Executive Master Cybersecurity: Thesis

The influence of human behaviour on cybercrime

Eline Hoogendoorn (s1033093)

e.s.hoogendoorn@umail.leidenuniv.nl

The Hague Security Delta / Universiteit Leiden

January 13, 2021

Preface

In front of you lies my thesis of the Executive Master Cybersecurity. I participated this course with great pleasure from 2019 to 2021, meeting many interesting people and made some close friends. For this experience, I am very grateful. Before the thesis starts, I would like to thank a few important persons that helped me throughout the process of writing this thesis.

First, I would like to express my gratitude to my supervisor Tommy van Steen. Without his guidance, the critical point of view and the supportive feedback, this thesis would not be at the level it has ended up. This acknowledgement also applies to Els van de Busser, the second supervisor of my research, for giving me her feedback and for taking the time to speak with me whenever I wanted to know if I was on the right track. Lastly, I would like to thank Chantal de Groot, for the clear answers to all my questions throughout the whole course and especially at the ending of this Master. Nevertheless, not only the supervisors of the Universiteit Leiden had a great, professional deal in this achievement. Two of my fellow students that I got to know very closely during this course, mainly helped me personally through the process of this thesis, which was not always an easy way to take. Therefore, I would like to thank Jacqueline Houweling and Rachid Loesink for their encouragements and pats on the back whenever I needed it the most.

I would also like to thank my manager, who always supported me with attending this Master and was tremendously flexible about my working hours when I was writing my thesis. This also applies to multiple colleagues, who not only attended immediately the digital survey the minute I published it, but who also were always interested in my research and were willing to talk whenever this was necessarily.

Lastly, I would like to thank my partner Rens de Groot for his unconditional support and patience throughout the process. Without him, I probably would not have found the motivation to achieve the ending of this thesis. He being there all the time in our home and providing a diversion whenever I needed it made the process a lot easier to handle.

Table of contents

Abstract

When discussing the concepts of crime and cybercrime, their victims are important key players to understand why these criminal acts takes place. More importantly, with these players taken into account, it is not only possible to understand this concept but also to predict and prevent the crimes that take place. In this thesis, the research focuses on individual victims of cybercrime in the Netherlands and their behavioural characteristics. The aim of this research is to study which behavioural risk factors have a predictive value for victimization, both in the offline as the online world. To answer this question, I designed a digital survey to compare two types of crime; one in the offline world and one in the online world. These two criminal acts have in common that they are comparable with each other, with the only difference that they take place in different worlds. The chosen criminal acts are doorstep scams in the offline world, and phishing in the online world. A scientific literature review, the data collected from the digital questionnaire and the subsequent analysis will answer the sub-questions of this research. It seemed that certain risk factors like socio-economic status, online activities, optimism bias, loneliness, capable guardianship and offline victimization had a significant correlation with victimization. For the factors optimism bias, capable guardianship and loneliness, these results had even a predictive value. Although there is quite an amount of scientific research available on risk factors and victimization, this research shows that there is still not enough knowledge about the behaviour of victims. This is because the studied risk factors have little to do with the actual behaviour of potential victims. Researchers must take a step back to study which existing theories should be better investigated for the existence of other, potential risk factors. With a descent description and formulation of the new risk factors, it would be easier in the future to reduce online and offline victimization based on these risk factors.

1. Introduction

In almost every (scientific) article regarding cybersecurity and cybercrime, authors tend to start their introduction to describe the importance of these new fields and the impact of these types of crime to our upcoming digitized society. My intention with this first sentence is by far not to criticize these renowned authors, on the contrary. However, the statements of these authors remain that cybercrime and cybersecurity are relatively new topics that are often misunderstood by scientists and the society. Their emphasis is still on the importance of putting enough focus on these topics, because the financial and social damages are huge, and rise every year. This remains true, however, the novelty and originality of these subjects is in the meantime hard to find. Fortunate, in the last few years the field has shifted from the debate above to a deeper exploration of offending and victimization of cybercrime (Bossler, 2019).

In addition, this is not the only shift in this field. Crimes that are committed in cyberspace often imply that computer- or IT-specialists should use their specific knowledge to improve cybersecurity and -safety to prevent crimes to occur. However, scientists are beginning to realize that the human side is even (and maybe more) important to investigate. For that reason, there is in the last decade another shift in the vision on which particular scientists should approach cybersecurity; instead of IT-specialists, for instance, psychologists or sociologists should execute this (Waldrop, 2016). These recent shifts are important, because it opens the possibilities for trying to make cyberspace more secure. It also could be helpful to understand why people are being victim of certain types of cybercrime and how they (should or could) solve their problems. This view on the subject of cybersecurity and cybercrime is consistent with the way we started this course. In the beginning of this Executive Master, it was already been made very clear to us that we should not see the phenomena of cybersecurity from a technological point of view alone. Every time we study this topic and its factors, we need to consider the social and governance layer as well. In this research, I tried to combine these factors to the field to create a view that is relatively new for this particular topic.

Put aside the aforementioned views and new developments for a moment, cyberspace and the Internet remain different worlds to interact than the so-called offline, or physical world. The concepts of time and distance between people are elevated to a whole new level in cyberspace; individuals experience far-reaching possibilities to interact with each other on a widespread platform where anonymity is the most important and common factor. This anonymity is part of the social psychology concept of deindividuation, which explains the increasing contribution to criminal acts in the digital world (Meško, 2018). Another relevant theory that emphasizes important characteristics of cyberspace is the digital drift theory. This theory, developed by Goldsmith & Brewer (2015), claims that it is easier for individuals to participate in criminal behaviour because of the majority of opportunities the Internet provides.

When discussing the concepts of crime and cybercrime, both their offenders and victims are important key players to understand why (cyber)crime takes place. More importantly, with these players taken into account, it is not only possible to understand this concept but also to manage to predict and prevent the crimes that take place. To do this, we need to figure out how offenders and victims think, how they behave and what their motives are to make specific choices that can lead into offending or victimization. It would therefore be very interesting to both study the offenders and victims at the same time to define how they act when crimes take place and if and how mutual interactions exist. It is however too big of a challenge for this research to fully analyze the characteristics of these very different key players. The motives of offenders to commit crimes are far

different from the reasons that victims are involved. That is why for now the focus of this research is on only one of the two players; the (potential) victims. Added to this, both in traditional as digitally related criminological theories the importance of offenders are mainly the scope of various studies (Aarten, 2018). That is not a strange development on its own; when you find out what the motives of the offenders are the possibility exists that you could pull them out of the world of (cyber)crime, which can lead to the disappearance of victims. The importance of victims should however not be put into the background (van de Weijer & Leukfeldt, 2017). For this very reason, I chose to investigate the (potential) victims of traditional crime and cybercrime in this research. Another reason to study these individuals is that the amount of participants of the conducted survey would be larger when looking at these (potential) victims. When looking at the most recent statistics of victimization in the Netherlands, reported annually in the Dutch Veiligheidsmonitor, there is an interesting development compared to previous years. Where the number of victims in the Netherlands decreased in 2019 for traditional (offline) forms of crime, an increase in the number of victims for cybercrime was measured in that same year (Centraal Bureau voor de Statistiek, 2020). However not yet proven, there is a possibility that the offenders and/or victims shifted from one field to another. It is interesting to investigate if the same persons that first were victims of traditional crime have shifted to victimization of cybercrime.

This research focuses on individual victims of cybercrime in the Netherlands. In the Western countries, the criminal justice system founds it origin in the fundaments of the Classical School (Bossler, 2019). The justice system obviously has developed over time with including digitized criminal acts in the law. The purpose of the Classical School, however, remains steady to this very day. The primary goal of this purpose is to deter offenders and to set an example to other, potential perpetrators by giving a severe and certain punishment. This so-called deterrence theory provides indeed fundamental and proven arguments, but does on the other hand not take into account that certain threats will not have the same effect in cyberspace because of the anonymity afforded by the Internet, something that decreases the certainty to get caught. Rather, it is the informal sanction that indicate emotions of guilt, embarrassment or judgements of other individuals as inhibiting factors (Pratt et al., 2006).

When we are discussing cybercrime, we also focus on the definition the authorities in the Netherlands use. In this country, there is a distinguished definition with a difference between cybercrime and digitalized crime. Cybercrime is described as any criminal act where computers, information systems and telecommunication are both being used as an instrument as aimed as target for the crime. Digitalized crimes are on the other hand crimes that already existed in the traditional way, where the implementation is executed with IT as a means (Boekhoorn, 2019). Subsequently to this, there is also a clear distinction in cybercrime between cyber-enabled crimes and cyber-dependent crimes (van de Weijer & Leukfeldt, 2017). Cyber-enabled crimes are crimes where IT only facilitates the offender to commit the crime, for example cyberfraud (Holt & Bossler, 2014). Cyber-dependent crimes are on the other hand offences that are new to the field and depend completely on IT; without the use of IT, the crime could not be committed in the first place (Leukfeldt, 2017). In this research, the focus will be on the latter form of cybercrime.

In our societies, it is almost unthinkable not to mention cybersecurity and cybercrime in the same sentence. We understand more and more that bad things can happen, due to not only errors in technologies, but also when individuals (or potential victims) do not handle this ‘power’ responsibly. Human (f)actors play therefore an important role in cybersecurity (Hadlington, 2017). For this very reason, scientists of different fields start to investigate more and more the human behaviour and potential risk factors of offending and victimization in cybercrime. It is my opinion, however, that these

scientists do not seem to give enough credits to the research that already exists on the topic in the offline world. This new focus on the human behaviour and potential risk factors in cybercrime resulted in a reduced interest in the field of traditional crime, while the foundation of our knowledge lies within these studies and the existing literature. Offline victimization exists a lot longer than online victimization, and for that reason, researchers are studying this field much more often than online victimization. Due to this long trajectory of research into offline victimization throughout the years, several studies were conducted multiple times to decrease potential limitations as much as possible. This recommends at least studying the methodology of these offline victimization studies and considering these research designs for studies that include online victimization. Admittedly, some research suggests that there were no similarities trying to compare the offline and online field, because we are dealing with two very different worlds. In this thesis, I would like to state that these worlds are more similar than most scholars think when it comes to the aspects of criminalization. When we look closer to the concerning aspects in the offline world it is my opinion that we will be able to detect previously undiscovered connections.

1.1 Thesis subject

The subject of this thesis is the human behaviour in cybercrime. More in particular, this study focuses on behavioural characteristics of (potential) victims in the Netherlands. The aim of this research is to study which behavioural risk factors have a predictive value for victimization, both in the offline as the online world. In the end, I would hereby like to answer the question if the occurring of cybercrime is predictable and maybe even preventable, if we closely understand the behaviour of its victims, and to what extent cybercrime differs from traditional crime. Do we really need new criminological theories, or can we rely on the existing theories that apply in the offline world for an effective approach? To answer all these questions, I designed a survey to compare two types of crime, one in the offline world and one in the online world. These two criminal acts have in common that they are comparable with each other, with the only difference that they take place in different worlds. The chosen criminal acts are doorstep scams in the offline world, and phishing in the online world. These two crimes have in common that the aim is to steal personal items of the victims; physical items are the target of doorstep scammers and digital items for phishing offenders. In Chapter 2, a further explanation will provide the definitions and backgrounds of these criminal acts. Before we dive deeper however, it is important to specify the questions this study will hopefully answer at the end of this thesis. In this light, the following main question is important to answer: *Are the behavioural risk factors, related to victims of doorstep scams and to victims of phishing similar to each other, and which behavioural change methods can we propose?* Using a literature review and a digital survey to answer this question properly, I formulated the following sub-questions:

1. Which (behavioural) risk factors occur for (potential) victims of phishing?
2. Which (behavioural) risk factors occur for (potential) victims of doorstep scams?
3. Looking at the (behavioural) risk factors, does victimization of doorstep scams relate to victimization of phishing?
4. Is the behaviour of victims and the occurring of these types of offline and online crimes predictable and even preventable?

The data collected from the digital questionnaire and the subsequent analysis will answer the first three sub-questions. The fourth question, however, arises from the results of the survey and are part

of the discussion of this study. The answer to this last sub-question circles back to the previously mentioned theories and the existence of behavioural change methods.

Before answering these questions, it is important to define a clear scope and formulate different kinds of definitions used in this study. This research focuses on individual victims of cybercrime in the Netherlands. However, the time frame of this research also deserves some attention before commencing to this research. The writing of this thesis started in 2020, amid the pandemic and the outbreak of the coronavirus. As later reports endorse, this pandemic has an effect on the way criminals act (Europol, 2020). Research suggests that criminals changed their modus operandi; the number of burglaries decreased, and criminals would focus more on the online world in which they find themselves. The expectation is this change of certain criminal acts and behaviour also applies to victims. We need to consider this knowledge and these developments during this study, as in the results and conclusion of this thesis.

In the next chapter, an explanation follows of the theoretical framework of used definitions, risk factors, and theories, reviewing the existing scientific literature. The independent variables of this study will derive from the studied risk factors. Chapter 3 provides an explanation about the methodology and the research design of this study. Following the findings, I will analyze the results of the conducted survey in the fourth chapter with a comparison between the factors found. In the last chapter, I will study whether there is a relationship between the (behavioural) risk factors and victimization of traditional crime and cybercrime. Before moving on to the second chapter, the following paragraph will first describe the occurring problem and the relevance for this thesis.

1.2 Problem statement and relevance

During the course 'Actors and Behaviour in Cyberspace' of this Master, I wrote a paper on the under-reporting of cybercrime by individual victims (Hoogendoorn, 2020). In this paper, I studied the possible influence of behavioural change methods on whether or not individual victims would report an act of cybercrime. However, this research concluded that the focus of behavioural change methods rely mostly on the traditional forms of crime instead of cybercrime, which made this research a bit of a challenge. Therefore, I want to study the possibilities of behavioural change methods on crimes in the digital space as well.

Each year, the statistics of cybervictimization[1] jumps to new records. Where in 2018 the percentage of victims of one or multiple types of cybercrime included 8.5% of the population, in 2019 the percentage increased to 13%. For phishing, the percentage of victims in 2019 contained 0.4% of the Dutch population (Centraal Bureau voor de Statistiek, 2020). In addition, according to the Dutch Association of Banks, the financial costs for phishing amounted to €8.38 million in 2019, against €3.81 million in 2018 (Nederlandse Vereniging van Banken, 2020). These percentages and costs are probably even higher, because of the aforementioned presence of under-reporting (Boekhoorn, 2019). It is, however, not only the dark number that hides in cybervictimization, but also the existence of a dark figure. This dark figure includes offending, victimization and the extent of the damage. This means that existing statistics from official organizations do not match the actual numbers in real life (Leukfeldt, 2017). In addition to this, the financial costs of cybercrime are €10 billion annually in the Netherlands (Groot, 2017). With a better understanding of the behaviour of victims it is possible to prevent a successful criminal attack and therefore decrease the financial costs.

[1] The definition of cybercrime according to Statistics Netherlands includes crimes that are related to the Internet or other digital information objects (Centraal Bureau voor de Statistiek, 2020).

Not only is the amount of victims of cybercrime expanding, but with the rise of this number, the chance of becoming an offender of cybercrime increases as well. Research suggests that victimization could also lead to committing crimes (Bossler, 2019). When a person has become a victim of cyberbullying, for example, it increases the possibility that this same victim will also commit an act of cyberbullying in the future. According to that same research, cyberbullying victimization may have a larger impact on future offending than physical bullying victimization. One of the most consistent predictors of cybervictimization is thus the participating in cyber-offending.

When looking at the existing scientific literature, there is without a doubt research that focuses on victims and predictive risk factors. The downside of these studies is that they only include adolescents or a younger sample in their research. To my knowledge, no previous research exists that reflects the entire Dutch population in combination with victimization. Furthermore, comparative studies are available between multiple criminal acts and victimization (Leukfeldt, 2015; Wilsem, 2013). Despite the scientific relevance and the promising conclusions these studies had, the main flaw is that these researches only compared two types of cybercrime. As stated above, it is equally interesting to compare traditional, offline crime with cybercrime using all of the corresponding theories and risk factors. That is why I want to expand the focus in this thesis back to the traditional, offline world of criminalization.

2. Theoretical framework

This second chapter describes the existing criminological theories that include a vision on victimization. When looking at cybercrime from a theoretical point of view, there are two different approaches. The first approach sees cybercrime as a completely self-contained type of crime that requires the elaboration of new criminological theories to understand the different factors, for example the Space Transition Theory (Meško, 2018). This theory focuses on offenders of cybercrime and states that the characteristics of cyberspace and the Internet plays an important role in the motivation to commit crimes in cyberspace. To quote Leukfeldt & Yar (2016): "The well-known traditional criminological explanations are therefore not fully applicable for explaining and understanding cybercrime victimization. Even though criminological interpretations prove to be useful for explaining the reasons leading to cybercrime, the applicability of such interpretations in determining the likelihood of cybercrime remain dubious." The second theoretical approach state, however, that cybercrime is merely a disguise of well-known criminal acts, which is why we use existing explanations of crime for their interpretation (Meško, 2018). In a search for the possibility of the appliance of traditional criminological theories to cybercrime (both offending and victimization), results showed that these theories could explain the commission of crime and deviance behaviour in cyberspace as well as they do in the physical world (Bossler, 2019). These findings mainly applied on the theories on an individual level, like the Routine Activity Theory and the General Theory of Crime. Researchers use these theories often to explain why some people are more likely to become a victim of cybercrime than others (van de Weijer, 2019).

2.1 Routine Activity Theory

Lawrence Cohen and Marcus Felson created the Routine Activity Theory in 1979. This situational theory provided the scientific community with three factors that contribute to commit to criminal behaviour: a motivated offender, a suitable target and the absence of capable guardianship (Cohen & Felson, 1979). The chapter about the methodology and research design will further discuss one of these factors, where I will explain the questions in the digital survey in relation to this factor. This further explanation also applies to the factors that Felson & Clarke (1998) developed based on the Routine Activity Theory. In their research, they built four elements on to the motivated offender and the suitable target, which answers the question why a victim could be appealing: with value, inertia, visibility and accessibility (Felson & Clarke, 1998). In the last decades, multiple scholars used the Routine Activity Theory as "a useful framework to study cybercrime victimization" (Bossler, 2019). This theory not only explains why crime occurs, but also has started to develop an explanation why individuals could become victims of (cyber)crime. The most important factor for reducing victimization is the impact of the capable guardianship (Leukfeldt & Yar, 2016). According to this research, the visibility-element clearly plays a role within cybercrime victimization. Another important conclusion regarding the factors of the Routine Activity Theory is that the presence of a (technical) capable guardian decreased the change on becoming a victim. This conclusion, however, only applied to college students in combination with a computer virus (Choi, 2008).

Hutchings and Hayes (2009) conducted a research among residents of Brisbane Metropolitan area (*N*=104). They applied the Routine Activity Theory to phishing and concluded that the activities of computer use and online banking increased the likelihood to become a victim of phishing. To establish if there are further certain risk factors that play a particular role in the victimization of cybercrime, Dr. Rutger Leukfeldt also conducted a research in 2014 on phishing victimization and the

Routine Activity Theory in the Netherlands (*N*=8,379). In his research, he studied several factors that could lead to an increased risk to victimization (Leukfeldt, 2014). Not one factor, however, was decisive enough for an increased risk to pinpoint at victimization. This same conclusion also was drawn in the research of Ngo and Paternoster (2011) when they studied victims (*N*=295) of seven types of cybercrime, including phishing. In a study performed in 2019, Weulen Kranenbarg, Holt and Van Gelder made a comparison between offenders, victims and victim-offenders of both cybercrime and traditional crime. The goal of this research was to conclude to what extent existing risk factors, like routine activities, could explain cybercrime offending and victimization in a way similar to traditional crime. The focus on this research was mainly on the overlap between victimization-offending.

2.2 General Theory of Crime

A few decades ago, two authors introduced the criminological community with the General Theory of Crime (Gottfredson & Hirschi, 1990). This theory focuses on the personality traits of, at that time, offenders of traditional crime. They studied the degree of self-control and concluded that low self-control increased the risk of criminal behaviour. Multiple years later, scholars still use this theory to not only for explaining the existence of cybercrime, but also for an interpretation of how individuals become victims (Bossler, 2019). Research shows that the relation between low self-control and victimization in the physical world also applies in the online world. Several studies have examined self-control among victims of different types of cybercrime. These studies also show that individuals with lower levels of self-control are more likely to become a victim of cybercrime (van de Weijer & Leukfeldt, 2017).

Scholars have shown that low self-control empirically relates to cybercrime victimization and which my occur more in large phishing attempts. Bossler & Holt (2010) found a mediated effect of low self-control on cybervictimization by delinquent peers, meaning “having low self-control increased a person’s interest in associating with delinquent peers who possibly victimized the person or placed them in risky situations that made them more vulnerable. The results of this study show that low self-control and time spent on online activities significantly relates with online victimization risk.”

2.3 Phishing and doorstep scams

In the research of my thesis, I chose to investigate two specific and both similar criminal acts: phishing as a digital crime and doorstep scams as a traditional crime. The reasons this study focused on these types of crimes, is that mainly the digital equivalent is a type of crime that can occur to almost everyone. Research suggests that everybody is at risk when it comes to phishing victimization (Leukfeldt, 2014). Phishing is a form of theft, which uses personal information of potential victims like usernames, passwords or banking information to gain access to their personal, online accounts. By using digital means such as emails or text messages, offenders pretend to be part of a trusted authority forcing users to click on a link that redirects them to a false website and login (Leukfeldt, 2014). According to another research by Leukfeldt (2015), there are two types of phishing: high-tech and low-tech. With high-tech phishing, the perpetrator uses malicious software to get to the personal information. With low-tech phishing, they use emails, texts or telephone calls to achieve this goal. In this research, the focus is on the latter form of phishing.

The second form of the criminal acts I chose to study are doorstep scams (in Dutch called the “babbeltruc”). The goal of doorstep scammers is the same as for phishing: to gain access to a person’s

life to steal personal items of that individual. Instead of doing this in a virtual world, the doorstep scammers literally show up at the physical doorstep of potential victims and pretend to be someone they are not to gain access in the residence (Noordenburg, 2020a). Most of the victims are elderly and are older than the age of 65 (van der Lubbe et. al., 2019). Furthermore, there is a distinction between three types of doorstep scams. The first one includes a perpetrator that claims he or she is working at a specific company or organization, like the postal company or a trusted organization like the police. The second form of a doorstep scam is when the person relies on social interactions instead of business ones. They are claiming to be a new neighbor for instance that wants to get acquainted. In the last form of the doorstep scam, perpetrators focus on the trust of people by pretending to have an urgent problem and that they are in need of help immediately (Noordenburg, 2020a). When we study the first, business form of these three categories, a new example comes up. Because of the outbreak of the coronavirus, perpetrators abuse the fear that people have of their health and the missing knowledge of the pandemic, to gain access into their houses. They pretend to be healthcare workers and scare people by stating, for example, that they must disinfect their house due to dangerous corona substances (Opgelicht, 2020). Since the rise of the amount of victims due to the coronavirus and the high (emotional) impact it has, "various campaigns in the Netherlands try to educate people in this topic in order to prevent doorsteps scams from happening. Such campaigns focus at behavioural aspects of the prevention of doorstep scams. A specific skill that is beneficial for the resilience against doorstep scams is assertiveness: behaving confident and daring to say what you think or believe" (van der Lubbe et. al., 2019).

2.4 Behavioural change methods

With behavioural change methods, it is possible to alter the behaviour of victims in their decision-making. These behavioural change methods are common to use in healthcare (Agha et. al., 2019). In addition to this research, it is interesting to discuss whether these behavioural change methods and the including theories could prevent potential victims to become a part of phishing or doorstep scams. According to the Fogg Behaviour Model (FBM), there are three important aspects that contribute to the change of behaviour: motivation, ability and triggers (Fogg, 2009). With the absence of one or multiple factors, the likelihood of adopting a behaviour decreases. In a recent study, van der Lubbe and colleagues examined the effects of Game Learning Theory to doorstep scams to prevent them of making additional victims (van der Lubbe et. al., 2019). They developed a serious game to address the dangers that lies in doorsteps scams and to study if this approach influences the future behaviour of potential victims, reducing the likelihood of victimization.

Another example to influence individual behaviour is with the use of awareness campaigns. The most common causes of cybercrime victimization include poor awareness of the threats in cyberspace and insufficient self-protection measures (Meško, 2018). For both phishing as for doorstep scams, the Dutch government has invested in multiple awareness campaigns over the years to increase the knowledge of the dangers. These campaigns teach us citizens what to look out for when it comes to these criminal acts and provide us with clear examples of factors that can contribute to becoming a victim. In 2018, famous Dutch comedian André van Duin joined an awareness campaign for the elderly to increase the awareness of doorstep scams (Politie, 2018). Furthermore, in September this year, the authorities launched a campaign that warns us for the dangers of phishing (Noordenburg, 2020b). The question for these campaigns that rises is to what extent individuals adopt these kind of messages from the authorities. The Psychological Reactance Theory, for instance, presumes that "individuals

have their own behavioural freedom and that any perceived restriction or adaption of their freedom triggers resistance, which manifests in behaviour opposite to the desired behaviour" (Miron & Brehm, 2006).

2.5 Risk factors

Based on the theoretical framework and theories described above, a selection of risk factors is made to examine in this research. Categorized by online and offline victimization, I will describe briefly the expectations between these risk factors and victimization, according to the literature (see Appendix 2 and Appendix 3 for a summarization of the risk factors). The first risk factors concern demographics about the potential victims in the online and offline world. According to multiple studies, females, younger people and higher educated people are more likely to become a victim (Meško, 2018; Leukfeldt & Yar, 2016; van Wilsem, 2013). The second type of risk factors concerns the online activities. According to the Routine Activity Theory and several studies following up on these online activities, the more hours a person will spend on the Internet, the higher the chance of becoming a victim of cybercrime (Leukfeldt & Yar, 2016; van Wilsem, 2013). This theory not only includes online activities, it also describes the presence of a capable guardian. This developed to a physical guardianship in the modern, online world, and indicates that the presence of security measures could lower the chance of becoming a victim in the online world (van Wilsem, 2013). Another theory describing risk factors is the General Theory of Crime, which states that a low amount of self-control increases the likelihood on victimization, both for traditional crime as for cybercrime (Bossler, 2019; van de Weijer & Leukfeldt, 2017; Bossler & Holt 2010).

According to Meško (2018), optimism bias also could have an effect on the victimization in the online world. This phenomena indicates that a specific person feels he or she has nothing to fear regarding dangers on the Internet and are smart enough to recognize these dangers. This bias, however, can lead to the exact opposite and increase the victimization in the online world. Another studied risk factor for victimization in the online world is offline victimization. Research suggests that people who experienced victimization earlier in their physical environment, are more likely to become a victim in the online world as well (Leukfeldt, 2015). Lastly, offline activities were included in this research. People who spend more time in places where crimes take place, are more at risk of being victimized in the offline world (Weulen Kranenbarg, Holt & van Gelder, 2014).

Two risk factors which were not directly associated with victimization are included in this study as well. There are minimal empirical studies available about the feelings of shame and loneliness in relation to victimization. According to Irwin et. al., there is a relation between cyberoffending and feelings of shame (2019), and feelings of shame played a role at the continuation of victimization. However, this research could not prove that shame existed as an actual risk factor. The role of shame is, however, studied as a reason to report a crime when certain people were victimized (Meško, 2018). The second risk factor conducted in this research for the first time, is loneliness. Again, several studies included loneliness in their research to (cyber)criminals, who experienced loneliness and for this reason (among other things), started their criminal activities (Webber & Yip, 2019). In addition to this, the research of Zimmer-Gembeck et. al. (2014), concluded that adolescents scored higher in relational victimization when they reported more loneliness.

3. Methodology

3.1 Participants

This part of the thesis describes the methodology and the research design of the study. Data collected for this study comes from the scientific literature review and the answers of (potential) victims of doorstep scams and phishing through a digital survey. I developed this digital survey in Dutch in the online program *Qualtrics* that was available by the University of Leiden. The collected data then was exported to the statistic application *SPSS* to analyze the data. The digital survey combines qualitative with quantitative findings to answer the aforementioned research questions from Chapter 1. The questions asked in the digital survey are at the end of this survey in Appendix 1.

An amount of 125 respondents was included in the analysis of this research in total. These respondents had completed the questionnaire; the respondents that did not do that were excluded from this research. In total, 65 males (52%) were part of the survey next to 60 female respondents (48%) with an average of 40 years (*SD*=11.7) in the range of 23 to 69 years. The education level originally consisted of nine answer possibilities, but after recoding in *SPSS* using the *Transform*-function, three new categories emerged. Based on Statistics Netherlands (Centraal Bureau voor de Statistiek, 2018), the nine possible answers on Question 3: '*What is your highest level of education*?', were classified into three new categories. The elementary, pre-vocational and secondary education fell into the category of lower education, the vocational education in medium education and the scientific education in higher education. 11 respondents (8.8%) were lower educated, 29 respondents (23.2%) medium and the majority of the respondents (68%) had a higher education level.

3.2 Measures

The dependent variables of this thesis are victimization in general, online and offline victimization, and the (perceived) victimization of doorstep scams and phishing. All but potential victimization of doorstep scams and phishing variables were coded dichotomously (0 = 'no victim'; 1 = 'victim'). The variables of potential victimization of doorstep scams and phishing had an interval ratio; the higher the score, the higher the chance of becoming a potential victim. Actual victimization in general and online and offline victimization in general were answered in *Question 10*: '*Have you ever been a victim of crime? And if so, did this type of crime occur in the offline, online or both the offline and online world?*'. This question and its four possible answers were then recoded into SPSS using the *Transform*-function into a new variable called *Victimization*, where the options were minimized to '*Yes'* and '*No'* (0 = 'no victim'; 1 = 'victim'). Of the 125 respondents in total, 53 respondents (42.4%) answered this question with '*Yes'*. When we look more in depth to these answers, 33 of the respondents (26.4%) indicated these crimes happened in the offline world, 13 crimes (10.4%) occurred in the online world and 5.6% of the respondents were victim in both the offline as the online world. The four answer possibilities were also recoded into two other variables called *VictimOffline* and *VictimOnline*.

Later in the survey, respondents received the question whether they had ever been in contact specifically with phishing or doorstep scams in *Questions 14* and *23*: '*Based on the above definition, have you ever been in contact with a doorstep scam / phishing?*'. 115 of the respondents (92%) answered this question with '*Yes'* for phishing, and only four respondents (3.2%) for doorstep scams. Compared to the previous finding, where only 40 respondents in total answered the question positively if they ever were a victim in the online world in general, the finding of 115 respondents

answered '*Yes'* on phishing is interesting. This brings us to the assumption that most of the respondents do not link victimization to only receiving a phishingstext or -mail. By further research, it appears that six respondents (4.8%) actually fell for the phishing-text or -mail in *Question 24*, next to 0 respondents for doorstep scam in *Question 15*. These questions only became visible when they were answered positively in the previous question about getting in contact with phishing or doorstep scams.

Next to the actual victimization in general and the actual victimization of phishing and of doorstep scams, this study also focused on the perceived victimization of doorstep scams and phishing. This because the assumption from the researcher that especially for doorstep scams, the actual victimization by questioning the respondents would be quite low. This was in fact also the case. To establish the potential victimization, the respondents first were presented with two scenarios in *Questions 12* and *13*: one where a doorstep scammer stood at the (virtual) door and one where the respondents received an email from the Dutch Rabobank. In both scenarios, the respondents could indicate how likely they were to fall for the doorstep scammer or the phishingsmail, without knowing at that point that they were being phished or scammed. The respondents could answer eight thesis in total on a seven-point scale from 1 being '*Very unlikely'* to 7 being '*Very likely*'.

3.2.1 Potential victimization for doorstep scam

First, the respondents saw a scenario where a female employee from the Common Health Service ("Gemeentelijke Gezondheidsdienst" in Dutch) ringed the door and said she was going around the neighborhood to spread important information about the local corona measures. This case was based on the fact that during the COVID-19 pandemic, multiple so-called employees of health care organizations were using the fear of (older) people to gain access in their house with the ultimate goal to steal something. In this scenario, the woman asked the person if she could come in for a moment to explain a few things about the recent corona measures. For this doorstep scam scenario, there were three statements where respondents could reply with an answer from '*Very unlikely'* to '*Very likely*'. They were introduced with the question: '*How likely are the following statements for you in this scenario?*'. The first statement was: *'I invite the woman into my house'*, the second statement: *'I will call the organization of the Common Health Service to inquire about sending the woman'* and the third statement was: *'I will send the woman away'.* The first statement is obviously the undesired one; by letting the woman in the respondents increased the chance of becoming a victim of the doorstep scam. The second and third statement were the desired ones; by calling the Common Health Service or sending the woman away, the chance of being a victim of doorstep scam will be close to zero.

For the first statement, the higher the score, the higher the chance of being a victim; a score of 7 means that the respondent is very likely to let the woman in, which increases the chance of being a potential victim of theft. For the second and third statement, this was not yet the case. For these statements, the higher the score, the lower the chance of being a potential victim; a score of 7 originally means that the respondent is very likely to call the organization or send the woman away, which decreases the chance of being a potential victim. For these statements, it was necessarily to first reverse the scoring to align the direction with the first statement. The two variables in SPSS that emerged from the second and third statement were recoded in SPSS using the *Transform*-function, with new labels signed to these variables that were exactly the other way around. After this, the direction for the second and third statements were the same as for the first statement; the higher the score, the higher the chance of becoming a potential victim (see Table 1 for an example).

Table 1

Example of reverse coding for doorstep scam 'I will send the woman away' (N=125)

Scale originally	**Frequency**	**Scale after reverse coding**	**Frequency**
1 Very unlikely	3	1 Very likely	50
2 Unlikely	3	2 Likely	38
3 Fairly unlikely	6	3 Fairly likely	18
4 Neutral	7	4 Neutral	7
5 Fairly likely	18	5 Fairly unlikely	6
6 Likely	38	6 Unlikely	3
7 Very likely	50	7 Very unlikely	3

After this, a reliability test in *SPSS* was executed by studying the *Cronbach's Alpha*. With $\alpha >$ .70, the alpha is valuable. However, when they are less than 10 items, $\alpha >$ .50 is also acceptable. The use of this reliability test is to determine the reliability of the questionnaire and to measure the degree of coherence between the three survey questions. A prerequisite for this test is to check whether the questions were measured the same way. In the previous step, this prerequisite is established using recoding in *SPSS*. After running the test in the *Analyze*-menu, the *Cronbach's Alpha* was $\alpha =$ .230, which is < .50 and therefore not useable for the following tests, with an *Inter-Item Correlation* of *M*=.165. When this happens, it is wise to look at the column of *Cronbach's Alpha if Item Deleted.* When the value of a specific cell is higher than the *Cronbach's Alpha*, the advice is to delete the regarding survey question out of the definitive variable. In this scenario, the second statement of calling the Common Health Service had a value of $\alpha =$ .651 in the column *Cronbach's Alpha if Item Deleted.* When deleting this item and testing the *Cronbach's Alpha* again, the $\alpha =$ .651, which is $\alpha >$ .50 for less than 10 items and therefore useable for further testing. For this reason, there was decided to work only with the two remaining items and delete the statement about calling the Common Health Service. The other two items were then put together using the *Transform*-function. By computing the two variables, the sum of the value of these two items created a new variable. The higher the score of this variable, the higher the chance of victimization. These scores could range from values from 2 to 14; the minimum score was two questions multiplied by the lowest answer of 1, to the maximum score of two questions multiplied by the highest possible answer of 7. Table 2 presents the scores of this variable, which shows that the majority of the respondents had a score of 5 or lower. This means that the majority of the respondents (*N*=105) had a lower chance of becoming a potential victim of doorstep scams.

Table 2

Scores of computed variable 'Potential Victimization Doorstep Scam' (N=125)

Score	Frequency	Percent
2	48	38.4
3	19	15.2
4	23	18.4
5	15	12.0
6	7	5.6
7	2	1.6
8	4	3.2
9	4	3.2
10	1	.8
11	2	1.6

3.2.2 Potential victimization for phishing

In the digital survey, the respondents faced a second scenario where they received an email from the Dutch Rabobank. With the official layout of the Rabobank in the header, this email introduced the receiver with a new type of debit card called the antibacterial debit card. Due to the coronavirus, this new type of card protects its users against the bacteria that can cause corona. The receiver is then asked to follow the link in the email to apply for this debit card. When they apply it in time, the card is completely free, but after the date mentioned, every new request will cost €44,99. The foundation of this scenario was an existing scenario that criminals used in real life to gain access to someone's bank account and steal their money (Kamp, 2020). For this phishing scenario, there were five statements where respondents could again reply with an answer from '*Very unlikely*' to '*Very likely*'. They were introduced with the question: '*How likely are the following statements for you in this scenario?*'. The five following statements were: *'I apply for the debit card by clicking on the link'*, *'I first check the security of the email'*, *'I delete the email'*, '*I move the email to my spam folder*' and: '*I will call the Rabobank to inquire about sending the email*'. The first statement is obviously the undesired one; by clicking on the link in the email, the respondents increased the chance of becoming a victim of phishing. The other four statements were the desired ones; by choosing one of these options, the chance of being a victim of doorstep scam will be close to zero.

For the first statement, the higher the score, the higher the chance of being a victim; a score of 7 means that the respondent is very likely to click on the link, which increases the chance of being a potential victim of theft. For the other four statements, this was not yet the case. For these statements, the higher the score, the lower the chance of being a potential victim; a score of 7 means that the respondent is very likely to call the Rabobank or delete, replace or check the email, which decreases the chance of being a potential victim. For these statements, it was necessarily to first

reverse the scoring to align the direction with the first statement. The four variables in SPSS that emerged from the four statements were recoded in SPSS using the *Transform*-function, with new labels signed to these variables that were exactly the other way around. After this, the direction for the second, third, fourth and fifth statements were the same as for the first statement; the higher the score, the higher the chance of becoming a potential victim (see Table 3 for an example).

Table 3

Example of reverse coding for phishing 'I will call the Rabobank to inquire about sending the email' (N=125)

Scale originally	**Frequency**	**Scale after reverse coding**	**Frequency**
1 Very unlikely	32	1 Very likely	9
2 Unlikely	25	2 Likely	13
3 Fairly unlikely	14	3 Fairly likely	9
4 Neutral	23	4 Neutral	23
5 Fairly likely	9	5 Fairly unlikely	14
6 Likely	13	6 Unlikely	25
7 Very likely	9	7 Very unlikely	32

After this, a test called the *Cronbach's Alpha* in *SPSS* made sure the results had a reliable outcome. With $\alpha > .70$, the Alpha is valuable. However, when they are less than 10 items, $\alpha > .50$ is also acceptable. The reliability test was used to determine the reliability of the questionnaire and measure the degree of coherence between the five survey questions. A prerequisite for this test is to check whether the measurements of the questions were similar. In the previous step, this prerequisite follows from the recoding in *SPSS*. After running the test in the *Analyze*-menu, the *Cronbach's Alpha* was $\alpha = .479$, which is < .50 and therefore not useable for the following tests. The mean of the *Inter-Item Correlations* was $M = .164$. When this happens, it is wise to look at the column of *Cronbach's Alpha if Item Deleted.* When the value of a specific cell is higher than the *Cronbach's Alpha*, the advice is to delete the regarding survey question out of the definitive variable. In this scenario, the statement of deleting the email had a value of $\alpha = .489$ in the column *Cronbach's Alpha if Item Deleted.* When deleting this item and testing the *Cronbach's Alpha* again, the $\alpha = .489$, which is still $\alpha < .50$. By checking the same column for the remaining four statements, the *Cronbach's Alpha if Item Deleted* is the highest for the statement about clicking the link to apply for the debit card. When deleting this item and testing the *Cronbach's Alpha* again, the $\alpha = .522$, which is > .50 for less than 10 items and therefore useable for further testing. For this reason, there was decided to work only with the three remaining items. These three items were then put together using the *Transform*-function. By computing the three variables, the sum of the values of these three items created a new variable. The higher the score of this variable, the higher the chance of victimization. Table 4 presents the scores of this variable.

Table 4

Scores of computed variable 'Potential Victimization Phishing' (N=125)

Score	Frequency	Percent
3	2	1.6
4	5	4.0
5	8	6.4
6	5	4.0
7	7	5.6
8	5	4.0
9	10	8.0
10	8	6.4
11	7	5.6
12	14	11.2
13	6	4.8
14	12	9.6
15	12	9.6
16	4	3.2
17	2	1.6

The behavioural risk factors described earlier in Chapter 2.5 formed the independent variables in this research. In Appendix 2 and Appendix 3, the risk factors for victimization based on the existing literature are further described and divided by the digital and physical components. In both tables, the question numbers and explanations (quotes) are linked to the risk factors to establish where in the questionnaire these factors were asked.

3.2.3 Self-control

One of the risk factors to point out is the amount of self-control. To test if the respondents experienced a high or low amount of self-control, the Grasmick-scale of self-control was used in *Question 32* of the digital survey. In this scale, the 24 statements of Grasmick were formulated which the respondent needed to answer on a 4-points scale (Grasmick et. al., 1993). The score 1 means '*Highly disagree'* and the score 4 means *'Highly agree'*. Table 5 presents the descriptive statistics of self-control of the Grasmick-scale. The higher the score on these statements, the lower the amount of self-control. All measurements for the 24 items for self-control were similar; the higher the score for each item, the lower the self-control. For the analysis, it was easier to reverse the coding, meaning that the higher

the score, the higher the amount of self-control would be. Using the *Transform*-function in *SPSS*, the 24 items were reverse coded into 24 new variables using the formula: *VariableNameReversed=(1+4)-Variable*. Where a respondent first answered with a 1 (meaning '*Highly disagree'*), the score would be turned around to a 4 (still meaning '*Highly disagree*'). This means for the reversed coded items, the higher the score, the higher the amount of self-control is. Using a reliability test (*Cronbach's Alpha*), the alpha was measured as α = .754, which is larger than > .70. Looking at the column *Cronbach's Alpha if Item Deleted*, two variables were larger than the original *Cronbach's Alpha*. When removing the statement about risks: '*I like to test myself every now and then by doing something a little risky*', the *Cronbach's Alpha* is α = .756. In addition, the item about having more energy than peers has still a larger value in the cell *Cronbach's Alpha if Item Deleted*. When deleting this item, the *Cronbach's Alpha* is again a little bit higher with a value of α = .760 and none of the other variables are higher than the *Cronbach's Alpha* if items were deleted. For this reason, I decided to work with an adjusted Grasmick-scale, with not 24 but 22 items. These 22 items were then put together using the *Transform*-function. By computing the 22 variables, the values of these items were summed into a new variable. The higher the score of this variable, the higher the amount of self-control. These scores could range from values from 22 to 88; the minimum score was 22 questions multiplied by the lowest answer of 1, to the maximum score of 22 questions multiplied by the highest possible answer of 4. Table 5 presents the descriptive statistics of the adjusted Grasmick-scale.

Table 5

Descriptive statistics on the adjusted Grasmick-scale for self-control (N=125)

Item	M	SD
Impulsivity		
I often act on the spur of the moment without stopping to think	3.15	.880
I don't devote much thought and effort to preparing for the future	3.05	.822
I often do whatever brings me pleasure here and now, even at the cost of some distant goal	2.94	.821
I'm more concerned with what happens to me in the short run than in the long run	2.87	.793
Simple tasks		
I frequently try to avoid projects that I know will be difficult	2.99	.884
When things get complicated, I tend to quit or withdraw	3.10	.827
The things in life that are easiest to do bring me the most pleasure	2.57	.836
I dislike really hard tasks that stretch my abilities to the limit	3.24	.837
Risk seeking		
Sometimes I will take a risk just for the fun of it	2.85	.890
I sometimes find it exciting to do things for which I might get in trouble	3.52	.747
Excitement and adventure are more important to me than security	3.37	.778
Physical activities		

If I had a choice, I would almost always rather do something physical than something mental	2.76	.797
I almost always feel better when I am on the move than when I am sitting and thinking	2.46	.876
I like to get out and do things more than I like to read or contemplate ideas	2.50	.819
Self-centered		
I try to look out for myself first, even if it means making things difficult for other people	2.91	.823
I'm not very sympathetic to other people when they are having problems	3.53	.642
If things I do upset people, it's their problem not mine	3.36	.734
I will try to get the things I want even when I know it's causing problems for other people	3.12	.736
Temper		
I lose my temper pretty easily	3.01	.857
Often, when I'm angry at people I feel more like hurting them than talking to them about why I am angry	3.72	.590
When I'm really angry, other people better stay away from me	3.02	.971
When I have a serious disagreement with someone, it's usually hard for me to talk calmly about it	2.97	.933

3.3 Procedure

The input for the questionnaire was developed in the tool *Qualtrics* through a review of the existing literature. A combination between different theories and (behavioural) risk factors resulted in a digital survey with a maximum of 44 questions. Depending on how the respondents answered the question, the following questions were automatically deleted or added. The survey started with a landing page that consisted of a short introduction where the researcher introduced herself and gave a short explanation of the goal of the survey. This text also included the information that responding to the survey was anonymous and that the subjects could stop anytime in any part of the survey. After this introduction, respondents received a question to confirm they understood and agreed with the informed consent.

The digital survey was published for over two weeks (November 17, 2020 to December 5, 2020) and was distributed through social media (Facebook and LinkedIn), email and text messages. A potential participant received a personal invitation via email or text messages or could click the link they encountered on Facebook or LinkedIn, with the kind request to participate in my research. After clicking the link in the invitation or on social media, every person landed on the introduction page with the official layout of Leiden University where I introduced myself and explained the purpose of the survey. At the top of the page, the potential respondents could see the progress of the survey with percentages and a blue progress bar. After finishing the introduction, the person must answer the question about the informed consent. By choosing the answer *'Yes',* the person continued the questionnaire. When the person chose '*No*' however, the survey immediately skipped to the end with a message that thanked the respondents for participating, leaving some useful links for phishing and doorstep scams for those who were interested.

After answering the first question positively, the person landed on a new page with the first three questions about demographics. Only the questions regarding age and educational level were

obligated to fill in, the question about gender could be left empty. Whenever respondents did this however, a notification popped up that warned the person that they did not fill in an answer, with the question if they were sure to proceed the questionnaire without answering. The respondents then came to a new page, which presented questions about specific online activities. After this, a new page with statements on online security emerged. After answering these statements, the respondents received questions about victimization, and whether they experienced criminal activities in the offline or online world. On a new page, respondents then received the first fictive scenario about doorstep scams. After the respondent answered the statements regarding this scenario, a second fictive scenario appeared about receiving a phishingsmail. After these scenarios, respondents received a brief introduction into the real subject of this study, with a definition on doorstep scam and phishing. After they finished the questions about the experience of doorstep scams and phishing, the respondents came on a new page where 24 statements appeared about self-control. The last questions were presented on a new page, where respondents had to answer questions about loneliness and offline activities. The questionnaire then ended with a message to thank the respondents for their time and for those who were interested, some useful links about phishing and doorstep scams.

After two and a half weeks, 158 responses were recorded and two responses were still in progress. The 158 responses provided by the website of *Qualtrics* then were exported to the statistical program *SPSS* to further examine and analyze the status of the responses. After further examination, it turned out that 126 respondents (79.4%) completed the full survey. One of the subjects responded with the answer '*No*' to the first question in the informed consent: "*I understand the text above and agree with it.*", which led the respondent automatically to the end of the survey without answering any of the questions. The data of the other remaining respondents was used in this study (*N*=125).

3.4 Analysis strategy

The demographics of respondents were collected with the answers of the first three questions of the survey using the functions *Frequencies* and *Descriptive Statistics* in *SPSS*. In these questions, the respondents were asked to give their gender, age and their highest level of education. In the following questions, the respondents could indicate how many hours they would spend on the Internet per week. First in general, then specified for email, social media, online banking, gather information, gaming, online shopping or other. This to identify the amount of hours they spent on online activities, which is one of the risk factors that could lead to victimization. Next up, there were a few statements given about the online security measures in *Question 6*. The respondents could respond with an answer on a 7-points scale from '*Highly disagree'* to '*Highly agree*'. This question was to investigate whether respondents used security measures and if so, which security measures they had taken to study the presence of capable guardianship. Respondents also received the question whether they had any knowledge of online security and of the dangers online to indicate whether optimism bias would occur among the respondents. In *Question 10*, respondents were asked if they ever had been a victim of crime, and if so, if this occurred in the offline and/or online world.

After these questions, the questionnaire focuses on potential victimization as described in Chapter 3.2.1 and 3.2.2 with two scenarios of doorstep scam and phishing. The choice that there was no introduction yet of definitions of doorstep scam and phishing was a conscious one; by saving these definitions after the scenarios, respondents were less likely to realize that these cases involved criminal behaviour. After answering the statements for the scenarios, respondents landed on a new page where the definition of doorstep scams was introduced: '*In a doorstep scam, the perpetrators will use*

an excuse or lie to talk themselves into a victim's home in order to commit theft'. According to this definition, respondents could indicate if they ever had been in contact with a doorstep scammer. Depending on their answer, the questions followed how the respondents had responded and whether they had experienced feelings of shame to study this as a risk factor. Next up, the same questions were asked after giving the chosen definition of phishing: '*Phishing is a form of digital crime with the goal to steal sensitive information from victims, such as usernames, passwords or bank information. With phishing attacks, victims are lured to a website via emails or text messages by sending a false link for entering personal details. The perpetrators often pose as a trusted organization, such as a bank*'.

The following questions contained statements about the amount of self-control using the Grasmick-scale in *Question 32, 33* and *34.* The higher the scores on these questions (with *Highly agree* as the highest possible answer), the lower the amount of self-control of these persons. These scores then were examined as described in Chapter 3.2.3 to study this as a risk factor for victimization. Finally, the last four questions existed of statements about loneliness and safety in the respondents' neighborhood. These answers were used to examine the risk factors loneliness and offline activities.

The first three sub-questions of this research proposed in Chapter 1.1 will be answered using the dataset in *SPSS*. First, the dependent and independent variables were analyzed using a reliability test to determine the reliability of the questionnaire and to measure the degree of coherence between the survey questions. With a *Pearson Correlation* test, the variables were contrasted to establish whether there is a coherence between the studied risk factors and phishing victimization and victimization on doorstep scams. Using existing risk factors according to scientific literature, this deductive research tested these factors for both (potential) victimization of phishing and doorstep scams. In addition, the cohesion between multiple given risk factors was studied with a logistic regression analysis. Only the potential victimization for doorstep scam and phishing were used as a dependent variable, because these were scored on an interval ratio scale that is continuous. The regression analysis determines whether certain risk factors could have a predictive value for a type of victimization. The fourth sub-question of this research will be partially answered using the dataset in *SPSS*. The predictable part of this question will be studied with the regression analysis. The part about prevention, however, arises from the results of the survey and is therefore a part of the discussion of this study. The answer to this last sub-question circles back to the previously mentioned theories and the existence of behavioural change methods.

4. Results

In this study, seven dependent variables of victimization were studied in total. This chapter shows the outcomes of the different types of statistical tests and analyzes these outcomes to eventually answer the sub-questions of this research. To check whether there is a significant correlation between the dependent variables and the given risk factors as independent variables, a *Pearson Correlation* test was executed in *SPSS*. The results of this test are presented in Table 6, which will answer the first two sub-questions of this research: *'Which (behavioural) risk factors occur for (potential) victims of phishing?'* and *'Which (behavioural) risk factors occur for (potential) victims of doorstep scams?'* by looking at the significant outcomes. The third sub-question '*Looking at the (behavioural) risk factors, does victimization of doorstep scams relate to victimization of phishing?'*, will also be studied using outcomes of the correlation test. The last sub-question partially will be answered using the regression analysis in Table 7. In this question, the predictable value of the occurring of offline and online crimes and victimization is questioned. Lastly, with the outcomes of the regression analysis, this test shows if certain risk factors not only correlate with victimization, but could also predict the presence of potential victimization. The given risk factors were not only tested for their assumptive hypotheses, but were also tested for the other types of victimization.

4.1 Victimization in general

Before the above sub-questions were answered, first the general types of victimization will be studied to see if there are any correlations. When looking at general victimization, Table 6 shows that five risk factors have a significant correlative outcome. Socio-economic status (N=125; M=5.95; SD=1.513) has a positive, significant correlation with victimization (r=.178; p<.05), which means the higher the education, the higher the chance of becoming a victim of crimes in general. The second risk factor is the hours spent on the Internet per weeks in general (N=125; M=44.74; SD=25.525), with a positive correlation for victimization (r=.245; p<.01). This means that people that spent more hours per week on the Internet have a higher chance of becoming a victim in general. The third risk factor is the amount of hours people spent on the Internet doing other things than the six other given possibilities (N=125; M=8.98; SD=14.163). This factor has also a positive, significant correlation with victimization (r=.194; p<.05), which means that the higher the amount of hours per week spending on other things on the Internet, the higher the chance of victimization will be. The fourth risk factor for victimization in general is the amount of hours per week on social media (N=125; M=9.66; SD=8.505). For this risk factor there is, however, a negative, significant correlation found for victimization in general (r=-.193; p<.05). This means that the higher the amount of hours per week on social media, the lower the chance of becoming a victim in general. Finally, the last risk factor is offline victimization (N=125; M=1.32; SD=.468). This significant, positive correlation means that people that were victimized in the offline world (r=.800; p<.01) have a greater chance of being victimized in general.

To study the difference between victimization in the offline and online world, the answers from the survey were further categorized and studied. Table 6 shows that for offline victimization, only two risk factors were significant correlated. Again, the amount of hours spent on social media has a significant, negative correlation with offline victimization as dependent variable (r=-.191; p<.05). This means that the higher the amount of hours spent per week on social media, the lower the chance of becoming a victim in the offline world. Finally, the risk factor loneliness (N=125; M=2.82; SD=1.742) has a positive and significant correlation with offline victimization (r=.178; p<.05). This means the lonelier a person feels, the higher the chance of becoming a victim in the offline world. Lastly, the

Table 6

Correlations for risk factors and victimization (N=125)

Variables			Victimization	Offline victimization	Online victimization	Doorstep scam victimization	Phishing victimization	Potential doorstep scam victimization	Potential phishing victimization
	M	SD	*r*	*r*	*r*	*r*	*r*	*r*	*r*
Demographics									
Gender (Male %)	0.52		-.047	-.007	-.070	.007	-.012	.027	-.077
Age	39.39	11.709	-.144	-.113	-.110	-.061	-.101	-.099	-.066
Socio-economic status	5.95	1.513	.178*	.090	.188*	.187*	.225*	-.010	.005
Online activities									
Internet in general	44.74	25.525	.245**	.191*	.228*	.048	.123	.072	-.041
Other things on the Internet	8.98	14.163	.194*	.126	.225*	-.038	.073	.143	.074
Online shopping	2.93	4.155	-.012	-.046	.055	-.063	-.214*	-.035	.039
Social media	9.66	8.505	-.193*	-.191*	-.070	.088	-.205*	-.065	-.204*
Email	12.73	12.334	-.026	-.095	.138	-.014	.082	-.097	-.061
Online banking	2.42	4.796	-.132	-.121	-.065	-.006	-.098	.025	-.085
Gathering information	11.57	10.293	.166	.126	.125	-.006	-.102	-.022	-.021
Online gaming	3.79	7.159	-.096	-.127	.016	-.090	.037	.004	.008
Shame phishing	2.83	2.483	-.572	-.362	-.362	-	-	-.117	-.620

Variables			Victimization	Offline victimization	Online victimization	Doorstep scam victimization	Phishing victimization	Potential doorstep scam victimization	Potential phishing victimization
	M	SD	*r*	*r*	*r*	*r*	*r*	*r*	*r*
Optimism bias	3.52	1.501	-.136	-.055	-.137	.089	-.055	-.062	.265**
Capable guardianship	1.10	.296	-.005	.009	.080	.095	.096	-.047	.193*
Self-control	42.99	7.317	-.006	.083	-.020	-.025	-.122	-.086	.106
Loneliness	2.82	1.742	.171	.178*	.019	.018	.089	.175	.018
Offline activities	2.79	1.284	.076	.018	.071	.065	.044	-.059	-.033
Offline victimization	1.32	.468	.800**	1	.028	.070	.202*	-.035	.151

* Correlation is statistically significant at the .05 level

** Correlation is statistically significant at the .01 level

independent variable offline victimization was excluded from this specific test, because it is similar to the dependent variable that is being measured.

For online victimization as a dependent variable, three risk factors had a significant outcome. The first risk factor is again socio-economic status; with a positive and significant correlation, the higher the education of a person, the higher the chance of being victimized in the online world (r=.188; p<.05). The second risk factor is the amount of hours spent on the Internet in general per week; with a positive, significant outcome, the higher the amount of hours on the Internet, the higher the chance of being victimized in the online world (r=.228; p<.05). Lastly, again as for victimization in general, the final risk factor is other things on the Internet. With a positive, significant correlation (r=.225; p<.05), the higher the amount of hours spent on other things on the Internet, the higher the chance of becoming an online victim.

4.2 Doorstep scam and phishing victimization

To answer the first two sub-questions of this research, the correlation between risk factors and actual victimization of doorstep scams and phishing were studied. For doorstep scam victimization, only one risk factor has a positive significant correlation, which is socio-economic status. The higher the education of a person, the higher the chance of being a victim of doorstep scam (r=.187; p<.05). For phishing victimization, there were four risk factors with a significant outcome. The first risk factor is again, socio-economic status. With a positive, significant correlation (r=.225; p<.05), the higher the educational level of people, the more likely these people are to become a victim of phishing. The second risk factor is online shopping for the first time (N=125; M=2.92; SD=4.155). With a negative, significant correlation (r=-.214; p<.05), this means that the more hours people spent on online shopping, the lower the chance of becoming a victim of phishing will be. The third risk factor is social media. With a negative, significant outcome, this means that the more hours people spent on social media, the less likely they are to become a victim of phishing (r=-.205; p<.05). The last risk factor is offline victimization as in independent factor. With a significant, positive correlation, victims in the offline world are more likely to become a victim of phishing (r=.202; p<.05).

Lastly, potential victimization of doorstep scam and phishing is measured using the digital survey. For potential victimization of doorstep scam, there were no significant correlations found in this study. For potential victimization of phishing, there were three significant correlations. The first risk factor is again social media, with a negative, significant correlation, the higher the educational level of a person is, the more likely this person is to become a victim of phishing (r=-.204; p<.05). Secondly, the risk factor of optimism bias has a positive, significant correlation (N=125; M=3.52; SD=1.501). This means, the more a person beliefs that dangers on the Internet are not applicable to him or her, the higher the chance of becoming a victim of phishing (r=.265; p<.01). The last risk factor that had a positive, significant correlation with potential victimization for phishing, is the factor capable guardianship (N=125; M=1.10; SD=.296). This means, the higher the presence of capable guardianship, the higher the chance of becoming a victim of phishing.

To answer the third sub-question of this research, the significant risk factors for both doorstep scams as for phishing are studied. Looking at the risk factors, there is no clear relation between the risk factors of doorstep scams and phishing. Not one of the factors occurs at all four of the types of victimization. The only risk factors that occurs at both actual victimization of doorstep scam and phishing is socio-economic status, but this risk factor does not occur for the potential victimization.

For potential victimization, not only the correlative outcomes were studied to answer the fourth and last sub-question. Using a regression analysis in *SPSS*, the risk factors were studied further for predictive values. Table 7 shows this test and its outcomes. For potential doorstep scam victimization, there is only one significant outcome found between this type of victimization and the risk factor loneliness (B=-.265; SE=.123; p<.05). Potential phishing victimization has two predictive risk factors according to this regression analysis. The first risk factor is optimism bias. This variable has a positive, significant outcome for potential phishing victimization (B=.984; SE=.291; p<.01). This means that the variable of not facing dangers on the Internet and thinking one is not susceptible for these dangers, is significance for predicting potential phishing victimization. Lastly, the other risk factor is capable guardianship. This factor has a positive, significant outcome on potential victimization on phishing (B=.3993; SE=1.509; p<.01), meaning the presence of security measures could predict the likelihood of victimization for phishing.

Table 7

Regression analysis for risk factors and victimization (N=125)

Variables	Potential victimization phishing		Potential victimization doorstep scam	
	B	SE	B	SE
Constant	3.157	5.182	6.271	2.472
Demographics				
Gender	-.354	.988	.484	.471
Age	-.012	.041	-.021	.019
Socio-economic status	-.096	.305	-.030	.146
Online activities				
Internet in general	-.043	.026	.012	.012
Other things on the Internet	.071	.040	.013	.019
Online shopping	.094	.117	.025	.056
Social media	-.106	.059	-.042	.028
Email	.013	.042	-.035	.020
Online banking	-.118	.102	.064	.049
Gathering information	.021	.051	-.004	.025
Online gaming	.050	.067	-.021	.032
Optimism bias	.984**	.291	-.102	.139
Capable guardianship	3.993**	1.509	-.177	.720
Self-control	.064	.062	-.021	.030
Loneliness	.133	.257	.265*	.123
Offline activities	-.263	.342	-.167	.163
Offline victimization	1.300	.976	-.706	.465
Nagelkerke R^2:	.240		.130	
N=125				

* Regression is statistically significant at the .05 level

** Regression is statistically significant at the .01 level

5. Discussion

5.1 Risk factors

In this study, multiple variables were tested using a digital survey to search for significant risk factors that can affect the presence of multiple forms of victimization and even predict potential victimization. Based on a literature review, different assumptions were formulated and transcribed into research-questions. In this chapter, the results of the different tests are further described to elaborate on the outcomes and discuss how these findings relate to the expectations starting this study. This research studies the risk factors using both a *Pearson Correlation* test as a regression analysis. The outcomes from these tests are respectively in Table 6 and Table 7. In this section, I will describe the significant findings categorized by risk factor.

5.1.1 Socio-economic status

Socio-economic status has a positive, significant correlation with victimization in general, online victimization, doorstep scam victimization and phishing victimization. This means that higher educated people are more likely to become victims in general and in the online world, and specifically for both doorstep scam as for phishing. No correlation was found between socio-economic status and the dependent variables of offline victimization and the two types of potential victimization, and this risk factor did not have a predictive value for any of the dependent variables of victimization. Based on the reviewed literature, this matches with the earlier expectation that higher educated people are more likely to become victims of crime (Leukfeldt & Yar, 2016), An explanation for this finding could lie in the assumption that higher educated people suffer more from an optimism bias, which was another significant finding for potential phishing victimization. Optimism bias indicates that a specific person feels he or she has nothing to fear for dangers on the Internet and are smart enough to recognize certain phishing-mails or doorstep scammers when exposed to (Meško, 2018). There was, however, no correlation between the variables socio-economic status and optimism bias to support this assumption.

5.1.2 Online activities

Eight risk factors concerning online activities were studied in this research, by asking the respondents how many hours per week they spent on different online channels. Four of these studied risk factors had a significant correlation with one of the seven dependent variables. The first risk factor is Internet in general. This factor had as expected a positive, significant correlation with the dependent variables of victimization in general, offline and online victimization. This means the more hours respondents spent on the Internet, the higher the chance of becoming a victim in general, in the offline world an in the online world. This finding was however not applicable to the specific types of doorstep scam victimization or phishing victimization.

The second significant risk factor is the amount of hours spent on other things on the Internet. It seemed that spending a certain amount of hours on other things on the Internet showed a positive, significant correlation with victimization in general and online victimization. This means that the more hours someone spends on the Internet doing other things than asked in the survey, the higher the chance of becoming a victim in general or in the online world. The survey, however, did not include a

question specifying what 'other' means according to the respondents. Because of this, we can only guess which specific acts were causing the significant correlation with victimization. For this very reason, it is difficult to link this finding to existing literature and earlier made assumptions. We simply do not know what kind of activities lie in the definition of 'other'.

The third risk factor that has a significant outcome is online shopping. This finding, however, resulted in a negative, significant correlation for phishing victimization, meaning the more time a person spent on shopping on the Internet, the lower the chance of becoming a victim for phishing. This is remarkable, because the expectation was that online activities should increase the likelihood to become a victim. To this author's knowledge, however, this online activity was never earlier measured for victimization, which results in a new finding on online victimization, specified to phishing. A same remarkable, reversed finding is found in the fourth and last risk factor, social media. This factor also has a negative, significant correlation with victimization in general, offline victimization, phishing victimization and potential phishing victimization, meaning the more hours a person would spend on social media, the lower the chance of being victimized for one of these four types. These findings contradict with the expectation in general about Internet use, stating that social media would increase the chance of being victimized. However, one other study matches these findings (Saridakis et. al., 2016). An explanation for this is perhaps the assumption that social media could educate the people to beware of the dangers there are, not only in cyberspace but also in the offline world, by putting news items on the channels that point out the presence of different types of crime (Saridakis et. al., 2016).

The use of email, online banking, gathering information on the Internet and gaming were the other four risk factors that were studied for online activities. These four factors, however, had no correlative outcome for any of the victimization types, although this was expected at the start of this study (Leukfeldt & Yar, 2016). In addition, none of the online activities had a predictive outcome. This means we cannot predict whether someone is a potential victim based on online activities.

5.1.3 Optimism bias

Optimism bias indicates that a specific person feels he or she has nothing to fear for dangers on the Internet and that they are smart enough to recognize certain phishing-mails or doorstep scammers when exposed to. For this risk factor, there is a positive, significant correlation on potential phishing victimization, meaning the higher the optimism bias for a person, the more likely this person is to become a victim of phishing. This risk factor did not only correlate, but also was significant in the regression analysis, meaning there is a predictive value for optimism bias on potential victimization for phishing. This corresponds to the earlier expectation based on the literature review (Meško, 2018).

5.1.4 Capable guardianship

Between the risk factor capable guardianship and potential victimization on phishing, there is a positive, significant correlation found, meaning the presence of capable guardianship (in this case, online security measures for the interviewed respondents), increases the likelihood of phishing victimization. In addition, capable guardianship could even predict potential victimization on phishing. This is remarkable, because security measures are believed to prevent such crimes, according to the Routine Activity Theory (Cohen & Felson, 1979). However, according to Van Wilsem (2013), taking computer security measures are not as effective as one should expect. The most common security measure in this research taken by the respondents was the virus scanner (75.2%). Perhaps this finding

explains a virus scanner detects more phishingmails than when people do not have implemented these measures, but the factor of victimization itself still is challenging to figure out.

5.1.5 Loneliness

For the risk factor loneliness, there is a positive, significant correlation for offline victimization, meaning that the higher the feelings of loneliness, the higher the chance is on offline victimization. The independent variable loneliness also predicts offline victimization in general and potential doorstep scam victimization. This is the only significant outcome in the whole study that applies to potential victimization on doorstep scams, meaning that the factor loneliness has a predictive value on potential doorstep scam victimization. This finding explains the social needs of these people; lonely people are more willing to engage social ties, even if this may involve certain risks.

5.1.6 Offline victimization

The last significant correlation is between the risk factor offline victimization and victimization in general and phishing victimization. This positive outcome means that people, who experienced victimization in the offline world earlier, have a higher chance to become a victim in general and for phishing. The expectation was, however, that this risk factor also applied on online victimization, and was the reason this factor was included in this study in the first place (Leukfeldt, 2015). This outcome only partially applied to this study, because phishing victimization is a part of online victimization.

5.1.7 Overview of other findings

Respondents received questions about actual victimization on doorstep scams. As expected, there were almost no victims of this type of crime. Only 3.2% of the respondents indicated they had ever been in contact with doorstep scammers. After further questioning, it turned out they never actually responded to the doorstep scam because they noticed in time they were scammed. According to the literature, perpetrators especially approach older people who are therefore victim of doorstep scams. In this study, over a third of the respondents were between 27 and 31 years old (36.8%). Furthermore, it is also a possibility that doorstep scams simply occur less than a few years ago. However, literature does not support this; the recent pandemic crisis caused an increase in the number of cases of doorstep scams since March 2020. By adding potential victimization as a dependent variable, the goal was to expose all the respondents to a fictive doorstep scam scenario to study whether more victims would emerge from this than that could actually be measured in this study. It is, however, interesting to conclude that even for the fictive doorstep scam scenario, the majority of the potential victims would not fall for these scams. Table 2 shows that the majority of the respondents had a score of 5 or lower on the variable *Potential Victimization Doorstep Scam*, meaning the majority of the respondents (*N*=105) had a low chance of becoming a potential victim of doorstep scams, even in a fictive setting. This brings us back to the earlier conclusion that older people are a target because they are more likely to fall to these doorstep scams, especially when it considers their health, their fear for the coronavirus and their feelings of loneliness.

Multiple risk factors did not correlate with or predict the different forms of victimization at all. The assumptions on the beginning of this research, however, stated otherwise and for that reason, these factors were included in the study. This applies to the risk factors gender, age, spending hours

on email, online banking, gathering information, feelings of shame, the amount of self-control and offline activities. Especially for the factor self-control, this is an interesting and contradictory finding. The General Theory of Crime is a well-tested theory that is executed on different forms of victimization and studied for decades. The majority of these studies concluded their research with a high correlation or even regression between low self-control and victimization; a conclusion this study does not support.

In addition to this, none of the 18 studied risk factors correlated with potential doorstep scam victimization, and only one risk factor predicted this type of potential victimization. This raises the question if the way potential victimization was set up, using the scenarios in the survey, was the right way. Luckily, this issue is slightly taken away by the fact that potential victimization for phishing has multiple usable, significant outcomes to work with, which was set up and executed the very same way. The explanation could be found for statements in the questionnaire that respondents needed to answer. For potential doorstep scam victimization, there were three statements given in the questionnaire. However, after testing the reliability of these statements, it appeared that the computed variable had a higher reliability without one of these statements, leaving only two for further testing. This might influence the results of the tests and the absence of any significant outcome.

5.2 Limitations and recommendations for future research

In this section of the discussion, a few limitations will be highlighted to keep in mind for further research. After this, various recommendations for future research will be described to decrease victimization, not only for doorstep scams and phishing, but also for victimization in general in the offline and online world. The first issue that I would like to address is the fact that there seemed to be a discrepancy on the definition of victimization. In the middle of the survey, respondents were asked whether they had ever been in contact specifically with phishing or doorstep scams. 115 of the respondents (92%) answered this question with '*Yes*' for phishing and only four respondents (3.2%) had the same answer for doorstep scams. Compared to a previous finding, where only 40 respondents in total answered the question positively if they ever had been victimized in the online world in general, the finding of 115 respondents answered '*Yes*' on phishing is interesting. This brings us to the assumption that most of the respondents do not link victimization to only receiving a phishingstext or -mail. In previous research, it would be advised to ask the respondents to their definition of becoming a victim to better understand this development.

Another unfortunate limitation is the fact that feelings of shame were not questioned enough through the digital survey. In *Questions 17* and *26* of the digital survey, respondents were asked if they experienced feelings of shame during the exposure of doorstep scams or phishing. These questions, however, only popped up when the respondents answered the previous question about victimization on these types of crime positive. This means that multiple respondents were not questioned about feelings of shame, while they had been victimized in the offline or online world. This low number of answers therefore resulted in the exclusion of the variable *Shame on doorstep scam* in the whole study, and removing the variable *Shame on phishing* in the regression analysis, with the simple reason that this could not be measured. Adding questions about shame for general types of victimization would increase the amount of respondents talking about shame, which perhaps could cause a more reliable risk factor to work with.

The third (and an important limitation in this research in my opinion), is the period of the study and the administering of the questionnaires. At the same time, this issue does not necessarily have to

be a limitation, but it most likely had a major influence on the research results of this study. The reason is that respondents were asked several questions using a digital survey in the middle of the pandemic of the coronavirus. According to multiple articles, this pandemic has left its mark on the way perpetrators act. These offenders adjusted their modus operandi and even changed their original criminal activities, all under the influence of the new developments in the world (Europol, 2020). Research shows that there are fewer burglaries, because the majority of the people works from home since the outbreak, but at the same time there is an increase in numbers of online criminal activities, because this same majority is overall permanent online. If this research was conducted before the pandemic, the outcomes most likely differ than the results described above. In addition to this, future research should not only be executed during another period, but perhaps also a bit longer than the two and a half weeks my digital survey was published. When looking at the outcomes of the correlation test and the regression analysis, only a few results were significant. Because I studied a high amount of risk factors in this thesis (18 in total), there is a chance that the sample size of this study was not adequate. It would be interesting to conduct this study again, with more respondents than the 125 that participated on this study and during a longer period of time. The expectation for future research is that it could increase the number of significant outcomes when more respondents would be questioned.

In the section above about the findings on online activities, the results show that the amount of hours spending online, doing other things on the Internet than the given activities, have a significant correlation on victimization. The survey, however, did not include a question specifying what 'other' means according to the respondents. This leaves a mysterious guess to the knowledge of which certain acts were causing the significant correlation to the increase of the likelihood of victimization. When adding this question to a future study, there is no room for guessing.

The last limitation is the low percentage of the *Nagelkerke* R^2, which explains the variance in the dependent variables by the explanatory variables. (Table 7). For potential victimization of phishing, this value is .240, meaning the different risk factors explain 24% of potential phishing victimization. For potential victimization on doorstep scams, this value is .130, meaning that only 13% of the risk factors explains the potential victimization for doorstep scams. For both studied dependent variables, this value is quite low, meaning there are probably other risk factors to consider, which are not included in this research. This limitation raises the question if there are risk factors for victimization that are not only included in this research, but in any other researches for that matter. As I stated in the introduction of this thesis, there is in that last decades a shift observed from only technical visions on victimization to more sociological and psychological visions. This is, however, a recent shift, and more risk factors could be discovered in these fields when it comes to studying victimization in both the offline as online world. More research should be done in the emotions, cognitions, environment and behaviour of people to establish whether there are more risk factors to include in the study to victimization. For this very reason, I chose to include the risk factors shame and loneliness. Only a few studies looked into these risk factors, however, none of these studied the direct influence of these factors on victimization and therefore did not establish if these could be considered risk factors for victimization. Another plausible risk factor that we can choose to study are the perceptions of the protective bodies, such as our judicial system, the police or the government. I anticipate that for people who believe in these governmental bodies, the likelihood of victimization would be lower than when people reject the legal system and do not have trust in the government.

5.3 Conclusion

The goal of my thesis was to establish whether the occurring of cybercrime is predictable and maybe even preventable, if we closely study the behaviour of its victims. Is it necessarily to come up with new criminological theories, or can we rely on the existing theories for an effective approach? The first sub-question of this research questioned the (behavioural) risk factors of (potential) victims of phishing. The risk factors that occur for this type of victimization are socio-economic status, the online activities shopping and social media, optimism bias, capable guardianship and offline victimization. For some of these risk factors it is easier to influence their effect on victimization than others. The level of education studied in the variable of socio-economic status, is for instance not an easy factor to adjust, simply because it is not possible to influence the level of education for potential victims. Another reason why it is not easy to adjust these risk factors lies in the fact that there is a reversed outcome than originally was presumed. This applies, for example, to the factors of spending time on online shopping and social media, and the presence of capable guardianship. The more time a person would spend on shopping online, the lower the chance on victimization. However, no logical reasoning so far clarifies why this could be the case. This first requires further research on these specific risk factors before implementing it in a method to adjust the behaviour to decrease victimization. For capable guardianship, this research suggests that implementing security measures online increases the likelihood of victimization. This also is no logical explanation; security measures are there to prevent online victimization in the first place and requires more attention in future research. The results on the variable optimism bias is on the other hand something we could use to decrease victimization, by for example educating the people with a high optimism bias that even they are potential victims and should not think too lightly about the dangers on the Internet and the consequences these dangers bring.

The second sub-question, regarding the risk factors for (potential) victims of doorstep scams, is answered with two factors: socio-economic status and loneliness. Socio-economic status is, as described earlier, not that easy to adjust. However, loneliness is somewhat better to tackle. By trying to reduce the feelings of loneliness, or at least warn the people who experience these feelings that they have a higher chance of becoming a victim of doorstep scams, a decrease of doorstep scam victimization could be established. It remains challenging, however, to find out which people experience these feelings. The third sub-question of this study questions the relation between the significant risk factors of phishing and doorstep scams. Unfortunately, there are no useable similarities that can answer this question properly. The only similarity is between socio-economic status and these two types of victimization, but as stated before, this factor is almost impossible to adjust effectively. The fourth and last sub-question questions if victimization of phishing and doorstep scams is predictable and thereby even preventable. The answer to this question is somewhat positive; looking at the significant outcomes on the regression analysis, two risk factors could predict the victimization for phishing, and one factor could predict victimization for doorstep scams. By knowing if people experience feelings of loneliness, optimism bias, or the presence of capable guardianship, they could be warned in time to beware of phishing messages or doorstep scams.

Although there is quite an amount of scientific research available on risk factors and victimization, including this research, it remains challenging to answer aforementioned questions properly. Taken the limitation of this research into account, this research shows that there is still not enough knowledge about the behaviour of victims. This is because the studied risk factors have little to do with the actual behaviour of potential victims. For this very reason, it is almost impossible to give a satisfying answer to the research question, questioning which behavioural change methods could be

used to decrease victimization. An easy conclusion to make is that existing theories do not apply on these results, and that we need to look further for new theories for online victimization. However, this research actually shows that little is known about the risk factors, and that this should be studied in depth. To establish this, researchers must take a step back to study which existing theories should be better investigated for the existence of other, potential risk factors. With a descent description and formulation of the new risk factors, it would be easier in the future to reduce online and offline victimization based on these risk factors.

References

Aarten, P. (2018, April 16). *Once a victim, always a criminal?* Leiden Security and Global Affairs Blog. https://leidensecurityandglobalaffairs.nl/articles/once-a-victim-always-a-criminal

Agha, S., Tollefson, D., Paul, S., Green, D., & Babigumira, J.B. (2019). Use of the Fogg Behavior Model to Assess the Impact of a Social Marketing Campaign on Condom Use in Pakistan. *Journal of Health Communication, 24*, 284-292.

Boekhoorn, P. (2019). De aanpak van cybercrime door regionale eenheden van de politie. *Politie & Wetenschap.* SDU Uitgevers: Den Haag.

Bossler, A.M. (2019). Contributions of criminological theory to the understanding of cybercrime offending and victimization. In R. Leukfeldt & T. J. Holt (Eds.), *The Human Factor of Cybercrime* (pp. 29-59). London, United Kingdom: Taylor & Francis.

Bossler, A.M., & Holt, T.J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice, 38*, 227–236.

Centraal Bureau voor de Statistiek. (2018, August 2). *Opleidingsniveau*. Retrieved from: https://www.cbs.nl/nl-nl/onze-diensten/cbs-urban-data-centers/arbeid-en inkomen/opleidingsniveau

Centraal Bureau voor de Statistiek. (2020). *Veiligheidsmonitor 2019*. https://www.cbs.nl/nl-nl/publicatie/2020/10/veiligheidsmonitor-2019

Centraal Bureau voor de Statistiek. (2020, March 2). *Minder traditionele criminaliteit, meer cybercrime.* https://www.cbs.nl/nl-nl/nieuws/2020/10/minder-traditionele-criminaliteit-meer-cybercrime

Choi, K.S. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology, 2*(1), 308-333.

Cohen, L., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review, 44*, 588–608.

Espinoza, G. (2015). Daily cybervictimization among Latino adolescents: Links with emotional, physical and school adjustment. *Journal of Applied Developmental Psychology, 38*(1), 39-48.

Europol. (2020). *How Covid-19-related crime infected Europe during 2020.* European Union Agency for Law Enforcement Cooperation 2020. https://www.europol.europa.eu/publications-documents/how-covid-19-related-crime-infected-europe-during-2020

Felson, M., & Clarke R.V. (1998). Opportunity makes the thief: Practical theory for crime prevention. In B. Webb (ed.), *Police Research Series*. London: Home Office.

Fogg, B.J. (2009). A behavior model for persuasive design. *Persuasive Technology Lab.* Stanford University.

Goldsmith, A., & Brewer, R. (2015). Digital drift and the criminal interaction order. *Theoretical Criminology, 19,* 112–130.

Gottfredson, M.R, & Hirschi, T. (1990). *A general theory of crime*. Stanford, California: Stanford University Press.

Grasmick, H.G., Tittle, C.R., Bursik, R.J., & Arneklev, B.J. (1993). Testing the core empirical implications of Gottfredson and Hirschi's General Theory of Crime. *Journal of Research in Crime and Delinquency, 30*(1), 5-29.

de Groot, N. (2017, September 25). *Jaarlijks 10 miljard schade door cybercrime*. Algemeen Dagblad. https://www.ad.nl/economie/jaarlijks-10-miljard-schade-door-cybercrime~a1e18a70/

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7).

Holt, T.J. & Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20-40.

Hoogendoorn, E.S. (2020, May 29). *Scientific paper on the reporting of cybercrime for individual victims.* Unpublished manuscript.

Hutchings, A., & Hayes, H. (2009). Routine Activity Theory and Phishing Victimization: Who Gets Caught in the 'Net'? *Current Issues in Criminal Justice 20*(3):433–451.

Irwin, A., Li, J., Craig, W., & Hollenstein, T. (2019). The Role of Shame in Chronic Peer Victimization. *American Psychological Association, 34*(2), 178-186.

Kamp, R. (2020, December 14). Corona: phishing en oplichting. Consumentenbond. https://www.consumentenbond.nl/veilig-internetten/corona-phishing-en-oplichting

Leukfeldt, E.R. (2014). Phishing for Suitable Targets in the Netherlands: Routine Activity Theory and Phishing Victimization. *Cyberpsychology, Behavior, and Social Networking, 17*(8), 551-555,

Leukfeldt, E.R. (2015). Comparing victims of phishing and malware attacks: Unraveling risk factors and possibilities for situational crime prevention. *International Journal of advanced studies in Computer Science and Engineering, 4*(5), 26-32.

Leukfeldt, E.R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior, 37*(3), 263–280.

Leukfeldt, E.R. (2017). *Research agenda: The Human Factor in Cybercrime and Cybersecurity.* Van Haren Publishing.

van der Lubbe L.M., Gerritsen C., Formolo D., Otte M., & Bosse T. (2019). A Serious Game for Training Verbal Resilience to Doorstep Scams. In: M. Gentile, M. Allegra & H. Söbke (Eds.), *Games and Learning Alliance* (pp. 110-120). Springer, Cham. https://doi-org.ezproxy.leidenuniv.nl:2443/10.1007/978-3-030-11548-7_11

Meško, G. (2018). On Some Aspects of Cybercrime and Cybervictimization. *European Journal of Crime, Criminal Law and Criminal Justice*, *26*(3), 189–199. https://doi.org/10.1163/15718174-02603006

Miron, A.M., & Brehm, J.W. (2006). Reactance Theory – 40 Years Later. *Zeitschrift für Sozialpsychologie, 37*(1), 9-18.

Nederlandse Vereniging van Banken. (2020). *Jaarverslag 2019.* Rotterdam: Media Center. Retrieved from: https://nvbjaarverslag.nl

Noordenburg, C. (2020a, March 27). *Babbeltruc.* Centrum voor Criminaliteitspreventie en Veiligheid (CCV). Retrieved from: https://hetccv.nl/onderwerpen/senioren-en-veiligheid/specifieke-themas/babbeltruc

Noordenburg, C. (2020b, September 18). *Campagne Senioren & Veiligheid: Phishing.* Centrum voor Criminaliteitspreventie en Veiligheid (CCV). Retrieved from: https://hetccv.nl/nieuws/campagne-senioren-veiligheid-phishing/

Opgelicht. (2020, October 10). *Politie waarschuwt voor corona-babbeltruc.* Opgelicht?! – AVROTROS. Retrieved from: https://opgelicht.avrotros.nl/alerts/artikel/politie-waarschuwt-voor-corona-babbeltruc/

Politie (2018, August 14). *Laat niemand binnen, wat ze ook verzinnen.* Politie.nl. Retrieved from: https://www.politie.nl/nieuws/2018/augustus/14/laat-niemand-binnen-wat-ze-ook-verzinnen.html

Pratt, T.C., Cullen, F.T., Blevins, K.R., Daigle, L.E., & Madensen, T.D. (2006). The empirical status of deterrence theory: A meta-analysis. In F.T. Cullen, J.P. Wright, & K.R. Blevins (Eds.), *Taking stock: The status of criminological theory.* New Brunswick, NJ: Transaction.

Saridakis, G., Benson, V., Ezingeard, J., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimization: An empirical study of social networking users. *Technological Forecasting & Socials Change,* 320-330. Elsevier.

Waldrop, M. M. (2016). The Human Side of Cybercrime. *Nature International Weekly Journal of Science, 533*(7602), 164-167.

Webber, C., & Yip, M. (2019). Humanizing the cybercriminal: markets, forums, and the carding subculture. In R. Leukfeldt & T. J. Holt (Eds.), *The Human Factor of Cybercrime* (pp. 258-285).

London, United Kingdom: Taylor & Francis.

van de Weijer, S.G.A., & Leukfeldt, E.R. (2017). Big Five Personality Traits of Cybercrime Victims. *Cyberpsychology, Behavior, and Social Networking*, 20(7), 407–412. https://doi.org/10.1089/cyber.2017.0028

van de Weijer, S. (2019). Predictors of cybercrime victimization: causal effects or biased associations? In E.R. Leukfeldt & T.J. Holt (Eds.), *The Human Factor of Cybercrime* (pp. 83-111). London, United Kingdom: Taylor & Francis.

Weulen Kranenbarg, M., Holt, T.J., & van Gelder, J.L. (2019). Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap. *Deviant Behavior, 40*(1), 40-55. https://doi.org/10.1080/01639625.2017.1411030

van Wilsem, J. (2013). Hacking and Harassment - Do They Have Something in Common? Comparing Risk Factors for Online Victimization. *Journal of Contemporary Criminal Justice, 29*(4), 437-453.

Zimmer-Gembeck, M.J., Trevaskis, S., Nesdale, D., & Downey, G.A. (2014). Relational Victimization, Loneliness and Depressive Symptoms: Indirect Associations via Self and Peer Reports of Rejection Sensitivity. *Journal of Youth and Adolescence, 43*(1), 568-582.

Appendices

Appendix 1

Digital survey from Qualtrics

Start of Block: Default Question Block

Welcome ...

... to my survey and thank you for taking the time to complete this digital questionnaire! As part of my graduation thesis for the Master Cyber Security at Leiden University, I am conducting a research into the online and offline behavior of people. This questionnaire is about your experiences on the internet. There is no right or wrong answer to the questions and statements in this survey; I am interested in your opinion.

This survey will take approximately 10 minutes of your time and is completely anonymous. Your participation is voluntary and you can stop at any time without giving a reason. In the meantime it is possible to save the survey and close it, to continue at another time. It is best to use a laptop or computer to complete this survey; the mobile view does not work equally well for all questions and statements.

At the bottom, you indicate that you agree with the above and have understood the information. If you choose 'yes', you can start with the questionnaire. If you choose 'no', the questionnaire will be closed.

Thank you again for filling in! If you have any questions, you can reach me via the email address below.

Eline Hoogendoorn
e.s.hoogendoorn@umail.leidenuniv.nl

---

0 I understand the text above and agree with it.

O Yes (1)

O No (2)

Skip To: End of Survey If I understand the text above and agree with it = No

---

Page Break

End of Block: Default Question Block

Start of Block: Block 1

1 What is your gender?

- O Male (1)
- O Female (2)
- O Otherwise, (3) _____

*

2 What is your age?
Enter your age in numbers down here.

_____

3 What is your highest level of education?

- O Elementary education (1)
- O Pre-vocational education (2)
- O Secondary education (3)
- O Secondary education (4)
- O Vocational education (5)
- O Higher professional education (6)
- O Scientific education Bachelor (7)
- O Scientific education Master (8)
- O Otherwise, (9) _____

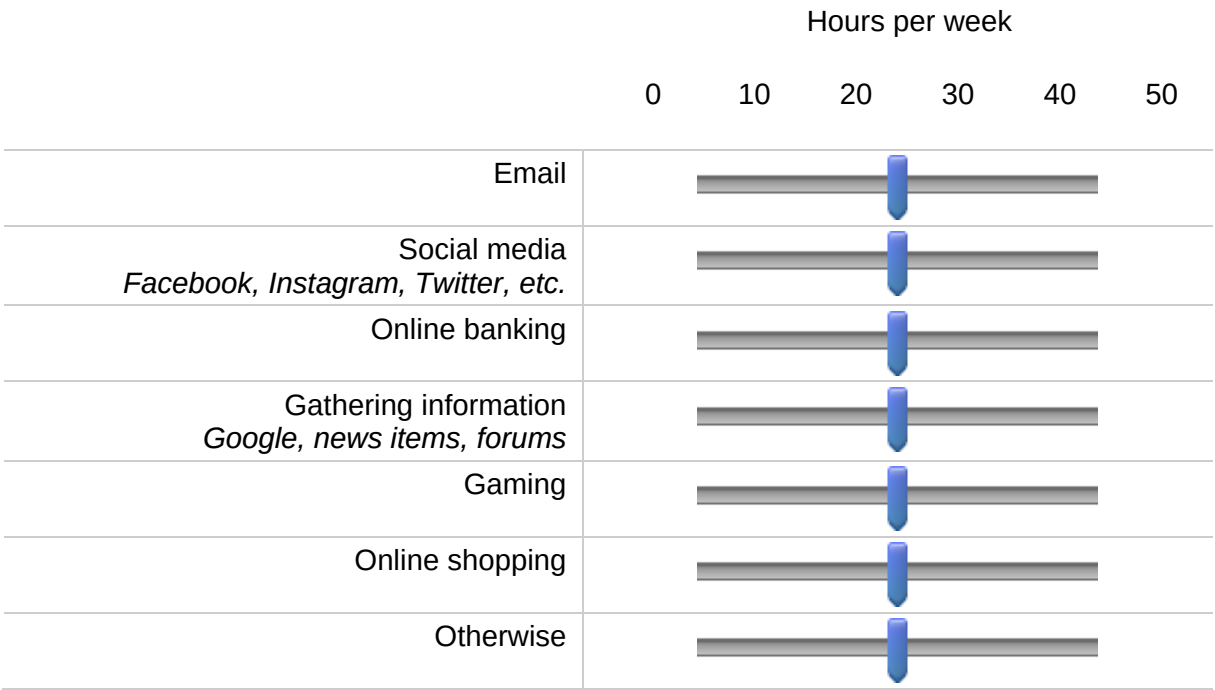
Page Break

*

4 How often (amount of hours per week) do you use the Internet in general?
Enter the amount of hours per week in numbers down here.

_____

5 How often do you use the Internet?
If you are not using the given online activity, click on the slider until it turns dark blue and is set to 0. If you use the given online activity for more than 50 hours per week, set the slider to 50 hours.



Page Break

6 In this question, you answer a number of statements.
There is no right or wrong answer; we are interested in your opinion.

	Highly disagree (1)	Disagree (2)	Partially disagree (3)	Neutral (4)	Partially agree (5)	Agree (6)	Highly agree (7)
I am well protected on the Internet (1)	O	O	O	O	O	O	O
I can influence my own safety on the Internet (2)	O	O	O	O	O	O	O
I know how to make my online behaviour safer (3)	O	O	O	O	O	O	O
I am aware of the dangers on the Internet (4)	O	O	O	O	O	O	O
I do not have fear for the dangers on the Internet, this will not happen to me (5)	O	O	O	O	O	O	O

Page Break

7 Did you take security measures to protect yourself on the Internet?
Firewall, virus scanners, VPN-connection, passwordgenerator, etc.

O Yes (1)

O No (2)

Display This Question:

If Did you take security measures to protect yourself on the Internet? = Ja

8 What security measures did you take to protect yourself?
It is possible to choose multiple answers.

- ☐ Firewall (1)
- ☐ Virus scanner (2)
- ☐ VPN-connection (3)
- ☐ Passwordgenerator (4)
- ☐ Otherwise, (5) _____

Display This Question:

If Did you take security measures to protect yourself on the Internet? = Nee

9 Why did you not take security measures?
It is possible to choose multiple answers.

- ☐ I do not need security (1)
- ☐ I do not know how to protect myself on the Internet (2)
- ☐ Otherwise, (3) _____

Page Break

10 Have you ever been a victim of crime, and if so, did this occur in the offline or online world?

- O Yes, this happened offline (1)
- O Yes, this happened online (2)
- O Yes, this happened both offline as online (3)
- O No, I never have been a victim of crime (4)

Skip To: Scenarios If Have you ever been a victim of crime, and if so, did this occur in the offline or online world? = No, I never have been a victim of crime

11 Can you indicate which type of crime you been a victim of?
This question does not have to be completed to continue with the survey.

_____

_____

_____

Page Break

Scenarios

In the next part of this survey, a number of scenarios are presented. For you, the intention is to indicate for these scenarios how you would react in real life if it happened to you. After reading each scenario, you will again answer a number of statements.

12 **Scenario 1**

Someone is at your door. On the sidewalk is a young lady who introduces herself as Chantal de Jonge of the Common Health Service. She says she is going around the neighborhood to spread information about the corona measures in your neighborhood. She shows a leaflet

from the organization and asks if she can come in to explain a few things.

How likely are the following statements for you in this scenario?

	Very unlikely (1)	Unlikely (2)	Fairly unlikely (3)	Neutral (4)	Fairly likely (5)	Likely (6)	Very likely (7)
I invite the woman into my house (1)	O	O	O	O	O	O	O
I will call the organization to inquire about sending the woman (2)	O	O	O	O	O	O	O
I will send the woman away (3)	O	O	O	O	O	O	O

Page Break

13 **Scenario 2**

You open your email and see the email below in your inbox.

How likely are the following statements for you in this scenario?

	Very unlikely (1)	Unlikely (2)	Fairly unlikely (3)	Neutral (4)	Fairly likely (5)	Likely (6)	Very likely (7)
I apply for the debit card by clicking on the link (1)	O	O	O	O	O	O	O
I first check the security of the email (2)	O	O	O	O	O	O	O
I delete the email (3)	O	O	O	O	O	O	O
I move the email to the spam folder (4)	O	O	O	O	O	O	O
I will call the Rabobank to inquire about sending the email	O	O	O	O	O	O	O

Page Break

The scenarios on the previous pages are two examples that actually took place in real life. We still see these forms of crime in our society on a daily basis. The first scenario involved a doorstep scam, the second scenario involved a form of phishing. These two types will be discussed in more detail in the next part of this survey.

Before we move on to the questions, here is the definition of doorstep scams I use in my research:

In a chat trick, a perpetrator uses an excuse or lie to talk himself into a victim's home in order to commit theft.

---

14 Based on the above definition, have you ever been in contact with a doorstep scam?

- O Yes, someone at my door pretended to be someone else (1)
- O No, but I do know people this has happened to (2)
- O No, I never encountered a doorstep scam before (3)

Skip To: Phishing If Based on the above definition, have you ever been in contact with a doorstep scam? = No, but I do know people this has happened to

Skip To: Phishing If Based on the above definition, have you ever been in contact with a doorstep scam? = No, I never encountered a doorstep scam before

---

15 Did you ever fall for a doorstep scam?
Did you, for example, let the person in question into your house or gave them money?

- O Yes (1)
- O No (2)

Skip To: 18 If Did you ever fall for a doorstep scam? = Nee

---

16 **How** did you fall for the doorstep scam?
It is possible to choose multiple answers.

- ☐ I let the person into my house (1)
- ☐ I gave the person money or transferred it (2)
- ☐ I shared my personal information with the person (3)
- ☐ Otherwise, (4) _____

17 Did you experience feelings of shame when it turned out you fell for a doorstep scam?

- O Yes (1)
- O A little bit (2)
- O No (6)

18 Could you briefly describe the situation when you encountered a doorstep scam?

_____

_____

19 How did you find out that it was a doorstep scam?

_____

_____

Page Break

20 Did you do anything else when you discovered it was a doorstep scam?
It is possible to choose multiple answers.

- ☐ I contacted the organization where the person said he belonged to (1)
- ☐ I asked some advice in my network (friends, family, colleagues) (2)
- ☐ I searched the Internet for information (3)
- ☐ I did not do anything (4)
- ☐ Otherwise, (5) _____

Page Break

Display This Question:

If Did you do anything else when you discovered it was a doorstep scam?= I asked some advice in my network (friends, family, colleagues)

21 In the previous question, you did not choose the answer option: 'I asked some advice in my network'. Do you feel that you could have asked for this advice in your network?

- ○ Yes, I certainly could get some advice (1)
- ○ No, I could not get some advice because of the lack of knowledge (2)
- ○ No, I was too scared to ask for advice (3)
- ○ Otherwise, (4) _____

Display This Question:

If In the previous question, you did not choose the answer option: 'I asked some advice in my network'. Do you feel that you could have asked for this advice in your network? = No, I was too scared to ask for advice

22 Could you briefly describe why you did not dare to ask your network for help?

_____

_____

Page Break

Phishing

Here is the definition of phishing I use in my research:

Phishing is a form of digital crime with the goal to steal sensitive information from victims, such as usernames, passwords or bank information. With phishing attacks, victims are lured to a website via emails or text messages by sending a false link for entering personal details. The perpetrators often pose as a trusted organization, such as a bank.

---

23 Based on the above definition, have you ever been in contact with phishing?
Did you, for example, ever received a message that contained phishing?

- O Yes, I received a phishing message by email (1)
- O Yes, I received a phishing message by text (2)
- O Yes, I received both phishing messages by email and text (3)
- O No, I never received a message of any kind (4)

Skip To: 32 If Based on the above definition, have you ever been in contact with phishing? = No, I never received a message of any kind

24 Did you ever fall for a phishing message?
Did you, for example, ever clicked on a link or put in your personal credentials?

- O Yes (1)
- O No (2)

Skip To: 27 If Did you ever fall for phishing? = Nee

---

25 **How** did you fall for the phishing message?
It is possible to choose multiple answers.

- ☐ I transferred money (1)
- ☐ I put in my personal credentials (2)
- ☐ I clicked on a link (3)
- ☐ Otherwise, (4) _____

26 Did you experience feelings of shame when it turned out you fell for a phishing message?

- O Yes (1)
- O A little bit (2)
- O No (6)

27 Could you briefly describe the situation when you encountered the phishing message?

_____

_____

28 How did you find out that it was a phishing message?

_____

_____

Page Break

29 Did you do anything else when you discovered it was a phishing message?
It is possible to choose multiple answers.

- ☐ I contacted the organization where the message was from (1)
- ☐ I asked some advice in my network (friends, family, colleagues) (2)
- ☐ I searched the Internet for information (3)
- ☐ I deleted the phishing message (4)
- ☐ I did not do anything (5)
- ☐ Otherwise, (6) _____

Page Break

Display This Question:

If Did you do anything else when you discovered it was a phishing message? = I asked some advice in my network (friends, family, colleagues)

30 In the previous question, you did not choose the answer option: 'I asked some advice in my network'. Do you feel that you could have asked for this advice in your network?

- ○ Yes, I certainly could get some advice (1)
- ○ No, I could not get some advice because of the lack of knowledge (2)
- ○ No, I was too scared to ask for advice (3)
- ○ Otherwise, (4) _____

Display This Question:

If In the previous question, you did not choose the answer option: 'I asked some advice in my network'. Do you feel that you could have asked for this advice in your network? = No, I was too scared to ask for advice

31 Could you briefly describe why you did not dare to ask your network for help?

_____

Page Break

32 On the following pages, you will find a number of statements about your personal characteristics. Please indicate to what extent you agree with this on the scale below. *There is no right or wrong answer.*

	Highly disagree (1)	Partially disagree (2)	Partially agree (3)	Highly agree (4)
I often act on the spur of the moment without stopping to think (1)	O	O	O	O
I don't devote much thought and effort to preparing for the future (2)	O	O	O	O
I often do whatever brings me pleasure here and now, even at the cost of some distant goal (3)	O	O	O	O
I'm more concerned with what happens to me in the short run than in the long run (4)	O	O	O	O
I frequently try to avoid projects that I know will be difficult (5)	O	O	O	O
When things get complicated, I tend to quit or withdraw (6)	O	O	O	O
The things in life that are easiest to do bring me the most pleasure (7)	O	O	O	O
I dislike really hard tasks that stretch my abilities to the limit (8)	O	O	O	O

	Highly disagree (1)	Partially disagree (2)	Partially agree (3)	Highly agree (4)
I like to challenge myself every now and then by taking a little risk (1)	O	O	O	O
Sometimes I will take a risk just for the fun of it (2)	O	O	O	O
I sometimes find it exciting to do things for which I might get in trouble (3)	O	O	O	O
Excitement and adventure are more important to me than security (4)	O	O	O	O
If I had a choice, I would almost always rather do something physical than something mental (5)	O	O	O	O
I almost always feel better when I am on the move than when I am sitting and thinking (6)	O	O	O	O
I like to get out and do things more than I like to read or contemplate ideas (7)	O	O	O	O
Compared to other people my age, I seem to have more energy and a greater need for activity (8)	O	O	O	O

Page Break

	Highly disagree (1)	Partially disagree (2)	Partially agree (3)	Highly agree (4)
I try to look out for myself first, even if it means making things difficult for other people (1)	O	O	O	O
I'm not very sympathetic to other people when they are having problems (2)	O	O	O	O
If things I do upset people, it's their problem not mine (3)	O	O	O	O
I will try to get the things I want even when I know it's causing problems for other people (4)	O	O	O	O
I lose my temper pretty easily (5)	O	O	O	O
Often, when I'm angry at people I feel more like hurting them than talking to them about why I am angry (6)	O	O	O	O
When I'm really angry, other people better stay away from me (7)	O	O	O	O
When I have a serious disagreement with someone, it's usually hard for me to talk calmly about it (8)	O	O	O	O

Page Break

On this last page of this survey you will answer a number of statements.
There is no right or wrong answer; we are interested in your opinion.

---

34 **Statement 1**
I sometimes feel lonely.

- O Highly disagree (1)
- O Disagree (2)
- O Partially disagree (3)
- O Neutral (4)
- O Partially agree (5)
- O Agree (6)
- O Highly agree (7)

---

35 **Statement 2**
I can turn to someone for advice if I have any concerns or problems.

- O Highly disagree (1)
- O Disagree (2)
- O Partially disagree (3)
- O Neutral (4)
- O Partially agree (5)
- O Agree (6)
- O Highly agree (7)

---

36 **Statement 3**
There is a lot of crime in my neighborhood.

- O Highly disagree (1)
- O Disagree (2)
- O Partially disagree (3)
- O Neutral (4)
- O Partially agree (5)
- O Agree (6)
- O Highly agree (7)

---

37 **Statement 4**
I feel safe in my neighborhood.

- O Highly disagree (1)
- O Disagree (2)
- O Partially disagree (3)
- O Neutral (4)
- O Partially agree (5)
- O Agree (6)
- O Highly agree (7)

End of Block: Block 1

Appendix 2

(Behavioural) risk factors of online victimization

Risk factors	**Explanation (quotes)**	**Question in survey**
Gender	A user's age, gender, (…) affect the level of victimization in cyberspace (Meško, 2018).	1
Age	A user's age, gender, (…) affect the level of victimization in cyberspace (Meško, 2018).	2
Online activities	Time spent on online activities are significantly related to online victimization risk. The more hours spent on these activities, the larger the chance of victimization (van de Weijer, 2019).	4, 5
Feelings of shame	Experiencing more shame following victimization may play an important role in explaining why victimized youth are at risk for experiencing continued victimization (Irwin et. al., 2019).	17, 21, 22, 26, 30, 31
Optimism bias	Cyberspace is characterized by an optimism bias (…), and those influenced by this bias know that they could be exposed to risks in cyberspace. However, they believe that the likelihood of their victimization in lower than the likelihood of victimization of other potential victims (Meško, 2018).	6
Capable guardianship	Victimization levels are higher when there is an absence of capable guardianship (van Wilsem, 2013).	7, 8, 9
Self-control	Low self-control is significantly related to online victimization risk (van de Weijer, 2019).	32, 33, 34
Offline victimization	Victimization in their physical environment affect the level of their victimization in cyberspace (Leukfeldt, 2015).	10, 14

Appendix 3

(Behavioural) risk factors of offline victimization

Risk factors	**Explanation (quotes)**	**Question in survey**
Age	A user's age, gender, (…) affect the level of victimization in cyberspace (Meško, 2018).	2
Socio-economic status	Victimization occurs more often among higher educated people (Leukfeldt & Yar, 2016).	3
Self-control	Low self-control is significantly related to online victimization risk (van de Weijer, 2019).	32, 33, 34
Loneliness	Tests of direct and indirect associations with structural equation modeling showed that adolescents higher in relational victimization reported more loneliness (Zimmer-Gembeck et. al., 2014).	34, 35
Offline activities	People who spend more time (…) in places where crimes take place, are more at risk of being victimized (Weulen Kranenbarg, Holt & van Gelder, 2019).	36, 37