Master Thesis

The effectiveness of hints for online banking customers on reducing phishing susceptibility: A Dutch customer's perspective

Author: Wietse van der Leest

Faculty: Behavioural, Management & Social sciences

Study: MSc Business Administration

Track: Financial Management

Delivery date: 02-05-2018

1st Supervisor: Prof. Dr. M. Junger

2nd Supervisor: Dr. H.C. van Beusichem

UNIVERSITY OF TWENTE.

Contents

Acknowledgements

I hereby would like to thank Prof. Dr. M. Junger for the supervision during my thesis and for the necessary help. I also would like to thank Dr. H.C. van Beusichem for his role as being the second supervisor in my thesis and providing me with useful insights and feedback during my thesis.

Management summary

This study aimed at finding the effect that the hints of Veiligbankieren.nl had on decreasing phishing susceptibility and whether these hints were actively used in the process of correctly judging a bank e-mail (by using eye-tracking glasses). An experiment was setup in which 27 participants were recruited to judge the legitimateness of 10 bank e-mails and answer questions to related topics. The participants were split into two groups, a group who read the hints (experimental group) and the other not (control group). Results portrayed a significant difference in the amount of bank e-mails correctly judged between the experimental and the control group, in favor of the experimental group. Therefore these hints showed to be effective in reducing phishing susceptibility. Results of the eye tracking heat maps displayed that on average four out of five hints were actively used by both groups. The only hint which was not used actively was the checking of the spelling. The difference between the experimental and the control group showed a positive effect with the hint about checking the sender and the spelling mistakes in terms of active use by the participants. The compelling character showed a negative effect in terms of use in favor of the control group. Therefore this hint creates confusion among the participants. The other hints showed little difference between the experimental and the control group (Non personal salutation and a link to the login screen). Therefore the conclusion was that the hints of Veiligbankieren.nl are the cause of a decrease in phishing susceptibility in an experimental setup. The hints which portrayed a positive influence in active use of the hints were the main cause of this decrease in phishing susceptibility.

1. Introduction

As Nelson Mandela once said: “Education is the most powerful weapon which you can use to change the world” (Brainquote, N.D.). Therefore, researchers tried to find the most suitable solutions for several problems which our modern world faces by learning and educating. One of these problems which emerged rapidly after the introduction of the internet is phishing (Dhamija, Tygar & Hearst, 2006).

Since these phishing attempts emerged quickly, both practitioners and researchers had to find solutions to prevent phishing. Several tools were developed to prevent e-mail phishing by using filters which can identify these types of e-mails (Kumaraguru, Rhee, Acquisti, Cranor, Hong & Nunge, 2007). Several studies also tried to pinpoint important issues or focal points to prevent phishing. One of the most studied relationships is the effect of demographics on phishing susceptibility (Sheng, Holbrook, Kumaraguru, Cranor & Downs, 2010; Kumaraguru, Cranshaw, Acquisti, Cranor, Hong, Blair & Pham, 2009). The goal of these studies was to find certain target groups with specific demographics characteristics on which several protective measures could be applied. Several groups were found to be more vulnerable to phishing, such as females and individuals aged between 18 to 25 (Sheng et al., 2010; Kumaraguru et al., 2009).

A second group of studies did not focus on demographic characteristics. These studies tried to discover what is most effective in reducing phishing susceptibility. The effectiveness of several tools such as Anti Phishing Phil or the Phish Guru (which were cartoons) were tested and mostly showed positive results in reducing phishing (Sheng et al., 2010; Mayhorn & Nyeste, 2012; Sheng, Magnien, Kumaraguru, Acquisti, Cranor, Hong & Nunge, 2007). Therefore, organizations who were also facing phishing related issues could introduce these tools into their organization to reduce phishing susceptibility.

A common problem in phishing susceptibility is that a large part of the susceptibility can be contributed towards a lack of awareness of phishing susceptibility (Sheng et al., 2010). Therefore organizations such as banks had to find a way to increase awareness of phishing and educate their customers in preventing phishing because of the damages lost (Brignall, 2016).

Thus, to combat phishers and to reduce damages, banks in the Netherlands introduced the hints of Veiligbankieren.nl to increase risk awareness and reduce phishing susceptibility (Veiligbankieren.nl, N.D.). However, until now no other studies tried to find the effect that the hints of Veiligbankieren.nl have on reducing phishing susceptibility. Therefore this study

focused on whether reading the hints of Veiligbankieren.nl reduced the phishing susceptibility through a better judgement of bank e-mails. To be able to reach a conclusive answer to the effect of these hints, the following research question was formulated: What is the effect of the hints of Veiligbankieren.nl on reducing phishing susceptibility of e-mails with bank related topics? Several sub-questions were formulated in order to answer the main research question.

1. What is the effect of the hints of Veiligbankieren.nl on reducing phishing susceptibility?

2. Do participants actively use the hints of Veiligbankieren.nl to correctly evaluate bank e-mails and reduce the phishing susceptibility?

    2.1 Does the group who read the hints during the experiment actively use the hints of Veiligbankieren.nl?

    2.2 Does the group who did not read the hints of Veiligbankieren.nl actively use the hints of Veiligbankieren.nl?

    2.3 Is there a difference between the experimental and the control group in the active use of the hints of Veiligbankieren.nl?

In order to test whether these hints are effective in reducing phishing susceptibility, an experiment was setup in which the participants had to judge legitimacy of the e-mails presented. The participants were divided into two groups, a group which read the hints during the experiment and a group which did not read the hints of Veiligbankieren.nl. A survey was used to guide the experiment and to collect data to test whether there was a significant difference in the amount of bank e-mails correctly judged between the experimental and the control group. Eye tracking was used in order to analyze whether the hints of Veiligbankieren.nl are actively used. By using a combination of these two methods, a conclusive answer was made about the effectiveness of the hints of Veiligbankieren.nl on reducing phishing susceptibility.

2. Theoretical framework

This chapter will review the most important literature for this study. The chapter consists of research performed about risk, drivers of banks and customers to adopt online banking, the current state of phishing and e-mail phishing, the countermeasures to prevent phishing from happening, the hints of Veiligbankieren.nl and the influence of demographics on phishing susceptibility.

2.1 Risk

Since phishing is all about making well thought decisions about whether an e-mail is genuine or poses a risk, it is important to start the theoretical review at the top of the funnel. Several researchers have studied the concept of risk within social sciences. There are several definitions of risk within the literature in which probabilities of losses or gains was one of the earliest (Lupton, 1999; Kaplan & Garrick, 1981). However, more modern researchers defined risk "as a term reserved for a negative or undesirable outcome" (Lupton, 1999, p. 12).

The risk which each person or entity experiences is different from other persons, which causes each person to have its own risk management. As it is well-known that reducing risks creates value for customers and other parties involved, it is important that the risk of being phished is minimized. The value is created by minimizing the chance of losses which could occur during the process of logging onto online banking or using it.

Also important in risk management is the presence of risk awareness by a customer. As Kaplan & Garrick (1981) state "if we know there is a hole in the road around the corner, it poses less risk to us than if we zip around not knowing about it" (Kaplan & Garrick, 1981, p. 12). Therefore if someone is aware of a risk, he/she will try to minimize the risk and make sure the risk will not occur again. Therefore it is important to increase risk awareness by minimizing the risk faced by customers of online banking. Introducing these hints could result in an increase in risk awareness and result in a lower phishing susceptibility.

By introducing the hints of Veiligbankieren.nl, banks try to minimize the chance of becoming a phishing victim. Banks try to do this by increasing the risk awareness of customers and therefore lowering the chance of becoming a victim of phishing due to a better judgement of bank e-mails. If the chance of being victimized by phishing lowers, trust in the online environments of the banks and loyalty will be improved (Gremler & Brown, 1996; Floh &

Treiblmaier, 2006). The increase in trust and loyalty can subsequently be a partial explanation for the decrease of the costs incurred by customers and banks through the lowered damages. Simultaneously the reduced likelihood of becoming a phishing victim will increase the likelihood that customers remain at their respective banks because a person knows information security levels are higher at their own respective banks (Floh & Treiblmaier, 2006). Therefore, these hints can play a crucial role for any banks. However, whether these hints do decrease the phishing susceptibility or that other explanations exist is not known yet. Therefore these hints have the potential to be crucial for banks in further reducing phishing susceptibility by the increase of the risk awareness among customers of online banking.

2.2 History and drivers of online banking

A next step is to know what online banking is, why online banking rose to prominence in the last 30 to 40 years and why phishing was inevitable. Online banking has been on the rise since the 1980s and is one of the mainstream tools used to transfer money between clients of banks through an online environment (GoBankingrates, 2016). A significant boost came when companies started to offer their products through the internet (also known as e-commerce), because the public needed to access their bank account online to purchase a product.

Motives for customers to use online banking are not well embedded within current research. The Technology Acceptance Model (TAM) (Venakatesh & Bala, 2008) (Appendix A) provides a theoretical explanation for the adoption of new technologies. The two main drivers behind the TAM model are the perceived usefulness and perceived ease of use. These two concepts explain why online banking was adopted since perceived usefulness and perceived ease of use relate to why a customer would consider using online banking (i.e. drivers).

2.2.1 Customer drivers for the use of online banking

Aladwani (2001) discusses several motivations for customers to use online banking, such as being faster than visiting a bank (saving time) and transferring money more easily (i.e. convenience) (Aladwani, 2001; Daniel, 1999). Customers now have control of banking activities and their own financial situation, which previously had been in the hands of the personnel of the banks (Daniel, 1999). The increased control also increased the privacy of customers, because no bank employee is involved in transferring money towards another account. An increase in privacy not only benefits the customer, because an increase in privacy for the customer also

increases the profit for a company (Shy & Stenbacka, 2013; Mukherjee & Nath, 2003)

2.2.2 Drivers from a banks perspective for the use of online banking

There are several perspectives on drivers of banks to use online banking. A noteworthy contribution of Aladwani (2001) is the finding that the introduction of online banking came 87.5% from senior management. The introduction by senior management could suggest that customers were less aware of the opportunities online banking had and the problems online banking could give them in the near future.

The most important drivers for a bank are providing customers with faster, easier and more reliable service to increase the perceived usefulness and perceived ease of use (Aladwani, 2001; Cheng, Lam & Yeung, 2006). Secondary drivers are according to Aladwani (2001) related to the competitive position of a bank towards the customers which make use of banks. On average the least important motivations for banks were cost related according to Aladwani (2001) (see Appendix B for an overview).

The previous portrays online banking as helpful, used and adopted by both banks and customers. A customer mainly profits from either convenience or time saving related factors. On the contrary, a bank profits in terms of a more reliable and faster service towards their customer (Aladwani, 2001). However, as with any system nowadays, there will be phishers who will try to fool and take advantages of any flaws in a system. Therefore phishing became an issue for banks, because there are persons who try to fool a banks' customer to profit from the scam themselves. Implying that deploying solutions to prevent phishing needs to be a main priority. The hints of Veiligbankieren.nl could be a front-end solution for phishing and thus reduce susceptibility towards phishing.

2.3 Phishing and the development of a phishing e-mail

2.3.1 Phishing and e-mail phishing

A method for breaching into an account of an online banking customer is called phishing. Phishing (or social engineering for company related phishing) is "a scalable act of deception whereby impersonation is used to obtain information from a target" (Lastdrager, 2014, p. 8). Phishers focus on the weakest link, which is a customer that has the least amount of protection and therefore will be most vulnerable to their attacks (Purkait, 2012).

There are several methods to perform phishing, of which a phishing e-mail (Bose & Leung, 2007) is one of the most common methods to approach customers (Crowe, 2016). The e-mail user is confronted with an e-mail from their bank or another entity. The e-mail states a problem or an urgent situation in which it is required to login to their bank account and provide personal information on the same (Purkait, 2012). If a person provides the information, he or she will see their account being monetized which results in damages. The reason behind the popularity of e-mail phishing is that e-mail phishing is "simple, are low cost and complicate attribution" (Oliveira, Rocha, Yang, Ellis, Dommaraju, Muradoglu & Ebner, 2017, p. 6412). A factor which causes these e-mails to spread even further is the large amount of systems which are connected to the internet. Thus if a computer within a system is hacked, it is possible that other computers will be infected too if there is malicious software at the location of a clicked link or an attachment.

The success of e-mail phishing depends greatly on psychological factors which can influence customers. These factors can encompass "authority, commitment, liking, perceptual, contrast, reciprocation, scarcity and social proof" (Oliveira et al., 2017, p. 6412). The previous factors can be strengthened if a hacker has personal information about a person because the hacker can address such a person more specific (Polakis, Iasonas, Kontaxis, Antonatos, Gessiou, Petsas, Markatos, 2010). All in all, this is a relatively easy method to deploy. Therefore especially e-mail phishing is used a great deal to spoof customers. Since not every customer can protect itself from being spoofed, quick and easy to remember hints can be useful.

2.3.2 The method of preparing a phishing attack

The method of e-mail phishing follows a three-step pattern according to Hong (2012). The process of phishing starts with the hacker creating the fake e-mail and gathering and eventually sending the e-mail towards as many e-mail addresses as possible. The messages of these e-mails contain social techniques, also called social engineering, to persuade end-users to click on the link and providing the hacker with private information (Hong, 2012). These social techniques can encompass a type of urgency to persuade e-mail users into clicking on the link (Hong, 2012).

The second step in the process is setting up the fake website to whom a customer needs to be guided (Hong, 2012). Several tactics are used to mimic the original website of a company to a

high standard and hereby fool the customer. Tactics such as using a double “vv” to look like a “w” or putting in “login” within the original link. Also putting ‘phisingsite.com’ behind an original website address is a technique to deceive individuals (Hong, 2012). The effectiveness of these tactics are mainly caused by the lack of time spend looking at the URL (Alsharnouby, Alaca & Chiasson, 2015; Whalen & Inkpen, 2005; Kunz, Volkamer, Stockhardt, Palberg, Lottermann, Piegert, 2016) which is a key indicator whether a website is a phishing website (Blum, Wardman, Solorio & Warner, 2010). However, the results from later studies do show an increase in the awareness of the importance of the URL. Therefore an increased awareness of the importance of the URL could be an additional reason that the phishing susceptibility has lowered (Iuga, Nurse & Erola, 2016).

The last step in the process is monetizing the stolen information from the customer. The path a phisher uses is either direct or indirect. For example using banking login information of a customer to transfer money away from the account (direct) or hacking an account of a computer game (Hong, 2012). Another option for phishers is to sell the stolen information since the information has monetary value for hackers which use this information to steal more money or other worthwhile objects from customers (Hong, 2012). These steps are performed by phishers to spoof for instance a customer of online banking. Therefore it is important customers can recognize whether the received e-mail is a phishing attempt.

2.4 The development of phishing

The emerging phenomena of phishing within cyber security related subjects was inevitable. An important facilitator of phishing is the increase in online activity in recent years (Dhamija et al., 2006). Therefore exposure to risks which involves using computers or other electronic devices rose drastically. In addition, the easy access to the internet, together with the popularity of the internet and vulnerability of computers and systems (Hai & Hsia, 2007), also made a prime target to trick persons into a scam. The issue of phishing is prominent as well (Crowe, 2016) because phishers come up with new methods every day to breach into bank accounts of customers. Therefore phishing is a prominent issue in today’s society.

Because the introduction of online banking came from banks (Aladwani, 2001), the awareness of issues with online banking was higher with banks than with customers. The lower awareness of problems emerged because these customers were faced with a new technology of

which the customers of banks did not know anything about. Subsequently phishing caused avoidable damages to both customers and banks. Customers lose money and banks lose trust of customers which do not actively do something against phishing issues

2.5 Preventive measures for phishing

2.5.1 Protective measures for phishing

Customers can employ several protective measures to prevent phishing. At first, a customer will be helped by the e-mail system operator (Almomani, Gupta, Atawneh, Meulenberg & Almomani, 2013). An operator systematically applies a filter which can recognize the phishing e-mails and delete or warn the retriever by putting the e-mail into the anti-spam filter (Bose & Leung, 2007). Despite these efforts, some e-mails are left unnoticed and will therefore go to the inbox of the customer which then needs to recognize whether the e-mail is an attempt at phishing.

Another important method to minimize phishing is to have a sufficient and up-to-date anti-virus system (Bose & Leung, 2007). The anti-virus system can scan the website and inform the user about a potential fraudulent website. There are several other methods described by Bose & Leung (2007) which could serve as preventive measures for phishing. However, these are less relevant for this study. All of the possible preventive measures as described by Bose & Leung are shown within Table 1.

Table 1: Possible preventive measures for phishing according to Bose & Leung (2007) and Purkait (2012) (2007, p. 550, transcribed to increase readability).

Anti-phishing measures	**Main features**
E-mail scan	Filter out phishing e-mails and reduce the chance of phishing (Bose & Leung, 2007; Purkait, 2012).
Takedown, transaction anomaly detection & log files	Monitor abnormal transactions stored in server logs and investigate if phishing has occurred or to monitor abnormal online traffic flows one can catch phishers before the crime begins (e.g., series of downloading activities from a IP) (Bose & Leung, 2007; Purkait, 2012). This can also encompass a created system which systematically

	detects phishing websites (Zhang, Hong, Cranor, 2007).
Proactive Web scanning	Check the visual and domain name similarity of newly registered Web sites and existing Web sites to deter phishing Web sites from burgeoning.
Poisoning phishing Web	Submit chunks of garbage information to the phishing Web site to dilute the actual data already gathered by the site and to thwart further phishing activity by overwhelming traffic flow to the site.
Legal solutions	Taking legal actions to prevent phishing from happening.

Anti-phishing measures for customers	**Main features**
E-mail scan	Filter out phishing prone e-mails and reduce the chance of phishing (Bose & Leung, 2007; Purkait, 2012).
Two factor and multichannel authentication	It is to use two factor authentication, i.e. not only use a single password to lock your account/information (Purkait, 2012).
Anti-Phishing training	Training customers to recognize phishing attempts (Purkait, 2012). Still, training can cause e-mail users to overreact and click away non-phishing e-mails by existing companies (Sheng et al., 2010).
Lock symbol in the URL/ read the URL/ increasing the awareness to look at the URL	The URL shows whether there is a secure connection or not. Can indicate whether the website is a phishing website or not. Important in the URL is that e-mail users look at the URL, which was less previously but increased over time (Alsharnouby et al., 2015).

Table 1 shows that both companies and customers can use various methods to prevent phishing from happening. There has been some discussion on the effectiveness of these preventive measures for both companies/legal institutions and customers. Whereas some measures which are taken have an effect (such as e-mail scan), there are also some measures

which require more labor-intensive work (takedowns and searching for phishing websites and providing the phishing website with junk data) and may be less effective.

As stated before, for customers it is all about creating awareness that phishing does happen in an online environment. The preventive measures which customers have are therefore all aimed at increasing awareness of the customer, which is therefore a vocal point for studies on phishing (Dodge, Carver & Ferguson, 2007; Hale, Gamble & Gamble, 2015). One of the most effective measures, as confirmed by many studies, are the anti-phishing training (Sheng et al., 2010; Arachchilage & Love, 2013) tools. Companies employ these to decrease the phishing susceptibility of their employees to prevent falling for a phishing e-mail.

Of the protective measures shown in Table 1, paying attention towards the URL and the lock symbol has increased among academic research in the past 5 years. Research shows, by using for instance eye tracking on 21 participants, an increase in the awareness of the URL (Alsharnouby et al., 2015). However, currently the awareness of the URL is still slacking and therefore the phishing susceptibility of customers is still present (Downs, Holbrook & Cranor, 2006). Research on the use of two factor authentication is increasing in related areas to phishing. Therefore it is not yet known what the effect might be, but it is reasonable to think that two factor authentication also decreases phishing susceptibility. Since it could mean that customers are more aware of phishing. Although, not all studies are convinced of the positive effect of two factor authentication (Dhamija & Tygar, 2005).

Overall these measures have received attention by researchers, but still these measures did not manage to decrease phishing to a neglect able amount for customers. Therefore, additional tools which can help reduce phishing susceptibility and the amount of e-mails get through in the inbox are useful.

2.5.2 The effectiveness of education and the hints of Veiligbankieren.nl

To reduce risk, a person must be educated to prevent a risk from happening. The same goes for phishing, education is key in reducing phishing susceptibility (Sheng et al., 2010; Arachchilage & Love, 2014: Arachchilage, Love & Beznosov, 2016; Kumaraguru, Sheng, Acquisti, Cranor & Hong, 2010). The most effective methods are therefore focused on training and providing easily understandable bullet points or tools. These are according to many studies one of the most useful methods to reduce phishing susceptibility (Sheng et al., 2010). Therefore

several educational tools have already been developed, such as anti-phishing Phil or other training methods as Phish guru. These training methods teaches users to handle phishing during the use of an e-mail system. Kumaraguru et al. (2007) studied the effectiveness of these methods in comparison to more simple methods, such as a security notice from the board of directors. Kumaraguru's study showed that the Phish guru or anti-phishing Phil training methods were more effective in reducing the phishing susceptibility (Kumaraguru et al., 2007). Other studies confirmed the importance of training or education in reducing phishing susceptibility (Hong, 2012). Though, motivating e-mail users to follow education or training is difficult, since the public thinks these type of treats are not relevant because e-mail users have full protection (Hong, 2012).

Since the hints of Veiligbankieren.nl focus on a better detection and an increased awareness through marketing campaigns, it is believed that these hints do have a positive influence in better judging e-mails from banks. This will subsequently result in a lowered phishing susceptibility because a person can better identify an e-mail from their respective bank. In line with the previous, hypothesis 1 is formulated.

Hypothesis 1: *There is a positive effect of reading the hints that Veiligbankieren presents on correctly judging e-mails from banks.*

The reason for the positive relationship is caused by the operationalization of the dependent variable phishing susceptibility which can be seen in Appendix C. The following hints which can help reduce phishing susceptibility were introduced by the Dutch initiative of Veiligbankieren.nl.

1. Check the sender: The hint indicates that one should check from whom one got the e-mail. For example, if the sender does not have @Rabobank.nl, then the sender is not legit. What the phishers usually do is put Rabobank before the @ in order try to fool a person. If looked at properly, one can easily identify whether the e-mail is legitimate.
2. The e-mail is not personally addressed towards you: The hint means that the salutation could be like dear <e-mail address before @> in the first sentence which means phishers do not know ones genuine name. The salutation could also be 'dear client' or 'dear reader' with phishing e-

mails whom have bank related topics. These un-personal salutations are used by phishers to send more e-mails at once. However, more sophisticated phishers can also personally address a person, which may seem more legit and increases phishing susceptibility.

3. Compelling character: The hint focuses on a threating character which a phishing e-mail can have but a genuine e-mail not. A common threat is that a person will lose money or must pay more after a certain timeframe. The threat is used to motivate e-mail users to pay, because a common man or woman does not want a missed opportunity or facing a situation which is not favored by them. By having a compelling character, psychological reactions happen and e-mail users will pay more often because of the compelling tone.

4. There are spelling mistakes in the e-mail: The hint means that there are spelling mistakes in the e-mail or that another element of the e-mail does not add up. Spelling mistakes is one of the easiest recognizable and most used hint to reduce phishing susceptibility because non-professional phishers usually have misspellings. However, more sophisticated phishing e-mails do not have spelling mistakes and therefore require more effort to recognize the e-mail as a phishing attempt.

5. There is a link to the login screen of the bank: There is usually a link towards the login screen of a bank at which a person is a client. A fake login screen is created by phishers to a mimic a genuine login screen to fool a person to fill in login codes through which a customer of online banking has access to one's bank account. The link towards the login screen is commonly in the e-mail, so the phishers might receive access if a person does not recognize the e-mail as a phishing e-mail.

6. Never sent your bank-card by mail: Some e-mails ask to send your bank card, because the card needs to be replaced or is broken. E-mail users will be asked to send their bank-card to a certain address because of these issues. The hint is often deployed in combination with the compelling character hint (Veiligbankieren.nl, 2017).

The hints of Veiligbankieren are the core of this study. These hints are aimed on giving customers of online banking easy understandable bullet points. The anti-phishing hints are therefore straight forward and easy to understand. By making these hints easy to understand and utilize, banks hoped for a reduction in damages incurred. However, no research has been done on the effectiveness of these easy to understand bullet points on reducing phishing susceptibility.

2.6 The influence of demographic factors on phishing susceptibility

According to the literature there are several factors which can influence phishing susceptibility. Factors such as demographic characteristics, personality and the level of technical expertise of a person about computers do have a certain influence on phishing susceptibility. Prior research focused on the influence of demographics on phishing susceptibility in order to target certain groups on which campaigns should be focused. These studies show several signs as to what they think is the influence of certain demographics on phishing susceptibility. Since these studies all present something different, the findings of these studies are summarized in Table 2. Table 2 portrays an inconclusive answer as to the influence of these two demographic variables. Therefore these demographic variables are included in the analysis (Sheng et al., 2010; Oliveira et al., 2017). The other demographic factors were either less embedded within the literature or more inconsistent in comparison to gender and age and were therefore excluded.

Table 2: A summary of studies of the effect of gender and age on phishing susceptibility.

Demographic	**The effect on phishing susceptibility**
Gender	Oliveira et al., 2017; Sheng et al., 2010; Jagatic, Johnson, Jakobsson & Menczer, 2007; Halevi, Lewis & Memon, 2013 conclude women are more susceptible to phishing in comparison to men. One study found the relationship to not be statistically significant (Kumaraguru et al., 2009).
Age	The first group (Sheng et al., 2010; Kumaraguru et al., 2009; Jagatic et al., 2007; Darwish, El Zarka & Aloul, 2012) believes that younger adults are more vulnerable towards phishing susceptibility. The second group believes that older adults are more vulnerable towards phishing susceptibility (Oliveira et al., 2017).

2.6.1 Gender

Several studies show that females are more susceptible to phishing in comparison to men (Sheng et al., 2010; Oliveira et al., 2017). An example of a study which confirms the higher

susceptibility towards phishing, is the study of Sheng et al. (2010). Sheng's study confirmed the positive influence of the variable gender on phishing susceptibility. However, other factors were mediating the relationship, namely the technical training and knowledge. Meaning females perform on average worse due to inferior knowledge on technical related subjects. However, after training the positive relationship disappeared (Sheng et al, 2010). Other studies found a similar relationship (Oliveira et al., 2017; Jagatic et al., 2007). However, not all studies showed a similar sign towards a difference in gender. A study by Kumaraguru et al. (2009) found no significant difference between males and females.

Altogether, most studies agree on the effect between gender and phishing susceptibility. This effect is that females are more susceptible to phishing and therefore judge the e-mails worse. Therefore hypothesis 2 is formulated as follows:

Hypothesis 2: *There is a negative effect between gender and correctly judging e-mails from banks.*

2.6.2 Age

The second most studied demographic variable was the age of the participant. Overall, age caused more debate on which groups were more vulnerable to phishing. There are two main groups of studies which are divided on the discussion of the influence of age. The first group, which has the most followers, found that young adults were most vulnerable towards phishing (Darwish et al., 2012). Simultaneously, the older a person becomes, the better it is in judging phishing e-mails (Sheng et al., 2010; Kumaraguru et al., 2009; Jagatic et al., 2007). For example, Sheng et al. (2010) concluded that "younger people have a lower level of education, fewer years of experience with the internet, less exposure to training material and aversion to financial risks, they tend to be more susceptible to phishing" (Sheng et al. 2010, p. 380). However, several of these studies have minor issues regarding the operationalization of age. Therefore issues in these studies could explain why not every study agrees on the same relationship between age and phishing susceptibility.

The second group of studies found an opposite relationship in comparison to the first group. Namely, that the older age group is more vulnerable towards phishing. Oliveira et al. (2017) found that older individuals, as opposed of Sheng et al. (2010), are more prone to phishing. The advantage which the study of Oliveira et al. (2017) has on the study of Sheng et al.

(2010) is that Oliveira et al. (2017) includes all the age groups until 65+. Including more age groups provides a more complete overview of the influence of age. Therefore the suggested relationship by Oliveira et al. (2017) is assumed. Since the older age group is assumed to be more susceptible for phishing, it can be reasoned that the older age group has a worse judgement of bank related e-mails. Therefore hypothesis 3 is formulated as follows:

Hypothesis 3: *There is a negative effect between age and correctly judging e-mails from banks.*

3. Methods

3.1 Participants

27 participants were included in this study, which is more than other studies which use eye tracking (Alsharnouby et al, 2015; Arianezhad, Camp, Kelley & Stebila, 2013; Whalen & Inkpen, 2005). A restriction of no connection towards the participant was applied in order to avoid issues regarding bias and to increase the reliability, validity and generalizability of this study. The sample consisted of individuals who were born and raised in the Netherlands (and are Dutch speaking) and use online banking active. Dutch customers of online banking were chosen because Dutch banks introduced the hints of Veiligbankieren.nl for their Dutch customers and advertised these hints in the Netherlands. Therefore including only Dutch participants was most sensible because the campaigns focused on these specific customers. An important aspect of the sample was that the sample should not be solely focused towards one group (for instance students) because this could had decreased generalizability. The participants of the experiment were approached through different channels of communication. These channels of communication were either through approaching possible participants in the university (younger age groups) or through the network of the researcher (usually middle and older age groups).

After the initial data collection, no participants were excluded from the study. However, one participant had a gaze quality of only 51% which made the analysis more time-consuming. The sample consisted of 18 males and 9 females. The participant's age ranged from 18 to 65. The mode age category ranged from 26 to 40.

3.2 Study design

3.2.1 The setting of the study

A combination of two methods were used in this study. A survey was used to gather data to test the effectiveness of the hints on reducing phishing susceptibility and to ask additional related questions. In addition, the survey was also used to guide the experiment and to minimize the time spent doing the experiment and to make the output as reliable as possible. The survey was divided into three parts. The first part asked questions related to general demographic information. The second part consisted of the judgement of the bank e-mails by the participants with the eye tracking glasses on. Before the eye tracking glasses were put on, the participants

were divided into two groups. The participants were appointed to the experimental or control group by putting the uneven participant's number (in chronological order of participation) in the control group and the even participant's number in the experimental group. The experimental group read the hints of Veiligbankieren, whereas the control group not read the hints. Each group had different but overall reasonable similar demographic characteristics and no contact with each other in any form. Hereafter the subjects had to put on the eye tracking glasses and the recording of the eye tracking glasses started. The task which the participants received was the following: determine whether 10 e-mails are phishing e-mails or genuine bank e-mails. The phishing e-mails were retrieved from the Fraudehelpdesk.nl (Fraudehelpdesk, N.D.) and the genuine e-mails from the researcher or other persons. The participant had to indicate whether it would answer the call to action. Five of these e-mails were phishing e-mails and five were actual bank e-mails from a Dutch bank (all these e-mails were in Dutch). Finally, the third part of the survey asked additional questions related to the experiment and other subjects.

Eye tracking was used as a second method during the second part of the study to measure active use of the hints of Veiligbankieren.nl. Asking a representative question on how active a person used a hint in each e-mail was not the most accurate method because a person could had misinterpreted itself. Eye tracking was determined to be a valid measurement instrument because it had already seen its use in several fields of studies such as marketing (Plassmann, Venkatraman, Huettel & Yoon, 2015). There are also a limited amount of studies which criticize eye tracking, which makes eye tracking a proper measurement instrument. Therefore eye tracking has already seen its application in studies regarding phishing and phishing susceptibility (Alsharnouby et al., 2015). Five out of the six hints were measured using the eye tracking glasses Tobii Pro glasses 2 (Tobii, Stockholm, Sweden) of the BMSLab at the University of Twente.

3.2.2 Measurement of the variables

The dependent variable used in all statistical tests was phishing susceptibility and was measured in accordance with Sheng et al. (2010) as the amount of correctly judged bank e-mails (excluding false positives). In a genuine bank e-mail a participant had to answer the 'call to action' question with 'yes' to correctly identify the e-mail and 'no' resulted in a false positive. Phishing e-mails had the opposite of the previous, namely a 'yes' was incorrect and 'no' was correct. Each e-mail had a dummy variable attached to it in which 1 indicated a correct

identification and 0 a wrong identification. The amount of correctly e-mails was summed up into one number which portrayed the total amount of correct answers. A reliability analysis was conducted after the initial data collection in order to analyze whether it was justifiable to sum the amount of correctly judged bank e-mails for each participant. The results presented a very low Cronbach alpha, which indicated summing the e-mails into one value was not justifiable. Additional reliability analysis showed that exclusion of certain e-mails led to a higher Cronbach alpha. However, the Cronbach alpha never reached an appropriate level of at least 0.6. The highest value of Cronbach alpha was reached with three e-mails, namely the genuine e-mail 1 & 2 and phishing e-mail 4 (0.482). In this scenario, seven e-mails would be left out of the further analysis. A likely cause for this value was the relatively small sample (N=27), because the minimum sample size should at least be over 300 (Charter, 2003). However, because leaving out seven e-mails out of 10 would be too rigorous, the choice was made to include all e-mails in the further tests. In addition to this, a factor analysis was conducted to explore whether the value of any e-mail was too influencing and therefore could be excluded. Results of this factor analysis, using a Direct Oblimin rotation, showed that indeed the second phishing e-mail was extracted as a component. Therefore this e-mail was influential. However, the other two components were also strong and contained both two e-mails (also higher Eigenvalues). Therefore the choice was made to not exclude any e-mail in the further analysis.

The independent variables used in the various analysis were measured as follows. At first, a dummy variable was used to differentiate between a person being in the experimental or control group (1 = experimental, 0 = control). Gender was measured as a dummy variable (1 = female, 0 = male), age was measured in five categories (18-25, 26-40, 41-55, 55-65 and 65+), education on a 7 scale (primary school, secondary school, intermediate vocational education, associate degree, bachelor degree, master's degree and doctorate), employment on a 3 scale (No, part time and full time) and relationship status on a 1 to 4 scale (single, LAT, relationship and living together and married and living apart or together). The third part of the survey consisted of several questions regarding the performed task or related subjects. These questions were mostly measured using a 7 (strongly agree to strongly disagree) point Likert scale, which had three different variations[1]. There were four questions which had a 5 point Likert scale, which had two

[1] 1. Scale was: strongly agree, agree, somewhat agree, neither agree nor disagree, somewhat disagree, disagree and strongly disagree. These were questions which used this scale: the amount of times a participant was

variations[2]. There were two exceptions, one question regarding the amount of times a participant encountered phishing used an interval variable (1-5, 6-10, 11-15, 16-20, >20) and the other was whether a participant would delete phishing e-mails quickly (measured as: I delete the e-mail straight away, I quickly scan it and delete the e-mail and I intensively read the e-mail but delete it).

By the use of the eye tracking glasses equipment, the precise movement of the pupils could be measured and it could be seen whether these hints were actively used by the analysis of the recordings of the judgement of the bank e-mails. Five out of the six hints were measured for active use by using the eye tracking glasses Tobii Pro glasses 2 of the BMSLab at the University of Twente. The active use of each hint of Veiligbankieren.nl was checked as follows for each e-mail:'

1. Checking the sender: The hint was analyzed by making a heat map of the part of the recordings which specifically focused on the sender in an e-mail.
2. Non personal salutation: The hint was analyzed by making a heat map which showed whether a participant was or was not checking the salutation.
3. Compelling character in an e-mail: Several parts of the phishing e-mails contained compelling character parts. It was checked whether there was a clearer focus on the part with compelling character or not in the heat maps.
4. Spelling mistakes in an e-mail: There were several mistakes in the phishing e-mails which were checked whether these were looked at for a longer period of time by using heat maps.

confronted with phishing e-mails, a participants' self-determined experience in detecting phishing e-mails, knowing what phishing is and their methods, whether a participant thought phishing was a prominent issue and whether a participant knew the hints of Veiligbankieren.nl.

2. Scale was: Extremely likely, moderately likely, slightly likely, neither likely nor unlikely, slightly unlikely, moderately unlikely, extremely unlikely. These were questions which used this scale: whether a participant thought phishing a prominent issue and whether a participant thought it was prone for misjudging phishing e-mails.

3. Scale was: Extremely easy, moderately easy, slightly easy, neither easy nor difficult, slightly difficult, moderately difficult, extremely difficult.

[2] 1. Scale was: a great deal, a lot, a moderate amount, a little or none at all. These were questions which used this scale: the years of experience a participant had in computer related areas and whether a participant followed previous education.

2. Scale was: Definitely yes, probably yes, might or might not, probably not and definitely not. These were questions which used this scale: whether a participant thought that an increase in awareness of the hints of Veiligbankieren.nl would reduce phishing even more and whether a participant would recommend everyone to read these hints to decrease phishing susceptibility even more.

5. A link towards the login screen: Each phishing e-mail was checked whether the link of the phishing e-mail was checked by the participant.

3.3 Analysis of the data

In order to answer the first research question regarding the influence of these hints of Veiligbankieren.nl on reducing phishing susceptibility, a Mann-Whitney U-test was used due to a non-normal distribution of the dependent variable across groups (tested by using a Shapiro-Wilk test). The dependent variable in the Mann-Whitney U-test was phishing susceptibility. The grouping variable was based upon the division of the participants between the experimental and the control group. The Mann-Whitney U-test was performed by using SPSS (Version 24.0, IBM Corporation, Armonk, New York, United States).

The data provided by the eye tracking glasses of Tobii Pro 2 was analyzed by using the analyzing program provided by Tobii. The output which the glasses of Tobii Pro 2 created was at first a video of the test person's view from their eyes. Afterwards, the eye tracking data was analyzed by making gaze plots or heat maps. From these heat maps it was determined whether a person used a hint actively. This data was processed in a word-document and further analyzed using ATLAS (version 8.1, Atlas.ti, Berlin, Germany), which presented the active use of each hint in a count. This was used to calculate the percentage of active use by dividing the amount of e-mails in which a hint was used by the total amount of e-mails in which a hint could be used. The threshold for active use was set at minimal 50%.

However, not every e-mail had the possibility of utilizing each hint because not every genuine bank e-mail contained all features of the hints of Veiligbankieren.nl. Therefore the analysis not always consisted of the 10 e-mails. The first hint (checking the sender) could be checked for active use in every e-mail (a N of 10*27 = 270), the second hint (un-personal salutation) could be used in 7 e-mails (a N of 7*27 = 189), the third hint (compelling character) could only be used in the 5 phishing e-mails (a N of 5*27 = 135), the fourth (spelling mistakes) and fifth hint (link towards the login screen of a bank) had the same amount of e-mails as the third hint. Therefore the analysis of the active use of these hints are based upon the amount of times a hint has been actively used in order to determine a legitimacy of an e-mail

The questions in the first and last part of the survey were analyzed by using a combination of Mann-Whitney U-tests and independent sample t-tests (by using SPSS). This was

dependent on whether there was a normal distribution across groups or not, which was tested by using the Shapiro-Wilk test. The dependent variable was always phishing susceptibility as described before. Each question which was asked in the survey was independently tested by using the variable as the grouping variable in either one of the two tests. The two demographic factors gender and age (and the related hypothesis 2 & 3) received the same treatment. Gender was the grouping variable in the first test, which measured the difference between females and males. For the variable age, the first and the second category were pooled to be the younger age group (18-40) and the older age group was pooled by the other three categories (41-65+). An additional remark for all the performed tests: all the tests have had their coefficient calculated for one tail because this study solely focused on the positive effect of the variables discussed above.

4. Results

4.1 Descriptive statistics

Table 3 Panel A shows the general demographic factors of the whole sample. Table 3 Panel A shows that the most important aspect of the sample of this study (to gain a more broaden view of the population) is fulfilled. The distribution of gender is not solely pointed towards one group. Age shows a similar sign in comparison to gender. In comparison to similar studies, this study not solely uses students (who fall in the age category 18-25) in the sample but has a broader spectrum of the population. The other demographic factors also show that there is no solely commanding part of one certain demographic factor.

Table 3 Panel B shows the general demographic information for both the experimental group and the control group. In total, of these 27 participants, 13 were placed in the experimental group and 14 were placed in the control group. The division of the participants between the experimental and the control group depicts a less diversified group for gender and education. The experimental group contained a higher ratio of males. Education depicts a same view, namely that the experimental group contains more higher educated participants and the control group lower educated participants. The other demographic factors such as age and employment show more diversification and are hence no issue. Still, overall the picture remains positive in comparison to other studies who focus on a particular group of participants. Therefore it can be concluded that there is a diversified sample.

Table 3: Demographic information of the whole sample and both the experimental and the control group. The numbers display the amount of participants which fall into that category.

Table 3 Panel A

Characteristic	
Participants	27
Gender	
Male	18
Female	9
Age	
18-25	14
26-40	5
41-55	2
56-65	6
65+	0
Education	
Primary school	0
Secondary school	1
Intermediate vocational education	9
Associate degree	2
Bachelor degree	9
Master's degree	6
Doctorate	0
Employment	
Unemployed	9
Part-time	13
Full-time	4
Missing	1
Relationship status	
Single	9
LAT	4
Relationship and living together	8
Married and living together or apart	6

Table 3 Panel B

Characteristic	Experimental group	Control group
Participants	13	14
Gender		
Male	10	8
Female	3	6
Age		
18-25	8	6
26-40	4	1
41-55	0	2
56-65	1	5
65+	0	0
Education		
Primary school	0	0
Secondary school	0	1
Intermediate vocational education	2	7
Associate degree	0	2
Bachelor degree	7	2
Master's degree	4	2
Doctorate	0	0
Employment		
Unemployed	5	4
Part-time	4	9
Full-time	3	1
Missing	1	0
Relationship status		
Single	4	5
LAT	1	3
Relationship and living together	7	1
Married and living together or apart	1	5

Table 4 Panel B shows the amount each individual e-mail has been answered correctly and incorrectly. Panel B shows a clear overall pattern for the whole sample, namely that phishing e-mails are more correctly evaluated in comparison to bank e-mails. Therefore the participants more often identified a genuine e-mail of a bank as a phishing e-mail (a false positive). Still the participants are better at determining legitimacy of genuine bank e-mails (86.7% correctly evaluated) in comparison to the participants in the study by Sheng et al. (2010). Therefore the population might became on average, assuming similar results in other countries, better at evaluating these type of e-mails. Similar to the previous, results from Sheng et al. (2010) displayed on average 72 % of the phishing e-mails were correctly identified after training. Therefore, based on the percentage of Sheng et al. (2010), the participants of this study were better in judging legitimacy of these type of e-mails (80.0% correctly evaluated).

Both results of these type of e-mails of this study are in sync with the results of the study of Sheng et al. (2010). Both studies show that phishing e-mails are on average better evaluated in comparison to genuine bank e-mails. Based on the observations during the experiment, the participants thought judging of phishing e-mails was often more difficult to assess phishing e-mails as so in comparison to genuine bank e-mails. However, based on the results in Panel B, the participants performed better on identifying phishing e-mails.

Other additional results show that in particular the second phishing e-mail was most difficult to identify. Other phishing e-mails were, in comparison to the second phishing e-mail, easier to identify which can be seen by the small numbers which identified the other phishing e-mails wrong. Within the bank e-mails the first and the third were most difficult to identify as a genuine bank e-mail.

Table 4: Panel A depicts summary statistics of the amount of correctly judged bank e-mails (out of 10). Panel B depicts the amount of correctly and incorrectly evaluated e-mails (N = 27) shown for each of the phishing and genuine bank e-mails with the percentage correctly evaluated of the whole sample.

Table 4 Panel A

	$\bar{X}$	Std.	Median	Min.	Max.	Number
The average amount of bank e-mails correctly judged	8.33	1.068	8	6	10	225

Table 4 Panel B			
Type of e-mail	Correctly evaluated	Wrongly evaluated	Percentage correctly evaluated
Phishing e-mail 1	25	2	92.6%
Phishing e-mail 2	13	14	48.2%
Phishing e-mail 3	27	0	100%
Phishing e-mail 4	26	1	96.3%
Phishing e-mail 5	26	1	96.3%
Genuine e-mail 1	19	8	70.4%
Genuine e-mail 2	23	4	85.2%
Genuine e-mail 3	19	8	70.4%
Genuine e-mail 4	24	3	88.9%
Genuine e-mail 5	22	5	85.2%
Totals (N =270)	224	46	

4.2 The effect of the hints of Veiligbankieren.nl on correctly evaluating bank e-mails

To test whether there was a significant difference between the two groups within the sample, a Mann-Whitney U-test was used. The dependent variable was phishing susceptibility and was measured as described in chapter 3.3.2. The grouping variable was whether the participant was included in the experimental group or the control group. The results are displayed in Table 5.

Table 5 shows the mean rank for both the experimental and the control group. The experimental group, which read the hints, had an overall better judgement of the e-mails compared to the control group, namely a mean rank of 16.73 versus a mean rank of 11.46, respectively. Therefore it seems that reading of the hints increases the likelihood of evaluating an e-mail correctly.

Table 5: The mean rank statistics of the amount of correctly judged bank e-mails across groups and the test statistics of an equal mean rank of the amount of correctly judged bank e-mails between the control and the experimental group.

Table 5

	Mean rank statistics across groups				1 tailed Z-test for equality of mean ranks		
	Experimental or control group	$\overline{X}$ rank	Sum of ranks	N	Mann-Whitney U	Z	P-value
The amount of correctly judged bank e-mails	Control	11.46	160.50	14	55.50	1.799	0.036**
	Experimental	16.73	217.50	13			

*Note. * P < α = 0.10, one-tailed; ** P < α = 0.05, one-tailed and *** P < α = 0.01, one-tailed.*

Table 5 also shows the outcome of the test statistics between the experimental and the control group. Table 5 presents a coefficient of 0.036 (z-statistic = 1.799) and is therefore significant. Therefore a positive effect exists between reading the hints of Veiligbankieren.nl and the amount of correctly judged bank e-mails, which decreases phishing susceptibility. Consequently hypothesis 1 will be accepted. The results underline the study of Sheng et al. (2010), who also found a positive effect of educational tools on reducing phishing susceptibility through a better judgement of e-mails.

4.3 The effect of gender, age and relationship status on correctly evaluating bank e-mails

The second and third hypothesis were related to age and gender. Table 6 shows the results of the whole sample and the experimental group for gender. The mean rank for the whole sample does not differ greatly across the two groups. Consequently, Table 6 portrays a non-significant coefficient of 0.468 (z-statistic = 0.080). Therefore there is no difference between the mean ranks of both males and females in correctly judging e-mails from banks. Additional tests were run with the experimental and the control group (using an Independent sample t-test) in order to see whether there were any differences in the groups which took part in the experiment. The experimental group showed a greater different mean rank for gender. Still, Table 6 displayed a non-significant coefficient of 0.178 (z-statistic = 0.923). In accordance with the experimental group, the control group also did not show any significance 0.323 (t-statistic = 0.472) according

to Table 7. Therefore, there is no indication that gender does have an effect on correctly judging e-mails from banks. Therefore hypothesis 2 is rejected.

Table 6: The mean rank statistics of the amount of correctly judged bank e-mails across gender and the test statistics of an equal mean rank of the amount of correctly judged bank e-mails between males and females.

Table 6

	Mean rank statistics across groups				1 tailed Z-test for equality of mean ranks		
	Gender	$\bar{X}$ rank	Sum of ranks	N	Mann-Whitney U	Z	P-value
The amount of correctly judged bank e-mails (whole sample)	Male	13.89	250.00	14	79.00	0.080	0.468
	Female	14.22	128.00	13			
The amount of correctly judged bank e-mails (experimental group)	Male	6.25	62.50	10	7.50	0.923	0.178
	Female	9.50	28.50	3			

*Note. * P < α = 0.10, one-tailed; ** P < α = 0.05, one-tailed and *** P < α = 0.01, one-tailed.*

Table 7: The mean statistics of the amount of correctly judged bank e-mails across gender and the test statistics of an equal mean of the amount of correctly judged bank e-mails between males and females.

Table 7

	Mean statistics across groups			Levene's test for equality of variances		T-test for equality of means		
	Gender	$\bar{X}$	Std.	F	Sig.	T	Sig (1-tailed)	N
The amount of correctly judged bank e-mails (control group) – equal variances assumed	Male	7.83	1.329	0.232	0.639	0.472	0.323	6
	Female	8.13	0.991					8
Equal variances not assumed						0.452	0.331	

*Note. * P < α = 0.10, one-tailed; ** P < α = 0.05, one-tailed and *** P < α = 0.01, one-tailed.*

The third hypothesis was related to the influence of age on phishing susceptibility. The results of the tests can be seen in Table 8 and 9. Table 8 depicts the results for the whole sample and the experimental group. At first, the rank statistics of the whole sample show similar mean

ranks, with the younger age group having a greater sum of ranks because of the higher N. Subsequently Table 8 depicts a non-significant coefficient of 0.428 (z-statistic = 0.182). Therefore there is no difference in correctly judging bank e-mails across the younger and older age group in the whole sample.

Table 8: The mean rank statistics of the amount of correctly judged bank e-mails across the age groups and the test statistics of an equal mean rank of the amount of correctly judged bank e-mails between the older and younger age groups.

Table 8

	Mean ranks statistics across groups				1 tailed Z-test for equality of mean ranks		
	Age	$\overline{X}$ rank	Sum of ranks	N	Mann-Whitney U	Z	P-value
The amount of correctly judged bank e-mails (whole sample)	Older age groups	14.31	114.50	8	73.50	0.182	0.428
	Young age groups	13.87	263.50	19			
The amount of correctly judged bank e-mails (experimental group)	Older age groups	12.50	12.50	1	0.50	1.020	0.154
	Young age groups	6.54	78.50	12			

*Note. * $P < \alpha = 0.10$, one-tailed; ** $P < \alpha = 0.05$, one-tailed and *** $P < \alpha = 0.01$, one-tailed.*

Additional analysis were performed to check whether the experimental or control group portrayed a different sign. Test results of the experimental group can be seen in Table 8 as well. In this instance, interpreting the non-significant coefficient of 0.154 (z-statistic = 1.020) from this test is not valid and reliable because of this small N (N=1) in the older age group for the experimental group. Thus, no conclusions can be made about the experimental group. The results of the independent sample t-test for the control group can be seen in Table 9. Table 9 depicts a small difference between the means of both groups, in favor of the younger age group. Hence, the control group depicts a non-significant coefficient of 0.323 (t-statistic = 0.467). Thus, the experiment and the control group portray a same image as the whole sample. Therefore

hypothesis 3 is rejected. Consequently there is no significant difference between different age groups in terms of correctly judging bank related e-mails.

Table 9: The mean statistics of the amount of correctly judged bank e-mails across the age groups and the test statistics of an equal mean of the amount of correctly judged bank e-mails between the older and younger age groups.

Table 9

	Mean statistics across groups			Levene's test for equality of variances		T-test for equality of means		
	Age	$\overline{X}$	Std.	F	Sig.	T	Sig (1-tailed)	N
The amount of correctly judged bank e-mails – equal variances assumed	Older age groups	8.14	1.464	2.229	0.161	0.467	0.323	7
	Younger age groups	7.86	0.690					7
Equal variances not assumed						0.467	0.326	

*Note. * $P < \alpha = 0.10$, one-tailed; ** $P < \alpha = 0.05$, one-tailed and *** $P < \alpha = 0.01$, one-tailed.*

Additional analysis of the data portrayed that a participant's relational status had an effect on the amount of bank e-mails which are correctly judged. Table 10 displays the results of this test in which the dependent variable was the phishing susceptibility. The grouping variable was a dummy variable: a 0 indicated being in a relationship and a 1 indicated being single. At first, Table 10 displays a higher mean rank for being in relationship across all three tests. Consequently, the whole sample displays a significant coefficient of 0.023 (z-statistic = 2.000). Therefore there is a significant difference in the mean ranks between being single or being in a relationship, in favor of the group in a relationship. Consequently being in a relationship has a positive effect on correctly judging bank e-mails.

Table 10 also shows additional analysis of the experimental group and the control group, with the goal to study which group being in a relationship mattered the most. The results of these additional tests depict that especially being in a relationship matters most in the experimental group due to the significant coefficient of 0.076 (t-statistic = 1.433) at an alpha of 0.1. Therefore the focus should be on single persons after the hints of Veiligbankieren.nl had a more intensive

marketing campaign. The opposite holds as well. Focusing the marketing campaign on either of these groups beforehand does not have a significantly higher positive effect in comparison to the other group because of the insignificant value of the control group.

Table 10: The mean rank statistics of the amount of correctly judged bank e-mails across the relationship status and the test statistics of an equal mean rank of the amount of correctly judged bank e-mails between being in a relationship and single.

Table 10

	Mean rank statistics across groups				1 tailed Z-test for equality of mean ranks		
	Relationship status	$\overline{X}$ rank	Sum of ranks	N	Mann-Whitney U	Z	P-value
The amount of correctly judged bank e-mails (whole sample)	In a relationship	16.11	290.00	18	56.00	2.000	0.023**
	Single	9.78	88.00	9			
The amount of correctly judged bank e-mails (experimental group)	In a relationship	8.00	72.00	9	9.00	1.433	0.076*
	Single	4.75	19.00	4			
The amount of correctly judged bank e-mails (control group)	In a relationship	8.33	75.00	9	15.00	0.890	0.187
	Single	6.00	30.00	5			

*Note. * $P < \alpha = 0.10$, one-tailed; ** $P < \alpha = 0.05$, one-tailed and *** $P < \alpha = 0.01$, one-tailed.*

4.4 The active use of the hints of Veiligbankieren.nl

The second part of the analysis focused on the active use of the hints of Veiligbankieren.nl by making use of the eye tracking glasses of Tobii. The results of each hint for the experimental and the control group will follow in chronological order. Table 11 Panel B shows the percentage amount of times a hint has been used in the total amount of e-mails analyzed for each hint. Overall, the hint of checking the sender, salutation, compelling character and a link towards a login screen were most actively used by the sample. The active use of the first two hints indicate that the participants paid attention towards the beginning of the e-mail. The active use of the compelling character indicated that the participants also paid attention towards the tone of the bank e-mail while reading, which is in the middle part of a bank e-mail.

The hint of a link towards a login screen was also actively used, which was usually near the end. Therefore, the participants showed on average that the beginning of the e-mail, the body with a compelling character and a link towards a login screen were the most important areas to determine legitimacy of bank e-mails.

Table 11: The active usage of the hints in percentages according to the eye tracking analysis is depicted in Panel A and Panel B displays the active usage for each hint across the experimental and the control group.

Table 11 Panel A

	$\bar{X}$	Std.	Median	Min.	Max.	N
Use in % of the whole sample	53.80	14.823	61.5	29	70	n.a.
Use in % of the experimental group	53.80	12.28	61	39	65	n.a.
Use in % of the control group	53.80	18.54	64	29	70	n.a.

Table 11 Panel B

	% actively used (experimental group)	% actively used (control group)	Average % actively used	N
Sender***	61	39	50	270
Salutation	65	70	67.5	189
Compelling character***	42	67	54.5	135
Spelling mistakes	39	29	34.5	135
A link towards the login screen	62	64	63	135

*Note. Chi Square * $P < \alpha = 0.10$, two-tailed; ** $P < \alpha = 0.05$, two-tailed and *** $P < \alpha = 0.01$, two tailed.*

Table 11 Panel B shows that the hint about checking the sender of a bank e-mail was used moderately to determine legitimacy of bank e-mails, though differences exist between the experimental and the control group. The experimental group showed a higher active use of 61% in all the e-mails applicable in comparison to the control group which showed an active use of 39% in all the e-mails applicable for this hint. Therefore reading the hints of Veiligbankieren.nl showed a positive tendency on actively using the hint about checking the sender. This indicates that a marketing campaign could have a significant effect in further increasing the use of this hint. However, the results also portrayed that there is room for improvement in order to reduce phishing further because the hint is still not used in all the e-mails in both groups.

Panel B shows that the hint about an un-personal salutation is used the most of all the hints included in the experiment. There is a small difference between the experimental and the control group in the active use of this hint, namely an active use of 65% (experimental group) and 70% (control group) in all e-mails applicable. Therefore no positive tendency exists in using the hint to determine legitimacy of bank e-mails when reading this hint beforehand. Concretely, this means that there could be improvement within the use of checking the un-personal salutation. Therefore, pinpointing that one should look at the salutation (and check whether the salutation is personal or not) of a bank e-mail can be stressed even further because currently the hint is not used in every e-mail in this experimental setup.

Panel B shows that the hint about a possible compelling character in an e-mail was used moderately by the participants to determine legitimacy of bank e-mails. Although differences exist between the experimental (42%) and the control group (67%), which is contrary to what one would believe happens when one read the hints of Veiligbankieren.nl (namely an increase in active use to determine legitimacy). Therefore a negative tendency exists in the active use of the hint about a compelling character when the hints of Veiligbankieren.nl are read during the experiment. This indicates that this hint creates more confusion for a customer of online banking after reading the hints of Veiligbankieren.nl. Therefore additional explanation could be necessary. Overall, the hint about a possible compelling character is still not used in all e-mails. Thus the importance of checking for a compelling character could be stressed even further.

Panel B shows that the hint about possible spelling mistakes in an e-mail is used the least of all hints in order to determine legitimacy of bank e-mails. Therefore the participants in this experiment do not pay a great deal of attention towards the spelling in bank e-mails. Thus there is room for improvement in the active use of checking the spelling. Though, there is a positive tendency in active use of this hint by the experimental (39%) and the control group (29%). Thus if the importance of spelling mistakes in a bank e-mail is stressed in an marketing campaign, the active use could also increase significantly because of the positive tendency in active use in this experimental setup.

Panel B displays that the hint about checking for a link towards the login screen of a bank was moderately used to determine legitimacy of bank e-mails. Therefore checking for a link towards the login screen is an important aspect in determining legitimacy of bank e-mails. The moderate use showed little difference between the experimental (62%) and the control group

(64%). Therefore there is no negative or positive tendency in the active use of this hint. The results indicates that there the importance of this hint can be stressed even further because the hint is not utilized in all e-mails.

Overall the hints of Veiligbankieren.nl display differences in active use between the experimental and the control group. The hints of checking the sender and the spelling mistakes showed a positive tendency in active use, the un-personal salutation and a link towards a login screen of a bank showed little difference in active use and the compelling character a negative tendency in active use in the experimental setup. Therefore the decrease in phishing susceptibility which was found in chapter 4.2 is caused by the positive tendency in the active use of checking the sender and checking for spelling mistakes in the bank e-mails. The hint about the compelling character showed a negative influence. Therefore additional explanation of this hint is required. The other two hints showed little difference and therefore require only a more extensive marketing campaign to increase the active use. This statement also yields for all the other hints because the hints are on average only used in 53.5% of (Panel A) all e-mails.

4.5 The effect of overconfidence on correctly judging bank e-mails

The last part of the experiment consisted of several questions regarding the experiment and other related factors. A combination of methods were used to analyze whether there was a difference between several groups present in the questions of the survey, which was dependent on a normal distribution across groups. All but one variable displayed no statistical significance. The variable which showed a statistical difference in the mean was related to the estimated difficulty of judging the correctness of the e-mails by the participants, which was consequently the grouping variable. The dependent variable was the amount of correctly judged bank e-mails. The results can be seen in Table 12.

Table 12 shows a clear difference in the overall sample. The participants whom thought that judging these bank e-mails were more difficult, have an overall better judgement of the bank e-mails according to the mean ranks. Subsequently, Table 12 displayed a significant coefficient of 0.066 (z-statistic = 1.511) for the whole sample at an alpha of 0.10 between the two groups. Therefore the results indicates that there could be a factor of overconfidence playing a role in the judgement of these e-mails. Thus, additional tests were executed to check whether the

overconfidence also plays a role in the experimental or control group. The results are shown in Table 12.

Table 12: The mean rank statistics of the amount of correctly judged bank e-mails across the estimated difficulty level and the test statistics of an equal mean rank of the amount of correctly judged bank e-mails between difficult and easy (with neutral).

Table 12

	Mean rank statistics across groups				1 tailed Z-test for equality of mean ranks		
	Estimated difficulty level	$\bar{X}$ rank	Sum of ranks	N	Mann-Whitney U	Z	P-value
The amount of correctly judged bank e-mails (whole sample)	Difficult	16.90	169.00	10	56.00	1.511	0.066*
	Easy (with neutral)	12.29	209.00	17			
The amount of correctly judged bank e-mails (experimental group)	Difficult	10.25	41.00	4	5.00	1.900	0.029**
	Easy (with neutral)	5.56	50.00	9			
The amount of correctly judged bank e-mails (control group)	Difficult	8.42	50.50	6	18.50	0.678	0.249
	Easy (with neutral)	6.81	54.50	8			

*Note. * $P < \alpha = 0.10$, one-tailed; ** $P < \alpha = 0.05$, one-tailed and *** $P < \alpha = 0.01$, one-tailed.*

Table 12 displays a similar pattern for the experimental group in comparison to the whole sample. For both groups, the more difficult a participant thought judging the e-mails was, the higher their mean ranks was. Subsequently, Table 12 displays a significant coefficient of 0.029 (z-statistic = 1.900) for a difference in mean ranks between the two groups in the experimental group. However, the control group does not show a significant coefficient (P= 0.249 = z-statistic = 0.678 > α = 0.05). Therefore overconfidence is mainly present with the experimental group, which had read the hints beforehand. Therefore the hints of Veiligbankieren.nl do increase the overall confidence of correctly judging bank e-mails, while the overconfidence is unjustified due to a decrease in the amount of correctly judged bank e-mails.

5. Discussion

The goal of the study was to discover whether the hints of Veiligbankieren.nl reduced the phishing susceptibility and were actively used in determining legitimacy of bank related e-mails. By using a combination of a survey and eye tracking, a positive effect of the hints of Veiligbankieren.nl on reducing phishing susceptibility was found. Moreover, this study showed that especially the increased positive use of checking the sender and the spelling was the cause of this positive effect.

Results showed that there was a statistically significant difference in the mean ranks of the amount of correctly judged bank e-mails between the experimental and the control group. Thus implying that hints, such as those of Veiligbankieren.nl, are effective in having a better judgement of the origin of a bank e-mail. This result conforms to the study of Sheng et al. (2010) and Arachchilage & Love (2013) whom also saw an improvement in the correct judgement of e-mails after a form of education or training.

An explanation for the positive effect of the hints of Veiligbankieren.nl could be the increased awareness of the prominent issue of phishing. When these hints were addressed to the participants, the issue of phishing sparked a thought in the participants that attention needed to be paid towards several important aspects which an e-mail can hold in revealing genuine and fraudulent e-mails. This subsequently increased the awareness of phishing by providing possible signs which could reveal the true identity of an e-mail.

However, the challenge lies in increasing (and maintaining) the awareness by addressing these hints to the public. Since the results also presents that the participants which were more confident of their judgement or their skills in correctly judging bank e-mails, performed worse in correctly identifying the selected bank e-mails. This overconfidence implies that not everyone has the same level of skill as perceived by themselves. Therefore the hints of Veiligbankieren.nl can be of guidance in order to increase their skill of correctly identifying e-mails from banks and reduce phishing susceptibility. As the study by Jansen & Leukfeldt (2016) also exaggerated is that increasing the awareness of these ‘fraudulent schemes’ (which follow after clicking on the link in an e-mail) “are critical in keeping online banking safe and secure” (Jansen & Leukfeldt, 2016, p. 79).

The hints of Veiligbankieren.nl can provide a front-end prevention before the public enters these ‘fraudulent schemes’. The second factor which Jansen & Leukfeldt (2016) also

identified as a key aspect in safekeeping a proper security was guiding the public “in how to apply protective measures” (Jansen & Leukfeldt, 2016, p. 79). The hints of Veiligbankieren.nl can also aid in the aspect of applying protective measures because these hints are relatively easy to utilize in identifying genuine bank e-mails and can therefore be used more easily. Therefore these hints can become key in keeping the online banking environment safe and secure. As these hints of Veiligbankieren.nl showed to be effective, a marketing campaign could effect in a safer online banking environment and eventually in a reduced phishing susceptibility and damages for banks.

The second part of this study focused on whether participants actively used the hints of Veiligbankieren.nl in determining legitimateness of the e-mails selected. Overall, not every hint of Veiligbankieren.nl showed a similar pattern in using these hints to determine legitimacy of bank e-mails. Checking the sender is together with the salutation (used the most), the compelling character and the link towards the login screen most actively used by either groups. Checking the sender is in comparison to the other three the least used. However, this hint is also considered to be in the most used hints because of the positive influence in the use after reading the hints of Veiligbankieren.nl. This image is portraying that overall the sample particularly paid attention towards the beginning of the e-mail, which indicates the sample of this study already knew these are important areas in order to determine legitimacy of bank e-mails. In addition, the hint about the compelling character was also actively used by the participants of this study. Thus the body of an e-mail is an important area to check for legitimateness of bank e-mails. The hint about a link towards the login screen is the fourth hint which is being actively used by the participants, which was usually near the end of the text in the bank e-mails. Concluding that together, with the beginning of the e-mail, the end of the e-mail (where the link is usually located) and checking the body for a compelling character are important areas (or signs) of interest for the participants in order to determine legitimacy according to the participants.

The hint about possible spelling mistakes was the least used by the sample, since the hint had the lowest amount of active usage in the selected bank e-mails. The hint about spelling mistakes focuses on intensively reading the e-mail and finding mistakes in the spelling or order of words. This implies that the low amount of active use of the hint about possible spelling mistakes could be caused by quick scanning and a quick judgement of the legitimacy of a bank e-mail. In order to accomplish quick scanning, the participants might not read the e-mails

intensively and look for spelling errors because checking for these errors will take more time. This could explain why the hint about the spelling mistakes is so low in use. Evidence for the previous is also provided in the more active use of the other four hints which are more focused on relatively small elements in the e-mail which quickly reveal a significant amount of information. Furthermore, if the spelling is not as bad, the other hints reveal more about the legitimacy. Hence, resulting in a greater use of these four hints and a lesser use of the hint regarding spelling.

The hints of Veiligbankieren.nl which were actively used by the experimental and the control group were almost the same. The experimental group exhibited an active use of hints regarding checking the sender, the salutation and the link towards the login screen. Therefore the experimental group which read the hints during the experiment, explicitly focused on the begin part of a bank e-mail and the link towards a login screen. A possible explanation for the outcome is that these hints were most easily recognizable and costed the least amount of time to utilize. The control group almost used the same hints actively. In the control group the salutation, the compelling character and the link towards the login screen were mostly used. Therefore the participants who not read the hints during the experiment showed that more obvious signs for a phishing e-mail are most used.

Various hints of Veiligbankieren.nl displayed differences in active use between the experimental and the control group in this study. At first, the hint which focused on checking the sender showed differences between the experimental and the control group. The experimental group had on average a higher utilization of this hint in comparison to the control group. Therefore, reading the hints has a positive influence on the use of checking the sender. Therefore focusing marketing campaigns on this tip could have the best possible effect on reducing phishing susceptibility. A possible explanation for the moderate use could lie in the low awareness of the customers of online banking that the sender can be an important sign of a phishing or genuine e-mail. Therefore, if this hint is marketed more together with the other hints, the correct identification of bank e-mails might increase because of the increased awareness. That there is room for improvement through a marketing campaign is underlined by the moderate use of this hint even after the hints have been read beforehand.

The hint regarding checking the salutation was used the most in determining legitimacy of bank e-mails. However, little difference in active usage of this hint was shown between the

experimental and the control group. Therefore, reading the hints of Veiligbankieren.nl beforehand did not help in increasing the active use of the hint about checking the salutation. A possible explanation of the high use could be that customers of online banking know that the salutation is an important area in order to determine legitimacy of bank e-mails. Another factor which could be of influence is that this hint is the first part of an e-mail which customers usually read. If a participant already recognizes the un-personal salutation, one could have had already identified the e-mail as a genuine or a phishing e-mail. Still, there is room for improvement in the most used hint as well because it is not utilized in all e-mails.

The hint regarding the compelling character portrayed a great difference between the experimental and the control group in the opposite direction of the hint about checking the sender. Therefore, the hint about a compelling character caused confusion towards the participants in the experimental group. Thus, potentially helping the criminals who want to take advantage of the customers of online banking. A possible explanation for the confusion can be caused by institutions of the government which might use similar methods to convince a person to do an action or to pay a bill (which creates confusion). Therefore additional explanation could be required for this hint about how a phisher portrays their compelling character and how the government does.

The hint regarding the spelling mistakes in an e-mail was the least used hint by the participants. Still, there was a positive influence in the use of the hint about checking for spelling mistakes between the experimental and the control group. Therefore the hint about spelling mistakes might help in better determining legitimacy of an e-mail. Thus this hint could be a vocal point for marketing in order to decrease phishing susceptibility more. A possible explanation for the low use of checking for spelling mistakes could be the quick scanning of an e-mail (as discussed earlier). Therefore the customers of online banking might miss the spelling mistakes in the e-mail. Another explanation could lie in the time required to find a spelling mistake in a phishing bank e-mail because of an increase in quality over time.

The last hint regarding the link towards the login screen was used moderately in order to determine legitimacy of bank e-mails in the experiment. There was little to none positive influence in the use of the hint regarding the login screen and thus reading this hint during the experiment does not increase the likelihood of using it. Therefore, checking for a link towards the login screen will help in the correct identification of e-mails, but not more than it does now if

there will not be an extensive marketing campaign. A possible explanation for a lack of a positive effect could be that the customers of online banking might think a link towards the login screen of a bank is present in the e-mail. Therefore the lack of a positive effect could use further research if the customers of online banking expect a link towards the login screen.

Overall the hints of Veiligbankieren.nl displayed a varying amount of use in order to determine legitimacy of bank e-mails. The most positive influence was seen in the hints of checking the sender and spelling mistakes, thus marketing campaigns will have the greatest effect on further increasing the use of these hints and decreasing phishing susceptibility. The hints of checking the salutation and the presence of a link towards the login screen displayed little difference in use. Therefore a less positive effect is expected when marketing campaigns are deployed. The only hint which saw a significant negative use was the compelling character. Therefore this hint requires a better understanding before it can be used in marketing campaigns. Another option would be to leave this hint out because checking for a compelling character is one of the most used hints, which might not need any further extensive marketing.

This study also provides additional analysis on the effect of certain demographics on phishing susceptibility. The two main factors in this study were age and gender. By using a combination of methods, no differences were found for both variables for the whole sample, the experimental and the control group (as opposed to the hypothesis). Therefore no difference exists in phishing susceptibility for gender. Consequently, this study contradicts the findings of for instance Oliveira et al. (2017) and Sheng et al. (2010) who find women to be more vulnerable towards phishing. A likely cause for a non-significant difference in gender is the small sample of this study because a small sample might not reflect the population properly. Therefore no proper conclusions can be made regarding this variable. The same conclusions holds for age. No significant values were found between the younger and the older age groups. These insignificant values mean that this study contradicts the views of other studies who find an age group to be more vulnerable (Sheng et al., 2010; Oliveira et al., 2017). The insignificant values for age are most likely caused by the small sample size. Therefore no proper conclusions can be made about this variable as well.

However, one demographic factor showed to have an influence on judging bank e-mails. This was the variable of whether a participant was in a relationship or not. The test which analyzed the whole sample portrayed a significant effect and a higher mean rank for being in a

relationship on the amount of correctly judged bank e-mails. Meaning a person was better in correctly judging the bank e-mails in this experiment when the participant was in a relationship. No other studies were discovered whom used this variable in their model or their analysis. Therefore this variable needs to be added towards the various existing models of which demographic variables have an influence on phishing susceptibility. A cause for this effect is argued to emerge from the consequences which falling for a phishing e-mail holds. If a person falls for a phish, it will have to incur damages of some kind. Therefore, their partner will also suffer from the persons' wrong judgement. This situation can cause a person to take more time for their judgement and be more careful. If a person takes more time in recognizing genuine bank e-mails or phishing e-mails, it is very likely that this persons' awareness increases and phishing susceptibility decreases. Therefore, the effect of being in a relationship could cause the correct judgement of bank related e-mails to increase.

A first remarkable additional result was the amount of e-mails (both phishing and genuine bank e-mails) correctly judged. 86.7% of the phishing e-mails and 80.0% of the genuine bank e-mails were correctly identified. These percentages display that on average the participants judged the phishing mails more correctly than genuine bank e-mails. Thus, implying judging correctness of a genuine bank e-mail is more difficult than a phishing e-mail, which is in line with the study of Sheng et al. (2010). This can result in missing important messages which are sent through e-mail by a bank towards their customer. A solution which might reduce the chance of missing an important e-mail is making sure all of these e-mails are standardized and without a spelling mistake. One particular e-mail in the experiment contained a small spelling mistake which caused a participant to misjudge the e-mail. Hence, emphasizing that only faultless e-mails need to be sent, or else face the consequences that a customer might misjudge the e-mail and not read it.

Secondly, a significant effect was discovered between how difficult a participant thought the judging of e-mails was and the amount of correctly judged bank e-mails. The results showed that the more difficult a person thought judging the e-mails were, the better a participant performed and vice versa. Thus displaying the role of overconfidence in correctly judging bank e-mails. The overconfidence was mainly present within the experimental group. Thus reading the hints during the experiment increased the self-confidence of a participant, but to such an extent that the participant became overconfident. Therefore it should be exaggerated that one should not

become to overconfident when these hints are marketed and stay alert towards possible threats. Thus implying that the studies on increasing awareness of phishing are indeed useful because of overconfidence in a persons' own abilities.

6. Conclusion

6.1 Conclusion

Phishing is still a prominent issue in today's society. Therefore an initiative was introduced by banks by providing e-mail users with easy to understand bullet points or hints in order to reduce susceptibility towards phishing e-mails. In this study, the focus was on the hints provided by Veiligbankieren.nl which focused its campaign here in the Netherlands.

A previous study showed that education or training can be effective in reducing phishing susceptibility (Sheng et al., 2010). Therefore the goal of this study was to find whether the hints of Veiligbankieren.nl have a similar positive influence on reducing phishing susceptibility since these hints are a form of education. An experiment was setup in which participants judged whether 10 e-mails were genuine bank e-mails or phishing e-mails. Two groups were used in the experiment, one group which read the hints during the experiment and the other group not. The dependent variable was phishing susceptibility, which was measured by the amount of bank e-mails correctly judged. In addition, eye tracking glasses were used to determine whether these hints were actively used to determine legitimateness of bank e-mails.

Results show that there is a significant difference in the mean ranks of the amount of correctly judged bank e-mails between the two groups, in which the experimental group has an overall better judgement in comparison to the control group. This indicates that there is a positive influence on the correct judgement of these bank e-mails when these hints are read during the experiment, which decreases phishing susceptibility. These results are in line with the studies of Sheng et al. (2010) and Arachchilage & Love (2013), whom found the same positive relationship between education and phishing susceptibility.

The results of the eye tracking data shows that hints related towards the sender, the salutation, the compelling character and the link towards a login screen are the most used hints to determine legitimacy. Though differences exist between the experimental and the control group. Both groups actively used the hint about the salutation and the link towards the login screen. In addition, the experimental group used the hint about checking the sender actively and the control group used the hint about the compelling character actively. The spelling mistakes, which is related towards the body of the e-mail, is used the least in all the e-mails by both groups. This

indicates that the hints of Veiligbankieren.nl could be the cause for the reduction in phishing susceptibility.

Reading the hints of Veiligbankieren.nl led to a difference in active use between the experimental group and the control group. The experimental group displays a positive influence in comparison to the control group in the use of checking the sender and the spelling mistakes. Two other hints (checking salutation and the link towards the login screen) display little difference between the experimental and the control group. A negative influence is seen with the compelling character because the hint probably causes confusion since other institutions might use similar methods in their e-mails. Therefore the positive effect of the hints of Veiligbankieren.nl is most likely caused by the increased awareness of the hints of the sender and the spelling mistakes. Therefore focusing marketing campaigns on these hints will result in the most positive effect in active use (and therefore a further reduction of phishing susceptibility). In addition to the previous, a better explanation of the hint about compelling character could also improve the use and reduce the phishing susceptibility further.

The results also presented that recognizing phishing or genuine bank e-mails does not differ by age or gender, which also holds for both the experimental and the control group. Therefore, this study contradicts several studies who find an effect between these variables and phishing susceptibility (Jagatic et al., 2007; Kumaraguru et al., 2009). A likely cause for the result is the small sample size. On the contrary, being in a relationship does show a positive effect on correctly judging e-mails from banks. This result is significant in the experimental group but not in the control group, which indicates one should focus on single persons after a possible marketing campaign to reduce phishing susceptibility further. No other known studies include ‘being in a relationship’ in their studies or show this variable to have an influence on phishing susceptibility. Therefore, various models regarding phishing susceptibility should include this variable. However, because of the small sample size, a larger study can be beneficial in order to prove that the effect of ‘being in a relationship’ on phishing susceptibility also holds with a larger sample.

Additional analysis shows that the easier a person thinks judging these e-mails are, the worse a participant is at judging the e-mails. This suggests overconfidence may play a role in judging legitimacy of e-mails. The overconfidence is mainly present within the experimental group, implying that the hints increased confidence in a participants’ abilities while this was

often not justified. Therefore marketing campaigns need to exaggerate that one should not become overconfident in their own ability if the hints of Veiligbankieren.nl are marketed.

6.2 Implications

This study aimed to investigate the effect of hints like those of Veiligbankieren.nl on reducing phishing susceptibility. This study shows a positive and significant effect of these hints on better judging e-mails which have a bank related topic. Moreover, this study shows that several of these hints are actively used and others not and that there is a difference in the active use between a group who read the hints of Veiligbankieren.nl and a group who did not.

The previous implies that easy to understand bullet points as provided by the hints of Veiligbankieren.nl are effective and can be introduced in other countries to decrease phishing susceptibility towards e-mails with a bank related topic. Furthermore, this study supports the hypothesis that education does help in reducing phishing susceptibility, as shown other studies as well (Sheng et al., 2010; Arachchilage & Love, 2013). Hence, this possibly could result in a decrease in costs for phishing for banks.

An important issue of the hints of Veiligbankieren.nl is whether the hints are actively used when read. Therefore, marketing campaigns need to deploy more methods to make these hints known to the public. This is underlined by the low to moderate overall active use of the hints. Thus while some hints are actively used, there is still room for a significant improvement in the active use of the hints of Veilligbankieren.nl. This implies that a bank could even be more active in pinpointing the importance of being safe online and provide useful tools such as these hints to reduce phishing susceptibility further. However, because not all hints portrayed a positive influence in active use after reading the hints, exaggerating the hints which show a positive influence could have the best positive influence in reducing phishing susceptibility. In addition, the other hint which showed a negative influence requires the public to have a better understanding of this hint which is the responsibility of Veiligbankieren.nl.

This study does not find a significant effect of gender or age on reducing phishing susceptibility. However, this study did find a significant relationship of the relationship status on reducing phishing susceptibility. These results indicate that a ‘single’ person is worse in correctly judging bank e-mails, which is mainly present in the experimental group. Therefore the focus of the marketing campaign should be on online banking customers which are single or in a

relationship beforehand. Afterwards the focus should be on single persons because the results show that this group performs worse in correctly judging bank e-mails after the tips have been read just before the experiment. Additional results also indicate that overconfidence played a role in correctly judging bank e-mails and more particularly in the experimental group. Therefore online banking customers need to be notified that one should not become too confident after the hints are marketed.

6.3 Limitations

There were several limitations in this study. A first limitation was the small sample which was not representative across the experimental and the control group. A second limitation was that the measurement instrument used to gather eye tracking data did not typically gave very reliable data. Sometimes, the gaze quality was only at a level of 50%, which increased the difficulty of analysis. A last limitation is that this study was performed in an experimental setup in which participants in the experimental group read the hints just before judging the e-mails. In a real life situation an online banking customer will not read the hints of Veiligbankieren.nl just before judging bank e-mails. Therefore the results of this study should be seen as an indication that there is a positive influence of the hints of Veiligbankieren.nl on correctly judging bank e-mails.

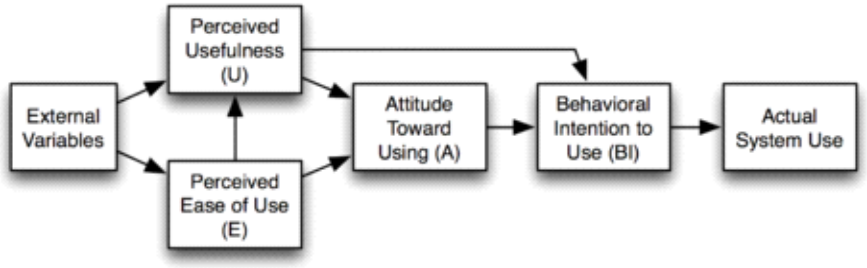
6.4 Directions for further research

There could be several directions for further research based on this study. At first, it can be studied if the hints can be integrated in theoretical models such as the model by Parrish et al. (2009). Such a model, which could include multiple variables of different origins, could show different or similar results for this variable. Secondly, future studies can focus on whether these hints increase the awareness of phishing over a longer term, because this study has shown the effectiveness of the hints of Veiligbankieren.nl in reducing phishing susceptibility over a short term. Lastly, it would be interesting to investigate whether the marketing campaigns to promote the knowledge of these hints, lead to more usage of these hints over time. This would especially be interesting for the hints that have a low usage or an indication of a positive or negative difference after reading the hints. Thirdly, the significant effect of the relationship status and overconfidence on correctly judging bank e-mails could be further investigated if the effect also holds in a study with a higher number of participants.

7. Appendix

A The TAM model

The technology acceptance model. Wikiwand (N.D.).



B Online banking drivers from a banks perspective

Online banking drivers			
Driver	**Rating of IT managers**	**Rating of senior management**	**Overall rank**
Providing faster service to customers	1	1	1
Providing easier service to customers	2	2	2
Providing more reliable service to customers	3	3	3
Improving the competitive position	4	5	4
Improving bank's image	6	7	5
Meeting customers demand for the service	5	9	6
Creating new markets	7	4	7
Reducing operational costs	8	6	8
Reducing administrative costs	9	8	9

C The operationalization of the variables

Experimental or control group	Measured whether a participant was in the experimental or control group.	A dummy variable in which 1 was the experimental group and 0 the control group.

Technical experience	1. The amount of experience that someone has with information security related areas. 2. Previous education on decreasing phishing susceptibility.	Measured on a 5 scale: A great deal, a lot, a moderate amount, little or none at all.
Gender	This indicates the gender of the sample.	Either female or male. 1 is female and 0 is male.
Age	This is measured by the age the sample has, which is divided into five categories.	There were five categories: 18-25, 26-40, 41-55, 56-65 and 65+.
Education	This measured the highest completed education of a participant.	7 point scale: primary school, secondary school, intermediate vocational education, associate degree, bachelor degree, master degree or a doctorate.
Employment	Measures whether the participant is employed.	Either full time, part-time or not.
Relationship status	Measures what the relationship status is of the participants.	Four categories: Single, In a relationship but living apart (LAT), in a relationship and living together and married and living together.
Confrontation with these type	1 - Measures whether a person is	1 - Measured on a 7

of e-mails	often confronted with these type of e-mails. 2 - Measures the amount of times a participant encountered phishing e-mails.	point Likert scale (strongly agree to strongly disagree). 2 - 5 categories: 1-5, 6-10, 11-15, 15-20, >20.
Experience in detecting phishing e-mails	The experience a participant thought it had in detecting phishing e-mails.	Measured on a 7 point Likert scale (strongly agree to strongly disagree).
Reading possible phishing e-mails.	Measured whether a participant deleted a possible phishing e-mail quickly or read it more intensively.	Measured in 3 categories: I delete the e-mail straight away, I quickly scan it and delete the e-mail and I intensively read the e-mail but delete it.
Correct identification of an e-mail.	Measured whether a participant correctly identified an e-mail.	Measured by using a dummy variable. 1 was correctly identified and 0 not.
Knowledge and prominence of phishing	1 - Measured whether a person knew what phishing was. 2 - Measured whether a person thought phishing was still prominent issue in society. 3 - Measured whether a participant thought phishing still existed a lot.	1 - Measured on a 7 point Likert scale (strongly agree to strongly disagree). 2 - Measured on a 7 point Likert scale (extremely likely to extremely unlikely). 3 - Measured on a 7

		point Likert scale (strongly agree to strongly disagree).
Difficulty of correctly identifying an e-mail.	1 - Measured how difficult a person thought identifying an e-mail was. 2 - Measured whether a person thought it was prone to fall for phishing e-mails.	1 - Measured on a 7 point Likert scale (extremely easy to extremely difficult). 2 - Measured on a 7 point Likert scale (strongly agree to strongly disagree).
Positive influence of the hints of Veiligbankieren.nl	1 - Measured whether a participant thought that there was a positive influence on decreasing phishing susceptibility if everyone knew these hints. 2 - Measured whether a person would recommend everyone to know these hints.	1 - Measured on a 5 point Likert scale (Definitely yes to definitely not). 2 - Measured on a 5 point Likert scale (Definitely yes to definitely not).
Correctly judging e-mails from banks	Measured the amount of times a participant correctly identified an e-mail.	The amount of 1s in the variable indicated correct identification of an e-mail. The amount 1s were added to single number. Therefore this value can range from 0-10.

8. References

Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., & Almomani, E. (2013). A survey of phishing email filtering techniques. *IEEE communications surveys & tutorials*, *15*(4), 2070-2090.

Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, *29*(3), 706-714.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312.

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, *60*, 185-197.

Arianezhad, M., Camp, L. J., Kelley, T., & Stebila, D. (2013). ACM. Comparative eye-tracking of experts and novices in web single sign-on. In *Proceedings of the third ACM conference on Data and application security and privacy,* 105-116.

Aladwani, M. A. (2001). Online banking: A field study of drivers, development challenges and expectations. *International Journal of Information Management*, *21*(3), 213–225.

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: user strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *82*, 69-82.

Blum, A., Wardman, B., Solorio, T., & Warner, G. (2010). Lexical feature based phishing URL detection using online learning. ACM. In *Proceedings of the 3rd ACM Workshop on Artificial Intelligence and Security,* 54-60.

Bose, I., & Leung, A. C. M. (2007). Unveiling the mask of phishing: Threats, preventive measures, and responsibilities. *Communications of the Association for Information Systems*, *19*(1), 544-566. Page 550 for citation.

Brainyquote, N.D.. Nelson Mandela quotes. Retrieved on 13, 12, 2017 from https://www.brainyquote.com/quotes/nelson_mandela_157855

Brignall, M. (2016, March 17). Banking scams push up UK financial fraud 'by more than 25%'. The Guardian, 1. Retrieved on 25, 09, 2017 from https://www.theguardian.com/money/2016/mar/17/banking-scams-uk-financial-fraud.

Charter, R. A. (2003). A breakdown of reliability coefficients by test type and reliability method, and the clinical implications of low reliability. *The Journal of General*

Psychology, *130*(3), 290-304.

Chen, J., & Guo, C. (2006). Online detection and prevention of phishing attacks. IEEE. In *Communications and Networking in China, 2006. ChinaCom'06. First International Conference on IEEE,* 1-7.

Cheng, T. E., Lam, D. Y., & Yeung, A. C. (2006). Adoption of internet banking: an empirical study in Hong Kong. *Decision support systems*, *42*(3), 1558-1572.

Crowe, J. (2016). Phishing by the numbers: Must-know phishing statistics. Retrieved on the 25, 09, 2017 from https://blog.barkly.com/phishing-statistics-2016#0.

Daniel, E. (1999). Provision of electronic banking in the UK and the Republic of Ireland. *International Journal of Bank Marketing*, *17*(2), 72-83.

Darwish, A., El Zarka, A., & Aloul, F. (2012). Towards understanding phishing victims' profile. IEEE. In *Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference on* IEEE, 1-5.

Dodge Jr, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & security*, *26*(1), 73-80.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. ACM. In *Proceedings of the second symposium on Usable privacy and security*, 79-90.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). ACM. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems,* 581-590.

Dhamija, R., & Tygar, J. D. (2005). ACM. The battle against phishing: Dynamic security skins. In *Proceedings of the 2005 symposium on Usable privacy and security,* 77-88.

Floh, A., & Treiblmaier, H. (2006). What keeps the e-banking customer loyal? A multigroup analysis of the moderating role of consumer characteristics on e-loyalty in the financial service industry. *SSRN Electronic Journal*, *7*(2), 97–110.

Gremler, D. D., & Brown, S. W. (1996). Service loyalty: Its nature, importance, and implications. *Advancing Service Quality: A Global Perspective*, *5*, 171-181.

Hale, M. L., Gamble, R. F., & Gamble, P. (2015). IEEE. CyberPhishing: a game-based platform for phishing awareness testing. In *System Sciences (HICSS), 2015 48th Hawaii International Conference on IEEE*, 5260-5269.

Lai, Y. P., & Hsia, P. L. (2007). Using the vulnerability information of computer systems to

improve the network security. *Computer Communications*, *30*(9), 2032-2047.

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. ACM. In *Proceedings of the 22nd International Conference on World Wide Web*, 737-744.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74-81.

Iuga, C., Nurse, J. R., & Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences*, *6*(1), 1-20.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94-100.

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: a qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79-91. Page 79 for citation.

Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis*, *1*(1), 11-27. Page 12 for citation.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). ACM. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, 1-13.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting people from phishing: the design and evaluation of an embedded training email system. ACM. *In Proceedings of the SIGCHI conference on Human factors in computing systems,* 905-914.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, *10*(2), 1-18.

Kunz, A., Volkamer, M., Stockhardt, S., Palberg, S., Lottermann, T., & Piegert, E. (2016). Nophish: evaluation of a web application that teaches people being aware of phishing attacks. *Informatik 2016*, 509-518.

Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, *3*(1), 1-9. Page 8 for citation

Lupton, D. (1999). Risk and sociocultural theory: New directions and perspectives. *Cambridge University Press,* 12-33. Page 12 for citation.

Mayhorn, C. B., & Nyeste, P. G. (2012). Training users to counteract phishing. *Work, 41*

(Supplement 1), 3549-3552.

Mukherjee, A., & Nath, P. (2003). A model of trust in online relationship banking. *International journal of bank marketing*, *21*(1), 5-15.

Neupane, A., Rahman, M. L., Saxena, N., & Hirshfield, L. (2015). ACM. A multi-modal neuro-physiological study of phishing detection and malware warnings. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security,* 479-491.

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., ... & Ebner, N. (2017). ACM. Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems,* 6412-6424. Page 6412 for citations.

Parrish Jr, J. L., Bailey, J. L., & Courtney, J. F. (2009). A personality based model for determining susceptibility to phishing attacks. *Little Rock: University of Arkansas*, 285-296.

Polakis, I., Kontaxis, G., Antonatos, S., Gessiou, E., Petsas, T., & Markatos, E. P. (2010). Using social networks to harvest email addresses. ACM. In *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society,* 11-20.

Plassmann, H., Venkatraman, V., Huettel, S., & Yoon, C. (2015). Consumer neuroscience: applications, challenges, and possible solutions. *Journal of Marketing Research*, *52*(4), 427-435.

Purkait, S. (2012). Phishing counter measures and their effectiveness–literature review. *Information Management & Computer Security*, *20*(5), 382-420.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. ACM. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 373-382. Page 380 for citation.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security,* 88-99.

Sun, J. C. Y., Kuo, C. Y., Hou, H. T., & Yu-Yan, L. (2017). Exploring learners' sequential behavioral patterns, flow experience, and learning performance in an anti-phishing educational game. *Journal of Educational Technology & Society*, *20*(1), 45.

Veiligbankieren.nl, (2017). Fraude betalingsverkeer wederom fors lager. Retrieved on 02, 07, 2017 from https://www.veiligbankieren.nl/nieuws/fraude-betalingsverkeer-wederom-fors-lager/

Veiligbankieren.nl, (2017). Nepmail, daar trapt u niet in. Retrieved on 26, 09, 2017 from https://www.veiligbankieren.nl/wp-content/uploads/2015/07/VBNL_flyer-bankiert-u-veilig-back.jpg

Veiligbankieren.nl, (N.D.). Over ons. Retrieved on 01, 02, 2018 from https://www.veiligbankieren.nl/over-ons/

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences, 39*(2), 273-315.

Whalen, T., & Inkpen, K. M. (2005). Gathering evidence: use of visual security cues in web browsers. *In Proceedings of Graphics Interface 2005,* 137-144.

Wikiwand. (N.D.). Technology acceptance model. Retrieved on 25, 09, 2017 from http://www.wikiwand.com/en/Technology_acceptance_model

Zhang, Y., Hong, J. I., & Cranor, L. F. (2007). Cantina: a content-based approach to detecting phishing web sites. ACM. In *Proceedings of the 16th international conference on World WideWeb*, 639-648.

Phishing e-mails used:

1 - Fraudehelpdesk (N.D.). ING. Uw account wordt in quarantaine geplaatst. Retrieved on 07, 11, 2017 from https://www.fraudehelpdesk.nl/vragen-meldingen-cpt/ing-uw-account-word-quarantaine-geplaatst/?_sf_s=quarantaine

2 - Fraudehelpdesk (N.D.). Uw e.dentifier2 vervalt voor gebruik. Retrieved on 07, 11, 2017 from https://www.fraudehelpdesk.nl/vragen-meldingen-cpt/abn-amro-e-dentifier2-vervalt-gebruik-2/?_sf_s=e.dentifier2

3 - Fraudehelpdesk (N.D.). Bankmail: Mand September nieusbrief 2017 !. Retrieved on 07, 11, 2017 from https://www.fraudehelpdesk.nl/vragen-meldingen-cpt/argenta-bankmail-maand-september-nieuwsbrief-2017/?_sf_s=bankmail:+M

4 - Fraudehelpdesk (N.D.). Introductie vernieuwde beveiligingsupdate. Retrieved on 07, 11, 2017 from https://www.fraudehelpdesk.nl/vragen-meldingen-cpt/ing-spam-introductie-vernieuwde-beveiligingsupdate/?_sf_s=introductie+vernieuwde+beveiligingsupdate
5 - Fraudehelpdesk (N.D.). Rabo Wereldpas opgeheven. Retrieved on 07, 11, 2017 from https://www.fraudehelpdesk.nl/vragen-meldingen-cpt/rabobank-onderwerp-rabo-wereldpas-opgeheven/?_sf_s=wereldpas+opgeheven'