



Universiteit Leiden

# PHISHING, A SUBTLE ART?

An analysis into phishing e-mails from a social  
psychological perspective

Kenney den Hollander  
S2025124

# COLOPHON

This document is a Master Thesis to complete the Master Crisis and Security Management at Universiteit Leiden, The Hague, The Netherlands.

Title:	Phishing, a subtle art? An analysis into phishing e-mails from a social psychological perspective
Version:	1
Author:	Kenney den Hollander S2025124
University:	Universiteit Leiden Wijnhaven Turfmarkt 99
First reader/Supervisor:	Dr.ir. V. Niculescu-Dinca
Second reader:	Prof.dr. B. van den Berg
Date	June 10, 2018

# Inhoudsopgave

<b>CHAPTER 1: INTRODUCTION</b> .....	<b>3</b>
<b>CHAPTER 2: THEORETICAL FRAMEWORK</b> .....	<b>6</b>
2.1: VICTIM-BASED THEORY .....	6
2.2: OFFENDER-BASED THEORY.....	9
<b>CHAPTER 3: METHODS</b> .....	<b>22</b>
3.1. RESEARCH QUESTION.....	22
3.2. RESEARCH DESIGN .....	22
3.3. OPERATIONALIZATION .....	25
3.4. UNIT OF ANALYSIS & UNIT OF OBSERVATION .....	26
3.5. CASE SAMPLING .....	26
3.6. METHODS .....	29
<b>CHAPTER 4: ANALYSIS</b> .....	<b>31</b>
4.1: GENERAL OBSERVATIONS .....	32
4.2: AN ANALYSIS OF DIFFERENT KINDS OF PHISHING E-MAILS .....	34
4.3: CONCLUDING REMARKS .....	41
<b>CHAPTER 5: CONCLUSION</b> .....	<b>42</b>
5.1: CONCLUSIONS.....	42
5.2: RECOMMENDATIONS.....	43
<b>BIBLIOGRAPHY</b> .....	<b>46</b>
<b>APPENDIX A: OPERATIONALIZATION TABLES</b> .....	<b>53</b>
<b>APPENDIX B: PROTOCOL FOR CONTENT ANALYSIS &amp; CODING SCHEME</b> .....	<b>57</b>
<b>APPENDIX C: CODING PROTOCOL</b> .....	<b>58</b>
<b>APPENDIX D: GENERAL TABLE</b> .....	<b>60</b>
<b>APPENDIX E: PHISHING E-MAILS</b> .....	<b>61</b>

## Chapter 1: Introduction

The Internet. Arguably one of the most important inventions of our time, and an instrument that has made our lives easier in almost every conceivable way. It has enabled people to ‘shop, socialize, communicate, network and also be entertained via their personal computers and mobile devices such as smartphones (Arachchilage, Love, & Beznosov. 2016: p.1). Society seems to have become dependent on the Internet to the extent that it is almost impossible to imagine a world without it.

But this dependency comes at a cost. People tend to value technology (i.e. the Internet) only for what it does or can do for them (Latour & Porter, 1996). This attitude means that generally, people feel the need to understand technology for as far as it can help them to execute the specific task it is designed for (Latour and Porter, 1996). Internet users therefore often do not possess the precise technical knowledge that is needed to make use of the Internet in the safest way possible (Dhamija, Tygar & Hearst, 2006). This lack of technical knowledge leaves them vulnerable as the possibility for hacking and other security breaches increases (Liang & Xue, 2010).

Hacking is defined as the act of deliberately gaining (or attempting to gain) unauthorised access to computer systems (Furnell & Warren, 1999). Hackers have a wide array of possible methods to achieve that goal, but a general distinction is made between technical methods and non-technical methods. Technical methods focus on the exploitation of flaws in computer systems while non-technical methods concentrate on taking advantage of human weaknesses. The application of the latter makes sense as humans are often the weakest link in a security chain (Sasse, Brostoff, Weirich, 2001). The abuse of the weakest link in computer systems (i.e. the people who use them) is known as social engineering (Bossworth, Kabay & Whyne, 2002; Huber, Kowalski, Nohlberg & Tjoa, 2009).

The term social engineering is an umbrella term that covers a wide range of different kind of attack vectors; phishing is one of them. Phishing is a form of hacking that is used by offenders to acquire sensitive information from unsuspecting customers by acting as if they are a trustworthy third party (Jagatic, Johnson, Jakobbson & Menczer, 2005: p.1; Garera, Provos, Chew, & Rubin, 2007: p.1). Phishers very often make use of spoofed e-mails to trick people into sharing this kind of information (Hong, 2009). This form of hacking directly targets the human, therefore circumventing the different technical security measures that are in place (Hong, 2009: p.1).

The Anti-Phishing Working Group (APWG), who advises national governments; global governance bodies; global trade groups; and multilateral treaty organisations on cybersecurity issues, claims that phishing is still a real problem. They found that: ‘in 2016, the number of phishing attacks, and the number of domain names used for phishing, reached an all-time high’ (Aaron & Rasmussen, 2016: p.5). A report by antivirus company Webroot (2017) supports this statement by arguing that phishing attacks are among the most prominent causes of data breaches, a claim that is supported by the European Union Agency for Network and Information Security (ENISA, 2017). Phishing attacks have already led to several kinds of damaging losses, including the loss of intellectual property and the loss of customer information by companies (Hong, 2009: p.1). These statistics reflect a tangible threat to citizens, companies and governments all around the world.

Understanding how these phishing attacks are executed could help to combat this threat. It would help to get a deeper understanding of the different methods that are used by phishing offenders to achieve compliance with their victims. This deeper understanding could first and foremost contribute to awareness among users of the Internet. Secondly, this detailed insight into different kind of attack vectors is needed to develop effective countermeasures and to protect knowledge workers from social engineering attacks (Krombholz, Hobel, Huber, & Weippl, 2015: p.9).

To be able to achieve this goal, this research aims to analyse a set of successful phishing attacks from a social psychological point of view. A theoretical framework will be developed that is built upon offender-based research as well as victim-based research. This process should provide an extensive overview of the different social psychological mechanisms that are used by phishers to achieve compliance with their victims, and why victims fall for such methods in the first place. This theoretical framework is then used to develop indicators that will make it possible to perform a qualitative content analysis on a set of phishing e-mails. This analysis should present the necessary information to answer the following research question:

*How have phishing offenders applied social psychological principles in phishing e-mails with a subject line that was among the most clicked general subject lines of 2017-2018?*

Prior research has found that social psychology is applied in phishing attacks, and in social engineering attacks in general, but this study adds new knowledge to the existing body of literature for a few reasons. The first distinguishing factor comes from the fact that most studies that have been conducted on this topic have taken a quantitative approach (Bullée, Montoya, Pieters, Junger, & Hartel, 2018; Workman, 2007). Secondly, there is relatively little research done on phishing as a specific attack vector. Often, researchers look at social engineering attacks in general and only discuss phishing as an element of a bigger phenomenon without going into great detail regarding the separate elements of social engineering (Thornburgh, 2004; Krombholz et al., 2015).

Qualitative research on phishing is scarce. Ferreira, Coventry & Lenzini (2015) aimed to develop a framework that can be used to analyse persuasive techniques in phishing e-mails. Although elements of this framework are quite useful, a re-evaluation is necessary for three reasons. The first issue relates to the lack of theory on visual deception, an issue that was brought up by the authors themselves (Ferreira, Coventry & Lenzini, 2015: p.11). The second issue is the problematic merger of different kinds of psychological principles. For their framework, they tried to merge social psychological principles from various theories, and in their attempts to do so have made some questionable decisions that will be discussed further in this research. In addition to that, the authors have failed to adequately substantiate why certain decisions were made.

This research adds to the study mentioned above by re-evaluating the merger of psychological principles and by expanding on the framework through the incorporation of additional theory on visual deception. In contrast to prior research, this renewed framework will be applied to a set of successful phishing attacks instead of a randomly selected set of phishing e-mails without any information regarding their possible success rate. This process should generate enough information to be able to develop some practical recommendations to combat phishing.

## Chapter 2: Theoretical framework

Most phishing attacks are carried out as a three-step process (Chandrasekaran, Narayanan & Upadhyaya, 2006; Hong, 2009) The first step is for phishing offenders to gather a set of e-mail addresses through social engineering attacks, web pages and forums. Then, they sent out a significant number of phishing e-mails using anonymous servers or compromised machines. These e-mails contain different types of content (depending on a phisher's selected method), but they all include some form of a hyperlink that a victim is supposed to click. In the last step, the website redirects the victim to a webpage where he/she is required to fill in personal details. This fake website usually contains input forms requesting details like credit card or social security numbers. If a victim shares these details, their information will be directly transferred to the phishing offender. The phishing offender can now abuse these data to steal money or services (Clayton, 2007).

The most common way for a phisher to abuse these details is by breaching the authentication protocol that is in place to guarantee a safe method for customers to log in to online services (Clayton, 2007: p.83). In its most simplified form, the authentication protocol that is used for an online session with an organisation is for the customer to supply a login name and secret password to that organisation. If a phisher can obtain a customer's details, he/she could then masquerade as the customer to log into their accounts (Clayton, 2007). This process could theoretically be repeated an unlimited amount of times until the customer changes the password or the account is frozen by the bank (Clayton, 2007).

This research, and therefore this theoretical framework, will focus on the second step of this three-step process. It will focus on the content of different kinds of phishing e-mails. More specifically, this research will look into how social psychology plays a role in the content of these e-mails. To be able to conduct such an analysis, a body of knowledge will be discussed that consists of victim-based theory and offender-based theory. It is necessary to examine both perspectives as they affect each other to quite a significant extent. The insights that will be gained from this body of knowledge will then be used to develop indicators that are used to conduct the qualitative content analysis that should provide the answers to the research question.

### 2.1: Victim-based theory

To be able to understand why phishing offenders choose a specific method, it is of importance to understand what makes victims vulnerable. What factors increase the chance of people

complying with the requests of a phishing offender? Two elements need to be discussed to be able to answer that question. The first is the cognitive process that underlies the decision-making process, and more importantly the way that process can be manipulated. The second element is the lack of technical knowledge and the effect this has on the online behaviour of victims.

#### 2.1.1: Central and peripheral routes to persuasion

People's brains do not always operate at their full processing capacity (Petty & Hinsenkamp, 2017). It would be impossible for someone to assess every single piece of information they receive with great detail. If people pondered about every single decision they make on a daily basis, they would not get much done. To be able to cope with the enormous amount of information that they encounter, people make use of decision-making shortcuts. These rule-of-thumb strategies allow people to function without always having to think about what to do next. These shortcuts are called heuristics, and they decrease the decision-making time, allowing an individual more time to process complex pieces of information (Petty & Hinsenkamp, 2017: p.2). This difference between relatively high degrees of thinking and relatively little thought has consequences for the way in which information is received and its persuasive impact (Petty & Hinsenkamp, 2017: p.3).

Persuasion that relies on relatively high degrees of thinking is described as the *central route* to persuasion (Rusch, 1999). The concept of the central route to persuasion is built on the idea that changes in attitude are the result of a person's careful consideration of information (Petty & Cacioppo, 1986; Rusch, 1999). People tend to think deeply about subjects when they are motivated to learn more about a topic, or when they are already relatively knowledgeable regarding a certain topic (Petty & Hinsenkamp, 2017). The success of the central route to persuasion therefore relies on systemic and logical arguments (Rusch, 1999). But this process of deep thinking is not enough to achieve compliance. This process only leads to persuasion when the arguments, that are used to force individuals to think deeply, trigger favourable emotions (Petty & Hinsenkamp, 2017:). If the arguments that are made in the message are compelling enough, favourable thoughts will be evoked that will increase the chances of compliance (Petty & Cacioppo, 1986; Rusch, 1999). In contrast, if the arguments are deemed too weak to be convincing, chances of compliance decrease (Petty & Cacioppo, 1986). This is why Rusch (1999) argues that the central route to persuasion is not the most effective way for social engineers to achieve compliance. Social engineers rely on deceit, they aim to achieve compliance by misleading their victims. They do not want to target highly knowledgeable victims that will process information with great detail as it would decrease their chances of success.



The *peripheral route* to persuasion seems more suitable for phishing offenders and social engineers in general. The offender that applies this route to persuasion aims to bypass logical argument and aims to achieve compliance from other individuals through relatively little thinking (Rusch, 1999). To avoid a process of deep thought and to evoke a process of relatively little thinking, social engineers aim to trigger decision-making heuristics. Such heuristics develop from a young age, and they are triggered when we encounter a phenomenon we experience as highly familiar. Trusting an authoritative figure is an example of such a decision-making shortcut. From a young age we have been conditioned to trust authority, and far more often than not it has brought us practical advantages to follow that social rule (Cialdini, 2009). This idea remains unchanged as we grow older and it slowly evolves into a mental shortcut that is applied whenever we deal with authority. Whenever we encounter an authoritative figure, there is a high probability that our first reaction is to assume that whatever they say is correct and that it will be to our advantage if we comply with their requests (Cialdini, 2009).

But there is a dangerous consequence that stems from this process. When the authority heuristic is activated for example, the decisions made by authority figures are hardly questioned. The possibility arises that when a clear error is made, nobody lower in the hierarchy will question it (Cialdini, 2009). This is what makes victims vulnerable. Heuristics are such a trusted mechanism in the decision making process, that the decisions that result from these heuristics are hardly challenged. Phishing offenders aim to exploit these dangerous side-effects of heuristics. An effective way to trigger these mental shortcuts is by evoking strong emotions in their targets. These strong emotions meddle with a victim's ability to call on his or her capacity for logical thinking, acting as a barrier to the process of deep thinking (Rusch, 1999).

#### 2.1.2: A lack of technical knowledge

A second factor that contributes to the vulnerability of Internet users is the lack of technical knowledge regarding the Internet. According to Dhamija, Tygar and Hearst (2006: p.2): 'Many users lack the underlying knowledge of how operating systems, applications, email and the web work and how to distinguish among these'. Generally speaking, users are aware that there are risks that have to be taken into account when the Internet is used and that it is necessary to protect their computer from certain problems like malware (Downs, Holbrook, & Cranor, 2006: p.10). However, they appear to be less aware of social engineering attacks that are aimed at obtaining information directly from them (Downs, Holbrook & Cranor, 2006: p.10).

Several cues can be used to determine if an e-mail or website is trustworthy, but Internet users very often misinterpret them. An example of this is the presence of a lock icon in a browser's chrome. A lock icon implies that the data that is passed between the browser and the server remains private. A website is then regarded to be SSL (Secure Sockets Layer) protected (Wagner & Scheijer, 1996). A phishing website will not have a lock icon in the browser's chrome, as the people behind that website will not have been able to obtain the SSL certificate that is needed for that to be possible. Users are often unaware that a site is only SSL protected if the lock icon is situated in the chrome of a browser. Many users believe that merely the presence of a lock icon somewhere on the webpage implies that the website is safe (Downs, Holbrook & Cranor, 2006).

A similar conclusion was drawn by Dhamija, Tygar and Hearst (2006) who found that a large percentage of the participants in their research, incorrectly judged web pages based on the content and how professional it looked, not taking into account that web pages can easily be copied. Their study showed that even when users expect certain cues, many of them cannot differentiate between a real and fake website (Dhamija, Tygar, & Hearst (2006: p.10). This lack of technical knowledge provides phishers with opportunities to trick people into handing over their personal details.

## 2.2: Offender-based theory

So how do phishing offenders aim to exploit these vulnerabilities? This part of the theoretical framework will discuss some of the different methods phishing offenders can apply to achieve that goal. The methods that will be discussed all have their origins in the field of social psychology but have been applied in other fields also. A small distinction will be made between methods that rely on visual deception and methods that consist of the use of social psychological principles.

### 2.2.1: Visual deception

Phishing offenders aim to give victims a false sense of security. One way they aim to do so is by designing their e-mails or websites to be similar to authentic e-mails or websites. According to Dhamija, Tygar & Hearst (2006) phishing offenders use visual tricks to mimic legitimate text, images and windows. According to the authors there are three different kinds of visual deception that are applied to mislead potential victims (Dhamija, Tygar & Hearst, 2006: p.4).

#### **1: Visually deceptive text**

The first method to apply visual deception relies on text to deceive victims. Text is often used

in a deceptive way by obfuscating a URL or e-mail address. With this method, phishing offenders deliberately obfuscate the URL that leads to the phishing website. According to Garera et al. (2007) there are four different ways to do so:

*Type 1: Obfuscating the Host with an IP address.*

‘In this form of attack the URL’s hostname is replaced with an IP address, and usually the organization being phished is placed in the path’ (Garera et al., 2007: p.1).

*Type 2: Obfuscating the Host with another Domain.*

‘In this form of attack the URL’s host contains a valid looking domain name, and the path contains the organization being phished. This form of attack usually tries to imitate URLs containing a redirect so as to make it appear valid’ (Garera et al., 2007: p.1)

*Type 3: Obfuscating with large host names.*

‘This form of attack has the organization being phished in the host but appends a large string of words and domains after the host name’ (Garera et al., 2007: p.1)

*Type 4: Domain unknown or misspelled.*

‘Here there is no apparent relationship to the organization being phished or the domain name is misspelled’ (Garera et al., 2007: p.1).

Figure 1 provides four different examples of obfuscation methods. These obfuscation types will also be used in the content analysis that will be applied to the set of phishing e-mails. Phishing offenders mainly obfuscate URL’s to evade antispam filters (Patil, 2010). A spam filter is a filtering solution that is applied to an e-mail system which uses a set of mechanisms to assess what messages are potentially harmful (spam) and which messages are not (Anslinger, 2013). If such a filter is evaded, there is an increased chance of their potential victim opening the phishing e-mail and reading it.

Type	Example
1	http://210.80.154.30/~test3/.signin.ebay.com/ebayisapidllsignin.html http://0xd3.0xe9.0x27.0x91:8080/.www.paypal.com/uk/login.html II
2	http://21photo.cn/https://cgi3.ca.ebay.com/eBayISAPI.dllSignIn.php      http://2-mad.com/hsbc.co.uk/index.html III
3	http://www.volksbank.de.custsupportref1007.dllconf.info/r1/vm/      http://spar-kasse.de.redirector.webservices.aktuell.lasord.info IV
4	http://www.wamuweb.com/IdentityManagement/      http://mujweb.cz/Ces-tovani/iom3/SignIn.html?r=7785

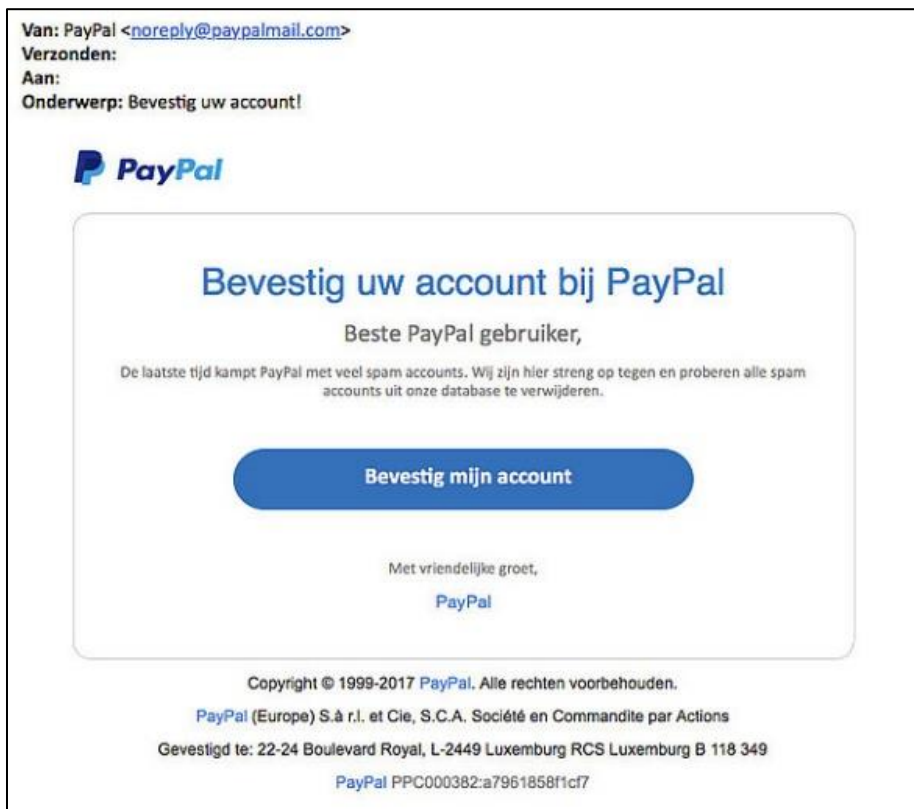
*Fig 1: Commonly Used URL Obfuscation techniques (Garera et al., 2007: p.1).*

When a spam filter is not able to block an e-mail, it could lead to the victim creating a false sense of security. As stated earlier, people often lack the underlying knowledge of how the technology works, and they are often unaware that carefully constructed phishing e-mails can sometimes slip through the spam filter and end up in a regular mailbox (Dhamija, Tygar, & Hearst, 2006: p.2). The people that are unaware of this might believe the phishing e-mail to be legitimate when it has not been blocked by the spam filter. In addition to this, ‘some users do not understand the meaning or syntax of domain names and cannot distinguish legitimate versus fraudulent URLs’ (Dhamija, Tygat & Hearst, 2006: p.2). A type 1 URL obfuscation might lead people to believe that the URL belongs to the company because it has the company’s name in it (Dhamija, Tygat & Hearst, 2006). If a victim believes that a URL is legitimate, this could potentially lead to the activation of a ‘trust-heuristic’ which guides victims to the peripheral route of thought (Cummings, 2014).

A second way to use text as a deceptive tool is by creating hyperlinks that are not obfuscated but consist of simple words like *Log in here* or *Activate your account here*. These hyperlinks are in sync with the rest of the content, to increase the chance of compliance. So when a phishing e-mail contains information regarding a new password, it makes sense to add a hyperlink that says log in here. Almost every phishing e-mail consists of an example of deceptive text as the victim has to click a hyperlink to either be directed to a phishing website or to have malware installed on their computer.

## 2: Images masking underlying text

To avoid the danger of someone noticing the obfuscated URL, phishers can also use an image of a legitimate hyperlink. When clicked this image redirects the user to the phishing website (Dhamija, Tygar & Hearst, 2006). Figure 2 provides an example of this kind of visual deception. As you can see, the victim is expected to press the blue confirm my account image, which is also used in legitimate PayPal e-mails. In reality the blue button will redirect the user to a fake website as there is a malignant hyperlink underlying the image.



*Fig 2: An example of an image masking underlying text. Obtained from: <https://opgelicht.avrotros.nl/alerts/item/let-op-valse-e-mail-paypal-bevestig-uw-account/>*

## 3: Windows masking underlying windows:

A third technique to apply visual deception is to place an illegitimate browser window on top of, or next to, a legitimate window. If they look alike, users may wrongfully think that they belong to the same source. This is especially a problem for users who make use of browsers that allow pop-ups without notification (Dhamija, Tygar & Hearst, 2006: p.4). Without a notification the illegitimate website could just pop-up without the user even noticing. And if the

illegitimate website is designed to look authentic, the user could quite easily come to believe that he/she is using the legitimate website.

### 2.2.2: Social psychological principles

A second way to effectively abuse the vulnerabilities of Internet users, is the use of social psychological principles. Following elements of the framework provided by Ferreira, Coventry and Lenzini (2015), two schools of thought regarding the use of social psychology in social engineering will be discussed: (1) Cialdini's (2009) theory on *the principles of persuasion* and (2) Stajano and Wilson's (2011) *principles for systems security*. Some of the different principles that will be discussed rely on the same psychological mechanisms to achieve compliance. The aim will be to merge the principles that share similar characteristics. In contrast to Ferreira, Coventry and Lenzini (2015) all these decisions will be substantiated. In addition to that, it will also be explained why some of the principles that were merged by Ferreira, Coventry and Lenzini (2015) have been treated as separate principles in this research.

Cialdini constructed six principles of persuasion that can be used to persuade somebody to comply with a request. In line with the argument made by Rusch (1999) and Petty and Hinzenkamp (2017), he discusses the idea that we have pre-programmed heuristics we rely on to process information, that can be used to dupe us into using them at the wrong time (Cialdini, 2009). Stajano and Wilson (2011) discuss the idea that many attacks on computer systems result from the fact that security engineers do not understand the psychology of the system users they aim to protect. By studying several kinds of scams and 'short cons' they have developed a set of general principles about the behavioural patterns of victims and discuss how these principles are by offenders (Stajano & Wilson, 2011).

#### 2.2.2.1: *The principle of authority*

The first of these six principles is the Principle of Authority (Cialdini, 2009). This principle comes down to the idea that people are more inclined to comply with requests of authoritative figures. People who are lower in the organisational hierarchy are often unable to make important decisions, which leads to them transferring the decision to someone they believe is in charge (Cialdini, 2009). The effect of authority on the decision-making process was studied in Stanley Milgram's (1963) shock experiment and the replications of that study (Blass, 1999). Milgram found that 26 of the 40 test-subjects that were part of his study, did not hesitate to deliver lethal doses of electric shocks to another human test-subject when they were instructed to do so by a man they genuinely believed to have legitimate authority (Bullée et al., 2017: p.4).

As we are conditioned to comply with authority, people often comply without questioning. Even if the assessment made by an authoritative figure is apparently wrong, the request still very often remains unchallenged (Davis & Cohen, 1981).

Stajano & Wilson (2011) also discuss the existence of an authority heuristic. They also support Cialdini's claim that the authority heuristic can be abused to persuade victims to comply with a request. They describe this mechanism as *The Social Compliance Principle*. In line with the argument made by Cialdini, they claim that the central psychological insight that should be taken from this principle is the idea that it is difficult for a random actor to force someone else to behave in the way he/she desires. Why would they listen to someone they do not know? It is much easier for an offender to achieve that goal by letting the victim 'behave accordingly to an already-established pattern, namely that of obeying a recognized authority' (Stajano & Wilson, 2011: p.12). Based on the abovementioned arguments, both principles rely on the same psychological mechanism to achieve compliance. These principles will therefore be merged into one authority principle.

The goal of the social engineer is to trigger this heuristic, to use it to guide the victim to the peripheral route of thought. Cialdini (2009) argues that three symbols of authority exist that can be used to evoke this heuristic. Of these three symbols (titles, clothes and luxury products), the use of titles is the only symbol that is used online. Research done by Hofling, Brotzman, Dalrymple, Graves, and Pierce (1966) found that 95% of their test-subjects complied with a blatantly incorrect request when they believed someone with an official title made the request. Phishing offenders make use of this by adding titles to their phishing emails. For example, that of a CEO (Stajano & Wilson, 2011).

#### *2.2.2.2: The principle of conformity*

The second principle is the Principle of Conformity. This principle is based on the idea that we determine what is correct by finding out what other people think is right (Cialdini, 2009). When we are unsure about our decisions, we look at other people for confirmation (Smith & Fuller, 1972). If a group of people act in a certain way, we often believe it to be the correct way to behave and are therefore more likely to follow that behaviour (Cialdini, 2009). Again, there is logic to this way of thinking. We are conditioned to abide by (social) rules, which is why it rarely occurs that people choose not to abide by them. Mimicking the behaviour of others will therefore generally allow us to make fewer mistakes and enjoy more advantages than when we would not follow these social rules (Cialdini, 2009; Bandura, Grusec & Menlove, 1967).

Stajano & Wilson (2011: p.13) share the idea that people tend to look at others to decide what actions to take. They describe this as *The Herd principle*. From a security perspective, this implies that people tend to let their guard down when they believe that the people around them appear to share the same risks. When somebody receives a request, they will feel safer when they think that others close to them have already complied with the same request and have not gotten into trouble (Stajano & Wilson, 2011: p.13-14). So, like Cialdini (2009), Stajano & Wilson (2011) argue that decision-making is influenced by the behaviour of others around the decision-maker. Both principles rely on the same psychological mechanism to persuade victims and will be merged into one conformity principle.

Like all principles that will be discussed, the Principle of Conformity can be manipulated to achieve more malignant goals. As stated, social engineers make use of this principle in their attacks by emphasising that other people have already complied with their request. An example could be an e-mail to an employee stating that a system check is being conducted throughout the company. This is done because a dangerous virus has been doing the rounds. It is then emphasised that his or her colleagues have already provided the offender with the necessary information and that the victim needs to send in his or her details so their computer can be checked. Stating that others have already complied with the request achieves a few goals. The first is that the conformity heuristic is activated, as the victim believes that the people around him have already complied. The victim does not want to be the only employee who refuses to give up information. Refusing to follow social rules could lead to negative social consequences. Secondly, none of the colleagues will have mentioned that something went wrong during the system check, which may give the victim a false sense of security. Thirdly, the e-mail evokes a sense of urgency. Fear, in this example resulting from the possibility of a virus, has the potential to affect the decision-making process (Hastings, Stead & Webb, 2004). When fear comes into play, a victim is far more likely to follow the peripheral route of thought. This leads to an increased chance of compliance with the offender's request.

#### *2.2.2.3: The principle of reciprocity*

Thirdly, the Principle of Reciprocity. This principle refers to the idea that people feel obliged to try to repay, in kind, what another person has provided them (Cialdini, 2009). As with most of the principles that are discussed in this theoretical framework, we have been conditioned from a young age to follow this principle. Each of us has been taught to follow this rule, and everybody knows the social sanctions applied to anyone who does not (Cialdini, 2009). The labels we assign to someone who does not adhere to this rule are mostly negative (Cialdini,



2009). Because people tend to dislike people who only take but don't try to give back, they will often try not to be seen as such a person (Cialdini, 2009; Regan, 1971). This principle has the potential to produce an affirmative answer to a request that, except for the existing feeling of indebtedness, probably would have been refused (Cialdini, 2009). It is the feeling of indebtedness that is of great importance in this process.

This feeling of indebtedness even remains when a stranger does us a favour we have not asked for (Cialdini, 2009). This provides the phishing offender with the possibility to do the victim a favour (or act as if he has done the victim a favour) and still being able to create a feeling of indebtedness within the victim. A second interesting feature is that it can trigger unfair exchanges, another feature phishing offenders use. A favour of small size can contribute to the idea that one should agree to a larger return favour (Regan, 1971). Phishers can do the victim a small favour and could still try to ask for a bigger request in return, without their chances of success diminishing. A third method that can be used by phishing offenders is called the rejection-then-retreat technique (Cialdini, 2009). To increase their chances of compliance, phishing offenders could make a substantial request, that will probably be turned down. After that refusal, phishers could ask for the smaller favour they initially wanted to be fulfilled. This trick often works as the rule of reciprocity also applies to concessions (Cialdini, 2009). The smaller request is seen as a concession made by the phisher, which leads to the victim feeling obligated also to do a concession and comply with the smaller request (Cialdini, Vincent, Lewis, Catalan, Wheeler, & Darby 1975).

#### *2.2.2.4: The principle of commitment and consistency*

The fourth principle is the Principle of Commitment and Consistency. It consists of the idea that when an actor makes a promise or adhesion, they are more likely to stick to that cause. People tend to do so because consistency is valued and adaptive in most circumstances, while inconsistency is seen as a negative personality trait (Cialdini, 2009). There is logic to this, as consistency provides people with a certain sense of security. A society where nobody would keep their promises would quickly fall into chaos (Cialdini, 2009). People rely on others to act consistently and others expect them to do the same. By doing so, people minimise the chance of social sanctions. But because it is usually in our best interest to be consistent, the consistency heuristic is easily activated (Cialdini, 2009). This tendency to act consistently is even strong enough to make us do things we would not do in a typical situation. Moriarty (1975) found that when people can make others commit to a request, they are far more likely to comply than when

an actor would just request something without any form of prior commitment. This is even applicable to a potentially dangerous request (Moriarty, 1975).

Phishing offenders have a few methods to activate the consistency heuristic and to make victims do something they usually would not. As shown by Moriarty (1975) an effective way to do so is by getting the victim to commit. After the victim has made such a commitment, the chance of compliance will increase (Sherman, 1980). An effective way to abuse the power of commitment is the so-called foot-in-the-door technique, which consists of the idea that one can achieve compliance with a large request by starting with a little request (Cialdini, 2009). The theory behind this is that even a small request has the potential to affect a victim's self-image in a way that he/she is more likely to comply with a request. As Freedman and Fraser (1966: p.201) put it:

‘What may occur is a change in the person's feelings about getting involved or taking action. Once he has agreed to a request, his attitude may change, he may become, in his own eyes, the kind of person who does this sort of thing, who agrees to requests made by strangers, who takes action on things he believes in, who cooperates with good causes.’

The study done by Freedman and Fraser (1966) proves that people should be cautious about agreeing to even the smallest request. It can lead to them agreeing to much larger requests, and even with a variety of large requests that are only remotely connected to the earlier requests (Cialdini, 2009). This is why phishers are so keen to persuade a victim to make a commitment. In addition to this, a written commitment has even more persuasive power than just a verbal commitment. When a commitment is written down the individual can no longer deny its existence. It is in writing, and as people feel the tendency to act consistent with their choices, people can be relatively easily persuaded to follow up on the commitment (Cialdini, 2009). A second contributing factor to the persuasive power of a written commitment comes from the fact that it can be shown to other people. Even more than being consistent with oneself, people do not want to appear inconsistent in the eyes of another person (Cialdini, 2009).

#### *2.2.2.5: The principle of liking*

The fifth persuasive principle is the principle of liking. It is a pretty straightforward principle in the sense that few people would be surprised that people prefer to comply with a request made by someone they know and like (Cialdini, 2009). But what factors cause one person to like another person? Cialdini (2009) defines these factors as ‘halo effects’. ‘A halo effect occurs when one positive characteristic of a person dominates the way that person is viewed by others’

(Cialdini, 2009). One of these characteristics is physical attractiveness. Several studies found that people often favour good-looking people without even realizing it themselves (Efran & Patterson, 1976). Phishing offenders do not have much options to make use of this halo-effect, although examples do exist of phishing offenders adding a picture to their e-mail attacks. Similarity is another factor that can make people like one another. People seem to comply more often with people who share personal traits (Locke & Horowitz, 1990). A third method is to make someone compliments. An interesting observation about compliments is that they do not have to be accurate. Compliments produce just as much liking for the person who makes the compliment when they are true as when they are untrue (Drachman & Insko, 1978). Especially this last halo-effect can be used by phishing offenders to achieve compliance, as it is fairly easy to add a compliment to a phishing e-mail.

#### *2.2.2.6: The principle of scarcity*

Cialdini's final principle of persuasion is the principle of scarcity. This principle encompasses the idea that opportunities seem more valuable to people when their availability is limited (Cialdini, 2009). The idea that one can potentially miss out on something plays a significant role in human decision making (Cialdini, 2009). The power of this principle relies on two different factors. The first is the positive association people have with scarcity. A lot of people seem to think that if something is scarce, it must be of high quality. If a product has been sold often, making the product scarce, it must be worth it. Scarcity is used as an easy method to assess the quality of a product (Cialdini, 2009). The existence of a 'scarcity heuristic' results from that, as by following the scarcity principle we are usually and efficiently right about a product or service (Cialdini, 2009).

The second factor that explains the power of scarcity is the effect of the loss of freedoms. According to Brehm and Brehm (2013 as cited in Cialdini, 2009) whenever free choice is limited or threatened, our need to retain our freedoms makes us want them (as well as the goods and services associated with them) significantly more than before. So when scarcity comes into play and interferes with our prior access to an item or service, we will react by wanting and trying to possess the product or service more than we did before (Brehm & Brehm, 2013 as cited in Cialdini, 2009).

These factors leave room for exploitation by phishing offenders. An effective way for phishers to activate the scarcity heuristic is by creating newly experienced scarcity with their victims. Worchel, Lee and Adewole (1975) found that a drop from abundance to scarcity produced a

more positive reaction to a product than constant scarcity did (Cialdini, 2009). In other words, a product becomes more attractive when the availability of said product decreases significantly. Phishing offenders could make use of this information through e-mail communication in which they offer a widely available product and follow that up by sending an e-mail that notifies the victim that the product is now almost sold out. The strength of this approach comes from the fact that it also makes use of a second technique to use the principle of scarcity. By claiming that the product is almost sold out they have created an idea of social demand (Cialdini, 2009). Research has proven that social demand strongly affects how much people want to possess a particular product (Worchel, Lee & Adewole, 1975).

#### *2.2.2.7: The need and greed principle*

Stajano & Wilson (2011) argue that a person's needs and desires make them vulnerable. In their extensive research on different kinds of scams, they found that it was often these two driving factors that would cause people to fall for a scam. They defined this as the *Need and Greed Principle*, referring to the entire spectrum of human needs and desires that could explain someone's rationale for decision making (Stajano & Wilson, 2011: p.17-18. Seuntjens (2016) found that greed is related to less self-control and more impulsive behaviour. The need for a product or service can put people in a vulnerable position when they are dependent on someone else to be able to obtain that product or service. Phishing offenders can abuse this principle in several ways, but it would be most effective in combination with the Principle of Scarcity. Scarcity exacerbates the longing for a particular product or service. An observation phishers could use to their advantage.

In contrast to Ferreira, Coventry and Lenzini (2015), this research will treat the Need and Greed Principle as a separate principle. Although some of its elements can be paired with aspects from other principles, the Need and Greed Principle seems to be more of a general principle that can account for observations that cannot be explained by Cialdini's more detailed principles. For example, the Principle of Scarcity could potentially trigger a feeling of greed, but the Need and Greed Principle is broader than that. A product does not have to be scarce for it to trigger a feeling of greed. The offer of a free product can still trigger such a feeling, even when the product is not scarce.

#### *2.2.2.8: The Distraction principle*

The distraction principle comes down to the idea that people tend to focus on whatever retains their interest, which leaves room for phishers or other social engineers to do something to them

with a smaller chance of victims noticing (Stajano & Wilson, 2011). This principle more or less exists within every aforementioned principle. Every principle aims to guide their victims to the peripheral route of thought, by distracting them from what is really the offender's goal: to obtain personal information. They do so by creating a situation that is likely to interest a victim. An e-mail regarding a virus or the opportunity to win a prize is highly likely to trigger our interest. While Cialdini's principles of influence focus on concrete ways to distract a victim, Stajano and Wilson (2011) discuss the distraction principle as a more general phenomenon.

Following Stajano & Wilson (2011), this principle will be used as a more general principle that can account for certain words, sentences, paragraphs or images that cannot be explained by Cialdini's principles of influence but do rely on some form of distraction to achieve compliance. As mentioned earlier, the offer of a scarce product is a method of distraction that falls into Cialdini's principles. But the threat of a virus, does not really fall into any of these rather specific principles. It is therefore necessary to have a more general principle that can account for the elements that cannot be explained by Cialdini's theory.

#### *2.2.2.9: The Time principle*

The idea behind the Time Principle is that when victims are under time pressure to make an important decision, they use a different decision-strategy (Stajano & Wilson, 2011). This decision-making strategy is known as the peripheral route of thought and it is the at the heart of all principles that are discussed in this research. Although the effect of some of Cialdini's principles can be exacerbated by applying time pressure, none of them solely rely on time pressure except the principle of Scarcity. Again, Stajano & Wilson (2011) discuss this in a general way to account for every instance where time pressure is used to persuade a victim to comply. For example, claiming that a product is scarce evokes a sense of time pressure. But there are far more general examples that cannot be explained by Cialdini's (2009) theory. An account that will be deleted if someone does not change their details within a certain amount of time, cannot be explained by Cialdini's principles. So, like the Distraction principle, the time principle will be used to account for words, sentences, paragraphs or images that cannot be explained by Cialdini's principles of influence.

#### *2.2.2.10: The Deception principle*

The deception principle encompasses the idea that things and people are not always what they seem (Stajano & Wilson, 2011) Social engineers aim to deceive you into believing something that is not true. Deception defines phishing, as people masquerade as a trustworthy third party.

The entire goal of phishing is to make victims believe that offenders are someone they are not. Deception is at the core of every principle discussed earlier. They all aim to create a fake situation that is constructed in such a way that the victim believes it to be true. Whether that be an angry CEO that wants his money transferred as soon as possible, or the tax-man who is requesting a tax form.

Like the two aforementioned principles, this is a more general principle that can account for the words, sentences, paragraphs and images that cannot be explained by the more specific principles discussed earlier. For example, offenders often masquerade as an employee from the IT-department. This is different from the Principle of Authority because the IT-employee is not necessarily someone with authority. It is also different from the Distraction Principle, because this principle purely focusses on the people behind the scam. Who are they masquerading as?

#### *2.2.2.11: The dishonesty principle*

Stajano & Wilson's (2011) principle of dishonesty comprises of the idea that when a victim has agreed to do something illegal, it will be much harder for him or her to go to the police whenever they found out they have been scammed. When the victim was in some way elicited to illegal actions, he or she will have strong incentives not to report the crime. These incentives build in some security safeguards for the offender, which puts him or her in a favourable position (Stajano & Wilson, 2011: p.14-15). The mention of some illegal action should therefore immediately trigger a warning sign with the victim that something is wrong. By evoking emotions that meddle with the ability for deep thinking, phishers aim to make victims ignore these warning signs. The Dishonesty Principle is not a tactic that can be applied to achieve compliance, it is more an explanation as to why victims would not report a scam. The reason as to why a victim would willingly agree to take part in something illegal is actually fuelled by other principles like the Need and Greed Principle. This principle will therefore not be included in the analysis.

## Chapter 3: Methods

The previous chapters provided the relevance of this study and a theoretical framework that can be used to analyse the data that is necessary to answer the research question. This chapter will address the way in which this analysis will be conducted. This chapter will explain how the abstract world of theories and the empirical world will be connected. Secondly, it will allow for a discussion regarding the quality of this research. ‘Quality in research is dependent on honest and forthright investigations’ (Marshall, 1990). It is necessary to look for alternative explanations and to be self-critical about the way research is conducted (Whittemore, Chase & Mandle, 2001). Every research has to deal with biases and certain threats to validity. All methods have limitations, and all research involves multiple interpretations of data and results (Marshall, 1990; Smith, 1990). It is of importance to discuss these factors and to take them into account while conducting this research.

### 3.1. Research question

*How have phishing offenders applied social psychological principles in phishing e-mails with a subject line that was among the most clicked general subject lines of 2017-2018?*

Explanatory research implies that the research in question is intended to explain, rather than just describe, a studied phenomenon (Given, 2008). The research question that will be answered in this research can therefore be regarded to be of an explanatory nature. The aim is to study how theory from the field of social psychology can explain how phishers aim to achieve compliance from their victims. Explanatory research can help to study a phenomenon that has not been studied before in-depth (Given, 2008). As stated earlier, the use of psychological mechanisms in social engineering attacks has mostly been studied from a quantitative approach. This explanatory research could provide a deeper understanding of how this specific attack vector is applied by phishing offenders (Bullée et al., 2017; Workman, 2007).

### 3.2. Research design

This study will have a multiple comparative case study research design that will be used to conduct a qualitative content analysis. A deductive approach will be used, in which theory is analysed and then applied to a certain phenomenon. This deductive approach differs from an inductive approach in which researchers start with observations and then formulate a theory towards the end of the research based on those observations (Thomas, 2006). Cialdini’s (2009) theory on the principles of influence, Stajano and Wilson’s (2011) theory on the principles of system security, and Dhamija, Tygar and Hearst’s (2006) theory on visual deception will be

used to analyse a set of phishing e-mails. By doing so a contextualised insight will be given into how theory from the field of social psychology can be used to explain a phenomenon from the field of cybersecurity.

According to Yin (2003 as cited in Baxter & Jack, 2008: p.545) a case study should be considered when the focus of the research is to answer 'how' and 'why' questions. A case study offers the opportunity to apply those questions to a specific phenomenon within its context. A distinction can be made between several kinds of case studies varying from explanatory case studies to multiple case studies (Baxter & Jack, 2008). A multiple case study allows researchers to explore the differences within and between different kind of phishing attacks (Baxter & Jack, 2008). This method is selected to be able to study certain expectations that resulted from the body of knowledge. From the quantitative studies on this topic, we know that social psychological principles are applied in phishing attacks. However, it is still quite unclear as to how these attacks are conducted. How and when are certain principles combined for example? The expectation is that the use of social psychological principles differs per phishing category (Subchapter 3.5).

For this research, comparisons will be drawn to see how and in what different ways phishing offenders employ social psychology across different types of phishing categories (Yin, 2003 as cited in Baxter & Jack, 2008). The expectation is that the analysis will lead to 'contrasting results but for predictable reasons (a theoretical replication)' (Yin, 2003: p.47). This expectation results from the literature in the theoretical framework that discusses the idea that phishers aim to evoke different kinds of emotions, that are triggered by different psychological principles. The analysis of varying phishing categories will therefore likely lead to varying results.

Limitations of a multiple case study design include the fact that it can be costly and time-consuming to study multiple cases (Baxter & Jack, 2008: p.550). This research has aimed to strategically select the cases to deal with these limitations in an effective way (Flyvbjerg, 2006). The purpose of this multiple case study is to 'generate background material to a discussion about a concrete problem' (Solberg, Soilen & Huber, 2006 as cited in Gustaffson, 2017: p.5). The information that will be generated from this research can contribute to the development of practical recommendations that can be used when discussing this issue.

A few potential issues regarding the research design need further elaboration. The first is the transparency of this research: the principle that every scientist should make the essential elements of their work available and visible to other scholars (Moravcsik, 2014: p.48). There are



three dimensions to the concept of transparency that will be dealt with separately. The first is the transparency of data, which comes down to the question if readers have access to the evidence or data that is used to answer the research question (Moravcsik, 2014: p.48). The data that will be analysed is taken from online databases, from companies that have been targeted by phishers, and from organisations that aim to combat phishing. Everybody with a working internet connection can access this data. None of the data that will be used for this research is classified which should guarantee an adequate level of data transparency.

The second aspect of transparency relates to the analytical process. Analytic transparency allows readers access to information about how the data is analysed. It provides readers with a better understanding of how a researcher is able to make certain claims about the data (Moravcsik, 2014: p.48). Every research has to deal with biases and threats to validity. This is why an account has to be provided of the basis on which a particular conclusion is reached (Moravcsik, 2014: p.49). The discussed body of knowledge and the indicators that followed from that will allow us to do so. By applying theory-based indicators to the data, results from the analysis will be directly linked to theory to ensure an adequate level of analytic transparency. For the results from the analysis that cannot be explained by the theory that was discussed in the body of the knowledge, alternative explanations will be sought that are also supported by literature.

Thirdly, production transparency. This element of research looks into ‘the methods by which particular bodies of cited evidence, arguments and methods were selected from among the full body of possible choices’ (Moravcsik, 2014: p.48). The measures, cases and sources that are selected in a particular research are only a small amount of the data that could be of importance to the study (Moravcsik, 2014: p.49). The danger of selection bias comes into play here. Selection bias is a general problem in qualitative studies, as cases are often hand-picked instead of using datasets (Moravcsik, 2014: p.49). The same goes for this particular research. A set of selection criteria have been developed to account for the choices made relating to the selection of cases. These criteria address how the cases that are analysed in this research have been selected. However, this does not take away the fact that there is a substantial amount of cases that had also could have been selected for this research.

Replicability is another requirement for proper research. Replicability of a research implies that readers should have the necessary information to conduct your research similarly. Replicability allows other scholars to test your findings and see if they are empirically correct. The aim is to make results understandable enough for readers to be able to implement the study in their own situation (Stake, 1995 as cited in Baxter & Jack, 2008). In other words, ‘researchers working at

different points in time and perhaps under different circumstances should get the same results when applying the same technique to the same data' (Krippendorff, 1980: p.18).

As a qualitative content analysis will be applied a few comments have to be made. To draw valid conclusion from text, it is of importance that the procedure of classification is consistent. 'Different people should code text in the same way' (Weber, 1990: p.12). In some cases this is problematic as the meaning of a word or the definition of a category is ambiguous (Weber, 1990). To deal with this specific issue indicators are based entirely on theory, leaving little room for ambiguity. A coding scheme, a coding protocol and a general protocol for content analysis have been developed that explain how the process of coding should take place (Stemler, 2001). These actions should lead to an adequate level of stability and reproducibility (Potter & Levine 1999).

### 3.3. Operationalization

The next step is to determine how the different principles will be measured. This will be done through the construction of three operational tables that will provide an overview of the different indicators that have been developed to be able to measure the social psychological principles (Appendix A). The different operationalization table consist of (1) the theory they are based on, (2) the concept that is central in that theory, (3) a definition of that concept, and (4) the different indicators that will make the concept measurable. As stated earlier, these indicators have been deducted from academic literature to guarantee a higher level of validity. All theories, and the indicators that stem from those theories, are supported by a large amount of research. This should contribute to a higher level of internal validity. The internal validity is of importance to assess if the indicators really measure what they aim to measure (Whittemore, Chase & Mandle, 2001).

It is of importance to mention that all elements of the different theories have been discussed in the theoretical framework, but not all of those elements can be applied to phishing e-mails. If we look at visual deception for example, it is possible to place an illegitimate browser window on top of, or next to, a legitimate window. This method is not applicable to a phishing e-mail. The principles that are not applicable to phishing e-mails will not be a part of the operationalization tables.

### 3.4. Unit of analysis & Unit of observation

*Unit of analysis:* Researchers who use a case study design to conduct their research often have the tendency to attempt to answer a question that is too broad or a topic that has too many objectives (Baxter & Jack, 2008). To avoid this issue, it is of importance to define what the unit of analysis is going to be for this research. This study aims to study how social psychology is used by phishing offenders to achieve compliance from their victims. The results of the analysis will therefore tell us about the psychological mechanisms that are (ab)used by phishers in their attacks.

*Unit of observation:* What will be studied to be able to say something about the unit of analysis (i.e. phishers)? To be able to analyse what psychological mechanisms are used by offenders, a set of different kinds of phishing e-mails will be analysed. A content analysis of these e-mails should provide us with the necessary information to be able to say something about the unit of analysis. These e-mails can therefore be regarded as the unit of observation.

### 3.5. Case sampling

The next step is to discuss how the cases are selected. Miles and Huberman (1994: p.25) define a case as: ‘a phenomenon of some sort occurring in a bounded context’. The phenomenon that is analysed is the use of social psychological principles in the field of cybersecurity and the bounded context is its use in phishing e-mails. But how to decide what phishing e-mails should be selected for analysis? When one wants to sample in qualitative research there are two ways to do so. A researcher could either select a unique case or focus on a composed sample of different units. The latter will be applied to this research to compare the different units as explained in the subchapter about the research design of this research.

The objective of this research is to obtain information on the use of social psychology as an attack vector. According to Flyvbjerg (2006: p.13), a representative case or random selection is not always the most effective method to obtain such information. He argues that the average case often does not provide a lot of data. ‘Typical or extreme cases often reveal more information because they activate more actors and more basic mechanisms in the situation studied’ (Flyvbjerg, 2006: p.13). Based on this assumption, this study has selected a set of typical cases that should provide the necessary information to answer the research question.

It is essential to realize that phishing attacks occur very often, but that most attacks fail to achieve the goal of obtaining personal details. A significant amount of the phishing e-mails that are sent out end up in spam filters (Trusteer, 2009 as cited in Prince, 2009). Google for example claims that it uses artificial intelligence that can catch 99.9% of all spam and phishing e-mails (Metz, 2015). Thus, a substantial amount of phishing e-mails is not even read by potential victims. However, according to cyber security firm Trusteer (2009 as cited in Prince, 2009), the ones that are actually opened and read cost societies millions. It would not make sense to analyse phishing e-mails that are not even read by victims, as it would not provide any useful information. For that reason, the main criteria for case selection is that there is a high probability that the phishing e-mail was actually read by potential victims.

*KnowBe4*, the world's largest security awareness training and simulated phishing platform, recently conducted a study in which they sent phishing test emails to roughly 6 million users to find what subject lines were most likely to be clicked by potential victims (KnowBe4, 2017; Sjouwerman, 2018a; Sjouwerman, 2018b) The research provided an overview of what kind of general subject lines were most likely to be clicked and what e-mails were most likely to be read. Ideally, the most successful phishing e-mails ever would have been studied in this research, but there was no data to be found on the success rate of different kind of phishing attacks. Thus, a concession had to be made. This is why cases were selected with a relatively high probability of success in comparison to the large amount of phishing e-mails that are not even opened.

Unfortunately, the research conducted by KnowBe4 only goes back to 2017, which makes it nearly impossible for this research to include phishing e-mails from before that year. When comparing 2017 and 2018 the subject lines (and the e-mails that are selected based on those subject lines) can roughly be divided into six different categories. As mentioned earlier, the expectation is that the phishing e-mails (that are selected based on their subject line) aim to evoke different emotions and thus differ in the way social psychological principles are applied.

(1): *Phishing e-mails that contain information on the delivery of a product:*

(2): *Phishing e-mails that contain information regarding social media:*

(3): *Phishing e-mails that contain information regarding holiday offers*

(4): *Phishing e-mails that contain tax-related information*

(5): *Phishing e-mails that contain information regarding a user's account.*

(6): *Phishing e-mails that contain information related to a user's work environment.*

Often when companies have been the victim of a phishing attack, it proves that their security systems are vulnerable in some aspects. To prevent similar attacks from happening in the future, companies are often reluctant in sharing detailed information about the attack with the outside world (Richmond, 2011). In these specific cases it is difficult to retrieve the phishing e-mail that caused all the trouble. To deal with that the e-mails that are analysed have mostly been gathered from online databases like the *Fraude Helpdesk*, which is a Dutch database where consumers can send their phishing e-mails. They provided permission to use their e-mails. This database makes it possible to distinguish between different kinds of phishing e-mails, which is useful for this research for two reasons. Firstly it guarantees that the phishing e-mails have actually been read, otherwise it would not have been posted in the database. Secondly it assures that phishing e-mails can be found that correspond with the most clicked phishing e-mail general subject lines. The e-mails that have been analysed that have not been retrieved from *Fraude Helpdesk*, have been retrieved from either companies that have had to deal with a phishing attack, or companies that operate in the field of cybersecurity. Before the images were downloaded from the various webpages, the Four Fair Use Factors were applied to assess if the images could be taken from those websites without infringing on copyright (Digital Media Law Project, 2018).

It is common in qualitative research that data are based on 1 to 30 informants (Fridlund & Hildingh, 2000). However, more importantly the 'the sample size should be determined on the basis of informational needs so that the research question can be answered with sufficient confidence' (Bengtsson, 2016: p.10). This research has selected 19 different e-mails, divided amongst the different categories. It was assessed that more e-mails would not provide any extra useful information that could help to answer the research question.

### 3.6. Methods

This research will apply a qualitative content analysis to a set of phishing e-mails. Content analysis is a systematic method used to analyse textual data (Mayring, 2000). The aim of this method is to systematically (and in a replicable way) categorize text in order to make sense of it (Miles & Huberman, 1994). As mentioned, this research uses a deductive approach, so the categorization of text will also be deductive. ‘Deductive category application works with prior formulated, theoretical derived aspects of analysis, bringing them in connection with the text (Mayring, 2000). Researchers have to decide whether the analysis should be a *manifest analysis* or a *latent analysis* (Bengtsson, 2016: p.10) In a manifest analysis, the researcher analyses what is said in the text, and uses the words to describe the visible and obvious in the text. The researchers looks at the text in a very literal way, leaving little room for additional interpretation. This research will conduct a latent analysis, as it leaves more room for interpretation. A latent analysis is useful to look into the underlying meaning of text (Bengtsson, 2016). To able to analyse the social psychology behind certain words, sentences, paragraphs and images it is necessary to leave room for interpretation as this will not show from the literal meaning of the text that will be analysed.

When applying qualitative content analysis, the focus is put on a small number of cases. The categorised data is interpreted through an in-depth discussion. The goal of this is to draw conclusions from studied data to theory, rather than to a population (Mayring, 2000). This research will follow Mayring’s (2000) model on deductive content analysis (Figure 3). Theoretically based categories have been developed to analyse the different elements of social psychology that will be applied to the different cases. These categories need to be clearly defined, and coding rules must be given to determine when a text passage can be coded with a specific indicator (Mayring, 2000). A coding protocol and coding scheme have been developed to address these requirements efficiently. The cases will be analysed carefully and codes (related to the different elements) will be assigned to words, sentences, paragraphs and images. This coding process will be conducted by using software program *QDA Miner Lite*, which is a software program specifically designed for content analysis.

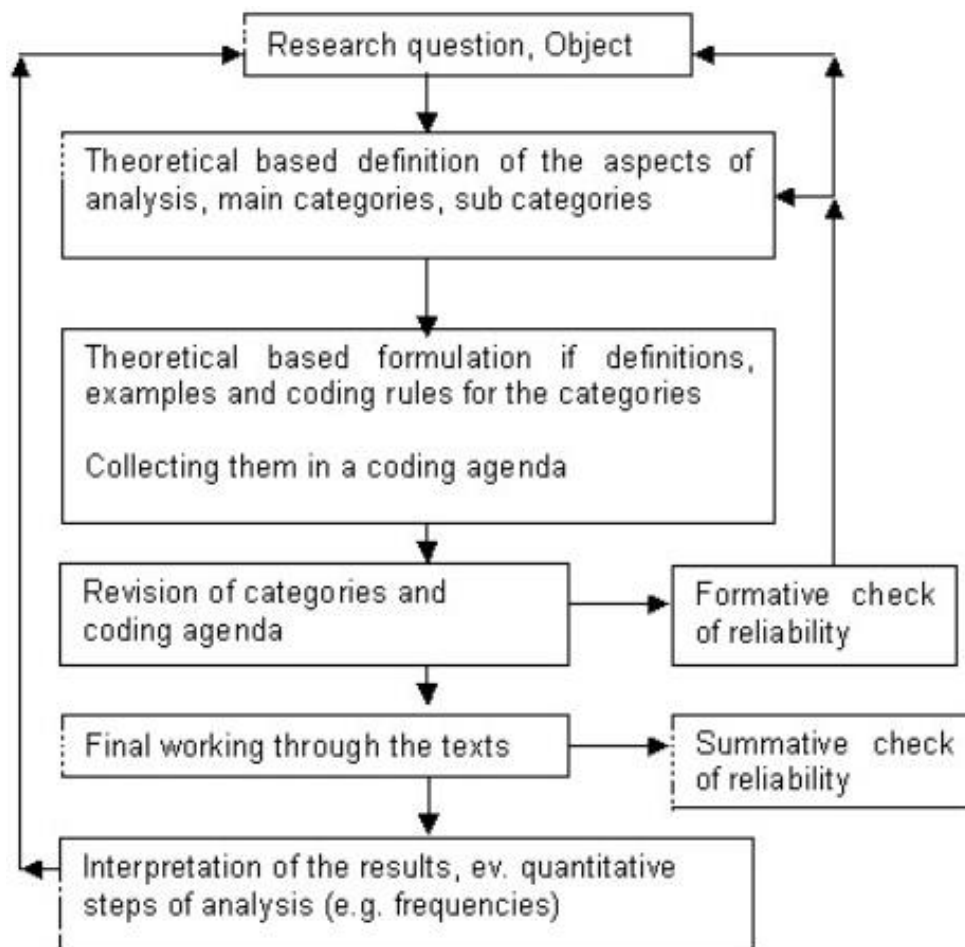


Fig.3: Step model of deductive category application (Mayring, 2000)

The protocol for content analysis (See Appendix B) gives an overview of the process that will be taken to conduct said analysis. This protocol could function as a guideline for other researchers who aim to replicate this study. As stated in the protocol, textual sources (based on research done by KnowBe4) will be download from online phishing databases like the *Fraude Helpdesk*. The findings from this analysis will be illustrated with marked words, sentences, paragraphs, and images and will be integrated into an in-depth discussion that will provide an answer to the research question.

The coding protocol (Appendix C) gives an overview of the different codes and their corresponding coding rules. These coding rules determine when a text passage can be coded with an indicator (Mayring, 2000). The coding scheme (see Appendix B) provides an overview of the different labels that have been assigned to the different codes.

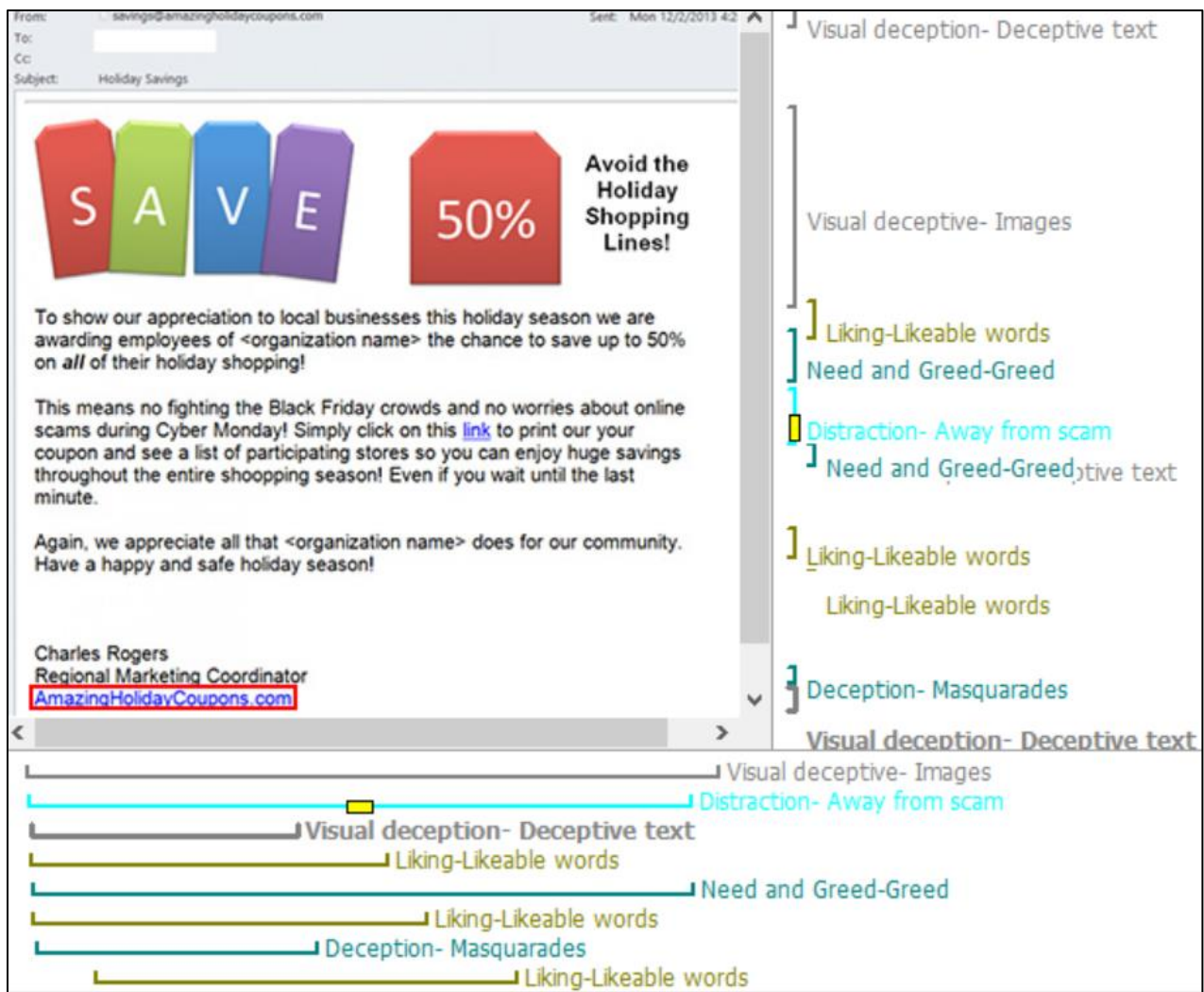
## Chapter 4: Analysis

Prior quantitative research has found that social psychological mechanisms are applied in phishing attacks. This qualitative content analysis will aim to focus on how phishers apply these principles. This chapter will report the findings of this analysis and will discuss what the meaning is of these research outcomes. The results will be linked to elements from the body of knowledge to guarantee a substantiated insight into the use of social psychological principles in phishing attacks.

Derived from the discussed body of knowledge, it is expected that social psychological mechanisms are applied differently across different attacks, depending on the kind of phishing attack and the method that corresponds with that attack. The different types of phishing e-mails that were discussed during the justification for case selection (Chapter 3.5) aim to evoke different kinds of emotions and therefore require the use of varying social psychological principles. The findings that result from this analysis will be integrated into a discussion on the question of whether or not this expectation was met.

Chapter 3 provided an insight into how concepts from the theoretical framework were operationalized and transformed into indicators that are used to conduct this qualitative content analysis. To get a better understanding of how this content analysis will be conducted Figure 4 provides an example of how these indicators have been applied to one of the cases that was studied in this research. All codes have different colours related to the principle they are grouped under. For example, all codes that belong to the Visual Deception principle (deceptive images and deceptive text) are grey. All e-mails have been added to Appendix E, so whenever the text refers to an e-mail it can be found in Appendix E. So what can be deducted from this analysis?





**Fig 4:** Example of how codes were assigned to the words, sentences, paragraphs or images that make up the content of a studied phishing e-mail. (14)

#### 4.1: General observations

Appendix D provides an overview of the total amount of times an indicator was assigned to certain words, sentences, paragraphs or images. Although the amount of cases that was studied for this research is not sufficient to make generalizing claims, this table still provides some interesting information. It can emphasise what principles require more attention. For example, the table shows that visual deception, and specifically the use of deceptive text, is the most common method applied by the phishers that constructed these different phishing e-mails. Deceptive text was applied in 94.7% of all studied cases, and the use of deceptive images was used in 63.2% of all e-mails. Visual deception was applied more often than any other social psychological principle, so it is of interest to discuss how this method was applied and what underlying factors might have contributed to this result.

When the theory from the body of knowledge is applied to this observation, this result does not come as a surprise. The act of masquerading as a trustworthy third party is at the heart of every phishing attack, and visual deception is a common method to appear as a legitimate party (Jagatic, Johnson, Jakobsson & Menczer, 2005; Dhamija, Tygar & Hearst, 2006). But why is it such a standard method? Firstly, it is a relatively easy method to implement. A simple way to appear trustworthy and authentic is by copying and pasting elements from e-mails or websites from an authentic party. In little over 60% of all phishing e-mails that were analysed, fake logos and other images were used by the phishing offender as a means to mislead the victim into thinking they were looking at an authentic e-mail. A similar observation can be made with regards to the use of deceptive text. In 94.7% of the studied cases, some form of deceptive text was used to mislead a victim. Some placed an image over a malignant hyperlink (E-mail 10), and in other cases they would simply create hyperlinks that consisted of words that were in sync with the overall content of the e-mail. The creators of E-mail 3 for example, merely created a hyperlink that consists of the words *log in to account*. Other phishers obfuscated a hyperlink in such a way that the victim could believe that the hyperlink belongs to the company that the phishers masquerade as (E-mail 5).

Apart from the fact that it is easy to implement, a second reason for the common use of visual deception is its effectiveness. Dhamija, Tygar and Hearst (2006) proved this when they found that more than 90% of their test-subjects were fooled by a phishing e-mail. People often incorrectly judge web pages based on the content and how professional it looks, not taking into account that web pages can easily be copied. As stated, phishers are aware of how easy it is to copy an authentic website. This shows from the studied cases in this research, as 94.7% of all e-mails consisted of some form of visual deception. So when done well, visual deception can be an effective and easy method to achieve compliance.

But there is an argument to be made that visual deception by itself is not enough to achieve compliance. In every studied e-mail, the principle of visual deception was accompanied by at least one other social psychological principle. This makes sense, as phishers would most likely want to hedge their bets instead of just relying on the persuasive power of just one principle. This idea is supported by Garera et al. (2007), who argue that phishers often combine social engineering techniques and sophisticated attack vectors in their attempts to obtain valuable information. The next subchapter of this analysis will focus on these combinations and how they are applied across the different types of phishing attacks.

Another observation that derives from Appendix D is that the Principle of Consistency has not been applied in any of the studied e-mails. This principle consists of the idea that whenever people make a promise or adhesion, they are likely to follow up on that promise or adhesion (Cialdini, 2009). An efficient way for phishers to abuse this is by making the victim commit to something. An explanation as to why this principle was not applied in the studied e-mails could be that for this principle to be effective multiple moments of contact are required. To come to a commitment, the victim will have to let the phisher know that he/she agrees to something. When this occurs, the phisher can abuse this heuristic by using the agreement to influence the victim's decision-making process (Cialdini, 2009; Sherman, 1980).

The fact that several moments of contact are required, does not fit into the common way that phishing attacks are conducted. As stated in the body of knowledge, phishing attacks usually consist of a three step process (Chandrasekaran, Narayanan & Upadhyaya, 2006; Hong, 2009). They first gather set of e-mail addresses and then send a substantial amount of phishing e-mails to all the e-mail addresses they were able to obtain. The aim of the regular phisher is not to focus on one specific target, but to reach as much potential targets as possible. This is the difference between regular phishing e-mails, that were studied in this research, and spear-phishing e-mails that contain content that is specifically focussed on individuals (Jagatic, Johnson, Jakobson, & Menczer, 2007). The Principle of Consistency seems more fitting for spear phishing than it does for regular phishing.

#### 4.2: An analysis of different kinds of phishing e-mails

So in combination with what other social psychological principles was visual deception used, and do these combinations differ per phishing category? The aim of this part of the analysis will be to see if, how and why the use of social psychological principles differs per category.

##### 4.2.1: Phishing e-mails containing information regarding taxes

Phishing e-mails that contain tax-related information consist of content that is aimed to mislead the potential victim by making them believe that they have to comply with a tax-related request. This could for example be a reminder from tax authorities to pay them (E-mail 16).

There seems to be a recurring pattern within this category. As mentioned before, the abundance of visual deception in the phishing e-mails is clear and logical. The interesting thing about this category is the observation that the use of visual deception is accompanied by the principle of authority in every e-mail that was analysed. The principle of authority consists of the idea that people are more inclined to comply with the requests of authoritative figures (Cialdini, 2009).

Phishers who construct phishing e-mails that could be put into this category often masquerade as tax authorities to achieve compliance. If tax authorities are perceived as a authoritative organisation by victims, the chance of compliance would increase as it is more likely that the authority heuristic is activated. So are tax authorities seen as authoritative figures?

A study conducted by Braithewaite (2003) provides an answer to that question. For a survey, done by the Centre for Tax System Integrity at the Australian National University (Braithewaite, 2001), 7754 persons were asked to agree or disagree with certain statements regarding Australia's Tax Office. The outcome was that most people saw the Tax Office as an authoritative organization, but they also seemed to have a largely positive attitude towards the Tax Office (Braithewaite, 2003). Participants agreed with statements like: *'No matter how cooperative or uncooperative the Tax Office is, the best policy is to always be cooperative with them'* and *'I accept responsibility for paying my fair share of tax'* (Braithewaite, 2003: p.20).

Statements like the one on cooperation prove why the authority heuristic has the potential to be effective. As argued in the body of knowledge, people have been conditioned to adhere to the requests from authoritative figures from a young age. Following the authority principle allows people to generally make fewer mistakes and enjoy more advantages than when they would not comply with authority (Cialdini, 2009). This is also applicable to the aforementioned statement. Throughout their lives people have experienced that in general it is better for them to cooperate with the Tax Office, as an uncooperative attitude could lead to negative consequences. The experiences they have gained with the Tax Office throughout the years, have contributed to the integration of the Tax Office into their authority heuristic. It is this aspect of the Principle of Authority that phishers aim to abuse. But there is a second principle that comes into play in a more implicit way. The answers from the survey also provide evidence for the Principle of Commitment. The majority of the respondents accepted responsibility for paying tax, and felt it as their moral obligation to do so (Braithewaite, 2003). The Principle of Commitment and Consistency consists of the idea that people tend to act in line with their past behaviour. So by claiming that they are cooperative towards tax authorities, they are more likely to do so in the future. This provides opportunity for phishers.

So that provides an explanation as to why the combination of these principles is potentially effective in this type of phishing e-mail. But how are these principles then implemented in the content. There are three different indicators that are used to measure the Principle of Authority in phishing e-mails. The use of titles seems to be the most common way to trigger the authority heuristic in phishing e-mails that belong to this category. Like the use of visual deception, it is

fairly easy to incorporate this method into the content. And as tax authorities are seen as authoritative figures, the presence of their name helps to activate this heuristic. The use of authoritative words, also contributes to this process. Braithwaite's (2003) study showed that people generally feel that they should be cooperative towards tax authorities, and words that set forth duties might pressure people to act accordingly to that attitude.

#### 4.2.2: Phishing e-mails containing information regarding holiday offers

Phishing e-mails that contain information regarding holiday offers aim to persuade the victim to comply with a request by offering them attractive holiday offers. The aim of phishing e-mails that belong to this category is to evoke an emotion that can lead to the victim applying the peripheral route to decision-making. The feeling that seems to be triggered most in these kind of phishing e-mails is a feeling of greed. This is what distinguishes this category from the other categories. Phishing e-mails containing information on holiday offers almost always offer the potential victim something, while the other categories usually request something from the victim. For that reason, this type of phishing e-mail relies on different social psychological principles to be potentially successful.

Stajano & Wilson (2011) argue that a feeling of need or greed can make people vulnerable. The wish to obtain a certain product or service can put people in a vulnerable position when they are dependent on someone else to obtain that product or service. This longing for certain products even leads to less self-control and more impulsive behaviour (Seuntjens, 2016). In other words, it can force people to use the peripheral route of thought. This explains why it would be attractive for phishers to evoke such a feeling of need or greed.

E-mail 11 provides an example of how such emotions are evoked. The e-mail gives the victim the possibility to win two free airline tickets to a destination of his/her choice. The only thing that needs to be done, is click a button that says *Ik wil meedoen!* (I want to join!). The fact that something relatively expensive is offered for free, is an exciting thought to many of us. It almost instantaneously evokes a feeling of greed within people. This seems quite obvious, but the interesting thing is that phishers seem to have figured out that this feeling of greed can be exacerbated even further. They are able to do this by pairing the Need and Greed Principle with the Principle of Scarcity or the Time Principle.

E-mail 10 shows how the principles are paired together to achieve maximum effect. The e-mail provides the victim with the opportunity to win six free tickets to a leisure park of his/her choice. Again, this evokes a feeling of greed as something expensive is offered for free. In addition to

this, the e-mail notifies the reader that this is a temporary offer and that the reader needs to act quick to be able to get the tickets. As argued by Brehm & Brehm (as cited in Cialdini, 2009), if scarcity comes into play and interferes with our prior access to a certain item, we will react by wanting and trying to possess the item more than we did before.

So by triggering a feeling of greed the phisher is able to grab a victim's attention, but by mentioning that the victim might miss out on that same product, the chance increases that a victim makes use of the peripheral route of thought and thus is more likely to comply with the request.

#### 4.2.3: Phishing e-mails that contain work-related information

Phishing e-mails that contain work-related information aim to achieve compliance by referring to certain circumstances that are related to a victim's work environment. E-mail 18 provides an example of such an e-mail. In this e-mail the phisher masquerades as someone from management and asks the victim to comply with a request. This is a popular way for phishers to achieve compliance (Infosec Institute, 2018). A second method could be for the phisher to masquerade as a third party that does business with the victim's company (E-mail 19).

Like phishing e-mails that contain tax-related information, phishing e-mails that aim to make the victim believe that they were sent by someone higher up in the organization, rely on the principle of authority. The difference between these two categories is that the effect of this principle may even be stronger. The effects of non-compliance can be felt almost immediately when it is the CEO who has requested something, while it takes a certain amount of time before the consequences are felt of non-compliance with the tax authorities. Not complying with their bosses could lead to direct negative social consequences, something every employee naturally aims to avoid (Cialdini, 2009).

So aside from the authority heuristic, which makes a victim believe that it is in his/her best interest to comply with authoritative figures, these kind of phishing e-mails also evoke a sense of urgency. It is very normal for employees to aspire a successful career, and not complying with the wishes of someone higher up in the organization could form an impediment to that goal. Nobody who aims to climb the organizational ladder would want to disappoint or annoy their direct bosses. This feeling of urgency can be exacerbated by pairing the Principle of Authority with the Time Principle. E-mail 18 serves as an example of how the two principles are combined. The Phisher/Management employee asks if his request can be fulfilled within a week, limiting the potential for the victim to overthink his/her decision, therefore guiding the victim to the peripheral route of decision-making.

E-mail 18 is also the only e-mail that contained the Principle of Conformity. This principle states that people determine what is correct by finding out what other people think is correct (Cialdini, 2009). At the start of this e-mail it is said that '*All employees must update their healthcare information*' (E-mail 18). By starting the e-mail with this sentence the phisher has the potential to activate the conformity heuristic by implying that the victim should act accordingly to the other employees. All employees must update their healthcare information and the victim is no exception. Like the Principle of Authority, the effects of not conforming to the behaviour of other employees can be felt directly. By stating that '*or else we cannot continue coverage this year*' the individual victim is made responsible for a group of people. If he or she does not comply, coverage cannot continue and if the victim is supposedly to blame for that, it could lead to severe social consequences.

#### 4.2.4: Phishing e-mails that contain information regarding social media

Phishing e-mails that contain information regarding social media, aim to persuade victims to click malignant hyperlinks or to share personal details by referring to something related to a user's social media accounts. This could be anything from fake friend requests (E-mail 14), to an e-mail claiming that the company is updating its privacy agreement (E-mail 12).

The interesting thing about this category, is that it is one out of two categories in which the Principle of Reciprocity is applied. E-mail 12 and E-mail 13 provide examples of how this is done. In E-mail 13 the phisher (who is masquerading as a LinkedIn employee) claims that: '*We're currently upgrading our systems to bring enhanced features to your LINKEDIN Account experience*'. In a world where social media plays a very prominent role, enhanced features are almost certainly welcomed by a large part of the users. This potentially evokes a feeling of indebtedness, as the company is supposedly doing its utmost best to maximize user experience. As discussed in the theoretical framework, this feeling of indebtedness even remains when a stranger does us a favour we have not asked for (Cialdini, 2009). So by simply acting as if the phisher is doing the victim a favour, he/she is potentially able to evoke a feeling of indebtedness which can then be exploited. All that is requested from the victim is that he/she fills in some personal details so that the company can make it happen for them (E-mail 13).

When it comes to fake friend requests, a different method is applied. Phishers that construct these kind of phishing e-mails tend to emphasize what the victim can gain from clicking a hyperlink or filling in personal details. In E-mail 14, it is emphasized what qualifications '*Timothy*' has and what he is looking for. At first glance that may look very interesting for someone

who works in the same field. The victim is distracted away from the scam by showing him something that possibly interests him or her. It also has the potential to activate the Need or Greed Principle, when someone is in real need of a job. When these principles in this setting are applied to the right victim, it could force them towards the peripheral route of thought. This is why phishers try to send their e-mails to as many people as possible, as it increases the chance of the e-mail reaching someone who would be interested by this profile.

#### 4.2.5: Phishing e-mails that contain information regarding a failed delivery

Phishing e-mails that contain information regarding a failed delivery, aim to persuade the victim to click a malignant hyperlink or fill in personal details by claiming that a product was not able to be delivered to the victim. An increasing amount of people is using the Internet to purchase products, and it has become very common for products to be delivered to your front door (Reagan & Gralnick, 2017). For that reason an e-mail claiming that a product was not able to be delivered is not something uncommon. And as people increasingly buy products online, it is very well possible that such a phishing e-mail is read by someone who has been waiting for a product to be delivered.

The Need and Greed Principle is automatically applied in these e-mails. If a victim is expecting a product to be delivered, it will inevitably be something he/she needs and/or wants. As the product has not been delivered, that feeling of longing has not been taken away. The victim still wants or needs the product that he or she is waiting for. This idea is at the heart of these kind of phishing e-mails, and it is very easy for phishers to abuse it. E-mail 7 shows how phishers claim that the product could not be delivered because a wrong address was provided, while the phishing offenders that constructed E-mail 6 wrote that nobody was present at the time the product was delivered. The aim is for victims to click a hyperlink that is either infected or will link the victims to a page where he/she has to fill in personal details.

In line with some of the e-mails from other categories, this feeling can be exacerbated by putting the victim under time pressure. The Time Principle is again used as a tool to exacerbate other emotions. The way this principle is applied differs per e-mail, but they rely on the same psychological reaction to achieve compliance. In one e-mail the phishers stated that: *‘Als het pakket niet binnen 15 werkdagen wordt ontvangen heeft ons bedrijf recht om schadevergoeding te eisen van u, de kosten van de opslag van goederen kost EUR 4,18 per dag* (if the product was not able to be delivered within 15 days, the company they masqueraded as would have the right



to charge €4,18 per day) (E-mail 7). Another e-mail simply let the victim know that if the product was not able to be delivered within 48 hours, it would be returned to sender (E-mail 5)

A second way this type of e-mail can be successful is when it evokes a sense of confusion within the victim. It can occur that the victim is sure that he or she has not ordered anything and that there is no product that should be delivered to them. As the victim is unaware of what product this might be, he or she might click a hyperlink that supposedly will tell them what they have ordered (E-mail 5). Confusion has the potential to interfere with a victim's capacity for deep thinking, therefore guiding the victim to the peripheral route.

#### 4.2.6 Phishing e-mails containing information related to a user's account

Phishing e-mails that contain information related to a user's account, aim to achieve compliance by tricking the victim into believing that something is wrong with their account (for whatever service that may be). There are several ways to achieve this goal. Phishers could for example claim that a victim's account is on hold because the company they masquerade as was unable to authorize the payment method (E-mail 3). Another method would be for the phisher to state that the company they masquerade as has noticed some unusual activity on a victim's account and they have blocked the account until the issue has been solved (E-mail 1, 2 & 4).

Especially the second method has the potential to be effective as it consists of multiple elements that could increase the chance of compliance. First of all it triggers a sense of fear. People increasingly make use of online systems for certain services, think of how many people use the Internet to organize their financial matters. As argued in the first chapter, this has led to an increasing possibility for hacking. People are aware that hacking can occur and what implications that might have (Downs, Holbrook, & Cranor, 2006). An e-mail stating that unusual activity was noticed is therefore likely to grab a victim's interest.

It is interesting to see that 75% of the e-mails that were studied under this category applied this method. And like other phishers were able to do in other e-mails, the phishing offenders behind these e-mails were able to intensify the effect of fear by applying two other social psychological principles. The first is the Principle of Reciprocity. The phishers write that the victim's account has been blocked only to protect his or her account (E-mail 1). By doing so they can convince the victim that they are doing everything they can to help him/her. The phishers behind E-mail 2 even go as far as to say that the safety of the victim's PayPal-account is their number one priority and that they want to work together to assure that safety.

Like in e-mails from other categories, the Time Principle to exacerbate the effect even further. In the e-mails from this category this is done by mentioning that the victim must verify his/her account '*binnen 24 uur*' (within 24 hours) or else their account will be deleted (E-mail 2)

#### 4.3: Concluding remarks

To summarize, social psychological principles seem to be applied differently across different types of phishing e-mails. As discussed, the intention of phishers is to evoke certain emotions that interfere with a victim's capacity for deep thinking. This analysis has shown that the emotion that is targeted by phishing offenders differs per type of phishing e-mail and for that reason, the social psychological principle that is at the centre of the phishing e-mail also diverges per type. In addition to this observation, some of the social psychological principles that were discussed in this research seem to have an intensifying effect on the main principle that is applied to achieve compliance. These exacerbating principles are applied across all different types of phishing e-mails.

However, although social psychological principles play a role in the studied phishing e-mails, their use should not be overestimated. The quality of the content in the e-mail differs quite significantly, and a substantive amount of phishing e-mails are hastily constructed with hardly any thought going in to them. Phishers mainly aim to copy as much from authentic e-mails or websites as possible. This also shows from the abundance of visual deception in the studied e-mails. If the elements of text that are copied contain psychological nudges, that could work to the offender's advantage but they are not always implemented purposely by the offender. In other words, phishers are not always aware of the psychological affect their content may bring about.

## Chapter 5: Conclusion

The aim of this chapter is to provide an answer to the research question posed in the first chapter of this research. The answer to this research question follows from the analysis conducted in chapter 4. The objective of this research was to analyse how phishers have applied social psychological principles in phishing e-mails with the most clicked subject lines of 2017 and 2018. These e-mails were analysed by applying a qualitative content analysis. By doing so, an increased understanding was developed of how phishers construct their e-mails to achieve compliance and why phishing victims fall for them.

In addition to answering the research question this chapter will also elaborate on several other aspects of this research. Firstly, it will be discussed whether or not the body of knowledge that was used for this research was appropriate for this analysis. Secondly, the question has to be answered how this research has enriched academic knowledge. Thirdly, this chapter will look at the strengths and weaknesses of this research. After that, suggestions will be made for future research.

### 5.1: Conclusions

*How have phishing offenders applied social psychological principles in phishing e-mails with a subject line that was among the most clicked general subject lines of 2017-2018?*

By studying the most clicked general subject lines of 2017 and 2018, it was possible to distinguish six different kinds of phishing e-mails. As was expected from the theoretical framework, the analysis proved that social psychological principles are applied in different ways across these different types of e-mails. The expectation that the analysis would lead to ‘contrasting results but for predictable reasons’ has therefore been fulfilled (Yin, 2003: p.47). The different kinds of phishing e-mails that have been studied aim to evoke different kinds of emotions, that are triggered by different kinds of social psychological principles. For example, the Need and Greed Principle seems to be at the heart of the phishing e-mails that contain information regarding holiday offers, while the Principle of Authority is at the centre of phishing e-mails containing tax-related information.

What the researched e-mails have in common, is that the social psychological principles that played a role in the e-mails have the potential to meddle with a victim’s capacity for deep thinking. When phishing offenders are able to trigger certain emotions, victims are forced to use the peripheral route to decision-making therefore increasing the chance of compliance.

So although the emotion that is triggered differs, the end-goal remains the same: to steer the victim away from the scam by triggering emotions and activating heuristics.

A second aspect the e-mails have in common is the way certain principles are used to intensify the effect of the main social psychological principle. The Time Principle for example, is used throughout the different kinds of phishing e-mails to apply time pressure to the victim. This limits his or her time to carefully assess what he or she is reading, thus exacerbating the effect of the main principle and therefore increasing the chance of compliance.

However the use of social psychological principles by phishing offender should not be overestimated. As argued in the concluding remarks of the analysis, phishers not always purposely include social psychology in their content. Sometimes it is just a lucky side-effect of simply copying and pasting from authentic websites or e-mails. In addition to that, the quality of the content differs to quite some extent. Although the e-mails that were studied for this research have selected critically, a lot of phishing e-mails are sent out every day and sometimes there is hardly any thought going into these phishing e-mails. An e-mail could merely consist of a link without any further explanation thus not including any form of social psychology. So although social psychology played a role in the analysed phishing e-mails, a substantial part of phishing e-mails do not include such social psychological principles. This has to be taken into account when developing effective countermeasures.

## 5.2: Recommendations

First of all, it is necessary to discuss if the theories that were used in this research were appropriate for the analysis that was conducted. The body of knowledge that was discussed in this research mainly consisted of three different theories. It is important to note that the selection of these theories did not come out of the blue. Their selection was based on previous research regarding this topic, thus justifying their use in this research. As argued earlier, quantitative research into the use of social psychological principles in social engineering attacks had already proven that Cialdini's principles of influence were used in phishing attacks. Secondly, Ferreira, Coventry and Lenzini (2015) showed that elements of Stajano and Wilson's principles of system security were applied in phishing attacks. And finally, Dhamija, Tygar & Hearst's (2006) theory on visual deception is from the field of cybersecurity and was specifically designed for phishing attacks. Resulting from the aforementioned, the theories that were used for this analysis seem appropriate.

Secondly, the contribution to academic knowledge needs to be discussed. As argued in chapter 3, the goal of this research was ‘to generate background material to a discussion about a concrete problem’ (Solberg, Soilen & Huber, 2006 as cited in Gustaffson, 2017: p.5). Phishing attacks are still a very concrete problem and what this discussion missed was an insight into how social psychology was applied in phishing attacks. This insight is useful as this deeper understanding of this specific attack vector can contribute to the development of effective countermeasures (Krombholz, Hobel, Huber, & Weippl, 2015: p.9). The practical contribution of this research is also its academic contribution. As argued in the introduction, qualitative research into this subject is scarce and the qualitative research that has been conducted is fairly limited. This research has added to the literature by analysing different kinds of phishing e-mails to give an extensive insight into how and in what ways social psychological principles are used to achieve compliance from victims.

Thirdly, the limitations of this research. Before some of the limitations are discussed, it is also important to discuss some of the positive aspects of this research. One of those positive aspects is the elaborate theoretical framework. In contrast to other studies on this topic, multiple theories were selected to analyse this phenomenon. This study did not rely on the explanatory power of one single theory, but applied multiple theories to get a more extensive insight into phishing attacks. A second aspect was the amount of cases that were studied. This research thoroughly analysed 21 different cases to obtain the right amount of information to answer the research question. Thirdly, the content analysis was conducted in a replicable and valid way. Measures were taken to assure that the procedure of classification was consistent. Think of the development of a coding protocol and coding scheme.

A factor that could have made this research stronger would have been the incorporation of a second method to acquire data. Interviews with phishers or victims for example or an experiment could have provided information that had the ability to verify the findings that resulted from the content analysis. They could have provided insights into aspects of the e-mail that were not measured by the indicators, or they could have provided a different view on some of the results. This content analysis was used as a tool to analyse how the social psychological principles were potentially able to mislead a victim, but the actual effect of these different principles remains unclear. Other forms of data collection could have provided information to incorporate these aspects in this research. Due to time constraints it was too difficult to incorporate this into this research.

The second limitation to this research is the case selection. Although selection criteria were developed, there were still a lot of other cases that could have been selected. At first the goal was to select the most successful phishing mails ever, but that proved to be very difficult mostly down to a lack of data. There were reports of phishing attacks that were successful in terms of money, but the phishing e-mails that were used to conduct these attacks were often not included in these reports. A concession had to be made, which is why the decision was made to analyse phishing e-mails that had the highest chance of being read (because of the most clicked general subject line) and thus the highest chance of success. But even with this selection criterium there are still loads of phishing e-mails to select from. The e-mails that were selected in this research were obtained from online databases that granted permission to use these e-mails and from websites where the Four Fair Use Factors were applied to use the images. As cases are often hand-picked, selection bias is a common problem for qualitative studies and this research is no exception (Moravcsik, 2014, p.49).

The main suggestion for future research is the incorporation of these limitations into their own research. The most important aspect is to include a second or even third method of data collection. Interviews and/or an experiment would provide an even more detailed insight into this phenomenon, potentially contributing to even more effective countermeasures. A second aspect could be the incorporation of more social psychological principles into the analysis. The field of social psychology is enormous and there is a possibility that other theories could complement the theoretical framework that was used for this research. A third suggestion would be a replication of this study with different cases, to see if other principles can be identified that cannot be explained by the theoretical framework from this research.

## Bibliography

- Aaron, G. & Rasmussen, R. (2017). *Global Phishing Survey: Trends and Domain Name Use in 2016*. San Francisco, CA: *Anti Phishing Work Group (APWG)*.
- Anslinger, J. (2013, November 12). How do Email Spam Filters Work? *Lieberman Technologies*. Accessed on May 1, 2018 from: <https://www.ltnow.com/email-spam-filters-work/>
- Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, 60, 185-197.
- Bandura, A., Grusec, J.E., & Menlove, F.L. (1967). Vicarious Extinction of Avoidance Behaviour. *Journal of Personality and Social Psychology* (5), p.16-23.
- Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The qualitative report*, 13(4), 544-559.
- Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus Open*, 2, 8-14.
- Blass, T. (1999). The Milgram paradigm after 35 years: Some things we now know about obedience to authority. *Journal of applied social psychology*, 29(5), 955-978.
- Bossworth, S., Kabay, M., & Whyne, E. (2014) *Computer security handbook* (6th ed.). New York: Wiley
- Braithwaite, V. (2001) The Community Hopes, Fears and Actions Survey: Goals and Measures. *Centre for Tax System Integrity Working Paper No. 2*, The Australian National University, Canberra.
- Braithwaite, V. (2003). Dancing with tax authorities: Motivational postures and non-compliant actions. *Taxing democracy*, 15-39.
- Bullee, J-W., Montoya, L., Pieters, W., Junger, M., & Hartel, P.H. (2017). On the anatomy of social engineering attacks: A literature-based dissection of successful attacks. *Journal of Investigative Psychology and Offender Profiling*. DOI: 10.1002/jip.1482
- Cialdini, R. B., Vincent, J. E., Lewis, S. K., Catalan, J., Wheeler, D., & Darby, B. L. (1975). Reciprocal concessions procedure for inducing compliance: The door-in-the-face technique. *Journal of personality and Social Psychology*, 31(2), 206.
- Cialdini, R. B., (2009). *Influence: The psychology of persuasion*. New York: Collins

- Chandrasekaran, M., Narayanan, K., & Upadhyaya, S. (2006, June). Phishing email detection based on structural properties. *In NYS Cyber Security Conference* (Vol. 3).
- Clayton R. (2007) Insecure Real-World Authentication Protocols (or Why Phishing Is So Profitable). In: Christianson B., Crispo B., Malcolm J.A., Roe M. (eds) Security Protocols. Security Protocols 2005. *Lecture Notes in Computer Science, vol 4631*. Springer, Berlin, Heidelberg
- Cummings, L. (2014). The “trust” heuristic: Arguments from authority in public health. *Health Communication, 29*(10), 1043-1056.
- Davis, N. M., & Cohen, M. R. (1981). *Medication errors: causes and prevention*. George F Stickley Co Pubns.
- Digital Media Law Project (2018, June 09). Fair Use. *Digital Media Law Project*. Accessed on June 09, 2018 from: <http://www.dmlp.org/legal-guide/fair-use>
- Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006, July). Decision strategies and susceptibility to phishing. *In Proceedings of the second symposium on Usable privacy and security* (pp. 79-90). ACM.
- Dhamija, R., Tygar, J. D., & Hearst, M. (2006, April). Why phishing works. *In Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581-590). ACM.
- Drachman, D., & Insko, C. A. (1978). The extra credit effect in interpersonal attraction. *Journal of Experimental Social Psychology, 14*(5), 458-465.
- Efran, M. G., & Patterson, E. W. J. (1976). The politics of appearance. *Unpublished manuscript, University of Toronto*, 19-25.
- European Nation Agency for Network and Information Security. (2017, October 12). Phishing on the rise. Accessed on March 27, 2018 from: <https://www.enisa.europa.eu/publications/info-notes/phishing-on-the-rise>
- Ferreira, A., Coventry, L., & Lenzini, G. (2015, August). Principles of persuasion in social engineering and their use in phishing. *In International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 36-47). Springer, Cham.
- Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Qualitative inquiry, 12*(2), 219-245.



- Freedman, J. L., & Fraser, S. C. (1966). Compliance without pressure: the foot-in-the-door technique. *Journal of personality and social psychology*, 4(2), 195.
- Fridlund, B., & Hildingh, C. (2000). Qualitative research methods in the service of health. *Studentlitteratur*.
- Furnell, S. M., & Warren, M. J. (1999). Computer hacking and cyber terrorism: The real threats in the new millennium?. *Computers & Security*, 18(1), 28-34.
- Garera, S., Provos, N., Chew, M., & Rubin, A. D. (2007, November). A framework for detection and measurement of phishing attacks. *In Proceedings of the 2007 ACM workshop on Recurring malware* (pp. 1-8). ACM.
- Given, L. M. (2008). *The SAGE encyclopedia of qualitative research methods*. Thousand Oaks, CA: SAGE Publications Ltd doi: 10.4135/9781412963909
- Gustafsson, J. 2017, "Single Case Studies vs. Multiple Case Studies: A Comparative Study." Retrieved from: <http://www.diva-portal.org/smash/get/diva2:1064378/FULLTEXT01.pdf>
- Hastings, G., Stead, M., & Webb, J. (2004). Fear appeals in social marketing: Strategic and ethical reasons for concern. *Psychology & marketing*, 21(11), 961-986.
- Hofling, C. K., Brotzman, E., Dalrymple, S., Graves, N., & Pierce, C. M. (1966). An experimental study in nurse-physician relationships. *The Journal of nervous and mental disease*, 143(2), 171-180.
- Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, 55(1), 74-81.
- Huber, M., Kowalski, S., Nohlberg, M., & Tjoa, S. (2009, August). Towards automating social engineering using social networking sites. *In Computational Science and Engineering, 2009. CSE'09. International Conference on* (3), 117-124.
- Infosec Institute (2018). Healthcare Phishing Attacks. *Infosec Institute*. Accessed on May 25, 2018 from: <https://resources.infosecinstitute.com/category/enterprise/phishing/the-phishing-landscape/phishing-attacks-by-demographic/phishing-in-healthcare/#gref>
- Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, 50(10), 94-100

- KnowBe4 (2017, October 11). KnowBe4 Releases Q3 2017 Top-Clicked Phishing Report. *KnowBe4*. Accessed on March 02, 2018 from: <https://www.knowbe4.com/press/knowbe4-releases-q3-2017-top-clicked-phishing-report>
- Krippendorff, K. (1980). *Reliability*. John Wiley & Sons, Inc..
- Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, 22, 113-122.
- Latour, B., & Porter, C. (1996). *Aramis, or, The love of technology* (Vol. 1996). Cambridge, MA: Harvard University Press.
- Liang, H., & Xue, Y. (2010). Understanding security behaviours in personal computer usage: a threat avoidance perspective. *Association for Information Systems*, 11(7), 394-413.
- Locke, K. D., & Horowitz, L. M. (1990). Satisfaction in interpersonal interactions as a function of similarity in level of dysphoria. *Journal of personality and social psychology*, 58(5), 823.
- Marshall, C. (1990). Goodness criteria: Are they objective or judgement calls? In E. G. Guba (Ed.), *The paradigm dialog* (pp. 188-197). Newbury Park, CA: Sage.
- Mayring, P. (2000). Qualitative content analysis. Forum: *Qualitative Social Research*, 1(2). Retrieved March 10, 2005, from <http://www.qualitative-research.net/fqs-texte/2-00/02-00mayring-e.htm>
- Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. sage.
- Metz, C. (2015, September 7). Google says its AI catches 99.9% of gmail spam. *Wired*. Accessed on May 29, 2018 from: <https://www.wired.com/2015/07/google-says-ai-catches-99-9-percent-gmail-spam/>
- Milgram, S. (1963). Behavioral study of obedience. *The Journal of abnormal and social psychology*, 67(4), 371.
- Moravcsik, A. (2014). Transparency: The revolution in qualitative research. *PS: Political Science & Politics*, 47(1), 48-53.
- Moriarty, T. (1975). Crime, commitment, and the responsive bystander: Two field experiments. *Journal of Personality and Social Psychology*, 31(2), 370.

- Patil, S. (2010, October 6). Soft Hyphen- A New URL Obfuscation Technique. *Symantec Official blog*. Accessed on May 1, 2018 from: <https://www.symantec.com/connect/blogs/soft-hyphen-new-url-obfuscation-technique>
- Petty, R. E., & Cacioppo, J. T. (1986). *The elaboration likelihood model of persuasion*. In *Communication and persuasion* (pp. 1-24). Springer New York.
- Petty, R., & Hinsonkamp, L. (2017). *The SAGE Encyclopedia of Political Behavior*. Thousand oaks: SAGE Publications, Inc.
- Potter, W.J. and Levine-Donnerstein, D. (1999) Rethinking validity and reliability in content analysis. *Journal of Applied Communication research*, 27, 258-284
- Prince, B. (2009, December 07). Phishing Attacks Cost Millions Despite Low Success Rate. *eWeek*. Accessed on May 25, 2018 from: <http://www.eweek.com/security/phishing-attacks-cost-millions-despite-low-success-rate>
- Reagan, C. & Gralnick, J. (2017, December 19). More than 75 percent of US online consumers shop on Amazon most of the time. *CNBC*. Accessed on May 22, 2018 from: <https://www.cnbc.com/2017/12/19/more-than-75-percent-of-us-online-consumers-shop-on-amazon-most-of-the-time.html>
- Regan, D. T. (1971). Effects of a favor and liking on compliance. *Journal of experimental social psychology*, 7(6), 627-639.
- Richmond, R. (2011, April 2) The RSA Hack: How They Did It. *The New York Times*. Accessed on May 1, 2018 from: <https://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/>
- Rusch, J. J. (1999, June). The “social engineering” of internet fraud. In *Internet Society Annual Conference*, [http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g\\_2.htm](http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm).
- Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the ‘weakest link’—a human/computer interaction approach to usable and effective security. *BT technology journal*, 19(3), 122-131.
- Seuntjens, T. G. (2016). *The Psychology of Greed*. Ridderprint.
- Sherman, S. J. (1980). On the self-erasing nature of errors of prediction. *Journal of personality and Social Psychology*, 39(2), 211.

- Sjouwerman, S. (2018a, Januari 19). KnowBe4 2017 Top Clicked Phishing Test Analysis. *KnowBe4*. Accessed on March 2, 2018 from: <https://blog.knowbe4.com/knowbe4-2017-top-clicked-phishing-test>
- Sjouwerman, S. (2018b, May 4). Q1 2018 Top Clicked Phishing Email Subjects [Infographic]. *KnowBe4*. Accessed on March 2, 2018 from: <https://blog.knowbe4.com/q1-2018-top-clicked-phishing-email-subjects>
- Smith, J. K. (1990). Alternative research paradigms and the problem of criteria. In E. G. Guba (Ed.), *The paradigm dialog* (pp. 167-187). Newbury Park, CA: Sage
- Smith, M.M. & Fuller, R.G.C. (1972). Effects of Group Laughter on Responses to Humorous Materials. *Psychological Reports* (30), p.132-134
- Stajano, F., & Wilson, P. (2011). Understanding scam victims: seven principles for systems security. *Communications of the ACM*, 54(3), 70-75.
- Stemler, S. (2001). An overview of content analysis. Practical assessment, research & evaluation, 7(17) *Practical Assessment, Research , & Evaluation* 137-146.
- Thomas, D. R. (2006). A general inductive approach for analyzing qualitative evaluation data. *American journal of evaluation*, 27(2), 237-246.
- Thornburgh, T. (2004, October). Social engineering: the dark art. In *Proceedings of the 1st annual conference on Information security curriculum development* (pp. 133-135). ACM.
- Wagner, D., & Schneier, B. (1996, November). Analysis of the SSL 3.0 protocol. In *The Second USENIX Workshop on Electronic Commerce Proceedings* (Vol. 1, No. 1, pp. 29-40).
- Weber, R. P. (1990). *Basic content analysis* (No. 49). Sage.
- Webroot. (2017) Quarterly Threat Trends: Phishing attacks Growing in Scale and Sophistication. Broomfield, CO: *Webroot*. Accessed on March 27, 2018 from: [https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/8415/0585/3084/Webroot\\_Quarterly\\_Threat\\_Trends\\_September\\_2017.pdf](https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf)
- Whittemore, R., Chase, S. K., & Mandle, C. L. (2001). Validity in qualitative research. *Qualitative health research*, 11(4), 522-537.
- Worchel, S., Lee, J., & Adewole, A. (1975). Effects of supply and demand on ratings of object value. *Journal of personality and social psychology*, 32(5), 906.

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security*, 16(6), 315-331.

Yin, R. K. (2003). *Case study research: Design and methods* (3rd ed.). Thousand Oaks, CA: Sage.

## Appendix A: Operationalization tables

Theory	Concept	Definition	Indicators
<p>-Cialdini's (2009) theory on influence.</p> <p>-Theory from the field of social psychology.</p> <p>-Discusses methods to influence the decision-making processes of actors.</p>	<p>'Principles of persuasion':</p>	<p>'Principles of persuasion':</p> <p>-'Social influences that can be used to change the odds of compliance in the favour of the offender'. (Bullée et al, 2017: p.3)</p> <p>- Cialdini (2009) distinguishes 6 principles of persuasion that can be used by offenders:</p> <p>-(1) <i>Principle of authority</i></p> <p>-(2) <i>Principle of conformity</i></p> <p>-(3) <i>Principle of reciprocity</i></p> <p>-(4) <i>Principle of commitment</i></p> <p>-(5) <i>Principle of liking</i></p> <p>-(6) <i>Principle of scarcity</i></p>	<p>-(1) <i>Principle of authority:</i></p> <p>(1.1) Offender uses an official title.</p> <p>(1.2) Offender provides contact details that give the victim the idea that the offenders has a position with authority.</p> <p>(1.3) Offender makes use of 'words of authority': Words that set forth duties, rights, prohibitions, and entitlements.</p> <p>(1.4) Offender uses official logos.</p> <p>-(2) <i>Principle of conformity:</i></p> <p>(2.1) Offender emphasizes the fact that other actors have already complied with the request.</p> <p>(2.2) Offender mentions the behaviour of other people with the intention that the victim will conform to it.</p> <p>-(3) <i>Principle of reciprocity:</i></p> <p>(3.1) Offender provides the victim with a favour to create a feeling of indebtedness and then aims for a favour in return</p> <p>(3.2) Offender aims for the victim to develop a feeling of indebtedness</p> <p>(3.3) Offender asks for large favour, and follows that up with a smaller request (Rejection-then-retreat)</p>

<p>-Cialdini's (2009) theory on influence.</p> <p>-Theory from the field of social psychology.</p> <p>-Discusses methods to influence the decision-making processes of actors.</p>	<p>'Principles of persuasion':</p>	<p>'Principles of persuasion:</p> <p>- 'Social influences that can be used to change the odds of compliance in the favour of the offender'. (Bullée et al, 2017: p.3)</p> <p>- Cialdini (2009) distinguishes 6 principles of persuasion that can be used by offenders:</p> <p>-(1) <i>Principle of authority</i></p> <p>-(2) <i>Principle of conformity</i></p> <p>-(3) <i>Principle of reciprocity</i></p> <p>-(4) <i>Principle of commitment</i></p> <p>-(5) <i>Principle of liking</i></p> <p>-(6) <i>Principle of scarcity</i></p>	<p>-(4) <i>Principle of consistency:</i></p> <p>(4.1) Offender tries to make the victim commit to something.</p> <p>(4.2) Offender starts with asking for a minor favour and gradually increases the size of the favour.</p> <p>-(5) <i>Principle of liking:</i></p> <p>(5.1) Offender gives compliments.</p> <p>(5.2) Offender emphasizes similarities between him/her and the victim.</p> <p>(5.3) Offender uses certain words or phrases that make him/her seem more likeable</p> <p>-(6) <i>Principle of scarcity:</i></p> <p>(6.1) Offender offers victim something with limited availability.</p> <p>(6.2) Offender emphasizes that victim might lose out on offered object if he/she does not act.</p> <p>(6.3) Offender offers victim something widely available and follows up by stating that product is no longer widely available</p>
--	------------------------------------	--	---

Theory	Concept	Definition	Indicators
<p>Stajano &amp; Wilson's (2011) theory on scamming</p> <p>-theory from the field of social psychology</p> <p>-Discusses the idea that many attacks on computer result from the fact that security engineers do not understand the psychology of the system users they aim to protect</p>	<p>'Principles of system security'</p>	<p>Principles of system security:</p> <p>' General principles about the recurring behavioural patterns of victims that hustlers have learn to exploit' (Stajano &amp; Wilson, 2011: p.1)</p>	<p>-(7) <i>The need and greed principle:</i></p> <p>(7.1) Offenders offers victim something he potentially needs (Stajano &amp; Wilson, 2011: p.17)</p> <p>(7.2) Offender offers victim something that spikes his/her interest and could trigger a feeling of greed (Stajano &amp; Wilson, 2011: p.17-18).</p> <p>-(8) <i>The dishonesty principle</i></p> <p>(8.1) Offender aims to make the victim complicit in an illegal act (Stajano &amp; Wilson, 2011: p.14)</p>



Theory	Concept	Definition	Indicators
<p>Dhamija, Tygar and Hearst's (2006) theory on visual deception</p> <p>-Although deception is studied in the field of psychology, this specific theory is from the field of cybersecurity</p> <p>-Discusses the idea that offenders make use of visual deception to fool their victims</p>	<p>'Visual deception in phishing'</p>	<p>'Phishers use visual deception tricks to mimic legitimate text, images and windows (2006: p.3)</p>	<p>-(9) <i>Visual deceptive text:</i></p> <p>(9.1) Offender obfuscates the URL</p> <p>-(10) <i>Images masking underlying text:</i></p> <p>(10.1) Offender uses image of a legitimate hyperlink that really serves as a hyperlink to a phishing website</p>

## Appendix B: Protocol for Content Analysis & Coding Scheme

<b>Step 1</b>	Download textual sources from online databases or companies that have been targeted
<b>Step 2</b>	Close read texts and assign codes (related to different elements of social psychology) to words sentences and paragraphs
<b>Step 3</b>	Integrate findings into discussion by illustrating with words, sentences etc.

### Coding Scheme

Authority - Title	Offender uses an official title
Authority- Contact details	Offender provides contact details
Authority- Words	Offender uses words of authority
Conformity- Compliance	Offender emphasizes compliance of others
Conformity- Behaviour	Offender mentions behaviour of others
Reciprocity- Favour for Favour	Offender provides favour and asks for favour in return
Reciprocity- Indebtedness	Offender aims to achieve feeling of indebtedness in a victim
Reciprocity- Rejection-then-retreat	Offender asks for large favour and follows that up with a smaller request
Consistency- Commitment	Offender tries to make the victim commit to something
Consistency- Increasing size favour	Offender starts with asking for minor favour and gradually increases the size of the favour
Liking- Compliments	Offender gives compliments
Liking- Similarities	Offender emphasizes similarities between them
Liking- Likeability	Offender uses words that make him/her more likeable
Scarcity- Limited availability	Offender offers victim something with limited availability
Scarcity- Miss out	Offender emphasizes that victim might lose out on offered object if he/she does not act
Scarcity- Abundance drop	Offender offers victim something widely available and follows that up by stating that product is no longer widely available
Need & Greed- Need	Offender offers victim something he potentially needs
Need & Greed- Greed	Offender offers victim something that spikes his or interest and could trigger a feeling of greed
Dishonesty- Illegal act	Offender aims to make victim complicit in an illegal act
Visual Deception- Deceptive text	Offender obfuscates the URL
Visual Deception- Images	Offender uses fake images of legitimate hyperlink
Time- Time Pressure	Offender aims to put victim under time pressure to guide them to peripheral route of thought
Distraction- Spark interest	Offender aims to evoke emotions to distract victim away from the scam towards what interests him or her
Deception- Fake situation	Offender aims to construct a fake situation in such a way that the victim believes it to be real.

## Appendix C: Coding Protocol

Authority - Title	E-mail contains official titles of authoritative figures. This could be from within the organizational hierarchy (CEO for example) or outside of the organizational hierarchy (Police for example).
Authority- Contact details	E-mail contains contact details of authoritative figures. This could be from within the organizational hierarchy (CEO for example) or outside of the organization hierarchy (Police for example).
Authority- Words	E-mail contains words of authority, which are words that set forth duties, rights, prohibitions and entitlements. Examples of these words include 'shall', 'must' and 'will' (Ward, 2006: p.1)
Conformity- Compliance	Offender emphasizes in text that others around the victim have already complied with the request.
Conformity- Behaviour	Offender mentions how people around the victim have behaved themselves. An offender could for example mention that others around him have decided not to ask a manager about the request
Reciprocity- Favour for Favour	Offender provides a favour for the victim and asks for a favour in return. An offender could for example mention to the victim that he/she has already filled in most of a victim's tax form (because it is such a hassle to do so), and that they only need to fill in some minor last details.
Reciprocity- Indebtedness	Offender aims to achieve a feeling of indebtedness in a victim. This is a more general indicator to account for feelings of indebtedness that cannot be explained by the two other reciprocity indicators.
Reciprocity- Rejection-then-retreat	Offender asks for a large favour which is likely to be rejected, and follows that up with a smaller request which is then more likely to be accepted.
Consistency- Commitment	Offender tries to make a victim commit to something. An offender could aim to make a victim agree to something, which increases the chance of them following up on that agreement.
Consistency- Increasing size favour	Offender asks for a minor favour and gradually increases the size of the favour. An offender could first ask for simple things like the e-mail address of a colleague and gradually ask for more personal details.
Liking- Compliments	Offender compliments the victim. The e-mail contains compliments made by the offender regarding the victim. An example could be to ask how a victim's beautiful children are doing
Liking- Similarities	Offender emphasizes the similarities between victim and him/her. An offender could for example mention that they work for the same company (at a different location).
Liking- Likeability	Offender uses words that make him/her more likeable. In some cases words can be used just to be nice to someone. Starting an e-mail with 'I hope you are well' is an example of this.
Scarcity- Limited availability	Offender emphasizes that victim might lose out on product or service with limited availability if they don't act.
Scarcity- Abundance drop	Offender offers victim a product or service that is widely available and follows that up by mentioning that this product or service now has limited availability.

Need & Greed- Need	Offender offers victim something he/she potentially needs. An offender might for example have figured out that a victim is in financial trouble and needs quick money to address that issue.
Need & Greed- Greed	Offender offers victim something that is not a necessity for the victim, but is very likely to spark his/her interest and might trigger a feeling of greed. An example is the chance to win a free holiday.
Dishonesty- Illegal act	Offender aims to make the victim an accomplice in an illegal act. An example could be an offender who aims to sell stolen products for a very cheap price to the victim.
Visual Deception- Deceptive text	Offender obfuscates a URL or e-mail address or connects a hyperlink to certain words or sentences.
Visual Deception- Images	Offender uses fake images as hyperlinks, or makes use of fake logos to make the e-mail look more authentic.
Time- Time Pressure	Offender aims to put victim under time pressure to guide them to peripheral route of thought. An offender could mention that a victim needs to act within a certain amount of time, or his or her account will be locked down.
Distraction- Away from scam	Offender aims to evoke emotions to distract victim away from the scam towards something that has his/her interest. This is a more general indicator to account for the words, sentences, paragraphs and images that cannot be explained by the more specified indicators. An offender could for example claim that someone's profile has been hacked which is likely to trigger a feeling of anxiety.
Deception- Masquerade	Offender aims to construct a fake situation in such a way that the victim could believe it to be true. Such a situation is likely to trigger some form of emotion, to guide victims to the peripheral route of thought. An offender could for example masquerade as someone from the IT-department.

## Appendix D: General Table

Category	Code	Description	Count	% Codes	Cases	% Cases
Authority	Authority-Title	Offender uses titles to be perceived as an authoritative figure	5	3,60%	3	15,80%
Authority	Authority-Words	Offender uses words of authority	5	3,60%	4	21,10%
Authority	Authority- Contact details	Offender provides official contact details to masquerade as trustworthy third party	2	1,40%	2	10,50%
Conformity	Conformity-Compliance	Offender emphasizes compliance of others	1	0,70%	1	5,30%
Conformity	Conformity-Behaviour	Offender mentions behaviour of other people				
Reciprocity	Reciprocity - Favour for favour	Offender provides favour and asks for favour in return	5	3,60%	5	26,30%
Reciprocity	Reciprocity-Indebtedness	Offender aims to achieve feeling of indebtedness in a victim	3	2,10%	3	15,80%
Reciprocity	Reciprocity-Rejection then Retreat	Offender asks for large favour and follows that up with a smaller request				
Consistency	Consistency-Commitment	Offender tries to make the victim commit to something				
Consistency	Consistency-Increasing size favour	Offender starts with asking for minor favour and gradually increases the size of the favour				
Liking	Liking-Compliments	Offender gives compliments				
Liking	Liking-Similarities	Offender emphasizes similarities between them				
Liking	Liking-Likeable words	Offender uses words that make him/her more likeable	17	12,10%	11	57,90%
Scarcity	Scarcity-Limited availability	Offender offers victim something with limited availability	2	1,40%	2	10,50%
Scarcity	Scarcity-Abundance drop	Offender offers victim something widely available and follows that up by stating that product is no longer widely available				
Need and Greed	Need and Greed-Need	Offender offers victim something he potentially needs	1	0,70%	1	5,30%
Need and Greed	Need and Greed-Greed	Offender offers victim something that spikes his or interest and could trigger a feeling of greed	5	3,60%	4	21,10%
Dishonesty	Dishonesty-Illegal act	Offender aims to make victim complicit in an illegal act				
Visual deception	Visual deception- Deceptive text	Offender obfuscates the URL or e-mail. Offender can also connect hyperlink to certain page	32	22,90%	18	94,70%
Visual deception	Visual deception- Images	Offender uses fake images of legitimate hyperlink. Offender could also use certain image	18	12,90%	12	63,20%
Time	Time- Limited time	Offender aim to put victim under time pressure to force them to peripheral route of thought	9	6,40%	9	47,40%
Distraction	Distraction- Away from scam	Offender aims to evoke certain emotions to distract away from the scam and towards that	19	13,60%	15	78,90%
Deception	Deception- Masquerades	Offender masquerades as a random trustworthy party to trigger some form of emotion in	16	11,40%	15	78,90%

## Appendix E: Phishing E-mails

E-mail 1:

**Van:** PayPal <[ht@240plan.ovh.net](mailto:ht@240plan.ovh.net)>  
**Datum:** 22 september 2016 01:26:49 CEST  
**Aan:**  
**Onderwerp:** UPDATE

p



Dear Client,

You still need to take action regarding your PayPal account. Until you do so, your PayPal account access will remain limited.

### **What's going on?**

We noticed some unusual activity on your PayPal account on 22/09/2016 on 10:25 UTC near Vienna AT and are concerned about potential unauthorised account access.

### **What to do next**

Please log in to your PayPal account and follow the steps there to confirm your identity and recent account activity. To help protect your account, your PayPal account will remain limited until you complete the necessary steps.

[Log in here](#)

Sincerely,

PayPal

© 1999-2016 PayPal. The PayPal service is provided by PayPal Pty Limited (ABN 93 111 195 389) . Any information provided is general only and does not take into account your objectives, financial situation or needs.

PayPal PPC000263:63bd4b26e46aa

[E-mail 1. This is an image of a phishing mail that was obtained by a Dutch online database for phishing e-mails. Fraude Helpdesk. Downloaded from:

<https://www.fraudehelpdesk.nl/wp-content/uploads/2016/09/pp-update.png>. On May 25, 2018]

E-mail 2:

**Van:** "paypal" <[redacted]>  
**Datum:** 23 mei 2018 om 20:20:20 CEST  
**Aan:** [redacted]  
**Onderwerp:** Onze veiligheidsteam heeft onregelmatige activiteiten op uw Paypal-Account waargenomen  
**Antwoord aan:** [redacted]



Geachte Client,

Onze veiligheidsteam heeft onregelmatige activiteiten op uw Paypal-Account waargenomen. Er zou geprobeerd toegang tot uw Paypal-rekening te krijgen via een voor ons onbekend IP-Adres (89.234.312.54), uit veiligheidsredenen hebben wij uw account al 3 dagen op non-actief geplaatst. U moet uw Paypal-rekening herstellen, tot dan is de toegang tot uw rekening en uw online betalingen beperkt.

Wij verzoeken u om uw account gebruik te verifiëren : > [Account verificatie](#) <  
**Let op: Verifieer uw account binnen 24 uur, anders komt deze te vervallen.**

De beveiliging van uw Paypal-rekening heeft topprioriteit voor ons en we willen graag met u samenwerken om uw rekening te beschermen in de toekomst.

Met vriendelijke groet,  
Paypal BV  
Postbus 42435, 1630 FT Amsterdam  
KvK Amsterdam nr. 53.231.535

---

[E-mail 2. This is an image of a phishing mail that was obtained by a Dutch online database for phishing e-mails. Fraude Helpdesk Downloaded from: <https://www.fraudehelpdesk.nl/wp-content/uploads/2018/05/PAYPAL2405.jpg>. on May 10, 2018]

E-mail 3:

**Van:** [REDACTED]  
**Onderwerp:** Update required - Netflix account on hold 28/03/2018 05:21:45  
**Datum:** 29 maart 2018 om 02:21:45 CEST  
**Aan:** [REDACTED]

---

## Update required - Netflix account on hold

**Dear Valued Netflix User,**

Sorry for the interruption, but we are having trouble authorizing your Payment Method.

Please visit the account payment page at

<https://www.netflix.com/YourAccountPayment> to enter your payment information again or to use a different payment method.

When you have finished, we will try to verify your account again.

If it still does not work, you will want to contact your credit card company.

To protect the informations of our customers, our system has temporarily placed restrictions on your account until your informations has been validated against our system.

You can validate your informations by either clicking on the link above or below, this will only take a few minutes and your account functions will be fully restored.

[Log In To account](#)

If you have any questions, we are happy to help. Simply call us at 0800-917812.

-Your friends at Netflix

Netflix Inc. : Netflix Corporate Headquarters 100 Winchester Circle Los Gatos, CA 95032.  
You can un-subscribe to security alerts by configuring your online account.  
We are sending this email to provide support for your personal online Netflix account.

28/03/2018 05:21:45

[E-mail 3. This is an image of a phishing mail that was obtained by a Dutch online database for phishing e-mails. Fraude Helpdesk. Downloaded from: <https://www.fraudehelpdesk.nl/wp-content/uploads/2018/03/Netflix-29032018.jpg>. On May 10, 2018]



E-mail 4

---

**Van:** Billing PayPal <userbilling1@nindyemot.com>  
**Verzonden:** zondag 29 januari 2017 22:05  
**Onderwerp:** Reminder: We detect fraud activity on your PayPal account  
(Limited Statement)

**schadelijke bijlage**

Dear \_\_\_\_\_@hotmail.com ,

We need your help resolving an issue with your PayPal account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

**Your account access has been limited for the following reason(s):**

January 27, 2017: We want to check with you to make sure that no one has logged in to your account without your permission.

Please take a moment to change your password and create new security questions. You should also take a look at your account information and recent transactions. Make sure that your account information (address, phone number, etc.) hasn't changed and that you recognize all of your recent transactions. If you see a payment that you don't recognize, let us know by going to the Resolution Center. Click "Dispute a Transaction" to report an unauthorized transaction.

**( Your case ID for this reason is PP-003-772-241-149 )**

How can I get my account access restored?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account and update your card detail. To help us with this and to find out what you can and can't do with your account until the issue is resolved .

[E-mail 4. This is an image of a phishing mail that was obtained by a Dutch online database for phishing e-mails. Fraude Helpdesk Downloaded from: <https://www.fraudehelpdesk.nl/wp-content/uploads/2017/01/We-detect-fraud-activity-on-your-PayPal-.png>. On May 10, 2018]

E-mail 5

----- Forwarded message -----

From: "Gwendolyn Maxwell" <sale@ewoolems.com>

To:

Subject: Delivery attempt fail notice #4441684364

Date: Tue, 18 Apr 2017 11:09:51 -0600

Dear customer, |

We attempted to deliver your package on April 16, 2017

The delivery attempt failed because no one was present at the shipping address, so this notification was automatically sent.

You can arrange redelivery by visiting the nearest Purolator Post office with the printed shipping invoice mentioned below.

If the package is NOT arranged for redelivery or picked up in 48 hours, it will be to the sender.

TRACKING: LD265357226CA  
Expected Delivery On: April 16, 2017  
Class: Package Services  
Service(s): Shipping Confirmation  
Status: eNote sent

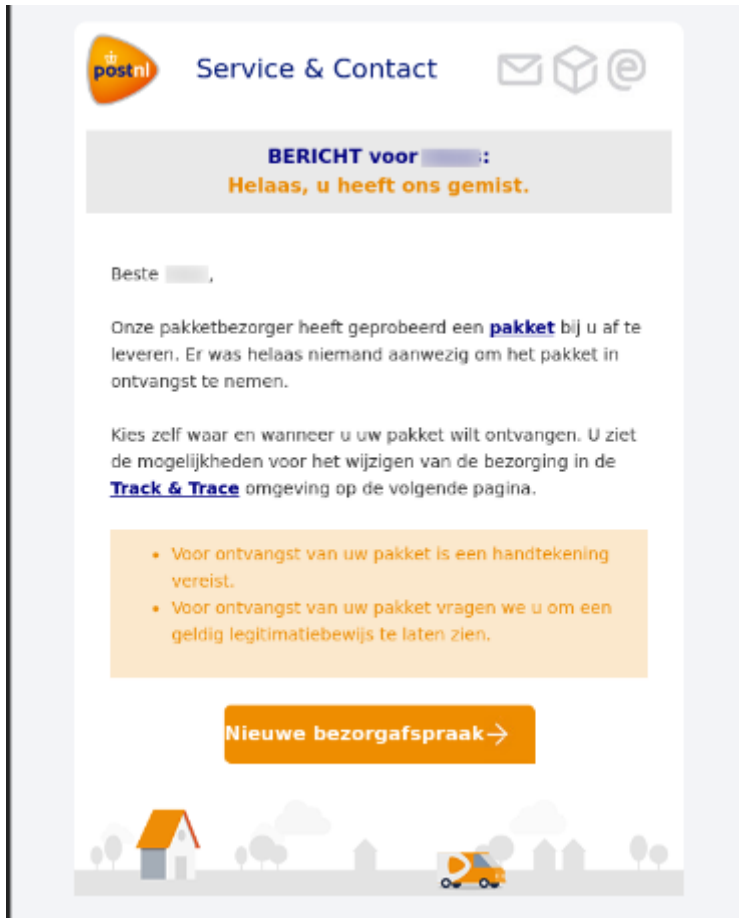
To download the invoice, visit the following link:

[https://purolator.ca/cpotools/apps/track/personal/findInvoiceByTrackingNumber?session\\_id=910938402](https://purolator.ca/cpotools/apps/track/personal/findInvoiceByTrackingNumber?session_id=910938402)

Thank you,  
© 2017 Purolator Post Corporation

[E-mail 5. This is an image of a phishing e-mail obtained from the University of Saskatchewan. Downloaded from: <https://words.usask.ca/phishingalerts/2017/04/>. On May 09, 2018]

E-mail 6



[E-mail 6. This is an image of a phishing mail that was obtained by a Dutch online database for phishing e-mails. Fraude Helpdesk. Downloaded from: <https://www.fraudehelpdesk.nl/wp-content/uploads/2018/06/Postnl0106.jpg>. On May 10, 2018]

## E-mail 7

Onderwerp: TRACKING BIJHOUDEN POSTSERVICE 95 \*\*\*\*\*  
Van: "Post NL" <[info@nlpostservice.com](mailto:info@nlpostservice.com)>  
Datum: 12-10-2015 7:21  
Aan:

..

Helaas hebben wij uw pakket niet kunnen leveren aan u, omdat het adres stond in de verkeerde indeling.

Uw pakket met het nummer 3194275045 is aangekomen op 9 oktober.

Onze koerier kon het pakket niet leveren, omdat de ontvanger niet thuis is.

Als het pakket niet binnen 15 werkdagen wordt ontvangen, heeft ons bedrijf recht om schadevergoeding te eisen van u, de kosten van de opslag van goederen kost EUR 4,18 per dag.

U kunt informatie over de procedure en voorwaarden van opslag bij de dichtstbijzijnde kantoor of op onze website vinden.

[http://post-servicenl.com/track-and-trace/?id.\\*\\*\\*\\*\\*](http://post-servicenl.com/track-and-trace/?id.*****)

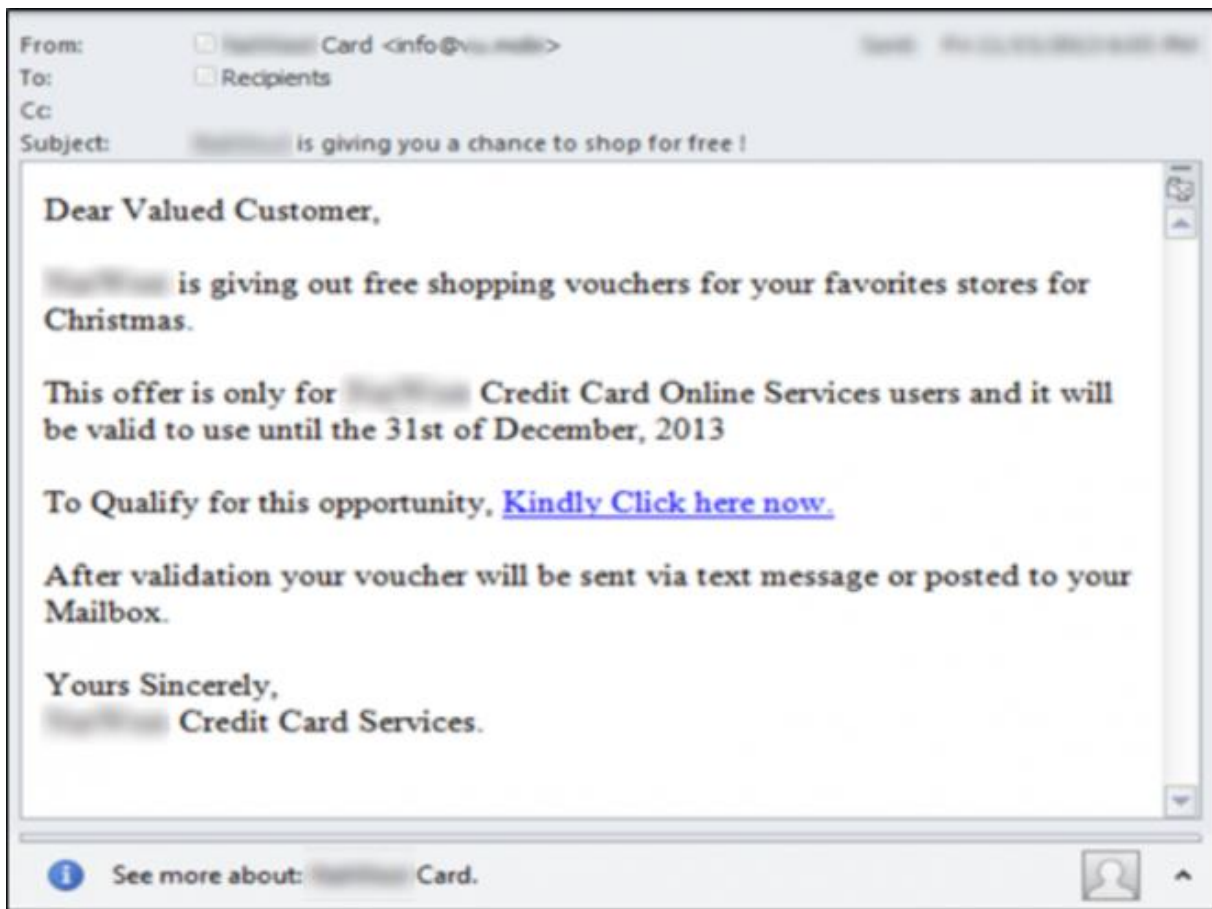
De volgende principes liggen ten grondslag aan de manier waarop wij uw privacy in acht nemen:

1. Wij waarderen het vertrouwen dat u in ons stelt door uw persoonsgegevens aan ons te verstrekken. We zullen uw persoonsgegevens altijd gebruiken op een eerlijke manier die recht doet aan het vertrouwen dat u in ons stelt.
2. U hebt recht op duidelijke informatie over de manier waarop wij uw persoonsgegevens gebruiken. We zullen steeds transparant met u communiceren over welke informatie we verzamelen, wat we ermee doen, met wie we de informatie delen en met wie u contact op kunt nemen indien u zich zorgen maakt.
3. Persoonsgegevens: Wij zullen alle redelijke stappen ondernemen om uw informatie tegen misbruik te beschermen en deze te beveiligen.
4. Wij zullen voldoen aan alle toepasselijke wetgeving inzake gegevensbescherming en regelgeving en wij zullen samenwerken met de betreffende autoriteiten. In gevallen waarin wetgeving inzake gegevensbescherming niet voorziet, zullen we handelen in overeenstemming met algemeen aanvaarde beginselen voor de bescherming van gegevens

[E-mail 7. This is an image of a phishing mail that was obtained by a Dutch online database for phishing e-mails. Fraude Helpdesk. Downloaded from:

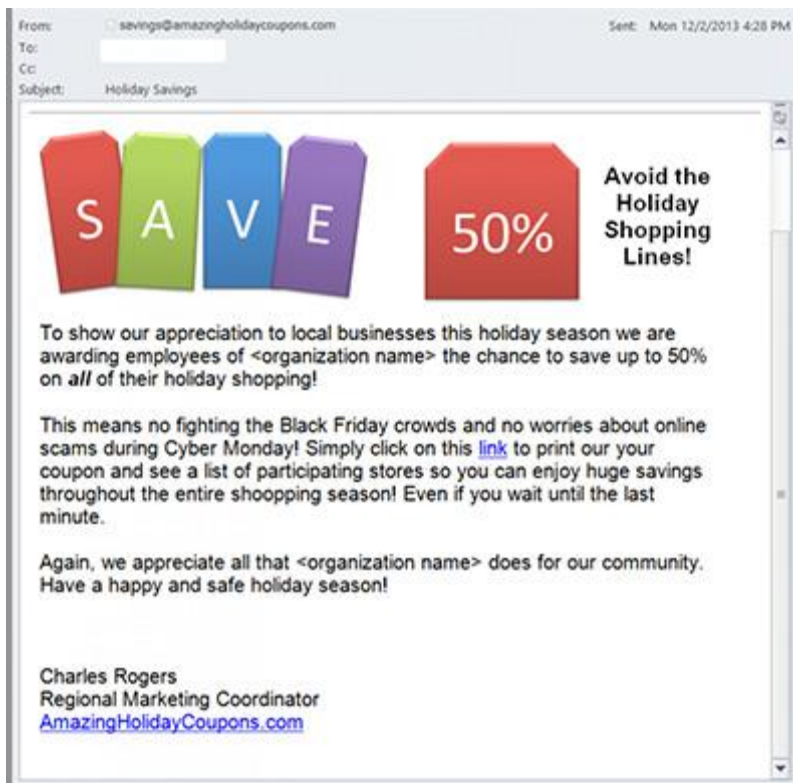
<https://www.fraudehelpdesk.nl/wp-content/uploads/2015/10/Post-NL12102015.jpg>. On May 10, 2018

E-mail 8



[E-mail 8. This is an image of a phishing e-mail that was obtained by information security magazine Helpnet Security. Downloaded from: <https://www.helpnetsecurity.com/2013/12/02/free-shopping-voucher-offer-leads-to-phishing/>. On May 10, 2018]

E-mail 9



[E-mail 9. This is an image of a phishing e-mail that was obtained by a cybersecurity firm (specialised in phishing) Cofense. Downloaded from : <https://cofense.com/popular-holiday-themed-phishing-attacks/>. On May 14, 2018]

**From:** Duinrell  
**Sent:** Sunday, August 27, 2017 5:32 AM  
**To:** [redacted]  
**Subject:** Wat doe jij deze zomervakantie, [redacted]?



Inclusief 6 Fastpass kaarten


**Beste [redacted],**

Het pretparkseizoen is weer begonnen en we geven je de kans om **6 kaartjes te ontvangen voor een pretpark naar keuze!** Inclusief 6 fastpass kaarten. Wees er snel bij, want dit aanbod is maar tijdelijk.

**GENIET NU SAMEN VAN EEN HEERLIJK DAGJE UIT!**

Doe mee op de volgende pagina

**GA NU VERDER!**



[E-mail 10. This is an image of a phishing mail that was obtained by a Dutch online database for phishing e-mails. Fraude helpdesk. Downloaded from: <https://www.fraudehelpdesk.nl/wp-content/uploads/2017/08/DUINRELL288.png>. On May 12, 2018.

E-mail 11

----- Oorspronkelijk bericht -----

Van: Ticket service <email@future-es.cccampaigns.com>

Datum: 25-10-2016 06:03 (GMT+01:00)

Aan:

Onderwerp: Bedankt, een vakantie naar keuze voor

**KRANTEN EN TIJDSCHRIFTEN** Als u dit bericht niet kunt lezen, klik dan hier voor de online versie.

KLM viert hun succes en geeft gratis tickets weg!

**Ik wil meedoen!**



**Win 2 KLM tickets naar keuze!**

**Gefeliciteerd, is geselecteerd om mee te doen aan onze wedstrijd om 2 KLM tickets naar keuze te winnen!**

Beste

**KLM viert hun succes en geeft gratis tickets weg!**

U bent geselecteerd om mee te doen aan onze wedstrijd om 2 KLM vliegtickets naar keuze te winnen! Om mee te doen met de wedstrijd hoeft u maar 5 vragen te beantwoorden. Het zal maar 2 minuten van uw tijd kosten.

Klik op de onderstaande knop om door te gaan. Succes en veel plezier!

**Ik wil meedoen!**

[E-mail 11. This is an image of a phishing mail that was obtained by a Dutch online database for phishing e-mails. Fraude Helpdesk. Downloaded from: <https://www.fraudehelpdesk.nl/wp-content/uploads/2016/10/klm2510.png>. On May 12, 2018]



E-mail 12

From: "LinkedIn"

Dear LinkedIn User

As part of our effort to improve your experience in LinkedIn access across our consumer services, we're updating LinkedIn Services Agreement and Privacy.

Click the link below to update your account.

<http://ipdosudan.org/un/a/sign.htm>

Your account will be De-Activated if you do not update.

This notice will Ends: Monday, October 31, 2016

We apologize for any inconvenience.

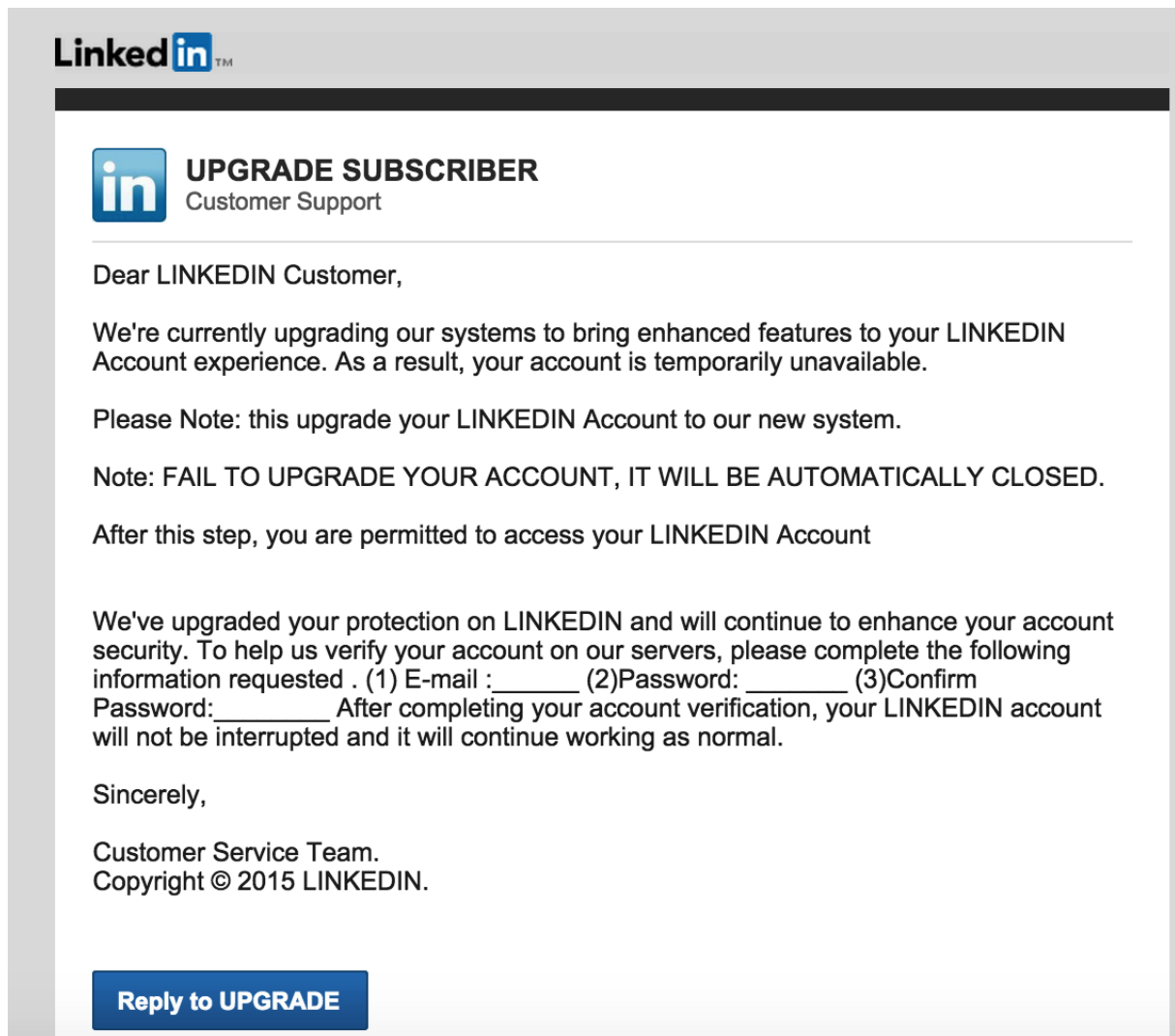
Thank you for your cooperation.

Sincerely.

LinkedIn Service Provider

Copyright © 2016 Information

[E-mail 12. This is an image of a phishing mail that was obtained by a Dutch online database for phishing e-mails. Fraude Helpdesk. <https://www.fraudehelpdesk.nl/wp-content/uploads/2016/10/update-linked-in.pn>. On May 10, 2018]



[E-mail 13. This is an image of an e-mail obtained by a firm who offers LinkedIn consultancy. Intero Advisory. <https://www.interoadvisory.com/2015/09/report-phishing-emails-in-linkedin/screen-shot-2015-09-06-at-2-23-23-pm/>. On May 14, 2018].

**Timothy Stokes** 500+ connections

Recruitment Consultant at Teledyne Technologies Incorporated  
Newbury Park, California | Electrical/Electronic Manufacturing

Current: Teledyne Technologies Incorporated  
Previous: ExxonMobil  
Education: University of California, San Diego

**Join LinkedIn and access Timothy's full profile. It's free!**

As a LinkedIn member, you'll join 300 million other professionals who are sharing connections, ideas, and opportunities.

- See who you know in common
- Get introduced
- Contact **Timothy** directly

[View Timothy's Full Profile](#)

**Summary**

I assist in selecting the best-qualified candidates during open hiring. I am involved with screening applications, interviewing candidates and checking references. Our contracts involve the recruitment and secondment of skilled engineers, technicians and managers to client facilities on a domestic or international basis to support major engineering, construction, installation and ongoing operations activities. Teledyne Technologies Inc. owns a globally focused operation, active in over 40 locations, driven by a professional and talented team of people, dedicated to achieving excellence.

**Experience**

**Recruitment Consultant**  
Teledyne Technologies Incorporated  
March 2012 – Present (3 years 5 months) | Thousand Oaks

- Remarkable experience in Recruitment Consultancy
- Project based recruitment, candidate screening & referral networking for both local and emerging
- Ability to identify and successfully qualify candidates
- Familiarity with payroll procedures and taxation issues relevant to contractors
- Good understanding of Consultants contracts and terms and conditions
- Amazing ability to manage independently

[E-mail 14. This is an image of a phishing e-mail that was obtained by cybersecurity firm Secureworks. Downloaded from: <https://www.secureworks.com/research/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles>. On may 10, 2018.

**Van:** Belastingdienst [mailto:noreply@web3.neoclan.net.mx]

**Verzonden:** zaterdag 3 december 2016 10:31

**Aan:**

**Onderwerp:** U heeft recht op een belastingteruggave van € 597,64 ontvangen



Belastingdienst

## Belastingdienst

Uniek Referentienummer: 5489563248

**Lieve** [REDACTED]

U heeft recht op een belastingteruggave van € 597,64 ontvangen. Klik op de onderstaande link om uw belastingteruggaaf verzoek op onze website te voltooien.

**VOORLEGGEN** ➔

Belastingdienst zal sturen over terugbetalingen binnen 2 weken. Het kan langer duren in sommige gevallen, bijvoorbeeld voor het verzenden ongeldige ingangen of vul boven het online formulier. Je moet vier weken na het maken van een online claim, en 6 weken wachten na toestemming voordat u contact opneemt Belastingdienst- van betaling.

© 2016 Belastingdienst.nl

Over de organisatie Toegankelijkheid Werken bij de Belastingdienst Contact

[E-mail 15. This is an image of a phishing mail that was obtained by a Dutch online database for phishing e-mails. Fraude Helpdesk. <https://www.fraudehelpdesk.nl/wp-content/uploads/2016/12/U-heeft-recht-op-een-belastingteruggave-1.png>. On May 10, 2018]

E-mail 16

**Onderwerp:** Nieuw bericht Belastingdienst

**Datum:** Thu, 18 Jan 2018 18:38:10 -0500

**Van:** [redacted] <[redacted]@[redacted]>

**Aan:** [redacted]



## Belastingdienst

Geachte heer of mevrouw,

Bij controle van onze administratie hebben wij geconstateerd dat er een betalingsachterstand is ontstaan van uw belastingaangifte. Wij hebben geprobeerd om het openstaande bedrag te incasseren op uw rekeningnummer dat bij ons bekend is, maar helaas is dit niet gelukt.

Het huidige openstaande saldo bedraagt € 98,02,- U ontvangt ook een schriftelijke herinnering die per post is verstuurd.

Wij verzoeken u daarom ook dringend het openstaande bedrag van € 98,02,- te betalen. U dient het verschuldigde bedrag over te maken naar bankrekeningnummer NL66 [redacted] 5605 63 ten name van "Belastingdienst " ( onderdeel van MijnOverheid) onder vermelding van betalingskenmerk: NL2372111107.

Wij willen u erop wijzen dat, bij het uitblijven van de betaling, wij € 10,- kosten in rekening zullen brengen. U loopt verder het risico dat wij voor het verdere aanmaningstraject volgens de "Wet Incasso Kosten" 15% over het door u verschuldigde bedrag met een minimum van € 40,- aan kosten in rekening zullen brengen.

Betaal het verschuldigde bedrag op tijd en voorkom extra kosten! Heeft u vragen ?  
Contacteer ons dan via onze website.

Met vriendelijke groet,  
MijnOverheid

Dit is een automatisch gegenereerd bericht. Een reactie op dit bericht wordt niet gelezen

[E-mail 16. This is an image of a phishing mail that was obtained by a Dutch online database for phishing e-mails. Fraude Helpdesk. <https://www.fraudehelpdesk.nl/wp-content/uploads/2018/01/Belastingdienst.png>. On May 12, 2018]

**Van:** "Belastingdienst"  
**Datum:** 2 november 2017 om 03:30:16 CET  
**Aan:**  
**Onderwerp:** Belastingaangifte 2016



## Belastingdienst

Geachte heer/mevrouw,

Bij controle van onze administratie hebben wij geconstateerd dat er een betalingsachterstand is ontstaan van uw belastingaangifte. Wij hebben geprobeerd om het openstaande bedrag te incasseren, helaas is dit niet gelukt op het rekeningnummer dat bij ons bekend staat. Het huidige openstaande saldo bedraagt **€ 35,25**. U ontvangt ook een schriftelijke herinnering die vandaag per post is verstuurd.

Thans verzoeken wij u vriendelijk om dringend het opstaande bedrag van **€ 35,25** te betalen. U kunt nu direct uw betaling doen via IDEAL.

- Klik [hier](#) op: online betalen om de factuur te voldoen, let op dat u de juiste bedrag:
- **€ 35,25** invult.
- Klik vervolgens op 'BUY'.
- Bij uw bitcoinsadres vult u:
- U kunt nu direct uw betaling doen via IDEAL. Kies hiertoe uw eigen bank.
- Zodra u het openstaande bedrag heeft betaald, ontvangt u een bevestiging email.

Wij willen u erop wijzen dat, bij het uitblijven van de betaling, wij **€ 10** kosten in rekening zullen brengen. U loopt verder het risico dat wij voor het verdere aanmaningstraject volgens de 'Wet Incasso Kosten' **15%** over het door u verschuldigde bedrag met een minimum van **€ 40** aan kosten in rekening zullen brengen. Betaal het verschuldigde bedrag voor **06-11-2017** en voorkom extra kosten!

Wij zien uw betaling graag tegemoet en danken u voor uw medewerking. Met vriendelijke groet,

Rob  
Directeur-General Belastingdienst

N.B. dit is een automatisch verzonden e-mail, het is niet mogelijk deze e-mail te beantwoorden.

[E-mail 11. This is an image of a phishing mail that was obtained by a Dutch online database for phishing e-mails. Fraude Helpdesk. <https://www.fraudehelpdesk.nl/wp-content/uploads/2017/11/BELASTING211.png/>. On May 13, 2018]

## All Employees: Update your Healthcare Info



[(customer)] HR (HR-Alerts@healthcare.updates.authorizednotifications.com) [Add to contacts](#) 10:29 PM

To: [REDACTED]

### IMPORTANT! PLEASE READ!

**ALL** employees must update their healthcare information or else we cannot continue coverage for this year. Follow this link to ensure this gets completed prior to next week. [www.securedata.com/employees/updateinfo](http://www.securedata.com/employees/updateinfo)

Help us stay healthy!

HR & Management  
Steve Smith

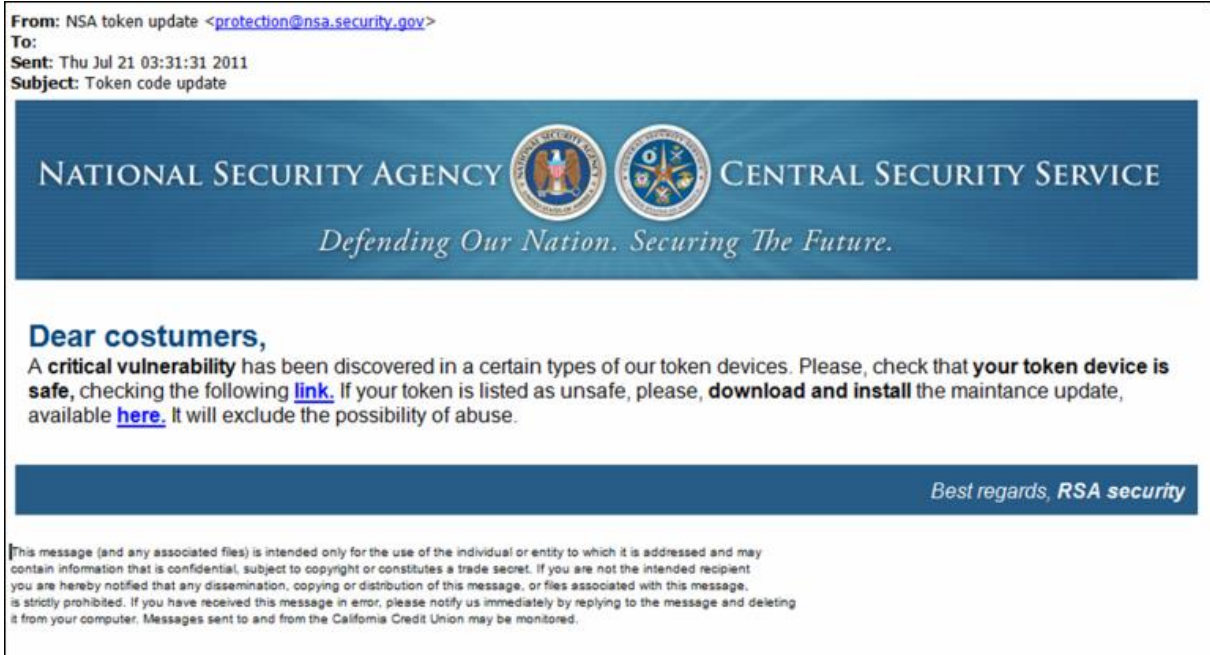
If you are reading this, you probably already know that this is a phishing test! It was sent by JohnGreving - [click here](#) (or copy/paste the URL) to report that you successfully detected it.

As per CAN-SPAM 2003 (US), Opt-In Directive 2002/58/EC (EU) and CASL (Canada), this is not a marketing message. This message is a specific test sent by JohnGreving to Justin Smith through the Phish.io security awareness web site. For more information, please see [Phish.io](http://Phish.io).

[Unsubscribe](#) - [Report Spam](#) - [Report Phishing](#)

[E-mail 18. This image shows a phishing e-mail that was recovered by Information Security training platform the Infosec Institute. Downloaded from: <https://resources.infosecinstitute.com/category/enterprise/phishing/the-phishing-landscape/phishing-attacks-by-demo-graphic/phishing-in-healthcare/#gref> on May 15, 2018]

E-mail 19



[E-mail 19. This image shows a phishing e-mail that was send to NSA employees. Image was obtained from cyber security firm Lookingglass. Downloaded from: <https://www.looking-glasscyber.com/blog/threat-reports/phishing/rsa-token-vulnerability-and-one-of-americas-most-secret-agencies-invoked-in-latest-spear-phishing-attack/> on May 15, 2018)



