victimizations and its impacts [53, 61, 97]. Tariq et al. mentioned the important role of narratives from multiple people in the identification of overall security holes providing insight into the cause of the security problem from different angles [95]. Narrative interviews as a method to collect data through storytelling seemed to be an appropriate method for capturing the stories of the victims [69]. However, to ensure consistency among interviews in order to maintain neutrality and validity specially during the analysis and comparison of the cases, there was a need for an interview protocol with a framework for themes and questions [69].

Yet the application of a semi-structured interview caused a new challenge which led to a reconsideration of our research method and set-up. As victims usually started with telling their stories passionately and we only needed to encourage this authentic narration, ask and answering questions not only interrupted the narration flow but could also make the participants defensive or reluctant to give further details. Furthermore, the stories were told retrospectively, therefore instead of a set of open-ended questions, I needed specific procedural steps that would support recalling prompts and narrowing the narration scope. The collective narrative and its potential to provide an insight to a fragmented event or incident [95], appeared to be very promising for capturing a vision to the cybercrime victimology from multiple stories of the victims. Moreover, since memories are captured through time, situation and events that form episodic within the peoples’ lives, the episodic interview could encourage the memory retrieval process [28].

Therefore, a fusion of the semi-structured interview, narrative inquiry, and episodic interview, as Müller introduced in his work [69], seemed to be more appropriate for studying my research question. However, Müller suggests this fusion in a way, which is not applicable for exploratory research questions.
Though the process might uncover phenomena, which require a parallel inquiry to the research question. Therefore, we used an adaption of the episodic narrative interview with grounded theory to be able to take an exploratory approach. Figure 5 shows the diagram and the 6 steps of the episodic narrative interview, based on Müllers technique [69].

Since the phenomena of interest could not be selected before the interview and were supposed to be explored during the process. We oriented our interview set-up in the following order:

1. Describe the interview process
2. Request a story about the whole incident
3. Request a story about an episode
4. Definition of the phenomenon
5. Request a story about the phenomenon
6. Semi-structured questions

After describing the goal and process of the interview and collecting their agreement through consent forms (see attachment A), we started the episodic narrative interview process. With a request for a story of the whole incident (first narration). Depending on the flow of the story, we usually drove the 3 episodes of before confronting the crime, during the crime occurrence and the time afterward. However, after conducting several interviews, an important phenomenon (“Denial Phase”) was discovered and explored by using the Grounded Theory, which can be seen as a separate episode between the time before and during the crime occurrence. Therefore, after several interviews, the number of episodes was increased to 4. In the third step, we asked the participants to tell a smaller story about the specific episode. These stories, which included the phenomena of our interest led to requesting definitions and sometimes, stories about them. In the last step, we asked some open-ended questions for future investigations.
The interview sessions lasted between 45 minutes to 1 hour and took place where the participants suggested being more comfortable. With the explicit consent of the participants, most of the interviews (except for two of them) were audio-recorded and transcribed for the further analysis.

<table>
<thead>
<tr>
<th>#</th>
<th>Victim Information</th>
<th>Criminal Act</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Gender</td>
<td>Age</td>
</tr>
<tr>
<td>Alex</td>
<td>M</td>
<td>26</td>
</tr>
<tr>
<td>Hanna</td>
<td>F</td>
<td>30</td>
</tr>
<tr>
<td>Anton</td>
<td>M</td>
<td></td>
</tr>
<tr>
<td>William</td>
<td>M</td>
<td>30</td>
</tr>
<tr>
<td>Emil</td>
<td>M</td>
<td></td>
</tr>
<tr>
<td>Kevin</td>
<td>M</td>
<td>21</td>
</tr>
<tr>
<td>Paul</td>
<td>M</td>
<td>24</td>
</tr>
<tr>
<td>Frieda</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>Tanja</td>
<td>F</td>
<td>38</td>
</tr>
<tr>
<td>Elena</td>
<td>F</td>
<td>25</td>
</tr>
<tr>
<td>Klaus</td>
<td>M</td>
<td>64</td>
</tr>
<tr>
<td>Ian</td>
<td>M</td>
<td>24</td>
</tr>
<tr>
<td>Victoria</td>
<td>F</td>
<td>25</td>
</tr>
<tr>
<td>Tim</td>
<td>M</td>
<td>25</td>
</tr>
</tbody>
</table>
4.2 Scope of investigation

Since the interviews were based on retrospective storytelling of the participants, to set an investigation frame we focused on the victims suffered from recent incidents. Therefore, we had a time interval of [2017-2019] for 11 incidents. However, to prove our findings, we added 4 older incidents (which occurred between 5 to 10 years ago) to our scope. Furthermore, we restricted the cases to those in which the victims could remember their experience to an acceptable extent and were willing to express it. Because forensic interviews have shown the superiority of the willingness to express the information to the remembering ability of the interviewees [59].

Table 1 shows the demographic information of the victims and fundamental details of the criminal activities, we used pseudo-names for the victims to describe the stories by respecting their privacy. As can be seen, we investigated 5 different types of cybercrimes, including fraud (10 cases), identity theft (5 cases), hacking (2 cases), phishing (2 cases), and one case of malware attack. However, the different types of cybercrime are not mutually exclusive, and, in most cases, one crime leads to several other criminal acts. Although, we did not restrict the investigation to the cases which involved financial loss, in ten cases there was a financial loss from 12 € to 6000€. As we were applying the grounded theory method [36], which means, data collection and evaluation were taking place at the same time, the exploited vulnerability and motivations' delay contributed to defining the 3 stages of the cybercrime experience and will be explained in their representative subsection of section 5.

4.3 Participants’ Sampling

Due to the sensibility of the topic, the participants were recruited by using convenience sampling [11] combined with the snowball method [37] among friends, family and university colleagues. Overall, 14 participants (9 m, 5 f) with the average age of 35 (30 at the time of the incident) and the academic background of over Bsc. were interviewed. All of the participants evaluated their tech affinity medium or higher, expect Klaus, who claimed, he did not see himself as a tech-savvy after the negative experience he had. More information about participants’ background and online behaviour can be found in section 5.

4.4 Data Analysis Technique

To provide a multidimensional view of the victims’ experience, we applied the three-stage analytic strategy, as introduced by Floersch et al. [29]. In the first and second steps, we used the thematic and
GT analysis. Therefore, we analysed the data with MAXQDA to assign the in-vivo codes to the respondents’ interviews. In the second stage after in-vivo coding, we integrated the thematic analysis to the GT for axial coding. Therefore, by comparing the participants’ answers within and among each other (inter- and intra-comparison) ten themes were defined: (1) emotions (2) actions (3) knowledge (4) profession (5) Internet usage (6) assumptions (7) expectations (8) behaviour (9) costs and (10) support. These 10 themes where used for axial coding to sort them in broader categories. In the last stage, we used the narrative -temporality and plot- and reconstructed the sequence of the stories. Finally came up with the following structure:

**Victims’ background (Before the incident):** profession, knowledge, behaviour, Internet usage, assumptions

To be able to understand victims’ mitigation strategy and consequences of the cybercrime they confronted with, it is important to analyse victims’ professional background, knowledge about cybercrime and victimization, online behaviour, dealing with internet and the exploited vulnerabilities (which was expressed by the victims themselves as assumptions in the narration process).

**Victims’ reaction (During the incident):** actions, support, assumptions, emotions

Victims’ reaction including the actions they performed based on the assumptions they had and the support they reached for, reveals the mitigation strategies during the incident. To comprehend victims’ assumptions and the decision they made, it is necessary to analyse the emotional status of the victims in this phase.

Furthermore, there were some codes that were evolved and added to the code set during the research process. These include victims’ other experiences, denial phase, social communications, support suggestions and blaming the victims. These codes contribute to explore and set the boundaries of the theories grounded in the data.

**Consequences (After the incident):** long-lasting effects, behaviour, costs, assumptions

The consequences of victims’ experiences which became visible after the incident involve long-lasting effects and behavioural changes and depend on victims’ costs and the regrets they had afterward based on their assumptions.

### 4.5 Generating Implications for Design

A difficult challenge in user-centered design is translating empirical findings into practical ideas for design or generating implications for design [24, 86]. Sas et al. [86] define implications for design as a
specific type of design knowledge based on fieldwork-, design-, and human science-informed design knowledge. In the field of cybercrime design implications have been used by previous researchers to translate their empirical findings to practical results for the process of user-centered design [91, 97].

By interviews with twelve expert HCI design researchers, Sas et al. synthesized different types of design implications and provided a guide for their generation [86]. These different categories include:

1. Sensitizing concept
2. Abstractions of Technology Functionalities
3. Instantiations of Abstractions
4. Prescriptions as Requirements for Specific Implementations

Abstractions of technology functionalities are formulated as suggestions for interpreting more abstract technology goals [86]. For example, in the context of designing a system for reading papers it can be formulated as: “to support note-taking or the ability to annotate as people read”[86]. Following this approach, we shaped our implications for design by mapping the collected data from narratives to abstract functionalities.
5. Results

This section elaborates on the results of the data analysis, starting from the first story of the victims and followed by the 3 episodes of before, during and after the incident. The first story describes the context of each case and the platform and service the victims have used. The sub-section “before the incident” explains victims’ background, knowledge, online behaviour of the victims and their assumptions about their vulnerabilities and the reason they fell into traps. Sub-section “during the incident” explains the reaction of the victims, the nature of the delay and the phenomenon of Denial Phase. Finally, the consequences, long-lasting effects and behavioural changes of the victims will be explained. Sub-section 5.5, 5.6 and 5.7 are dedicated to the data related to the data relevant for new discoveries and further studies.

In the following the context of the cases and the first story of victims about their experience as they narrated themselves is explained:

5.1 First story of the victims: Tell me what happened

As mentioned before, in this work we investigated 5 different types of cybercrime including fraud, identity theft, phishing, hacking and malware attack. This section presents and investigates each case through 3 different parts, including the interviewer’s perspective, the first story of the victims and the further relevant information collected from other sources such as service providers’ websites or other similar cases.

5.1.1 Cyber fraud

Online marketplaces can be an unsafe platform, where not only serious business takes place, but also fraud. Out of the ten fraud incidents 6 of them took place on the eBay online marketplace. These cases are described as follows:

**Alex and the Apple Watch on eBay**

I visited Alex at his home, as he wishes. He is a young dentistry student (26), who is now living in Germany for almost 3 years. A little bit uncomfortable with talking about his experience, he asks if the audio-record will only be heard by me and deleted afterward. Not only his avoidance to look at me, but also some contradictions in his story especially in terms of his emotional state and costs revealed some amount of embarrassment to me. For someone with a non-technical background, I found Alex
surprisingly knowledgeable about cybercrime and digital security. The interview session was started with the story of his experience:

“There was an item on eBay in an auction and although I never do such mistakes and I’m very careful, I saw the good price and as I never had problems with eBay I thought nothing would go wrong, I didn’t really pay attention because I was at work and all of a sudden I had this notification that one item was about to be sold, I was supposed to decide quickly, so I was not able to check out the details, I just offered a price much lower than the actual price, and thought let’s see. The watch costs 520 and I was paying 420 €, the seller wrote to me right in a very accurate and high-level language, he gave me his payment information and mentioned that he will send the item right away. I sent the money and then for 2 days there weren’t any messages from him, the item didn’t arrive either, so I messaged him to see what has happened and if he had received the money, he answered that the money was transferred but there was a problem and he was at hospital, so he couldn’t send the watch. I said, “ok if you are at the hospital there is no problem, just let me know, when you can send my purchase” and he didn’t answer me afterward.” (Alex)

Bidding on an eBay auction: In an auction-style listing, sellers name a starting price and the buyers bid against each other. To see how the bidding goes, the bidders can watch the item and the highest bidder wins the item when the listing ends. eBay warns the bidders, that they are committed to buying the item if they win it [47]. Figure 5 shows this warning [47].

Tip
Remember, a bid is considered a binding contract. That means that when you bid on an item, you’re committing to buy it if you win.

Investigation of the case: Since eBay auctions can last during longer periods of time (e.g. one week) Alex marked the item to follow watching the auction. After one week he received a notification from eBay, that the listing ended soon. Alex was at work and did not have time, so he named a price quickly and won the auction. As the seller had mentioned the Apple watch was new, but he could not return it because he had received it as a gift from America, Alex got a little bit sceptical after checking the details. However, the warning for payment commitment made him complete the purchase.

“I thought there was a bidding contract and the buyer could file a complaint against me” (Alex)
What Alex did not know was that, if he had refused to buy the item and the seller did not agree to cancel the transaction, he would have received unpaid records in his account and in the worst case scenario, his account could get limited or suspended, but nothing more [49].

**Hanna and the Handbag from an eBay Trusted Shop**

Hanna is a master student of information technology (37), whose boyfriend is a police officer. I interviewed her in the open calm area of a cafe. Although the incident happened 5 years ago, she assured me, she could still remember it very accurately. She had no concerns about the audio recording and was willing to share any information I needed. She explained her experience as follows:

“Let me start from what happened to me, I ordered a handbag on eBay and it was a pretty expensive handbag and I tried to do a good shopping, it was a typical auction. So, there were other customers and I suggested the highest price. Then the seller asked me to transfer the money. I asked him if I could pay with PayPal and he said, “oh no I don’t have a PayPal account.” I checked it and he had very good ratings and he was a trusted eBay shop as well. But he never mentioned I could only pay with PayPal in his auction. I paid because I thought, ok he has good ratings, he is a trusted eBay seller, so why not. And I transferred the money, but nothing happened. I waited and waited and waited for the handbag to arrive, I think after two or two and a half weeks, I sent him a couple of e-mails and asked him about the handbag. At first, he didn’t answer but I think after something like 4 weeks, which I know is pretty much a long time, but I was in a very stressful period, he answered and said, “oh no, I was on holiday but I will send it right now.” and at that point I felt a little bit confused, because if you are a trusted eBay seller and you do not answer for a long time and after that you send such a weird e-mail back, I should have known something was wrong, then nothing happened again and suddenly out of the blue I saw, there came first bad ratings, I saw “fraud”, and “I didn’t get my stuff”, and “I didn’t get this and I didn’t get that” and “he is a fraudster, he lied to me all that stuff” and then I started to check all of the positive ratings and realized they all came in a very short period of time, it was a high number at least 100 or even more but there were all made in maybe one week and then I thought ok, maybe someone fooled me.” (Hanna)

_eTrusted Shops_

are shops that are using a service from eBay for protection against warnings. Warnings, due to the incorrect or defective legal texts in offers are an annoying and sometimes costly problem for many online traders. Therefore, eBay offers the „Trusted eBay shop“-subscribers packages (available also free of charge) to protect them.
Investigation of the case: Although Hanna was sceptical as she found out, she could not purchase the item by using PayPal, she purchased the item because of the wrong interpretation of the phrase “trusted shop” and assumed the logo is meant to assure buyers, that the shop was trustworthy.

Emil and E-reader on eBay Classified Ads

Emil was interviewed on the phone as he preferred. He had not experienced a severe crime case but contacted me for an interview, because he saw himself as a victim. He is in Germany for 2 years and cannot speak the language well yet. Emil is obviously not a storyteller and prefers specific questions. He starts with a short description:

“This was an e-reader and I bought it for 12 € from a private seller. He gave me his bank account information and I transferred the money, but nothing arrived. I tried to contact him almost every week but there was no response. Finally, I contacted my bank and I think I could cancel the transfer.” (Emil)

Investigation of the case: Banks usually do not execute transfers to foreign institutions immediately, but at one or more fixed times a day [54]. So, if the victim contacts the bank immediately, there is still a chance, that the transfer can be cancelled. However, since Emil did not contact the bank immediately (but after 4 weeks), it is very improbable that he could have cancelled the transfer and he probably lost the money.

Kevin and the kitchen machine on eBay Classified Ads

Kevin was a 27-year-old economy student, who had several experiences with online trading and had become a victim both as a seller and buyer. He was very comfortable with talking about the incident and believed he learned the online trading rules the hard way.

“I have made two experiences in this field actually, one succinct and one difficult one. The succinct one happened a lot of years ago, at least 10 years ago, when I sold a spare part for a motorcycle via eBay classified ad or in an internet forum and the DHL shipping company selected the package format for it, a package has no tracking guarantees and this spare part had a value of about 20 €, the buyer claimed, that the packet never arrived and it could not be proved. So, I thought at that time, well then never mind. However, I have concluded afterward to use the dispatch pursuit even with smaller values and to ask buyers to pay the additional cost.
In the serious incident, I was seller, this is still an on-going judicial case, it happened about 5 years ago, I actually fell for an offer of a very high-quality kitchen machine, similar to a Kitchen aid, so the new one costs around 800 € and is traded between 600 and 700 € second-hand, and I bought this kitchen machine on eBay classified ad for 460 €, so a very unusual market price, but 5, 6 years ago I was 20, or 21, young and stupid, right? I took it and there I have made 2 mistakes, A. eBay classified ad B. Bank transfer, then I waited, and the good didn’t arrive, the 2 men from Lübeck have sold it under a false name and were online fraudsters, real fraudsters, about whom you could read on Google and I have reported it and have a warrant running, that means, I have on the two men a warrant for their entire assets, but they are both unemployed and there is nothing to get and therefore it is an on-going case, right? at the moment it is my job to follow both of them in the media and, as my lawyer advised me, as soon as I see one of the two men are stating a new employer or something of a value, then I can get my warrant, because in court they said, they had nothing, right? I mean, just stupid, that’s the story actually. And how do I deal with it, never again bank transfer, except with friends and family, clearly PayPal, PayPal with buyers’ protection which comes with an additional fee, which I negotiate with the sellers, meanwhile I am very concrete there and make a real purchase contract, with the exact date and time, identity card copy and so on, and had again a case, where I have sold something again, a very high quality bag, selling price was 350, 360 €, the buyer did not receive the bag, it was a DHL package with insurance and there has someone, really exciting, there has someone at DHL, probably an employee or a service provider, who tore the sending label off my package, put it on another package and took the bag, so my buyer received an unknown package and my bag got lost, but that was insured by DHL, I had everything in hand, I had also the contract of sale, that was great that I made the contract of sale, because DHL could prove that the package got lost and accepted to refund the exact payment.” (Kevin)

Victoria and the rare Video Games on eBay Classified Ads
I interviewed Victoria in my office at university. As a master student of Human Computer Interaction Victoria was a true example of a digital native, who spends more time in cyberspace than the real world. She tried to train herself for detecting the fraudsters on the online trading platforms and was proud of some experiences in recognizing the traps and skipping from them. She described the 3 cases in which she found herself a victim as follows:
“The first time (I fell for cyber fraud) was with my mother together and we bid on a watch. So, we found a watch quite cheap on eBay and were very excited about it and it was an auction so you could bid on it, there the problem was, that we transferred the money and after we transferred the money the watch did not arrive and then we wrote more often to the seller and asked what was going on and then there was no answer (...) we bought the watch for 60 € I think.

In the PlayStation case apparently a boy made a joke and put his PlayStation for sale, that was just before Christmas and my mother wanted to do my brother a favour by buying him a PlayStation, it just unfortunately never arrived before Christmas and there was a boy, who probably wanted to improve his pocket money before Christmas and somehow his mother noticed it and contacted us and then they actually came to us and apologized in person because they lived close by.

(...) I tried to get some games for my brother and those were 2 games for 20€ in total. There I had a list of games; that my brother had given to me. These games could rarely be found. That was why I went for the eBay classified Ad and tried to buy them second-handed (...) As the seller said, he had all these games, I became very sceptical, but it was before Christmas time and I wanted to do everything very fast.” (Victoria)

**Online eBay Classified Ads in Germany**: Emil, Kevin, and Victoria bought some goods via eBay Classified Ads. This platform service enables private sellers to offer their second-hand products and their fixed or agreeable prices to the buyers in a close neighbourhood. Our participants mentioned that the main reason for them to use eBay Classified Ads was the low prices compared to first-hand products. Victoria also addressed the unavailability of some products first handed.

**Klaus and Bitcoin investment on KAYAFX**

Klaus, a 65-year-old university professor, invited me to his home to talk about his terrible experience with cyber fraud and to show the documents he had gathered to file his complaint against the KayaFX company and the business manager, whose website was still active. Laughing at this sad truth, he told me, I could contact them myself if I were ready to invest through their website. Klaus was still angry and hopeful to get the 6000€ back. His unrealistic hope and trust in people even after his experience was surprising to me. Before we start the interview, Klaus insisted on showing the house and talking

---

*4 eBay-Kleinanzeigen*
about his achievements through his life, which I associated with improving his ego in my eyes. Here is the story:

“The following story happened to me; I’ve been getting calls asking me if I was interested in the so-called online Bitcoin trading. I said that I didn’t have the time to trade and I needed one of those brokers to do it for me and yes they could do that for me and they would only trade 10% of the profits they made for me. That sounded highly attractive to me and then the requested that I pay a small amount (300 euros), which I did, a week later they called again, they offered me a to a platform and showed how they have opened a so-called trading account for me as a stock exchange and how they have increased my balance to 300 €. So, after one week I think, there was already 450 € on my account. I liked that. Then came the request that I should invest more money, which I did. I invested 4000 € there and likewise after one or 2 weeks I got a call and saw the 4000 were actually 4800 already. So, for a while I didn’t bother myself at all, because I thought, they worked for me wonderfully and after half a year I needed some capital and wanted to see how my account balance looked like, I went to their internet platform the ”http://www.kayafx.com” and entered my account number and my password and I got the message that the password was not correct. I have requested a new password and inserted the new password with “copy and paste”, again it was not correct. Then I wrote emails to the helpdesk, I called the persons I was in contact with by phone, nobody answered anymore.” (Klaus)

KayaFX is a fake company, which apparently facilitates online investment in Bitcoin by offering users’ personal trading accounts, which make monitoring and controlling the online transactions possible. They claim to use 10% of the customers’ profits for further investments. To rich their victims they advertise their service with phone calls and the victims have the chance to talk with the manager directly and ask their possible questions. After some time, victims’ access to their accounts will be denied and the contact will be completely broken.

Investigation of the case: The last victim in the fraud category (Klaus) was defrauded through investment in KayaFx. He fell in the trap by step by step instructions through phone calls and 3 sample investments with a lower amount of money, which made the investment experience on their platform straight forward and pleasurable.
5.1.2 Identity Theft

In six of the cases, victims were affected by identity theft. Attacking user accounts on popular websites (e.g. Facebook) was the most common type of identity theft in our sample pool. It should be mentioned, that in some of the cases this crime led to other types of crime (e.g. fraud). In the following, the stories of identity theft victims are explained.

William and his Wish Account

I visited William, a 30-year-old PhD researcher in his office at university. As a researcher, he was excited about his curious experience and mentioned his personal interest to study the subject, which made him inform himself more in the field of digital security and resilience. I found William over-cautious and very sceptical, especially with regard to online shopping and credit card information. He started passionately:

“The most negative experience I had was with Wish, I heard about it from my sister, it’s a Chinese cheap site, where you can buy products very cheaply, besides website, there’s also an app for it, and then you get all kinds of stuff like technology, tech stuff, clothes etc. from China every few months. You never know if you will really receive something, but you have huge discounts instead, right? 300% discount and then you buy a drone for 1 € or 2 €. So, I thought I’d look at some of the stuff. I think I wanted to order something, and then I ordered it, but it didn’t arrive. 9 months later I still got things though, but at the beginning they didn’t arrive, so I thought, ok, let it go, after a while I got a confirmation email, because with every order you make you get a confirmation email and you have an account with a connection to Klarna, Klarna is a portal, which apparently H&M and others are using more and more now, but it didn’t exist like that in Germany at that time, it wasn’t well known, it is similar to PayPal, you give your account data, your address, and then when you pay something, they automatically bill Klarna. Then I got an order confirmation email for a USB-stick or a memory card something unimportant for € or €, and then I thought okay, is this a mistake now?! did I order something?! for this price I might have taken this. But that can’t be right, I wasn’t that shocked at first, because I thought €, € isn’t that high, I was just surprised if it was a mistake or a spam mail, I opened the page and then it said, I just ordered and then I thought it can’t be just ordered at all, then I cancelled it, which happened successfully, I logged out and in again, then I saw that in the shopping basket a product is mentioned. then I clicked on it and it was a laptop for 1008 € or 1006 € and then the order had been already so far executed, that one only had to click on order,
and the difference was that this time the delivery address was in somewhere San Francisco, and last time the delivery address was my own address and then I thought for a moment, who does that, who orders things and sends them to me, that makes no sense, but then I saw that there was another address filled out, and of course I immediately cancelled, and I thought okay, I want to delete my account, then tried deactivation, but I checked if I can log in again and I could, then I found out somehow like on Facebook, you can't delete the page, then I checked contact data and called Klarna, and they checked it for me.” (William)

Wish (wish.com) [116] is an online marketplace that facilitates transactions between sellers and buyers for a variety of products. It’s famous for low price tags on so-called expensive items. However, the products are sold by different sellers and Wish only takes a portion of the profits. The low prices are due to the cheap material and shipment from China. In order to view the prices of the products on Wish, buyers need to make an account by entering their full name and email address. Wish also tracks computers’ IP addresses, social network information, location, internet browser, and even the items users click on [113]. Figure 7 shows the landing page of the Wish [116].

![Figure 7: Landing page of the wish, to be able to see the prices users need to log in](image)

Klarna Bank AB commonly referred to as Klarna, is a Swedish bank that provides online financial services such for online storefronts, direct payments, post-purchase payments and more [123]. Apart from the website, there is a klarna app for making purchases without payment at some selected online stores, i.e. the buyers will pay for the goods later. Klarna claims to be a simple, fair, transparent and helpful bank. Right now there are variety of shops that use Klarna, including: H&M, Ray-Ban, Michael Kors, Dr Martens, Gymshark, and more [111].
**Frieda and her Facebook Account**

I met Frieda, a young PhD student in an IT-related field in her office at university. She prefers to give warnings rather than taking the role of a storyteller, who is talking about her own experience and sees her experience as an informative mind-opening incident without any risks and negative effects.

“I was a victim of identity theft in the social network Facebook. Without my knowledge some attackers gained access to my account and had access to my data. These included not only harmless information like the name or the e-mail address but also more sensitive data such as photos. At the beginning, I didn’t notice that at all. I noticed that, as there was information shown in my newsfeed for which I had no interest at the time. So, pages were liked and subscribed, and I had several new Facebook friends. I didn’t know these persons and they were not friends of my friends either. I can remember that I was wondering that my account was liking posts for which I showed no interest. Once I realized that I couldn’t do anything about it and that I didn’t feel like I wanted to keep my account I took the most radical step and deactivated my entire account and deleted it.” (Frieda)

**Facebook helpdesk:** Facebook help centre provides a step by step instruction for the cases of hacked accounts. They also suggest the users review their account login history, in the case of unusual activities [26]. Figure 8 shows the bot, which they have provided for the users in the case of security issues with their accounts [27].

![Figure 8: Facebook bot for the case of hacking](image)
**Tanja and the Tickets**

Tanja works at an international company, she was interviewed at her place and did not want me to record her voice, as I asked her why, she said, she did not want to be connected to this crime at all and only a few colleagues knew about it. So, it was kept secret. Here is her experience:

“During a business trip to Singapore, I had to make a short visit to a colleague who was at one of our offices at Dubai airport DXB. I realized then that I had forgotten the special connector of my notebook. Nobody else had it so I could not borrow it, but I knew that I would need it for staying in Singapore. Therefore, I ordered it online on a webpage that promised same-day delivery and it was delivered right away. But afterward somebody bought several flights for more than 6000 Euros in my name and with my business credit at emirates.com. Somehow, somebody must have stolen my data when I bought some electronic devices online. I did not even realize it, because it was a business credit card and I do not receive any bank statements for it. A colleague from our accounting department called me and asked why I bought several flights on behalf of unknown people. I could not believe it at first. My colleague informed my boss and arranged to block my credit card immediately.” (Tanja)

**Elena and her private eBay Shop**

Elena is a self-employed designer, who does not want people to remember what happened to her. She said that her brands’ reputation had suffered from negative consequences enough. She did not want me to record the interview, because of the fear of judgement and the possible abuse of the recording. I found her overcautious.

“I design, create and manufacture jewelry that I sell online in Germany, Austria, and Switzerland and sometimes on faires. These days, I have my own homepage and use DaWanda. But back in 2009, I used several platforms especially eBay. I offer a range of pieces that you may call “basic offerings” that I can change or extend to the wishes of my buyers. So, in the end most of my work are individual items. I only use materials of high quality. So, my pieces are not that cheap. In my payment model, customers pay ca. 80% in advance when they place the order and all details regarding the jewelry are defined. They can pay the left amount. Afterward, when they receive the pieces and they are satisfied with the piece. The customers accept these payment rules because their 80% is kind of deposited on PayPal. As soon as I send out the pieces, I get 80% and then most of the time the outstanding 20%. So, it is fair to both sides. The whole system builds on trust and valuations which is very important for my business. And exactly this system was used by the hackers.
I offered this system on eBay back in 2007. It was in my very early days when I just started the business. In the summer of 2007, I went on a journey for several weeks. I posted on all platforms where I sold my jewelry that I will be gone for the summer. I did not mention the exact dates because I did not know how long this journey would take. We had flexible return flights. So, I went on that journey. Back in 2007 I had no smartphone so I could check my Emails only rarely. Once I checked my business Emails, I could not believe what I read. eBay and PayPal tried to contact me, telling me that there were some serious complaints against me and so on. When I tried to log myself in, I could not. My own passwords were invalid. I could manage to set them back and I saw that somebody removed my “gone for the summer” posting, some ridiculously cheap offers I did not make and all the bad evaluations. I immediately contacted eBay to close my account and asked them what happened. I told them that I did not use my account for more than three weeks. I contacted PayPal as well, asking them to freeze all outstanding payments although at the beginning I did not even know what was happening. In the end, due to my ongoing requests, it could be proven by eBay that the offenders hacked my account, used my page with the positive valuations, posted these strange offerings and added new addresses they used afterward for communication with the customers. They sent out some scrap to get the 80% advanced payments. All in all, they earned ca. 2000 Euro with it.” (Elena)

5.1.3 Hacking

In two of the cases victims were confronted with the hackers, as no personal information was involved in these cases, hacking did not lead to identity theft. However, in the first case, the offender tried to use Amazon AWS at the expense of the victim and in the second case the hacker asked for money in exchange for the Instagram account.

Anton and Amazon API on GitHub

Anton was a PhD researcher in the field of IT-Privacy and Security. The interview took place in his office at the university. Through his research studies Anton had gathered a good knowledge of cybersecurity. Therefore, he saw the incident as a valuable experience for his further work and research. He started with his story before I asked him to and shared the whole process openly with me:

“I developed a kind of software, which used an account on Amazon web services, which I used as a student and it was free of charge. But you could book paid services and you have an API key, which was supposed to be private and I just upload the whole software to the
GitHub to share it between my computers and I didn’t realize that it was public. I mean it was a repository, it was totally new, I don’t have any followers or something so someone must have been using a repository to browse, searching for API key of Amazon web services. And put them to use, so all of a sudden, I got an email from Amazon web services, saying “Hey, there are 40 virtual machines running is that you” and I got it around evening so I was like ok let’s read it tomorrow, I didn’t even realize that something could have happened. At first, I was really like this is a scam. This is Phishing, I don’t know but afterward I was like, you should login and have a look at this, maybe this is legit. So actually, I called Amazon support and I think if I remember correctly, they found the GIT-Hub themselves and then they said there is a public key is that your repository and I said yeah that’s my repository.” (Anton)

**Amazon API Gateway:** The Amazon Web Services (AWS) environment is a collection of hardware and software services with the aim of enabling an easy, quick, and inexpensive use of computing resources [121]. The AWS application programming interface (API, for short) represents a way to communicate with a computing resource, which is literally the only way that external users can interact with AWS resources, and there’s no possibility to use AWS resources without using the API [121]. APIs work as the “front door” for applications to access data or functionality from the users’ backend services [3, 121].

**GitHub:** GitHub is a development platform for hosting and reviewing code, managing projects, and building software alongside other developers [13]. At the heart of GitHub is Git, a command-line tool, GitHub provides a Web-based graphical interface, access control and diverse collaboration features, such as wikis for the projects [124]. A repository is a location where all the files for a project are stored. Each project has its own repository, and they can be accessed with a unique URL [110]. Figure 9 shows the setting options in a GitHub repository [110].

**Investigation of the case:** Anton has used an ASW service by using an API key in his software and uploading it to the GitHub. Based on his words, he did not know, that only by using his API key another person could access the AWS service. Therefore, he made a mistake by sharing it on GitHub publicly.

“With this key from Amazon web services I wasn’t sure, and I wasn’t aware of the fact that you don’t need any more authentication other than the key.” (Anton)
Ian and his Instagram Account

I interviewed Ian in an office room at the university. He is a 24-year-old student of information system and has gained relevant knowledge about this topic through his studying program. Ian is somewhat satisfied with the experience he had and does not see it negatively at all. Here is the story of his incident:

“It happened last year, we had an Instagram account with 2 friends together and we had used the password of the friend of mine, and our password was not the hardest, I would say, a capital letter, a word and behind it a number and special characters. Then we have uploaded photos from our travels and so on and at some point it was so that I wanted to upload a photo and then I noticed that somehow I could not upload anything, so something did not fit there, then I logged out and wanted to log in again and then it did not work, and this “This email address doesn’t match the account, it was the outdated email address for the account and the email address had been changed and then I wrote to the friend who owned this email address, then he looked there and saw a .ru, So a Russian email address cracked the account and hacked it and threw his email address out and put his own email address in there and changed the password and so on, my friend with the same email address created a new account or something and then he contacted the hacker, so we got an answer, yes, if you want your account back, you have to pay me 50 €, so that was Fraud in the end and we said you can have the account.” (Ian)
Instagram accounts’ security: Instagram supports victims of identity theft by sending a registration link to the email or phone number of the account owner. This would only help if the hacker has not changed the email or phone number related to the account. Which they normally do. If the email is changed, the victims have still the chance to report the account and confirm their identity, which of course only works if the account was under their real full name [35].

Investigating the case: Since Ian owned a trip account, which could not be identified, Instagram security team could not help him and the only way to get the account back was to pay the fraudster.

5.1.4 Phishing

Out of 18 cases, which were investigated in this work, only in two of them victims reported phishing cases. The first victim (Tim) was fallen into a trap by a fake email from the Tibia (video game) website and Paul was phished by a fake email from PayPal. He then was a victim of malicious software which will be explained in the next subsubsection.

Tim and Tibia

Tim is a 38-year-old Spanish man, who is working at the Kaspersky user support department. He normally has to support users with criminal activities, especially malicious software attacks. We also talked about his experience with the users and how frustrated they were when confronted with a crime. Although he was responsible for the technical support, he mentioned the necessity of calming the victims down before he can start in most of the cases. Here is the story of his experience with phishing email:

“I received an email in my personal email. This was sent from an email address that looked like a popular online game that I was playing those years. Inside the email there was a link to a website that was a perfect copy of the official online game website inviting me to log in through my username and password in order to get some prizes in the game. It took me some minutes to realize that it was a phishing website; there were some differences between the true game URL and that one and I realized that after typing my login-data, so this website had now my data; I changed my password as fast as I could.” (Tim)

Tibia.com [99] is a free-to-play hardcore-fantasy-MMORPG. It is one of the oldest and most successful online role-playing games in Europe [18]. In 2019, the game won the German developer award in the

---

5 Massively Multiplayer Online Role-Playing Game
category "Dauerbrenner" ("long runner"). Right now, about half a million active players from over 200 countries play Tibia actively [18].

**Paul and PayPal email**

Paul was a 24-year-old student of information systems, who was interviewed at university. He identifies himself as a tech-savvy who can also solve computer-related problems of family and friends. So, it was difficult for him to explain the incident, which he needed to do. Here is the rest of his story:

“I have received an e-mail from PayPal which looked like an original PayPal e-mail. There it was said that I needed to update my information. and I clicked on the link and then relatively quickly noticed that I am not on PayPal but then I had already clicked on the link and it was already too late.” (Paul)

PayPal has provided a guide for its customers to distinguish between a fake email and an email that is genuinely from PayPal [48]. However, the users probably inform themselves in this area when it is already too late.

### 5.1.5 Malware attack

The only malware attack in this work was reported by Paul who was at first victim of a phishing email. In the following the rest of his story will be explained:

**Paul and Malware Attack**

“So finally the thing that happened, was that after clicking on the link I had a virus, and the virus effected my e-Mail account and simply sent 100 e-mails to any contacts but not to the ones in my address book, if you write an e-mail and enter something in the address-line above, most of the time you will get some suggestions, and these suggestions are stored in GMX as well as in such applications like Apple Mail, if you use for example a MacBook. So it used them and sent emails to all of the auto-completion suggestions, with a content about some kind of weight-loss cure, so it said that I had used a weight-loss cure that worked great, and it had worked so well that, I could only recommend it and you should see it and there was a link underneath. I have basically no clue about it, because there was nothing in the outgoing emails. I only found it out when my mother wrote to me on WhatsApp about a weight-loss program and I didn't know what she was talking about. Then she pointed out this email that she got from me. I looked at my mother's email and I immediately realized that it was a spam email, but my mother has unfortunately clicked
on the link and has therefore forwarded this email to all her contacts. The good thing was that my mother didn’t have so many email contacts or such a long list of suggestions, so it did not spread much further. In my case, the problem was that most email contacts to whom the email was sent were rather old contacts. For example, I have also sent this email to my teachers but at that time I also applied, and the email was sent to that Company. Of course, that didn’t look so good on my application. Finally, I only got a rough idea of how many emails were going out, so I wrote that there was an incident and they fortunately recorded it and that was then also clarified. But I had also applied for another company at the same time and I didn’t get anything from them heard more. So how far this went is difficult to say, because in the end, I still don’t know if all of these were suggestions from GMX or Apple Mailing. So if that was Apple Mail, then these were all addresses or proposals of the last four years and thus already over 100 and if that was from GMX/ I have had this email address for about 10 years I don’t even want to think about how many years it was then. Anyway, I’ve found out through Google that this is probably what happened. Because I had not saved the addresses of my old teachers and they appeared only in auto-complete. In the end, I deleted all suggestions from both GMX and the Apple mailing program. That was the only thing I could actually do except for changing the password.” (Paul)

5.2 Before the Incident

In this section, the background of victims as they explained will be described. The following table shows the code set used. This includes, victims’ profession, their knowledge about cybercrime, how they evaluate their online behavior themselves, how they dealt with the internet before the incident happened and the vulnerabilities, which they believed haven abused by the criminals. Finally, we will discuss previous experiences of the victims and their comparison with the traditional crime experience, if they had any.

5.2.1 Victims’ Profession, Knowledge & Online behaviour

As can be seen on the table half of the respondents had an IT-related background and therefore good knowledge and understanding bout cybercrime and different types of it. Only one of them (Frieda) evaluated her behaviour insecure before the crime. However, we observed a difference between victims’ understanding of their knowledge and what we as researches consider as security awareness. Therefore, we requested one small story about how they dealt with the internet before, what they did
online and security aspects of it. And categorized the results into two groups of “online behaviour” and “Internet usage”. The latter shows victims’ argumentation of their evaluation from their personal online behaviour.

Table 2: Victims’ background: before the incident

<table>
<thead>
<tr>
<th>#</th>
<th>Profession</th>
<th>Knowledge</th>
<th>Online behavior</th>
<th>Internet usage</th>
<th>Exploited vulnerability</th>
</tr>
</thead>
</table>
| Alex | Dentistry Student                              | Good knowledge about different types of cybercrime | Very careful    | 1. Frequent online shopping  
2. Only https websites  
3. Updated Antivirus  
4. Only Apple devices  
5. Only Firefox browser with ad blockers | 1. Lack of knowledge  
2. Past positive experiences  
3. Time and mental pressure  
4. Lack of self-control |
| Hanna | Master student of information business         | Good knowledge about different types of cybercrime | Somewhat secure  | 1. Frequent online shopping  
2. Always PayPal for online shopping | 1. Misunderstanding  
2. Lack of self-control  
3. Past positive experiences |
| Anton | PhD Student (research area: usable privacy)   | Good knowledge about different types of cybercrime | Secure          | Frequent use of online services                                   | 1. Lack of knowledge  
2. Over confidence |
| William | PhD student (research area: smart cities)  | Good knowledge about different types of cybercrime | Very careful    | 1. Frequently informing himself about this topic  
2. Permanently checking his accounts | 1. Weak password  
2. Lack of self-control |
| Emil  | –                                              | Basic knowledge about cybercrime              | Very careful    | Frequent online shopping                                           | Lack of self-control |
| Kevin | Master student of economy                      | General knowledge about cybercrime            | Somewhat careful| Frequent online shopping                                           | Lack of self-control |
| Paul  | Master student of information systems          | Good knowledge about different types of cybercrime | Conscious behavior | 1. Very familiar with computer related issues  
2. Helping others with computer related problems | Over-confidence |
<table>
<thead>
<tr>
<th>Name</th>
<th>Role/Status</th>
<th>Knowledge about Cybercrime</th>
<th>Insecure behavior</th>
<th>Weak Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frieda</td>
<td></td>
<td>No knowledge about cybercrime and the danger of it</td>
<td>Insecure behavior</td>
<td>1. Frequent use of Facebook with weak password 2. Insecure dealing with personal data</td>
</tr>
<tr>
<td>Tanja</td>
<td></td>
<td>Basic knowledge about cybercrime</td>
<td>Somewhat secure</td>
<td>Frequent online shopping</td>
</tr>
<tr>
<td>Elena</td>
<td>Self-employed professional goldsmith and designer</td>
<td>No knowledge about cybercrime</td>
<td>Not good with computer and cyberspace security</td>
<td>A professional firewall and antivirus protection software</td>
</tr>
<tr>
<td>Klaus</td>
<td>Professor of management</td>
<td>No knowledge about cybercrime (doesn’t know any type of cybercrime)</td>
<td>Very skeptical and careful about personal data and privacy</td>
<td>1. No social media services 2. Frequent use of Email 3. Antivirus program</td>
</tr>
<tr>
<td>Ian</td>
<td>Master student of information systems</td>
<td>Good knowledge about different types of cybercrime</td>
<td>Careful with personal data and privacy related issues</td>
<td>1. 45 minutes to 1 hour daily on social media 2. No personal data or posts on social media</td>
</tr>
<tr>
<td>Victoria</td>
<td>Master student of HCI</td>
<td>Basic knowledge about cybercrime</td>
<td>Somewhat secure</td>
<td>1. Frequent online shopping 2. Checking seller profile carefully</td>
</tr>
<tr>
<td>Tim</td>
<td>Working in IT support</td>
<td>Good knowledge about different types of cybercrime</td>
<td>Secure, aware of online dangers</td>
<td>1. Over average internet usage 2. Never visiting insecure websites 2. An updated antivirus</td>
</tr>
</tbody>
</table>

**Do victims know, what they don’t know?**

**Victims’ understanding of cybercrime:** The major inconsistency between our evaluation and victim’s perception was in the case of Emil, who claimed a high-security awareness, but was not able to name cybercrime he had experienced.

*“Interviewer: Can you talk about cybercrime and different types of cybercrime you know?*
Emil: I know spam, scam dating, and fraud.

Interviewer: Can you tell me which type of crime happened to you?

Emil: I don’t know how it’s called"

Klaus and the common misunderstanding

“I was always very sceptical with my personal data, I have no personal data in the cloud, I deliberately don’t have a WhatsApp, because you lose the right to the sent picture and I was never on Facebook or Instagram, I was always very stingy with my personal data. I felt very competent (in dealing with the Internet) before the incident. I had antivirus and I fell into the trap of a fake website. I was so gullible, and I didn’t even have the idea that the website or news could be fake. I still do not know any type of cybercrime.” (Klaus)

Taking online privacy precautions for cybersecurity: In most cases, the respondents were confused as they wanted to talk about the security of their behaviour and did not know, which aspects of their behaviour should be mentioned. They often were not able to distinguish between privacy aspects and security of their online interactions. The Problem occurs when a victim like Klaus, takes privacy precautions for security of his online behaviour and neglects the necessity of any further considerations.

When Ian’s privacy precaution leads to insecurity

“We couldn’t contact Instagram because it wasn’t a personal account, it wasn’t called Matthias Schmitz or anything like that, it was just a travel account and you couldn’t identify yourself with your ID card, like it’s possible on Facebook or something, you really have an account with first name and last name and you can really guarantee an identification by showing your ID card, but that wasn’t possible with Instagram because it wasn’t a personalized account (...) I did not have any private accounts on Facebook.” (Ian)

Are privacy and security always two sides of one coin? Although security and privacy are closely linked, they are different concepts. Specifically, in Ian’s case, the anonymization of the Instagram account made claiming the account impossible. For any user, who wishes to use Instagram anonymized to protect their privacy, there is a risk of being attacked by hackers. Therefore, in this case, privacy considerations caused a security vulnerability.
5.2.2 Exploited vulnerability

In cyber-security vulnerability is a flaw in a system, that can leave it open to attacks [112]. However, apart from the technical flaws of the system, vulnerabilities in the users of the system can be exploited by the offenders. Due to the complexity of cybercrimes, these vulnerabilities are not clear in many cases (e.g. William). In the following, we will see how victims explained their vulnerabilities:

William and the ambiguity

“I won’t use this payment service provider again, but maybe it was not the payment service provider itself but the connection to it, maybe my password was too weak and maybe the server was hacked. I still don’t know what happened.” (William)

Do we all have low self-control?

“It (kitchen machine) costs 800 € new and is traded between 600 and 700 € second-handed and I bought this kitchen machine on eBay classified ad for 460 €, so a very unusual market price, but I was so 20, 21, young and stupid and I naively thought, I take this wonderful offer.” (Kevin)

Low self-control must be the reason why fraudsters usually offer the products for much lower prices than the usual market price. Although Kevin, Alex and Victoria explicitly blamed their greed for falling prey for the “too good to be true” offers, Tim believed low self-control cannot be seen as a reason, as there is always a social engineering technique with different level of complexity, which can tempt and fool you.

What is a lack of knowledge?

“I posted on all platforms where I sold my jewelry that I will be gone for the summer and my account got hacked by the hackers, I never thought this information could be misused this way.” (Elena)

“So, in the end I think it only happened because we had an insecure password, they attacked randomly any accounts and it was just ours that had bad luck.” (Ian)

“Most of the users, like myself, don’t know the difference between Amazon and eBay and believe, eBay will support them like Amazon in case of a problem with the order.”
Because of the past positive experiences, I had with Amazon, when a product didn’t arrive or was defected, I tended to trust eBay” (Alex)

By using the well-known trading platforms like eBay, criminals usually use the past positive experiences of the victims to defraud them. If they are offering a new platform, they consider building a positive experience before committing the actual crime. Klaus explained, how criminals built a positive experience for him, on the platform he never had used before:

**Time and mental Pressure before Christmas**

“I sent him the list of the games, my brother gave to me and they are rare games, then the seller said, he had all these games, I became very skeptical, but it was before Christmas time and I wanted to do everything very fast. (Victoria)

Time and mental Pressure were also exploited, by offering the goods in auctions, where buyers need to decide very fast and do not have enough time to check sellers’ profiles and the information of the products more accurately. Scammers also use mental pressure by offering their products near Christmas time or at holidays, when victims have several other tasks to deal with.

**A common misunderstanding?**

“The seller never mentioned I could only pay with PayPal in his auction. I paid because I thought, he had good ratings, he was a trusted eBay seller, so why not. And I transferred the money. “ (Hanna)

Misunderstandings have also been used as a vulnerability. Hanna mentioned the expression “Trusted eBay shop” as a guarantee for the buyers triggered her trust.

**Was Anton overconfident?**

“I didn’t take it seriously because I felt like I was kind of used to using online services and I would say I knew what I did online (...) I couldn’t think, that it was something new that I did, and I needed to look at it more closely because it might have been insecure.” (Anton)

Overconfidence was also mentioned by three victims, who never thought cybercrime could happen to them, due to their knowledge and background.
5.2.3 Are victims’ past experiences related?

During the process of interviews, we found out that victims’ pervious experiences with traditional and cybercrime affect their future reaction and coping strategy. Therefore, we asked victims about their previous experiences and their reaction before.

**Reporting the case: Online vs. Offline crime**

“How Alex: I didn’t have time (to go to the police station) and I knew that reporting is a long and time-consuming process because I lost my wallet once and took so long, I was at the police station for hours.

Interviewer: Did you find your wallet at the end?

Alex: Yes, I did, but the police didn’t find it. It was maybe dropped somewhere, I received it by post, and it didn’t have the sender name of the packet, so don’t know who it was.”

The results showed, if the victim reported the case to the police because of physical crime, they did not do it in the case of cybercrime, due to the previous experience they had.

**Feeling naïve: Robbery vs. Fraud**

“Unlike eBay fraud, I did not feel naïve in this case, I was only angry with the criminal, but not naïve, because I could not do anything against it.” (Elena)

Those victims who had experience with online and offline fraud, believed they felt naïve because of cyber fraud but in the offline experience this was not the case.

**How previous problems with the same service provider effects**

“I had an accident a couple of weeks earlier not a cybercrime, but I booked something on Amazon Alexa, you can connect to APIs and I didn’t know that it costs money and I connected I got an invoice of 400 something euros and I thought OK that was stupid but you need this and you pay the money and with the second one and the top of this I felt double stupid. and honestly, I was like it didn’t happen to you before, and both of them the Amazon services so I thought next time you do something with Amazon you better be a little bit more careful. On a contrary it was a free account so I thought ok I have a free account lets you see so I think the next time I want to connect to an API I will be more aware of the costs.” (Anton)
Previous problems or issues with the same or similar services or service providers see connected to the victims, even if they are not related at all. Table three shows the previous experience of the victims, as it can be seen 5 of the victims had also experience with the traditional crime.

Table 3: Previous offline and online experiences of the victims

<table>
<thead>
<tr>
<th>#</th>
<th>Offline</th>
<th>Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alex</td>
<td>Robbery (Porte-monnaie on the street)</td>
<td>_</td>
</tr>
<tr>
<td>Hanna</td>
<td>Robbery (Porte-monnaie on the street)</td>
<td>_</td>
</tr>
<tr>
<td>Anton</td>
<td>_</td>
<td>Other experience with spam Emails, negative experience with the same provider</td>
</tr>
<tr>
<td>William</td>
<td>Spam posts</td>
<td>Other experience with spam, Identity issues with Netflix</td>
</tr>
<tr>
<td>Emil</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>Kevin</td>
<td>_</td>
<td>One other experience with cyber fraud as a seller</td>
</tr>
<tr>
<td>Paul</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>Frieda</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>Tanja</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>Elena</td>
<td>Her car was demolished deliberately</td>
<td>_</td>
</tr>
<tr>
<td>Klaus</td>
<td>Robbery (bicycles from his basement)</td>
<td>Other experience with spam Emails</td>
</tr>
<tr>
<td>Ian</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>Victoria</td>
<td>_</td>
<td>2 times eBay fraud</td>
</tr>
<tr>
<td>Tim</td>
<td>_</td>
<td>Other experiences with identity theft</td>
</tr>
</tbody>
</table>

5.3 Denial Phase: Not Accepting yourself as a victim of cybercrime

In contrast to physical crimes such as robbery, assault, and burglary, in the case of cybercrime such as online fraud or identity theft, it is not always evident that a crime has been committed. Moreover, in the interviews we often observed that our conversation partners took first clues that something was unusual (e.g. the good did not arrive) not serious, as they did not initially want to admit, they had become victims. Hence, typically there was a period of delay between when the crime was committed and when it was admitted as a crime by the victims. The main characteristic of this phase was the fact that victims deliberately suppressed or ignored the first signs and warning signals. Therefore, we decided to address this recurrent pattern as the denial phase. The denial phase usually leads to a delay in taking countermeasures. Table 1 shows the delay in taking these countermeasures, which had been
seen in 85% of the cases. The maximum amount of delay was 5 weeks. The boundaries and characteristics of the denial phase have been investigated during the interviews and conceptualized in the following:

5.3.1 How denying starts?

For an outsider, the question which arises is “why people do not immediately accept the crime and delay the countermeasures?” From the internal perspective, however, several patterns can be observed in victims’ delayed acceptance. Moreover, it seems that criminals try to exploit some vulnerabilities (often through social engineering techniques), so that the crime is not discovered, and victims’ countermeasures are postponed as long as possible.

*It can be a mistake!*

From the criminals’ point of view, the best-case scenario is when the criminal act is not revealed. In the case of fraud, for example, the biggest challenge is to steal from someone without them realizing it. Here, for example, careless or fast online shopping as an everyday routine can be used by the criminals through charging the account with small amounts each day. This strategy is supported by the fact that after a short while people normally forget which items, when, where and of which price, have been purchased, especially for the cheap purchases. Moreover, unlike forgetting about online purchases after some time, online fraud is not a common experience. Therefore, people take clues for granted and the abnormalities seem plausible at first.

“At first, I thought maybe it was a mistake, or I have ordered the item. For that low price (6€ or 8€) maybe I have done it. I know my account was hacked as I checked and saw it was just ordered.” (William)

*I did everything the same way!*

Another explanation for delayed reactions was the repeated experiences and being used to the process since one had the same experience before, they believed there was no reason to become suspicious, or even think that they have become a cybercrime victim.

“The worst thing is still that I do not exactly know, what I did wrong. I did everything exactly the same as I always did.” (Tanja)
**Past positive experiences**

In the case of the investment fraud of Klaus, the criminals even created a positive customer experience at the beginning. By giving a step by step telephone tutorial on how to use the website and testing the platform three times with smaller investments, which worked out exactly as promised. This created a positive brand image and the customer becomes familiar with the trading platform. From the criminals' point of view, building trust has two advantages: Victims get prepared to do greater investments on the platform and they do not react immediately, as they trust the platform and believe that everything will work well again.

“You get a phone call and they introduce you to their business model. First, they want a small amount and they show that it works. Also, with the second and third, larger amounts, it’s still working and only then they are pulling out. That is really ingenious.”

(Klaus)

**A Personal relationship with the offender?!**

It was also noticeable that our interviewees often talked about a personal relationship. Instead of communicating with anonymized customer support, there was often the feeling to communicate with a real, very friendly and sympathetic person.

“I know I did not want to believe that is was a fraud, I focused on the positive side, that the communication had been very nice and so on, although I knew the situation was not normal. I believed as the first negative feedback was online.” (Hanna)

**A Personal relationship with the offender**

From the criminals’ point of view, establishing a personal relationship has two advantages: First, bonding makes it emotionally more difficult for the victims to get suspicious. They don’t see themselves up against an abstract service provider or anonymous person, but against a seemingly gentle, friendly and sympathetic person.

“They try to establish a personal relationship, e.g. by addressing you very quickly as “Du”. And at the end of the conversation, when he told me about his wife and children in Stuttgart, I had no reason to doubt anymore.” (Klaus)
Problematic mailing process

In many cases, our interviewee doubted the mailing process. For instance, when filling out an online form, mistakes like mistyping a word, or that a checkmark was not placed correctly, are very common. Hence, the immediate doubt when the goods are not delivered, is that they must have been returned. An additional handicap to uncover that a story is fake is that victims cannot verify their accuracy, or only with difficulty.

“I thought maybe a mistake in the mail. I already had experience with problems with the mail, somehow the wrong address, or that I was not at home and the delivery was returned. I thought maybe something like that happened again. I waited for almost a month.” (Emil)

5.3.2 Why denying continues?

Although there is always continuous insecurity during the denial phase, there is always hope for a good end. This hope is usually empowered by social engineering techniques from the criminals, which shows that the fraudsters themselves seem to have a good feeling for the time and know when people start to doubt.

Denying is easier!

As denying an abstract unfavourable incident is easier, especially if they cause dismissive feelings, we often heard that our conversation partners suppressed their negative feelings with the hope that things will somehow work out.

“I somehow knew it was fraud long before I go to the lawyer, as the sellers’ answers were delayed, but I wanted to believe, there was still some chance of getting the item.” (Alex)

Low self-control or passion

Hanna mentioned her passion and excitement for having the item made her remain hopeful for the item to arrive by post and wait for a longer period.

“The fraudster wrote to me that he was on holiday, so I waited another 2 weeks, it was a little bit naïve, but I really wanted to have that handbag.” (Hanna)
Be ready to take the blame

We also got aware of another vulnerability offenders took advantage of, namely people's obsession with their own mistakes. For example, Klaus was locked out of the platform and by believing that he has forgotten the password, he tried several times to log-in and also reset his password.

“For days I thought you were stupid enough to go in there, it can't be. After trying several times, my account was locked and I could reset the password after 24 hours, then I waited until the next day, after resting the password several times and giving it in with copy and paste, I knew there was something wrong there.” (Klaus)

Such tricks become even more perfidious when fake security mechanisms are built in, making password resetting and access restoration very difficult and time-consuming for the user, e.g. due to missing instructions, the obligation for authentication via phone call, when the line is constantly busy, etc. This gives criminals additional time because victims try to access their accounts first. At the same time, offenders make it more difficult for victims to save documents and secure evidence.

“I tried to contact the seller again, but his account was deleted, I couldn’t find our messages either and I didn’t know if eBay deletes the messages after the account was deleted or the fraudster had done that.” (Emil)

In addition, offenders take advantage of the complexity of e-commerce, where there are many plausible reasons for delays and disruptions at any point in the process and value chain. As problems are very probable, one shouldn’t be too suspicious immediately, but be patient and wait. Based on the interviews, we categorised the disruption sources in two 3 groups: (1) the fraudster blames an imaginary dealer (2) the fraudster blames the mailing process (3) the victim blames his own problems with the mailing system. In the first category, the seller claims that the delay is caused by an imaginary dealer of the good or transportation issues. Since operational disruptions during transportation can always occur for example, because goods are not in stock, suppliers cannot deliver, IT maintenance work being carried out, etc. In addition, in our cases fraudsters also acted as small merchants or private individuals on eBay.

All humans make mistakes

In contrast to large concerns such as Amazon, here the professional operational procedures are not expected. And typical human errors (e.g. E-Mails are overlooked, the seller is not reachable, or was not able to send the good yet) are more understandable.
“After one week, there was an answer from the seller, which said he was sick and was at the hospital, that message comforted me, and I replied, oh if you are at the hospital it’s totally ok, then I waited one more week.” (Alex)

In addition, this also prepares the ground for personal excuses regarding the delays, such as an accident or death in the family members. As in such cases understanding, empathy and compassion are expected, these excuses do not cause mistrust for a while. The transport of the good present another source of delay. For instance, goods may be lost during transport or the delivery was impossible as the customer’s address is incorrect. Since these are common problems in e-commerce, fraudsters can use this as a plausible excuse for delays, without the victim having to become suspicious.

“I had the contact with the seller, phone, SMS, email it was just a tactic, yes has been sent, oh sorry it has been returned, please wait another week, and 3 or 4 weeks, I already knew everything clear it will not arrive.” (Kevin)

5.3.3 How denying ends?

To make the dimensions of denial phase clear I requested the respondents to tell me how they knew there was definitely a criminal case and they needed to take countermeasures against it. Basically, the victims pointed out 5 factors, which contributed to the end of the denial phase. In some cases, 2, 3 or even all 5 factors summed up and caused enlightenment.

Intervention of others

Victims emotional and mental pressure usually led them to share their experiences with others. Although others typically blamed the victim and scaled the emotional damage, they also contributed to the clarifications of reality. As victims’ communication partners, were not under the influence of social engineering and were not going to suffer from the consequences of the crime, they evaluated the situation more accurately and logically.

“Interviewer: And when did you exactly know that it was over and will never get the bag
Hanna: It felt strange, and honestly, I was still looking forward to having the handbag, so I told my boyfriend, hey I’m still waiting for my handbag or something like that. He asked: why did you do that? And I said he was very nice, and he said: yeah, he was nice, how naive are you? And I thought he was right; I should have known it.”
Victims help victims

Another factor, which contributes to accepting the criminal act, is the experience of others with the crime. In some cases, the victim could read the same experiences from other users or get informed by the police officer or lawyer.

“Interviewer: When did you know it was over and he was a fraudster?

Alex: When the lawyer told me that it was a typical case and he even had another client with the same case (where the fraudster claimed, he was in hospital), I accepted that the money was gone.”

accumulation of irregularities

When the suspicious irregularities add up, the probability of a usual mistake or everyday routine accident decreases, and victims start drawing conclusions out of them and the denial ends.

“I wasn’t really concerned about these things in my newsfeed in the beginning. But by the time I noticed that in my newsfeed information was shown for which I had no interest at the time. So, pages were liked and subscribed, and I had several new Facebook friends. I didn’t know these persons and they were not friends of my friends either. I can remember that I was wondering that my account was liking posts for which I showed no interest.” (Frieda)

William started to put different irregularities together and act before it is too late, he explains how denial ends as follows:

“At first I thought it was a mistake, or I myself ordered something before but then I logged in and there I saw “recently ordered” then I thought, wait a minute, it cannot be recently ordered at all (...) and this time the address was somewhere in San Francisco. The first time it was my own address and I thought who orders stuff and sends them to me apart from myself?” (William)

Service provider CAN help

Anton denied the case as he saw the service providers’ email by assuming, that it was just a spam email. But after one day he read the email again more carefully and got suspicious. Therefore, service providers can play an important role in drawing users’ attention to irregularities and hackers.
“I waited until the other day just overnight. I still didn’t feel like it was urgent I was like ok you got this email from Amazon web services let’s take a look at it Whatever that was and then I was like hey wait you probably should login, this sounds weird. At first, I was really like this is a scam. This is Phishing I don’t know but then I was like you should login and have a look at this maybe this is legit.” (Anton)

**Time solves everything**

If none of these has worked, the only factor which made the victim come out of denial was time. In other words, as time went by, the victims lost their hope and believed they have fallen into a trap.

“Interviewer: When did you exactly know that it was a fraud?

Kevin: As time went on. I had the contact with the seller, phone, SMS, email, it was just a tactic, they said, yes it was sent, aaah has come back, please wait another week, and after 3 or 4 more weeks, it was clear nothing will arrive anymore. Because the time had progressed so far and then he did not get back to me, did not respond to any calls.”

### 5.3.4 What are the consequences?

Although the denial and victims’ hope for a happy ending helps them to fight against the dismissive feelings related to the criminal act temporary, our results show that in the long run, it creates long-lasting negative effects on the victims.

**Am I fooling myself or is something wrong here?**

Victoria lives in fear of falling into the denial phase again. Therefore, she gets obsessed with checking the seller’s profile and reviewing the whole process over and over again during the time in which she waits for the purchase to arrive.

“I have this denial phase over and over again when, for example when the package does not arrive after a while and I try to tell myself that no, this can’t be a fraud, it will surely come, the person just hasn’t had time or the post takes longer and it takes about a week or two. You keep struggling and ask yourself if you are denying again or not, and all the time you go back and forth and I watch the person the whole time, so the profile of the person during this week and then I keep checking to see if they’re still active or if they’re still offering something or if their profile is being deleted all at once, so I just check if everything is going well or not. I recently bought something on eBay and after 2 weeks the package still didn’t arrive, so I just followed the tracking and found out that Hermes...
claimed that my address didn’t exist and then the whole thing got stuck at a station and
was about to ask the seller again because I thought I was denying the crime.” (Victoria)

Too Naïve to find that out?
As can be seen in table six some of the respondents regretted their delayed reaction. Even if an earlier reaction did not change anything about the incident, victims wished to have known it sooner and found themselves naïve due to their hope for a happy ending.

“He just confirmed that the money arrived, he said he was at the hospital and he apologized for the delay a lot and confirmed my mind because he apologized very politely and I waited some more days but nothing happened, so I went to the lawyer (...) I could have gone a little bit earlier.” (Alex)

Self-blame
Moreover, others often especially blamed the victims for their hope and denial. Although the victims could have hidden their hope from others, their passiveness and postponing countermeasures reveals the hope and enable others to judge and blame them more easily, which in some cases led to postponing the reactions even longer.

“I was still looking forward to having the handbag, so I told my boyfriend, hey I’m still waiting for my handbag to arrive and something like that (...) he asked: why did you do that and you still wait for the handbag to arrive? I said he was very nice, and he said: yeah, he was nice, how naïve are you? And I thought he was right; I should have known it.” (Hanna)

More difficulties for solving the case
Apart from the negative effects of the denial on the victims, it makes the forensic and crime investigation process very complicated and reduces the chance of compensation. This is probably one of the most important reasons, why criminals design social engineering techniques and try to make victims remain in this doubt as long as possible. It might be because of the possibility of cancelling the transaction if victims react soon enough. Moreover, the denial phase makes victims unsure about when and how the incident happened, in some cases that was the reason why they did not report the crime to the police.

“At the beginning, I didn’t notice that at all. So, I didn’t know exactly when and how the incident happened.” (Frieda)
5.3.5 The theory of denial

By gathering data about the denial phase and investigation of its dimensions we summarized our findings in a theory, which we introduce as the theory of denial and describe it as follows:

“There is usually a certain amount of delay between when the victim perceives the first clue and when he/she perceives the crime. The duration of the delay depends on the ambiguity of the clues for the victim and the frequency of receiving them.”

5.4 During the incident

During the incident, victims take different actions and strategies to mitigate with the cybercrime they had suffered from. To analyses victims experiences in this phase, we focused on the actions they took themselves and the support they reached for, the emotional aspects and how they felt during the whole process, assumptions that they had about what has happened to them and what would have happened if they had taken different actions and finally the expectations from the support or service provider. Table 4 shows the results of coding of the interviews in each of these categories.

5.4.1 Victims’ action

Table 4: Victims’ reaction during the incident

<table>
<thead>
<tr>
<th>#</th>
<th>Victims’ actions</th>
<th>Support</th>
<th>Emotions</th>
<th>Assumptions (what has happened, what will happen)</th>
<th>Expectations</th>
</tr>
</thead>
</table>
| Alex | 1. Contact the criminal  
2. Google  
3. Check the criminals’ profile | 1. Family  
2. Service provider  
3. Lawyer | 1. Naïve  
2. Self-blame  
3. Helpless  
4. Angry  
5. Sad | I think the fraudster want you to doubt about crime act as long as possible, because if you go to the bank right after that, you might be able to cancel the transaction | I thought eBay could at least give me some information about this person, so that I could do sth or at least contacting this person themselves |
<table>
<thead>
<tr>
<th>Hanna</th>
<th>Anton</th>
<th>William</th>
<th>Emil</th>
<th>Kevin</th>
<th>Paul</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. My boyfriend is a police officer and I thought his colleagues would have reacted like him, if I went to them.</td>
<td>1. I thought my account was hacked so I replaced my password and used a two Factor authentication.</td>
<td>The fraudsters claimed they were unemployed, and they had no money, so it is my responsibility to follow them online (to prove they are lying)</td>
<td>What I expect from eBay was a little bit fairness, that they say ok we mentioned him as a trusted eBay seller so we pay some part of your money but they just said if you didn’t pay with PayPal go to the police and don’t bother us again.</td>
<td>The emails were probably sent to GMX or Apple Email suggestions. The people who receive this will think you are stupid; and in the end they’ll probably still be mad at you for sending this shit around</td>
</tr>
<tr>
<td></td>
<td>2. protection here and there, because I often think, that protection offers fool the buyers.</td>
<td>2. I thought the costs will be increasing within minutes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Actions</td>
<td>Emotions</td>
<td>Comments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------</td>
<td>----------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frieda</td>
<td>1. Delete account</td>
<td>1. Naive 2. Stressed 3. Shocked</td>
<td>I guess that it was somehow the connection between this page where I bought this device and the credit card payment that was not safe.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>I still do not know which ones. That is what drives me kind of crazy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If someone listens to my interview, they might think that I am not good in security and will try it again.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>I have documented everything and I’m planning to deactivate the website, because it is still running.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>I am only now convinced in retrospect that what they showed me with my account movement was pure fake. That it was artificially created. But that’s just a supposition that I can’t prove.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>I have documented everything and I’m planning to deactivate the website, because it is still running.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Contact the criminal</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Google</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>I have this feeling as a victim that the police can’t really do anything about it, what do they want to do against anyone in Chichin or something? And the police are in Siegen, so I don’t have this feeling myself in the end that I am supported by the police.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Inform others</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>I have this feeling as a victim that the police can’t really do anything about it, what do they want to do against anyone in Chichin or something? And the police are in Siegen, so I don’t have this feeling myself in the end that I am supported by the police.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Check the criminals' profile</td>
<td></td>
<td>I check if the seller rights correctly, the fraudsters are mostly the people who don’t know German so well, I don’t know, that sounds kind of bad, but I noticed that.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tim</td>
<td>1. Change password</td>
<td>1. Naive 2. Shocked</td>
<td>You can never trust something that looks too much good to be true.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
As can be seen on Table 4, when confronted with a crime, even if the victim was not sure yet, what had happened and therefore which countermeasure they had to take, they performed some actions themselves based on their common sense.

**Contact the offenders or check their Profiles**

“I watch the person itself, i.e. the profile of the person during this week and then check again and again if they are still active or if they still offer something or if their profile is deleted at once.” (Victoria)

In the case of cyber fraud victims always contacted the criminal at first by whatever contact information, which was provided in their profiles to ask for their explanations. Alex, Hanna and Victoria also mentioned checking fraudsters’ profiles frequently to see if there are some irregularities e.g. negative ratings or deleting the account.

**Let’s ask Google**

“I have searched on the Internet afterward there was a woman, who has lost €60000, she has described the case and there I came across the same name a Thomas Bermann, with whom one spoke at last.” (Klaus)

Almost half of the victims used Google to search for similar experiences of the users and find out what others have done in the same situation. Some of them like Klaus and Ian also searched the offenders’ names and websites to find more information and in both cases the criminals were known on the internet as scammers.

**Logging in and out, delete the account/info or changing password**

“I tried to delete my account somehow, I waited somehow and checked if I could log in again, the page worked again, I then found out somehow like on Facebook, you cannot delete the page.” (William)

However, in the phishing and identity theft cases victims usually started with logging out and in (William and Ian) or changing their password, even though they were not sure if this could help.

“Later I understood that it was my API key that was public so actually I called the support and I think if I remember correctly they found the Git-Hub themselves and then they said there is a public key is that your repository and I said yeah that’s my repository (...) and I deleted the API key out of my code.” (Anton)
Paul mentioned it as the only thing that he could do at that time. Anton and Paul also changed and deleted the Information they held relevant to the incident. In the first case, Anton had shared his program on GitHub which included the API key to his Amazon AWS, when he found out his Amazon AWS account could be accessed without any other authentications, he deleted the virtual machines running on his account and removed the API key out of his code.

“I only found out through Google that the suggestion had probably been used. For example, because I hadn’t saved the addresses of my old teachers and they only appeared in the auto complete. In the end I deleted all of these suggestions from GMX and from the Apple mailing program.”

As Paul realized the email addresses from his contacts have been used, he searched to find out the possible ways, criminals might have used namely GMX or Apple email suggestion. To reduce the damage he deleted the suggestions, although he did not know if it could help.

**Informing Others**

“I only let my close friends, who were following us know about it. They thought it was weird that we were hacked, especially me, because I’m always careful, especially with passwords, but then I said yes, it wasn’t my email address and not my password, so I didn’t care.” (Ian)

Paul informed those, to whom he assumed the email was sent. Despite the embarrassment this countermeasure caused, Ian also informed his close friends, who were following him on Instagram.

**5.4.2 Support**

When the victims found out that, they could not solve the problem themselves, they reached for external support. In this part, we will explain the different external supports our interviewees mentioned and analyse their possible reasons.

**Let’s report the case!**

“I didn’t have time to report the case to the police and I knew that reporting is a long and time-consuming process because I lost my wallet once and took so long, I was at the police station for hours.” (Alex)
Out of the 14 victims, only two of them (Tanja and Elena) reported the case to the police and in both cases, they were obliged from others (PayPal and victim’s boss) to file the case. As the reason why victims did not report, most of the victims mentioned their assumption that police could not help them. Two of the victims explained their unwillingness to contact the police with the past experience they had through the traditional robbery.

“It was kind of a joke. I had to wait for hours because they had to search for a translator and when they heard that it was about credit card fraud relating to a German credit card and a crime that probably happened in Dubai they were annoyed as well.” (Tanja)

Unfortunately, Tanja and Elena were not satisfied with the experience they had with reporting the case, Tanja blamed the complexity of her case:

“I had to report the case due to the legal and insurance issues with PayPal. But they never found out who committed the crime and why. I did not expect it as well. They could not believe at first because the story sounded a little weird and confusing.” (Elena)

Elena mentioned, she had no expectation, that they find the criminal, but she was annoyed by the explanations she needed to give about the whole incident which happened to an account, that she had already deleted.

Let’s visit a lawyer

“The lawyer was a very understanding and pleasant guy. He knew such cases, and it went wonderfully.” (Kevin)

Unlike the police support, victims were satisfied with the experience they had with lawyers. As the reason why, Alex and Kevin both mentioned the knowledgeability and objectivity of the lawyers and direct confrontation with the truth.

Let’s contact the helpdesk

“The communication was very sobering, so they couldn’t really help and only said, please be more careful.” (Victoria)

Almost half of the victims tried contacting the service provider, eBay and Instagram did not seem to be much helpful for the participants in the case of fraud.
“It was a little bit foolish, I had to contact them twice, so at first I contacted them and said, hey they didn’t send the good and they if I had contacted him and then I said of course I contacted him several times he lied to me, it was so many weeks ago, he won’t send me the handbag, then they said, ok we take your concern seriously but we can’t tell you anything else. So, I said okay but after one or 2 weeks I contacted the seller again and he was still able to sell goods. And I saw there were other negative ratings. Of course I sent a negative rating as well and I said that he was a fraudster and he never sent the handbag and I could see that they were also other negative comments and I couldn’t understand that eBay doesn’t block the shops account so I wrote them again, and again they said they take my concerns seriously but they can’t tell me anything else because of privacy issues and then I thought, okay I won’t contact them anymore.” (Hanna)

Hanna was especially disappointed with eBay support, because they did not block the summer’s account and he was able to sell the products further.

“We couldn’t contact Instagram, because it wasn’t a personal account, it wasn’t called Mattias Schmitz or something, but it was just a travel account and so you couldn’t identify yourself with your ID card, like it’s possible on Facebook or something like that, you really have an account with first name and last name and you can really guarantee an identification, show your ID card and send it there, but that wasn’t possible with Instagram, because it wasn’t a personalized account. Therefore, we could not get it back that way. (...) There you communicate with a bot and these bots are totally annoying and that’s why the main feeling there is totally annoyed.” (Ian)

As Instagram does not provide support for the hacked accounts, which are not personalized and cannot be identified with identity cards, Ian could not use any help. He was also dissatisfied with the communication process.

“I then found out somehow like on Facebook, you can’t delete your account, you have to deactivate it somehow and then somehow wait for a week and then it will be deleted, but every time you log in, it will be reactivated again, then I looked up contact details and called Klarna I think it was because Wish was a Chinese website and there was no German support, Klarna is from Holland or so I think they could speak German.” (William)
As a service provider Wish did not provide a communication possibility for William, therefore he had to contact Klarna to get support for deleting his account.

“\textit{I logged in and shut down the machines and you was like pain pain pain pain. But then I counted them because they didn't go away, they just stop there and terminated. they were still there so I counted them, and they were 30 but they said it was 49 or something. so, I counted them, and I was like well 30 but there are the 19 ones left. that was a major source of insecurity for me. because I knew I had to shut them down immediately so that was probably why I called the tech support.}” (Anton)

Although Amazon played an important role in informing the Anton and provided him with good support, the mistake they made in the warning they sent to him, caused the victim with a senseless concern. However, after realizing that it was a mistake Anton gained the self-confidence, which was damaged through the fact, that his account was hacked.

“\textit{It was stupid but then I felt confirmed in my own actions. It was not my mistake not to see anything and I turned all of the virtual machines off. actually, it could have been an IT strategy action of Amazon ok let's make it 40 something and then you're not stupid you did everything right. maybe a psychological effect I don't know.}” (Anton)

\textbf{Let's ask friends for help}

“\textit{I have a colleague, a research assistant with us at the university, who is doing his PhD on Bitcoin. I asked him to look at my computer and he discovered that it was definitely a fraud.}” (Klaus)

Family, friends and colleagues were also a support source for more than half of the victims. The results showed, these consultants had played an important role in taking further steps and emotional aspects of the incidents on the victims.

\textbf{5.4.3 Emotional Analysis}

To analyse victims emotionally, we asked them to explain how they felt during the occurrence of the incident. The results show, all victims, regardless of the type of cybercrime felt naïve and stupid. Alex and Hanna compared this feeling with their experience with traditional robbery.
**Self-blame, Stupid and Naive**

“Interviewer: Did you feel the same when you were robbed on the street? 
Alex: No, I was sad and I thought I will never put my wallet in my back pocket again and if I’m in a crowded place I take it in my hand, but still I see it less my own fault, because this one was easier to prevent than when I was robbed. Because I could get more information before buying the item.”

It is interesting to compare how Alex and Hanna believed they could prevent incidents from happening. Alex mentioned he could have avoided the fraud by eBay buyers’ protection and checking the scammers’ profile and ratings, because even paying with PayPal does not guarantee a complete refund. However, Hanna who had checked the ratings before completing her purchase, did not believe in buyers’ protection and mentioned only paying with PayPal could survive her.

“So many years ago, someone robbed my wallet, I just felt very angry, but I thought what could I do better? And it was a situation in which I wasn’t focused, and they punched me twice and robbed my wallet. There was only money in it, so no cards no passports or something but it wasn’t that bad. The feeling to be robbed was the worst thing. But I couldn’t do anything because they came to me and eBay incident was different because I was in a position to prevent this by just saying ok, if you are a trusted seller, then you should consider the possibility of paying with PayPal, so in my view it is completely different. (...) The only way I could prevent the incident from happening was by paying with PayPal.” (Hanna)

**Helpless and lonely**

“At that moment I felt very alone and helpless, I did not know who to contact for help, the persons were just my son and then the well-known employee and it was very complicated for me even to write down a letter in English, to go to the post office with a letter and send it off.”

In more than half of the cases victims felt helpless in the situation, usually because they did not know who could help them and where they could find support. Especially if they needed to reach for support in another language or country.

**Angry and Annoyed**

“The scammer wrote to us to pay 50 € if we wanted to have our Instagram page back (...) I checked the page a couple of times, so first he had uploaded a picture of himself and then
a video where he drives through ChiChin, in his Mercedes no idea, then he deleted all posts, changed the name and content quite often, at some point there were some Arabic videos on the page (...) I was a bit angry, I was also annoyed, that was what my main feeling, when I thought how unnecessary it was to hack a travel account and use it for other nonsense, that was just completely unnecessary the action of them, right? And that they have the power in the end, they had us in their hands." (Ian)

As Ian explained, sometimes the criminal used emotional pressure to force the victims to perform a specific action they wanted e.g. paying money.

**Incompetent**

“I didn’t think cybercrime could happen to me, computers are something I want to be good in, so it shows me that I’m not.” (Anton)

We found out, that some of the victims felt they were incompetent during facing the crime and because of that, they asked for support. However, they often mentioned they did not feel like that in the time before the incident.

### 5.4.4 Victims’ Assumptions: Did victims know what went wrong?

Since victims fought against an unknown enemy with limited information and support, they usually made some assumptions based on the incomplete information they had to be able to react to the problem. In some cases, these assumptions proved to be wrong with gathering more information but in most of the cases these assumptions cannot be proved. We categorized these assumptions into three groups, the first group contains the assumptions about the reason what they did wrong and why the crime act happened.

**Assumptions on why the incident happened**

“I thought my account was hacked so I replaced my password and used a two Factor authentication (...) I thought the costs will be increasing within minutes.” (Anton)

Anton assumed his account has been hacked because of his weak password and as he did not use automatically generated password he got stressed out by the thought, that all of his passwords needed to be changed. Moreover, as he assumed his account might get charged with the costs and the costs will increase every minute, he was under time and mental pressure to take countermeasures.
“I check if the seller writes correctly, the fraudsters are mostly the people who don’t know German so well, I don’t know, that sounds kind of bad, but I noticed that.” (Victoria)

Due to her past negative experiences, Victoria assumed the criminal acts were usually performed by the non-native speakers. Therefore, she did not want to trade online with foreigners:

“You can never trust something that looks too much good to be true.” (Tim)

Tim assumed he fell into the trap, although there was no reason for him to receive some prizes from the website. Therefore, he decided to never ever trust things which do not seem to have logical reasons behind them:

“The fraudsters claimed they were unemployed, and they had no money, so it is my responsibility to follow them online (to prove they are lying.” (Kevin)

Assumptions on how the criminal act was carried out

The second group of the assumptions contains those which were related to how the criminal act was carried out. Kevin assumed the scammers lied in the court, so that they are not forced to pay him back, so he needed to prove that himself:

“I think the fraudsters want you to doubt about crime act as long as possible, because if you go to the bank right after that, you might be able to cancel the transaction.” (Alex)

Alex believed the fraudster lied about himself being at the hospital so that he would not contact the bank and a transition cancelation will not be possible anymore:

“I am only now convinced in retrospect that what they showed me with my account movement was pure fake. That it was artificially created. But that’s just a supposition that I can’t prove.” (Klaus)

As criminals built some positive experiences for Klaus with online investment through their web service before the criminal act, Klaus believed the whole website and online trading was fake and it has not worked in the past either:

“The emails were probably sent to GMX or Apple Email suggestions (...).” (Paul)

Paul assumed his automatic suggestions in his email address services to have been used for the phishing attack:
“I thought that Klarna was maybe a fraudulent website (...) Their server could have been hacked, I couldn’t know, because I didn’t have contact with them.” (William)

Since Klarna was not well known in Germany before, William assumed it to be a fraudulent website at that time, but as he could not contact the wish support team either, he also found server-hacking possible:

“I guess that it was somehow the connection between this page where I bought this device and the credit card payment that was not safe.” (Tanja)

Tanja could not discover the mistake he has made, which has led to the crime act. Therefore, she only had some assumptions about what went wrong:

“My boyfriend is a police officer and I thought his colleagues would have reacted like him, if I went to them (...) protection here and there, because I often think, that protection offers want to fool buyers.” (Hanna)

Assumptions on how others will react

The third group consists of the assumptions, victims have on how others will react to their case. In some of the cases the victim decided on reaching for help based on these assumptions. For example, Hanna did not contact the police as her boyfriend was a police officer and she assumed, his colleagues will judge her and react the same way to the case:

“As a victim I have this feeling that the police can’t really do anything about hackers, what do they want to do against someone in Chichin or something? And the police are in Siegen, so I don’t have this feeling myself in the end that I am supported by the police.” (Ian)

Ian assumed the police could not help him with his problem, as the case was complicated and the criminal was not in Germany, so he did not contact them:

“Those who receive this email will think you are stupid, and in the end they’ll probably still be mad at you for sending this shit around.” (Paul)

In the case of malware attack, Paul believed people will judge him because of what happened as a stupid person, who forwarded a senseless email, however the email had been sent from his email account automatically and he had nothing to do with it.
“If someone listens to my interview, they might think that I am not good at security and will try it again.” (Elena)

Moreover, some people even had this assumption afterward about whoever that might hear the story of this crime. Elena did not agree to voice recording because of the judgment others could have which could have caused reoccurrence of the incident:

5.4.5 Victims’ Expectations

When reaching out for support, victims usually had some expectations from the service provider and the police. These expectations played an important role in their online behavioural changes and might probably contribute to their future decisions about their reaction in the case of recurrence.

**Expectations from eBay**

“I thought eBay could at least give me some information about this person, so that I could do something or at least contacting this person themselves.” (Alex)

“What I expected from eBay was a little bit fairness, that they say ok we mentioned him as a trusted eBay seller so we pay some part of your money but they just said if you didn’t pay with PayPal go to the police and don’t bother us again.” (Hanna)

**Expectation from Amazon**

“I hoped to get compensated.” (Anton)

Anton expected a refund from Amazon so that he would not need to pay the costs of the crim act.

**Expectation from Wish**

“I expected that when I delete my account, it is deleted.” (William)

William explained the expectation he had from the service he was using, he expected to be able to delete his account without contacting the support team, which was unfortunately not the case.

**Expectations from the police**

“I might have made a mistake; I still do not know which ones. That is what drives me kind of crazy.” (Tanja)
Kevin and Tanja explained the expectations they had from the police which were not fulfilled. Although Klaus had not contacted the police until the time of the interview, he was supposed to contact them in his next step, and he shared his expectations with me in this regard.

5.5 After the Incident

The story of cybercrime did not finish with the end incidents. Cybervictims explained the behavioural changes they had and the long-term effects of the incidents on them. To analyse the dimensions of this phase we also took the costs of the criminal act and the victims regrets afterward into considerations. Table 6 shows the results of the interviews with regard to this phase:

<table>
<thead>
<tr>
<th>#</th>
<th>Long lasting effects</th>
<th>Online Behaviour changes</th>
<th>Costs</th>
<th>Regrets</th>
</tr>
</thead>
</table>
| Alex| 1. Loss of trust  
2. Loss of reputation | 1. Limiting the usage  
2. Changing trading strategy | Financial, emotional, time, effort        | I could have gone to the lawyer earlier   |
| Hanna| Loss of trust                             | Changing trading strategy                   | Financial, time                         | 1. I should have known it earlier  
2. I could send my concern to eBay a little bit earlier |
| Anton| Self-confidence damage                   | Security awareness                          | Time, emotional                         | Should have been more aware of the fact that my GIT-Hub is public and actually browsable |
| William| 1. Loss of trust  
2. Incident related concerns | 1. Limiting the usage  
2. Security awareness  
3. Secure Password | Time, emotional                         | I should have saved everything and made screenshots to have proofs |
| Emil | _                                        | Security awareness                          | Emotional                               | I should have gone to the Bank earlier     |
| Kevin| 1. Loss of trust  
2. Effects on real worlds’ interactions | 1. Changing trading strategy               | Financial, emotional, time               | I should have got suspicious because of the attracting price |
| Paul | 1. Fear of reoccurrence  
2. Receiving spam emails  
3. Incident related concerns | 1. Security awareness  
2. Limiting the usage  
3. Secure Password  
4. Privacy settings | Reputational, time, emotional, effort, data | I already knew the spam email and didn’t click on everything, but I should not have clicked on the link to update my data. I should have logged in on PayPal |
<table>
<thead>
<tr>
<th>Names</th>
<th>Loss of contracts</th>
<th>Loss of reputation</th>
<th>Security awareness</th>
<th>Losing Data</th>
<th>Emotional, Time, Effort</th>
<th>I should have used a safe password and changed it often</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frieda</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Tanja</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Elena</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Klaus</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Ian</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Victoria</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Tim</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

**5.5.1 Long-lasting Effects: What remains with the victims?**

The consequences of cybercrime are not limited to the shame and embarrassment victims suffer from during the incident. Our research showed, the main consequences of cybercrime are revealed as time goes by and victims try to get over their experience and interact with and within the cyberspace again. We divided the obstacles in the victims’ devastating struggle after the incident into 10 different groups and explored the dimension of each effect through the victims’ stories. It should be mentioned, that apart from privacy awareness the long-lasting effects were judged as negative consequences normally.

_Hanna and her trust in buyers’ protection_

“_It would be really interesting to search for the terms eBay trusted shop and buyers’ protection, protection here and there, because I often think, that protection offers they fool the buyers. That was the most annoying thing._” (Hanna)
**Klaus and his trust in the Internet**

“I couldn’t even think that the website or news could be fake before. Today it’s different, I don’t believe anything that’s on the internet anymore and I find that so sad, because it’s not a reliable source.” (Klaus)

**William and his trust in Klarna**

“Meanwhile Klarna is everywhere in Germany, it is used by H&M and other sites and many use it but actually I don’t like to use it again, but maybe this was not Klarna.” (William)

**Alex and his trust in eBay**

“You always have this feeling, that eBay will support you if there is an incident. This trust was ruined because I saw eBay doesn’t do anything to help you. I thought eBay could at least give me some information about this person, so that I could do something or at least contacting this person themselves but the only thing they do is sending a message in eBay and giving them a deadline to answer, and when the time is over nothing happens.” (Alex)

**Analysis of the loss of the trust in the victims:** Hanna, Klaus, William, and Alex experienced different dimensions of losing their trust. From losing trust they had in expressions like “buyers’ protection” to losing the trust in service providers and their partners to losing trust in the whole internet and cyberspace and finally losing trust in the strangers and private sellers. The wide range of distrust build by the incident is as William mentioned, probably due to the ambiguity of the cases and the fact, that victims do not know who they should hold responsible for what happened.

**Elena and her brands’ reputation**

“I do not know – especially in the time directly after the incident – how many orders I lost because somebody read those bad valuations. The brand of my online shop is somehow connected to unsafety.” (Elena)

**Tanja and her professional reputation**

“I am now the one who could not deal with her credit card and was hacked. At the beginning I had the feeling that especially the legal department treated me as not trustworthy. I had to wait until my name was cleared.” (Tanja)
Paul and his reputation

“That I, the tech guru, would be the one who sends the crap around, was silly. I was standing there like an idiot. I’ve sent in the job applications and the emails were also sent to those companies, that was just not so cool. Well, I mean, it kind of screws up a job for you. It’s stupid to screw up a job interview with something like that.” (Paul)

Analysis of loss of reputation in the victims: As Elena mentioned the loss of reputation may not be only about the victim themselves but also their brand or product. Therefore, it might lead to some hidden financial costs e.g. losing the customers, losing the job opportunities or losing positions because of what happened.

Elena and her confidence

“I think I am not good with computers and cyber systems, so I hired an It support company that regularly checks my computers and advises me.” (Elena)

Anton and his confidence in programming

“Maybe in the programmers’ world it happens again, because there I’m kind of a newbie, it can happen to me obviously, that’s something I want to be good at, so this incident shows that I’m not.” (Anton)

Tim and his self-confidence

“I believe that I had so much confidence that these things would never happen to me. Now I know it is not enough to know many things about something to avoid it.” (Tim)

Analysis of the self-confidence in the victims: Feeling guilty and incompetent during the incident leads in long-term to less self-confidence. Elena believed she was not good with computers she hired a security company and was even afraid of an audio recording, because she thought someone might abuse this weakness again, Anton mentioned the incident showed that was not good at programming and Tim believed he does not feel confident as he did before, because you cannot achieve 100% self-control and there will still be a trap that you will fall in.
Victoria and her fear

“If, for instance, the parcel does not arrive after a while I keep struggling with the thought that it could be a scam but I try to trust the person, no it can’t be a scam, and all the time I go back and forth and I watch the person’s profile during this week and then check again and again if they are still active or if they still offer anything or if their profiles is deleted at once, so I just check if everything is going well or not. I recently bought something on eBay and after 2 weeks the package still didn’t arrive, so I just tracked it and found out that Hermes for example claimed that my address didn’t exist and then the whole thing got stuck at a station and the parcel was about to be sent back, but I was about to ask again.” (Victoria)

Ian and his fear

“2 or 3 days ago I had some strange search suggestions, things I was not looking for, I thought something did not fit there again and I changed my password again, even directly, logged out again and in with my new password, I was not been hacked, but you are more careful (after the incident) and as soon as something is strange, although it is nothing important, you think was I hacked again?” (Ian)

Paul and his fear

“So actually, since then I’m extremely careful and I’m always a bit afraid that something like that might happen to me again. That’s why I now have a second e-mail address, which I use explicitly for job applications and for communication with companies, landlords, just something that’s really important.” (Paul)

Analysis of the fear of reoccurrence: Victoria, Ian, Paul and Tanja mentioned explicitly, that they were afraid of recurrence of the experience they had. Victoria believes she is overcautious now and overreacts to any sudden change, Tanja thought she was going crazy because she did not know which mistake, she had made and therefore, she might repeat the mistake again. Paul does not want to use one email account for all of his emails and despite this separation he is always afraid that it could happen again, and Ian overreacts to the search suggestions he had once. Therefore, the results show overreaction and overcautiousness and even obsession with the sellers’ profile are the results of the fear victims had from the reoccurrence of their experience.
**Klaus and mistrust culture**

“What I think is a great pity is that this kind of cybercrime creates such a culture of mistrust, because nobody trusts the other anymore, i.e. as soon as you have had a bad experience you protect yourself, you become even more mistrustful, every betrayal is being accused, every stranger is looked at with suspicion and that is such a pity, because it destroys a lot of our culture. It rubs off on the real world.” (Klaus)

“eBay was a platform for me, where I could trust a stranger (...) This trust is ruined.” (Alex)

“I have less trust in others today also in the real world and if I have it is combined with a great deal of caution.” (Kevin)

**Analysis of the consequences on the real worlds’ interactions:** Klaus, Alex and Kevin believed that the mistrust in cyberspace affected their real world’s interaction and finally the cybercrime causes a mistrust culture in the society.

**Paul and Spam Emails**

“I get significantly more spam emails. Well, before that all spam emails ended up in my spam folder, but meanwhile some crap slips in.” (Paul)

**Klaus and the Spam Calls**

“The scammers are connected with each other, I receive lots of telephone calls from them after this incident and they know how much money I have lost, they promise to help me to get my money back and then I found out, they want me to pay them beforehand, and then I say, I’m not that stupid yet.” (Klaus)

**Analysis of receiving spams:** As Klaus mentioned, the results show, that no only there should be a blacklist, as the list of vulnerable users, on which the victims appear to be placed after one incident, but also there should be an interconnection between the offenders, so that once the victim falls into one trap other offenders try to set the same baits for him. Therefore, the number of spam emails or mails increases.
Tanja and her concern about her mistake

“The worst thing is still that I do not exactly know, what I did wrong. I used a known page and not an open network. It was the intranet of my company. I still think about it quite often.” (Tanja)

Paul and his concerns about emails and the virus

“I don’t know how many emails were sent; I don’t want to think about it at all (...) I can’t be sure that the virus can’t still do some damage. I just tried to delete the suggestions and everything but there is nothing you can do to prevent this from happening. Maybe run a virus scanner on it, but you don’t have any real security that way either.” (Paul)

William and his concern about his account

“After that the account was still in my head for a few weeks, even now I sometime think about it, I think to myself what happened, is the account still there, has someone tried to log in again.” (William)

Ian and his concerns about the hackers’ activities

“Interviewer: Did you check again later what is posted on the site?
Ian: Yes, definitely. In the beginning even more often and then he changed the content.”

Analysis of the incident related concerns in the victims: Due to the ambiguities of the cybercrime, sometimes victims deal with their concerns, long after their victimization. These concerns might be about the causes of the incident or the loss they had. Tanja is still obsessed with the mistake she believes she has made, according to her words “she still didn’t know, what she has done wrong and it was driving her crazy” because she does not know, how she herself can prevent the incident from happening again. Paul still cannot think about the number of emails that have been sent, he still thinks about future harm that can occur due to the emails and the virus they carried. William is still concerned about his account, which he could not delete himself. He still thinks about it sometimes and there is nothing he can do about it. Ian was concerned with the content of his account, which had been hacked and kept checking the posts often long after the incident.

Ian and his emotional harm

“This has burned me because I still remember how I click on it and want to upload the picture, I still have it in front of my eyes and will never forget it.” (Ian)
Elena and her emotional harm

“I still cannot believe it. So much work, not only the hacking but they even send out some goods and, in the end, the earned only 2000 Euros.” (Elena)

Analysis of the emotional harm: Cybercrime victimization is usually combined with severe emotional harm which sometimes continues even long after the incident. Ian explains how he still remembers the moment he wanted to post the picture and how he cannot log in to his Instagram page. Elena is also still suffering from the shock she faced and cannot believe what happened. Anger, sadness, and insecurity were some of the other emotional harm victims were still bearing.

Ian, Frieda and the data they lost

“I lost Facebook friends, but it was not so important that it affects me very negatively.” (Freida)

“We already had 10k Followers and that was gone (...) It was so much effort to create such an account again” (Ian)

Analysis of losing online data: Ian and Frieda lost their online contacts, due to the loss of their accounts on social media. Although, none of them suffered from this loss severely, but they both mentioned the effort they had invested in building their online network which they had lost all of a sudden.

5.2.2 Online behavioral changes

Building some assumptions about the causes of the incidents usually leads to some online behavioural changes. Even though the victim was not sure if that change would contribute to decreasing the possible future costs or prevention from similar future incidents. These changes vary from choosing a more secure password to hiring a security company, which usually depends on the costs and severity of the incident. Let’s take a look at some of the stories on the online behaviour of the victims, changed as the result of the incident.

Klaus doesn’t do phone investments any more

“I say now basically I do not do telephone business anymore and I say, if you have something to offer me, then please send me this by e-mail that I have a verifiable document with trade register number and from you personally I would like a copy of the identity card and then they say, yes okay, we will send you that and then you usually you never hear from them again.” (Klaus)
Kevin and the trading contract

“I will never again transfer money, except with friends and family, for others I use PayPal with buyers’ protection, it comes with a fee, about which I make an agreement with the seller, meanwhile I make a real purchase contract, which with time, identity card copy.”

(Kevin)

Analysis of changing trading strategies: Unlike traditional trading in online trading it is not common to negotiate a contract. Consequently, online traders do not expect to sign a contract. As a result of cyber fraud victims got aware of this necessity and changed their trading strategy. Moreover, the high risk of faking identities forces the users to take an active role in the identification of their counter partners by asking for copies of their identity cards.

William and bank account information

“Now with other websites, I do not know if I would log in with my bank account information.” (William)

Frieda and personal information

“I got aware of the cybercrime or in this case identity theft. Therefore, I changed my online behaviour, especially with regard to personal information. Be it E-Mail, address or birthday date. Or even my full correct name and photos. But especially the usage of passwords. Like the creation of passwords. So that they cannot be guessed easily. Combinations of numbers, letters, special letters and many different words.” (Frieda)

Elena and her Location

“I will never let the whole internet know when I am gone, I never did that long journeys again and I check everything regularly.” (Elena)

Analysis of security awareness: As William, Freida, and Elena mentioned, victims usually get aware of the risk of cybercrime and that it is real. Therefore, they care more about the information which can be abused by offenders easily, these include bank account information and location.

Limiting the usage of online and offline services

“I will never use that page again, although I am not even sure if it was that page (...) I use my credit card as seldom as possible.” (Tanja)
"Facebook does not have very high importance for me anymore and from and I primarily use it for university causes and not to show myself." (Freida)

"Funnily enough I was glad when the page was taken away, it was compulsively gone, but then you think, okay now I have a lot of time that I don't put into this account, I can use it for something else.” (Ian)

**Analysis of limiting usage:** Limiting the usage after having a negative experience with the service seems very logical to any internet user. As can be seen in Tanja’s case, this limit does not only include the online service or service provider and can have some restrictions on the usage of physical properties (like a credit card). In Ian’s case the limit revealed the negative consequences of being active in social media, which caused a change in his lifestyle.

*William and the Wish account*

“I’ve changed the data in my account, I could somehow delete them from Klarna, I think I have then blocked Klarna, then I thought okay here no financial problems can happen anymore, I have removed the data and changed my name my address nothing more.” (William)

*Ian and a private Instagram account*

“I thought we will never take back our account again, so I made another account, but a private one and there I have only friends and families.” (Ian)

*Paul and two email addresses*

“I have two emails and I use them separately; I make sure that I do really important things with the email address, with which I don’t register myself on any pages.” (Paul)

**Analysis of privacy settings:** Our study showed, users related to online security and privacy automatically, in other words, they usually do not see them as separate subjects. Accordingly, Ian, Paul, and William have explained their privacy considerations, whenever they want to share their personal information online.

*Elena did not want to deal with the situation alone*

“I am not good with computers and cyber systems, so I hired an IT support company that regularly checks my computers, advises me, installed a security system and so on.” (Elena)
Analysis of hiring IT-security company: Due to the feeling of incompetency caused by the cyber victimization, Elena did not believe in her own capability to handle the situation on her own and made her hire an IT-security company to check her systems frequently.

5.5.3 Costs

Apart from financial, emotional temporal and reputational costs, which are pretty much self-explanatory, our interviewees mentioned two other forms of costs, which might not be obvious to an outsider. In the following we will present these two costs:

_Alex and the focus his lost_

“I was during my exams’ period (...) so, I see the focus I could have had on my exams as a cost.” (Alex)

_What about my effort?_

“I always put so much effort in checking the person’s profile (...) then it was before Christmas time, so I needed to search again to find and buy and another present for my brother.” (Victoria)

5.5.4 Regrets

Interviewees regrets have been presented in table 4. To analyse these regrets, we have categorized them into the following groups:

_I should have ... earlier_

“I could have gone to the lawyer earlier.” (Anton)

_Denial phase_: As was mentioned before, usually the denial phase led to regretting and self-blaming for the victims, because they believed they could have taken the countermeasures earlier than they did.

_I should have checked ..., used ..._

“I should have checked first if I am on the game official URL.” (Tim)

_Security awareness_: Sometimes the interviewees have regretted their cyber safety and security awareness. This might be due to the abstract concept of cybercrime, which made it unreal or unprobeable to the victims.
I should not have shared ...

“I should not have posted that “away for summer”. I think that attracted the hackers.”

(Elena)

Privacy awareness: Some victims, like Elena regretted the information they shared online and change the way they dealt with their personal information accordingly.

I should have known ...

“I Should have been more aware of the fact that my GiT-Hub is public and actually browsa-
ble.” (Anton)

More knowledge about service and service provider: As some victims had used the service and service provider before, they neglected the importance of informing themselves about the service and service provider.

5.6 Support suggestions: Do victims really want to have a passive role in the cycle?

Unlike many of the user-centred processes in which the users are not aware of their needs and re-
quirements, victims of cybercrime were ready to express their needs very specifically from the begin-
ning of the interview session. This reveals the amount of pressure, the misfortunate users have to bear, because of being neglected and disrespected. To address these needs, we tried to translate users’ wishes for better support and understanding from the involved parties into implications for design. Here are the unheard wishes of the victims:

Anonymity is the enemy

“They could verify the sellers and you could have the address. But this is the business model of eBay and they don’t want to give you these services. But it would have been good if they could support you in such a situation. It’s like buying a product from the market, which is damaged, you don’t blame the one who offered the product and there is a place for the seller on the market.” (Alex)

“Instagram maybe can check the account’s behaviour, for example, if suddenly completely different posts are shared and different pages are followed or something in the direction that doesn’t fit into the topic area, then that means, that you were hacked, and something was going on.” (Ian)
“A kind of step by step know-how, if I am affected by it, I could imagine this very well for online marketplaces, number 1, number 2, then a buyer ID Check, that in the larger marketplaces, such as eBay classified ads, that you can only sell there, if you have a valid postal identity procedure or a video identification with an identity card.” (Kevin)

“Let’s face it, it is partly very easy for the sellers to get away somehow, because they can fake their personal data and so on somehow very easily, that’s a pity, if there would be a possibility that eBay accepts only the real addresses and I have to give the confirmation that I live there, it would be very practical.” (Victoria)

“I think the subject is very important. I also think banks, which offer such cybercrime insurance, are very good. I think that happens much more often today. Maybe a protection could help, like we guarantee you in case of identity theft we take over the costs or something like that, or every user is insured.” (William)

Many of the victims pointed out anonymity in cyberspace as a facilitator of cybercrime. Therefore, they suggested different methods to make the identification of the offenders possible. These possibilities vary in terms of users’ autonomy, for example for Alex it was enough if eBay could contact the offender, but Kevin and Victoria wished to have a valid address from the victim. Service providers should acknowledge that a crime has happened and support users in contacting the offenders. Sending a message within the platform is not acceptable for the users. Furthermore, in the time of artificial intelligence, asking for users’ identity cards in order to verify an identity theft does not seem logical.

**Design Implications:**

1. Do not request the user to prove the crime afterward. Specially if you have not made the documentations you need clear before the incident happens.
2. Provide support to all groups of users. If users can have anonymized accounts, you should consider this in the support process.
3. Take an active role in acknowledgement of the crime. Contacting the offender within your platform is not enough!

*Please enlighten me!*

“I don’t know how to prevent this attack from happening again, that is why I hired this IT support company.” (Elena)
“I can’t say, okay, someone hacked my account, but I’ll still buy stuff on Wish, if I don’t know why, then it could be that Wish sold my data or something like that.” (William)

“I would love to know how the attacker was able to get the information, I can just guess that it was somehow the connection between this page where I bought this device and the credit card payment” (Tanja)

Some of the victims still did not know, why the incidents happened in the first place. As a consequence, they could only hang on to their assumptions, which made them reluctant to use the service again. They wished for more information so that they can prevent the incident in the future.

**Design Implication:**

Inform about the reasons for the incident. And how they can prevent this from happening again.

**I want to know what the risks are**

“But honestly what I can’t understand is how eBay could have somebody like him as a trusted eBay shop? It wasn’t a private person, I said ok it was my fault, but I think eBay should check the trusted eBay shops a little bit better.” (Hanna)

“Every single user should be aware that cybercrime or in this case identity theft can hit everyone. As you can see from my example, I am not someone these criminals could have used my information for something. I am just a normal user.” (Frieda)

For most of the users, cybercrime is an abstract concept. Some of them believe that cybercrime only happens to stupid or naïve users. Our findings show, the victims believe that the general knowledge about cybercrime and its risk is not realistic. Specially because of the diverse complicated terms and services like “eBay trusted shop” which can easily be misunderstood by the users.

**Design Implications:**

1. Choose names of your services so that they are self-explanatory, try to avoid names that arise misunderstandings and ambiguities.
2. Make the security risks more visible and real to the users.
**I want to be in charge!**

“It is helpful to have a service hotline, where you can call people, or a contact form or a history, who logged in, that I notice in case of emergency they give me something I can use, then it’s something else. To give the user this security. You could also make such a Snapchat if something happened on the website, who logged in, the last 10 IPs, maybe something like that. That you have a PDF at the end that you can print out with a code that you know the police can contact the fraudsters with such a code, and you have all the information you need to go to the police without having to search as a user. (William)

“It was stupid but when I found out Amazon support team had made a mistake about the number of virtual machines, I felt confirmed in my own actions. It was not my mistake and I turned all of the virtual machines off. Actually, it could have been an IT strategy action of Amazon ok let’s make it 40 something and then you’re not stupid you did everything right. Maybe a psychological effect I don’t know.” (Anton)

Unlike some users who wished the service provider could take the whole control of the situation and handle the problem. Some others like William wished for more autonomy and control over the services they used and their actions. Anton felt more confident and confirmed in the action, he took himself. Considering the negative consequences of cybercrime on the confidence of the users, this aspect is of great importance.

**Design Implications:**

1. Respect the victims’ control and autonomy. Confirming victims’ reactions to the crime helps with controlling the damages of the negative incident on their digital competency and confidence.
2. Consider providing log files, snapshots or other relevant documents for the case of hacking account.

**Why communication with the helpdesk matters**

“The Instagram bot is really annoying, and I wish that there was a place on Instagram somewhere that really did something, I wish the act harder against hackers. That’s why the main feeling is being annoyed, because the person is aware that he’s committing a crime, but in the end, nothing happens to him. They have a very strong sense of security.” (Ian)
“If they had called me instead of an email, then I thought it was super serious. I think it was a little bit about the wording they used it wasn’t too clear for me that there was an accident.” (Anton)

“ebay just said if you didn’t pay with PayPal, we can’t do anything for you, it was like go to the police and don’t bother us again.” (Hanna)

Communication with the victims played an important role not only in coping with the incident but also in perceiving the crime at first place. Unsuitable communication with the victims can lead to negative assumptions about the benevolence of the service provider.

**Design Implications:**

1. Offering help bots for the case of security incidents is not enough. Victims wish for a help desk with a real person, who can decide according to their specific case. Just the way offenders contact them.
2. Choose your means of communication according to the aim of communication. Be more specific and direct in the case of irregularities.

**A digital Police Station?**

“So I would like to have an email, a link where I can send such anomalies directly to, there should probably be something like that but I still have a lot to bury, so there is a lot of effort involved to find out, I probably click through to this BSI website, I wish, I was as when fire breaks out, you dial 112 on the phone and so, I would wish for such an Internet platform, where you can forward spam or fraud emails to, as soon as you receive them, and they take care of it, so that would be a kind of nice blacklist, where you might give a few details, in what amount, what is being traded and where did it happen and police federation or wherever could categorize them, based on their size, their severity, frequency and so on.” (Klaus)

The Complexity of the help process can be mentioned as one of the major problems of cyber victims. Unlike physical crime, in the case of cybercrime, the urgency of providing help can be easily neglected. What Klaus was trying to communicate was the difference between physical and online risk management.
5.7 Coping strategies: Damage control & recovery

To answer our research question (“How victims cope with the cybercrime?”), we analyzed different aspects including victims’ actions during the crime, the support they reached out for, victims’ communications with others and the pattern behind their narratives. Finally, we summarized our findings into the following strategies.

5.7.1 Draw positive results from the negative experience

To reduce the negative feeling caused by the costs and damages of the incident, victims tried to discover some positive aspects as the results of the experience such as learning effect and increasing security awareness.

Was Ian manipulated by social media?

“Ian: It is funny because I was glad when the site was taken away, it was compulsively gone, but then you think, okay now I have a lot of time that I don’t put into this account, I can use it for something else

Interviewer: Did you immediately have this feeling?

Ian: After a couple of weeks I thought I could use my time for something better, because I think, okay it’s totally unnecessary, it doesn’t help you, because you’re not doing marketing”

Social media can manipulate us. Ian lost his popular travel account and his online identity as an influencer; he drew a positive consequence from this experience to be able to recover himself cope with negative consequences. He believes that he can use the time he invested in social media in more meaningful activities now, that bring him forward.
Sensitizing and security awareness

“The most positive thing is that I got aware of the cybercrime specially in this case of identity theft and now I will deal differently with my provided information and the strength of my passwords.” (Frieda)

Victims who did not suffer from huge costs of cybercrime saw their experience more as a warning which has realized the abstract concept of cybercrime and the real risk of it for any normal internet user, for them. Frieda believed that this warning has sensitized her to security issues and will probably contribute to the prevention of more severe cases for her.

Entertaining aspects

“I have detected three scammers so more or less, one was, as I said, someone with bad German, I then realize as they suddenly got negative comments like “do not trust the user Babalola” I watch the sellers and I’m pretty good at it now and detect the fraudsters most often correctly. What I also find very interesting is that many scammers or some scammers just want to have some techniques for getting your money, for example instead of paying via PayPal or bank transfer, they ask you if you can give them the code from some online store for a 20 € voucher or something like that. I once allowed myself to have some fun and then sent a cheat fake code simply.” (Victoria)

Victoria talks about her experience as entertaining adventures. As she mentions herself, she tries to trick the scammer back to have fun and enjoy her experience as a victim. The entertaining aspects of the crime help the victims to forget about their role in the cycle and see the whole situation as a game between two equal players in which they both can win or lose.

5.7.2 Denying the costs

“This was my first experience with cybercrime.” (Anton)

“Interviewer: What kind of cybercrime did you know then or do you know now?

Klaus: Nothing yet, I’m very naive and gullible and I don’t even think that the website or news could be fake.”

When confronted with the question of “past negative experiences” victims usually refused any other cases, however during their narration they usually mentioned some other experiences. Klaus and Anton both mentioned receiving spam emails quite often before the cybercrime. Moreover, we found some contractions in the data or between the body language and victims’ narration especially with
regard to emotional costs. They usually preferred to refuse the emotional costs and change the focus of the research from their costs to how to support future victims.

5.7.3 Commonality

“As I googled and read other victims’ experiences, I felt a little comforted that I was apparently not alone in being so stupid and that my sum was still small compared to those who wrote their reports there.” (Klaus)

“I looked at the Stack Overflow and if you have the most stupid question about programming somebody has already asked that. I mean the most basic questions. It was more important to see if others got compensated.” (Anton)

Finding other victims and reading about their experiences help victims with the feeling of being naïve and stupid and reduction of self-blame. Anton chose his platform purposefully so that he can find someone with the same issue definitely and does not feel disappointed.

**Design Implication:**

1. Providing the possibility of sharing the user experiences with the service or products, supports users in the time of difficulties, sometimes users can help themselves better
2. Consider letting victims know, that they are not the only user with this issue, rather than denying the problem.

5.7.4 Humor

“exactly, we didn't have a name or anything, we only had one picture, so I checked it a few times, so he first uploaded a picture of himself and then a video of him driving through ChiChin, having fun in his Mercedes I don't know (...) at some point there were some Arabic videos on it and I don't know if it's the same type, but yes.” (Ian)

“Now I get calls quite often, offering me to get back my money, but then it comes out, that I have to pay again. So, I tell them, I’m not that stupid yet.” (Klaus)

Through their narrations, victims often used humor to downplay the negative consequences of the incident. Although they mentioned they were annoyed by them.
5.7.5 Social recognition

“Today I feel differently I got over it, I talk to others about what happened to warn them and they get usually surprised that it really happens, for many it is so, yes I read about it in the news, but I am never affected by it, right? They are also interested, how was that exactly? How can I protect myself from that?” (Kevin)

Some of the victims used their case to impress and surprise new or unfamiliar users. This feeling of having a meaningful experience, which is worth sharing and can help others made victims see what happened from another perspective and cope with the negative results easier.

**Design Implication:**
Allow the victims to share their experience with the helpdesk. Show interest in the details and ask them for their advice. Let them know they have made a meaningful and vulnerable experience, which can be helpful for others.

5.7.6 Deliberate confrontation

*How Victoria practiced online trading: train with pain*

“It had a learning effect for me, so I check several things before I buy an item, I generally check how many items were bought, then the reviews from the person and how fast the person writes back, how long the person is logged in, so I’m very sceptical if the profile was recently created, then I only do cheap purchases so that I have not lost much and otherwise it’s better on eBay Classified ads if you first contact the person and that you offer him something, I check how the person writes, that may sound a bit mean but if the person’s German is bad, if all articles are missing or whatever, I’m very sceptical.” (Victoria)

Victoria used her experience to create a pattern for herself and be able to separate a trustworthy and non-trustworthy seller. She also checked her assumptions by deliberate confrontation with non-trustworthy sellers. She also mentioned she is pretty good at recognizing the scammers, quite proudly which shows the role of these deliberate confrontation in improving her damaged ego and confirming her digital competency. Especially as she saw other peoples’ comments for the traps she did not fall for.
5.8 Blaming & Shaming: Who is responsible for a crime?

During and after the crime, there are different forms of blaming the victims involved. Table 6 shows the communication of our interviews with others during and after the crime. As can be seen on the table communication with others does not only happen due to the victims’ need for support but also as a part of their coping strategy, to share and gain social recognition and express themselves. However, in many of the cases, the communication partner blames and shames the victim for being stupid and naïve which usually leads to self-blaming and feeling guilt in the victims. Although traditional criminology researchers have conducted several studies in this area, cybercrime, due to its different contexts and complicated nature, involves some specific aspects of blaming and shaming the victims, which will be discussed in the following.

<table>
<thead>
<tr>
<th>#</th>
<th>With whom</th>
<th>Motivation</th>
<th>Expectations</th>
<th>Others reaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alex</td>
<td>Uncle, girlfriend, lawyer</td>
<td>Ask for their experiences</td>
<td>I expected the same reaction</td>
<td>They found it naïve and careless of me</td>
</tr>
<tr>
<td>Hanna</td>
<td>Family, Freinds</td>
<td>Sharing</td>
<td>I thought he was right (that I was naïve)</td>
<td>my boyfriend asked: how naïve are you? my friends had already the same experiences</td>
</tr>
<tr>
<td>Anton</td>
<td>Colleague, boss</td>
<td>Sharing</td>
<td>I expected a laugh</td>
<td>Everyone was very supportive</td>
</tr>
<tr>
<td>William</td>
<td>Family, colleagues</td>
<td>Sharing</td>
<td>Others get surprised</td>
<td>Schocked</td>
</tr>
<tr>
<td>Emil</td>
<td>Friends</td>
<td>Ask for their experiences</td>
<td>Be supportive</td>
<td>—</td>
</tr>
<tr>
<td>Kevin</td>
<td>Father, friends</td>
<td>Sharing</td>
<td>—</td>
<td>Supportive, surprised, shocked, interested</td>
</tr>
<tr>
<td>Paul</td>
<td>Family, mailing-list</td>
<td>Warn others</td>
<td>To find me an idiot</td>
<td>One company accepted my apology and I didn’t hear from the other one</td>
</tr>
<tr>
<td>Frieda</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Tanja</td>
<td>Colleagues, Boss</td>
<td>Warn others</td>
<td>In a way I could understand that</td>
<td>My boss understood it. The ones from the legal department were pretty annoyed</td>
</tr>
</tbody>
</table>

Table 6: Communication of the victims

**Design Implication:**
Fake risk exposure can be used as a method to empower cyber victims.
Ambiguities and self-doubts

“Some colleagues of the legal department let me realize that they thought that I was a careless person. In a way I could understand that, but I did everything the same way I always did.” (Tanja)

Because of the ambiguity and complexities of the cybercrime, especially in the cases, in which the victims do not know what they did wrong, it is easier to blame the victims than to believe in a complex social engineering or technological trick which they do not know and cannot think of. Therefore, the risk of blaming the victims is higher.

There not no predefined rules

“Due to the fact that my card was blocked, I had to wait until my “name was cleared” before I could get the compensation. The worst thing is still that I do not exactly know, what I did wrong. I used a known page and not an open network. It was the intranet of my company. I still think about it quite often. And it was very hard to be treated as a non-trustworthy person by some people. Of course, I know, that they were just doing their jobs but at some time, I felt like an offender.” (Tanja)

As Tanja’s credit card information was blocked after the incident, she had to pay herself for the costs and was only compensated after her case was cleared. As the rules and counter measurements for the cybercrime is not clear and predefined in most of the cases, victims do not know what they should expect in the time of being affected by such a situation and therefore might feel the reaction of others is not proportional to the crime and therefore feel like an offender rather than a victim.
**Wording matters**

“*I contacted eBay and they just told me if you didn’t use PayPal then it’s your, it’s your,\nthey didn’t tell me that it was my fault but it was like go to the police and don’t bother us\again.*” (Hanna)

Unlike physical crime in which the producers of the products do not blame the customer for the incidents (for example the producer of your wallet does not blame the customer for being robbed) in the case of cybercrime the provides usually blame the victims, for example if the account is hacked or they buyers have not paid with PayPal the service providers blame them for the incident, not the offenders.

**Digital incompetency**

“He cursed me and asked, how I could be that naïve, but I expected the same reaction,\nbecause young people are more competent in using media and would never do something\like it.” (Klaus)

Apart from blaming the victim for the crime that has happened, cybercrime usually leads to blaming the victims for being incompetent for using technology, especially if the victims are digital immigrants or newbies. Thus, victims usually see themselves in a position, where they need to prove their competency and knowledgeability, which was the case in most of the narrations.

**Never-ending misery**

“I can’t be sure the virus isn’t still causing damage. I tried to delete the suggestions but\nthere isn’t anything I could do to be sure that it was stopped. Maybe it’s still running, and\npeople blame me for the virus, but you don’t have any real security there either.” (Paul)

In the case of cybercrime sometimes we are not dealing with an individual offender, but a virtual machine, generating automatic emails or viruses, therefore estimating the costs and future blames in unknown. As Paul mentioned, he could not be sure that the emails had been stopped and he would not be blamed in the future from others. Hence this is sometimes more difficult to get over blaming and be sure that it is finished.

**Design Implication:**

1. Be aware of the fear of the victims from future costs and the never-ending misery in the cybercrime and give them an overview of what might happen in the future.
2. Watch for the wordings of the messages and the indirect blaming and shaming hidden between the lines.
6. Discussion & Conclusion

To compare and contrast our findings, in this chapter we will evaluate and discuss our results concerning the related work and state of the art. This evaluation is divided into how victims perceived themselves and their role, our method and its suitability for driving design related suggestions and implications, how we contribute to digital resilience and finally the limitations of our work and possibilities for future research studies.

6.1 Victim, survivor or normal users?

“Interviewer: so, you saw yourself as a victim?
Anton: yeah totally.

Interviewer: and why is it you feel like you were a victim?
Anton: somebody used my authentication information and that’s a crime.

Interviewer: ok so you are not sure which kind of crime that was, but you are sure that you were a victim.
Anton: it’s not a fraud, I’m not sure how to categorize that, somebody used my authentication.” (Klaus)

Previous studies have criticized the term victim for referring to those affected by cybercrime, because of the negativity implied from it [89], our results are consistent with the previous studies in this matter. Although our interviewees always defined themselves as a victim if there was a financial cost involved, their agreements expressed their unwillingness because of belonging to a group of people, which are characterized by their vulnerabilities. Our findings also revealed that the criteria, based on which the respondents decided if they were victims or not, were not fixed and varied case by case. For instance, Emil and Victoria had cases in which they could refund their money but perceived themselves as victims because they did not receive what they expected when they needed it.

“I saw myself as a victim because I thought I would get the device but that was just a waste of time and hope.” (Emil)

“Basically, it was a fraud, and we were victims, because we transferred the money and never got the PlayStation” (Victoria)
Nonetheless, William whose account was hacked and misused did not find himself as a victim of cybercrime because he did not have any financial disadvantages.

"Interviewer: But do you see yourself as a victim?

William: Well, if the order had been done and the money had been lost and I couldn't get it back, then definitely, now I don't know."

We also investigated the dimensions of victims’ blaming in cyber victimization and its unique characteristics. By introducing the differences of victims’ blaming in cyber space and following the transformationists’ perspective, we aimed at changing the focus from the traditional victimizations theories which put the blame on victims and categorize them by neglecting social engineering and complexity of dealing with the potential non-human or skilful offenders, to understanding each case in its unique sociotechnical context. With the ubiquity of artificial intelligence and low error-rate algorithms with a performance far better than ever compared to those of humans, maybe it is time to see beyond traditional victims’ blaming theories and the typical victim categorization, by accepting cybercrime as one type of user experience, which can occur to any normal user. From this point of view, a more helpful approach would be to acknowledge users’ coping strategies with cybercrime as meaningful and valuable experiences for further development of more user-friendly systems.

6.2 Why victims’ stories matter? Reflection on our method regarding the research question

In the past scholars have argued for the suitability of in-depth interviews to understand cybercrime victims [97]. Our results confirm the power of victims’ collective narration in the construction of a wider context of victims’ coping strategies. Previously Cross has introduced humour as one coping strategy of the cyber fraud victims [20]. By acknowledging her work, we addressed five other strategies, which have been used by our respondents, namely drawing positive results, commonality, denying the costs, social recognition, and deliberate confrontation. Our method was successful in giving victims a voice and encouraging them to contribute to the research study. They showed their interest in the results of our report and asked if they could also receive a copy from us. They also offered to help more in the research process.

To our surprise, victims knew exactly what they expected from and usually suggested improvements without any hesitation. Some victims needed a more structured interview and frequent prompts to recall and some led the interview completely themselves. Our respondents wanted to be investigated as unique cases rather than an instance of a category with a repetitive pattern. Hence, we evaluate
the episodic narrative interview as a suitable method for addressing our research question and target group.

Despite the advantages of our method in addressing such a sensitive topic, we would like to encourage HCI practitioners to apply research methods in which victims can have a more active role in the research and design process. Our experience with the victims showed, that each of them was a naive researcher of their case. They usually investigated their cases themselves and were already aware of the social engineering used against them and could easily compare and evaluate their countermeasures. Hence, we recommend the application of more creative participatory research and design techniques, like future workshops, to give them the opportunity to contribute more to the research project by building communities in which mutual learning, exchange and finding a joint solution are possible.

6.3 Towards designing for digital resilience

Like previous studies on phishing simulations, our study on behavioural changes of the victims showed that the exposure of users to cybercrime increases their digital resilience [50]. Interestingly, those victims who did not suffer from dramatic costs (e.g. Frieda and Ian) referred to their experience as valuable warnings that act as a basis for building digital resilience. Following this perspective, we argue for low-cost risk exposures as vaccination for the users. If the damage is controlled a minimal and weak cybercrime exposure, which can be defeated by normal users can build immunity against bigger security issues in the future. In this context, the exact stimulation of cybercrime, as it was conducted by Jansson et al. [50] might cause undesirable feelings such as sadness and dissatisfaction of the users. When practiced in a longer period, this approach can be seen as a virus break-out which requires a non-stop defence mode of the society, overwhelming, stressful and counterproductive. Thus, we would like to suggest a more harmless approach in building cybersecurity incidents than using products such as PhishMe which target employees’ business email address to phish their awareness in a simulated environment.

6.4 Limitations and future work

Like any research study, this work also was affected by some limitations and difficulties, some of which will be addressed in the following.

First of all, due to the sensitivity of the research question and the social pressure on the victims, we were restricted in accessing suitable interview partners and had to snowball method combined with a
convenience sampling technique. Moreover, the inconveniences of this access left us no choice but to consider those types of cybercrime, which have been experienced by our sample pool.

Secondly, as participants were narrating retrospectively the details and order of different elements might be manipulated and biased by memory flaws and wrong interpretations rather than the exact facts and information.

Moreover, some specific aspects of our study e.g. comparison of self-blaming in offline and online crime interviews need to be investigated with a larger number of participants who have experienced both of these crime types.

In the future, we would like to investigate the applicability of the denial theory to other contexts like exposures to other unpleasant, unprobeable and unknown abstract incidents. We would also like to find out, if we can intervene in this cycle and provide specific support against the manipulation of social engineering. Furthermore, the applicability of our design implication should be tested in practice.
References


References


References


[73] Cross, Cassandra (2013) “Nobody’s holding a gun to your head...” examining current discourses surrounding victims of online fraud


References


[121] APIs and How They Work in Amazon Web Services. *dummies*.


**Confirmation**

Hereby I confirm that I have composed the present thesis independently. I have used the sources and means specified in the thesis. Especially from the internet, I only have used the denoted references. I have taken note of the section in the examination regulations concerning attempts to cheat. I confirm that the electronic version of thesis which I deliver is identical to the printed version with respect to the content. I agree that an electronic version of the thesis will be stored for purpose of inspection of plagiarism.

__________________________  ________________________
(Date)                      (Signature)
Appendix

A: Declaration of Consent

B: Interview Guide

- Request a story about the whole incident
  Tell me what happened, I would not interrupt you and just want to hear your story, tell me when the story is finished

- Request a story about an episode
  1. Before the incident
     How would you describe your online behavior before the incident?
     How would you describe your knowledge and past experiences?
  2. During the incident
     How would you describe your reaction? (describe what you did as you were affected by the crime step by step)
     How would you describe your emotional state?
  3. After the incident
     How would you describe the consequences of the incidents and the long-lasting effects?
     Describe your online behavior now, did you change?

- Definition of the phenomenon
  1. Denial phase
     Does it apply to you? How?
  2. Victims’ blaming and self-blaming
     Who did you talk to about your experience? How did they react? What did you expect?
     Did you blame yourself? Why?
  3. Online vs. Offline crime
     Do you have experience with an offline crime? If yes, describe the differences in consequences for me.

- Semi-structured questions
  Demographic information
  Do you have any help suggestions?
  Do have any other ideas, which can help us?