Awareness of Phishing under the Dutch Population

Bachelor thesis
Supervisor: Roeland Aernoudts
Student: Jakub Kulikowski
Student number: 279857

December 13 , 2013

Erasmus University Rotterdam
Erasmus School of Economics
Economics & Informatics

ERASMUS UNIVERSITEIT ROTTERDAM
ERASMUS SCHOOL OF ECONOMICS

Table of contents

Table of contents 2
Chapter 1 3
1.1 Introduction..3
1.2 Research question..3
1.3 Scientific relevance 4
1.4 Societal relevance 4
1.5 Research methodology...4
1.6 Thesis structure 5
Chapter 2 Literature Review..6
2.1 Introduction..6
2.2 Important findings 6
2.3 Conclusion...11
Chapter 3 Insight into phishing 12
3.1 What is Phishing ? 12
3.2 Phishing attacks 12
3.3 Detecting phishing 13
3.4 Anti-Phishing measures...13
3.5 Modern phishing attacks..14
Chapter 4 Survey and results..15
4.1 Introduction..15
4.2 Development of measures..16
4.3 Hypotheses development 17
4.4 Survey set-up 18
4.4.1 Measurement validity 18
4.4.2 The survey 19
4.5 Results and findings 20
Chapter 5 Conclusion...23
5.1 Future research & Limitations..24
5.2 Practical use of the acquired knowledge..24
References 25
Appendix..26

Chapter 1

1.1 Introduction

Phishing, as defined by Anti Phishing Working Group (APWG)[1], is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social engineering tactics use fake emails to lure recipients to a fraudulent website that tricks the user to give away his personal information such as social security number, credit card number or username and password. Technical subterfuge tactics plant malicious software on user's computer to directly steal their credentials, often by logging user's keyboard strokes or seamlessly redirecting users to fraudulent websites by using proxies. With 445,004 phishing attacks in 2012 (56% increase from 2011), phishing is responsible for estimated global losses of USD 1.5 billion in 2012 (22% increase from 2011), according to RSA, the Security Division of EMC [2]. This significant increase in phishing occurrences is very concerning from the social point of view as it reaches wider audience each year. The countermeasures against phishing include filtering of phishing emails, blocking phishing sites, taking down phishing websites, improving browser interfaces and possibly the most effective countermeasure, educating users about phishing.

Not many studies have performed on the phishing phenomenon, the ones that exist, primarily focus on researching the susceptibility and the process of phishing and/or on the strategies used to detect phishing (e.g. Vishwanath et al., (2011), Bose and Leung (2007), Jagatic et al. (2007), Blythe et al. (2011), Dhamija et al. (2006)). However, none of the prior research examines the magnitude of phishing problem and the consequences of awareness of phishing. This thesis therefore examines the current state of research into phishing and provides an exploratory study into the awareness of Phishing under the Dutch population. It also provides a description of how a phishing attack works, why people fall for them and on the countermeasures against phishing. By exploring phishing awareness and the consequences of (the lack of) awareness of phishing, this study attempts to close the gap in knowledge of current research and consequently adding scientific value.

1.2 Research question

Due to evermore increasing number of phishing attacks, the economic loss is increasing as well. This can be attributed for instance to the use of more sophisticated phishing tools, such as website cloning tools and the ease in which a less experienced hacker can use such tool. To be able to understand the economic consequences of Phishing, this thesis addresses the question

[1] Anti-Phishing Working Group (2013). Phishing Activity Trends Report 2nd Quarter 2013. Available At: http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf

[2] EMC Corporation (2013). RSA Monthly Online Fraud Report -- January 2013. Available At: http://www.emc.com/collateral/fraud-report/online-rsa-fraud-report-012013.pdf

of to what extent people in the Netherlands are aware of the phishing phenomenon. The research question guiding this study is thus formulated as follows:

“To what extent are people in the Netherlands aware of phishing and the risks of phishing?”

The first sub-question that supports the research study, consist of the following:

“*To what degree do the people in the Netherlands know how to protect themselves against phishing*”.

Furthermore to test the findings from the prior literature in the context of the Netherlands, the second sub-question is formulated as follows:

“*Does phishing awareness, computer self-efficacy, email load, gender or age have effect on susceptibility to phishing in the Netherlands ?* “.

1.3 Scientific relevance

When examining the current state of knowledge with regard to Phishing it became clear that there is only limited knowledge on this phenomenon. There have been several studies regarding the subject, however, most of the existing phishing studies originate from the United States. The scientific contribution of this paper is twofold. Firstly, it provides an exploratory investigation focused on the phishing awareness of the people in the Netherlands. Secondly, this study through the literature review performed, provides an assessment of the current state of knowledge with regard to this subject. The aim of the review is to assess the lacuna in current research.

1.4 Societal relevance

Because of the increasing economic losses due to phishing attacks, this thesis also has social relevance. This due the fact that when for example a client of a bank is successfully phished and the phishers have stolen money from the clients bank account, the bank issues a refund for the loss of clients money. With the increasing occurrences of such attacks, the total compensated losses will accumulate to a significant amount. This money has to come from somewhere so the banks will obviously shift the losses to their clients. Which means that the bank’s other clients that weren’t initially affected by phishing attacks will eventually be negatively affected by them.

1.5 Research methodology

An exploratory study was carried out in this thesis about the risks of phishing and awareness of the risks of phishing in the Netherlands. To answer the research question, a survey about the awareness of phishing in the Netherlands was conducted. The survey was posted on social media sites like facebook to quickly gather data. Responses from social media sites returned, as expected, a representative sample of the Dutch population. The number of responses the survey has reached was 78.

1.6 Thesis structure

The remainder of this thesis is structured as follows, chapter 2 describes literature review, first it explains the methodology used to select 20 papers about phishing from the top ranked journals in the field of Information Systems. Then it summarizes the 10 most relevant papers found. The thesis will build upon these 10 articles from that point forward. Chapter 3 is concerned with the insight into the phishing phenomenon. It starts with the origins of the word “phishing” then follows it with the description of a typical phishing attack. Subsequently the various techniques in detecting phishing attacks are covered followed by an overview of the most important anti-phishing measures. The chapter concludes with recent examples of phishing attacks in the Netherlands. Chapter 4 presents results of the carried out survey as well as the analysis of the results. The final chapter 5 concludes with a brief summary and the findings.

Chapter 2 Literature Review

2.1 Introduction

In order to position this study within prior research in the field of Information Systems and to examine the status of current knowledge this chapter provides an overview of the extant literature. First a search for prior literature was carried out. To select suitable articles for the literature study, the Association for Information System (AIS) website served as a source for selecting journals. The AIS website features the rankings of scientific journals in the field of Management Information Systems (MIS), see table 1. From this ranking the top journals in IS were selected. Starting with the highest ranked, database of each journal was searched for empirical studies focusing on the subject matter of phishing. When no more articles could be obtained from a specific journal source the next ranked journal was then searched. Using this method top 20 journals were searched and articles were collected. From the collected journal articles from highest ranked MIS journals, including their references, 10 studies were selected for inclusion in the review based on criteria of relevance.

The selected articles in no particular order were Jagatic et al. (2007), Vishwanath et al. (2011), Hong (2012), Dhamija et al. (2006), Bose and Leung (2007), Downs et al. (2006), Berghel, H. (2006), Baker et al. (2007) , Blythe et al. (2011) and Bose and Leung (2013).

2.2 Important findings

The findings of Vishwanath et al. (2011), based on survey among 325 undergraduate students, indicated that the urgency cues in phishing emails are the most deceitful for the recipients, as they turn their the attention away from other cues that may potentially help the them in correctly dismissing phishing emails. The other main finding of Vishwanath et al. (2011) was that users who admitted to habitual media (Internet) use, coupled with high email load, were more likely to automatically respond to relevant looking emails thus increasing the odds of response to phishing emails. Technological self-efficacy and prior experience proved to have no effect on phishing susceptibility, implying that the phishing victims fall for phishing attacks not because their lack of ability but because of the lack of cognitive involvement.

The article of Hong (2012) outlines the current state of phishing, and gives insight into anti-phishing techniques. Hong (2012) predicts that the spear-phishing and whaling attacks will likely increase in quantity, as phishers look to target users with valuable information. He concludes that the problem of phishing cannot be solved but it can be limited so that the worst impacts of phishing can be prevented.

Ranking	Journal Name
1	MIS Quarterly
2	Information Systems Research
3	Comm. of the ACM
4	Mgmt. Science
5	Journal of Mgmt. IS
6	Artificial Intelligence
7	Decision Sciences
8	Harvard Business Review
9	IEEE Trans.
10	AI Magazine
11	European Journal of IS
12	Decision Support Systems
13	IEEE Software
14	Information and Mgmt.
15	ACM Trans. on Database Systems
16	IEEE Trans. on Software Eng.
17	ACM Trans.
18	Journal of Comp. and System Sciences
19	Sloan Mgmt. Review
20	Comm. of AIS

Table 1. MIS Journal Rankings by AIS (2013)[3]*, Ranking based on various studies e.g., Rainer and Miller (2005), Lowry et al. (2004) and Katerat-tanakul et al. (2003)*

Jagatic et al. (2007) send (spear) phishing email to unaware students as an experiment. The sender of the phishing emails was spoofed to a person that they knew, an information that was collected from the publicly available friends data on receiptians' profiles on social sites (social group). The control group received the same email but the sender was spoofed to an unknown fictitious person. The results revealed among others that success rate of social group (72%) was significantly higher than that of the control group (16%), that the highest rate of response (70% of total responses) occurred in the first 12 hours (out of 4 days) and that users were more likely to fall for the phish is the sender was of the opposite sex. Results demonstrated de facto the impact of spear phishing and the importance of rapid takedowns of phishing websites.

[3] Association for Information System. MIS Journal Rankings Available At: http://start.aisnet.org/?JournalRankings

Bose and Leung (2007) described phishing techniques and how phishing attacks can be divided in four phases: preparation, mass broadcast, mature and account hijack. Based on tools and measures, legislation and standards aimed at fighting phishing Bose and Leung (2007) presented an Anti-Phishing Framework (Figure 1) that can be applied to disrupt four phases of phishing.

It's worth noting that it was concluded that all of the tools and measures against phishing had vulnerabilities that could be exploited. It was stated that 2-factor authentication becomes of no use when faced by the man in the middle attack where phisher can modify the bank account number and total amount of money to be transferred. This statement is currently only partially true as in the Netherlands, the banks (e.g. Rabobank) verify the total amount the customer is transferring by asking him to input the amount into his hardware security device (provided by the bank). The key the hardware security device generates is then only valid for that specific amount of money thus only the unmodified amount would be authorized.

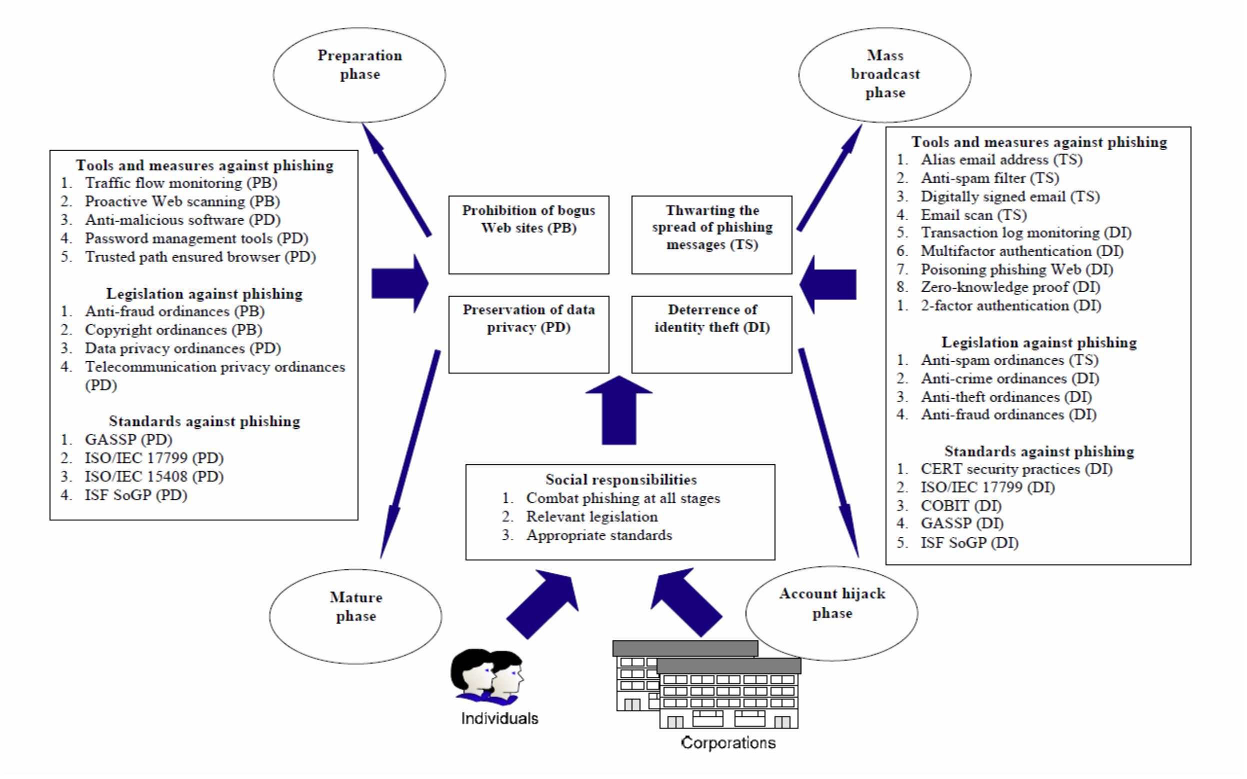

Preparation phase
Mass broadcast phase
Mature phase
Account hijack phase
Tools and measures against phishing
1. Traffic flow monitoring (PB)
2. Proactive Web scanning (PB)
3. Anti-malicious software (PD)
4. Password management tools (PD)
5. Trusted path ensured browser (PD)
Legislation against phishing
1. Anti-fraud ordinances (PB)
2. Copyright ordinances (PB)
3. Data privacy ordinances (PD)
4. Telecommunication privacy ordinances (PD)
Standards against phishing
1. GASSP (PD)
2. ISO/IEC 17799 (PD)
3. ISO/IEC 15408 (PD)
4. ISF SoGP (PD)
Prohibition of bogus Web sites (PB)
Thwarting the spread of phishing messages (TS)
Preservation of data privacy (PD)
Deterrence of identity theft (DI)
Tools and measures against phishing
1. Alias email address (TS)
2. Anti-spam filter (TS)
3. Digitally signed email (TS)
4. Email scan (TS)
5. Transaction log monitoring (DI)
6. Multifactor authentication (DI)
7. Poisoning phishing Web (DI)
8. Zero-knowledge proof (DI)
1. 2-factor authentication (DI)
Legislation against phishing
1. Anti-spam ordinances (TS)
2. Anti-crime ordinances (DI)
3. Anti-theft ordinances (DI)
4. Anti-fraud ordinances (DI)
Standards against phishing
1. CERT security practices (DI)
2. ISO/IEC 17799 (DI)
3. COBIT (DI)
4. GASSP (DI)
5. ISF SoGP (DI)
Social responsibilities
1. Combat phishing at all stages
2. Relevant legislation
3. Appropriate standards
Individuals
Corporations

Figure 1. Anti-phishing framework by Bose and Leung (2007)

Dhamija et al. (2006) focused on the question of why phishing works. They performed a lab experiment with 22 participants and asked the subjects to decide which of the 20 showed websites were fraudulent and why. The results showed that a good phishing website was able to fool 90% of the participants and more noteworthy no significant correlation was found between education, age, sex, previous experience, hours of computer use and the susceptibility to phishing. Other important finding was that 15 out of 22 participants ignored pop warning about self signed certificate, proving this type of warnings ineffective.

Downs et al. (2006) performed an interview study about the strategies and susceptibility to phishing with 20 participants. Participants were chosen by their level of expertise in computer security and only those inexperienced were selected. The results for this study revealed that inexperienced computer users applied 3 simple strategies for whether to trust an email of to be suspicious of it. The strategies found were: 1) this email appears for to be for me, 2) it's normal to hear from companies you do business with and 3) reputable companies will send emails. Downs et al (2006) concluded that these strategies would not work for spear phishing attacks, where the phishing emails are personalized to appear more trustworthy. Other significant finding of Downs et al (2006) was that the amateur users ignored the pop up warning about security issues in browsers because they didn't require any further action to be taken by user.

Bose and Leung (2013) conducted a research on the impact on firm value of adoption of anti-phishing measures, referred in this study as identity theft countermeasures (ITC). It was found that on average the firm's stock prices would increase by 0.63% as a result of an announcement of adoption of ITC. The other finding was that early adopters of ITC received higher reward than late adopters. In addition the type of ITC adopted had also effect on stock price, specifically sophisticated security measures like two factor authentication had significant positive effect, measuring 0.69% increase in stock price. The study concluded that the increases in stock prices as effect of ITC adaptations are due to shareholder recognizing the firm's actions to care about the security of their customers.

Baker et al. (2007) zeroed in on the question of what online public relations strategies organizations are implementing to combat phishing. Research focuses on top 10 companies most affected by phishing. Public relations strategies are measures aimed to help organizations protect online information of the users, recommended by anti-phishing advocacy organizations including APWG, TRUSTe, FraudWatch International, CyberTrust and the Federal Trade Commission. Study revealed that the most used strategy was to list the types of information that the organization will not ask their customers (e.g. account number, password, social security number). Second most used strategies were describing steps for protection against phishing and providing examples of current phishing techniques, then followed by providing links to other phishing awareness information, providing examples of phishing emails and the inclusion of a phone number to report suspicious email. None of the top 10 companies made a permanent email for contact about phishing available on the website and only one company indicated which media will be used for customer contact or what information they will ask for. The final important finding was that none of the organizations used the strategy of putting the term “phishing” on their homepage.

Berghel (2006) wrote an article about the differences in phishers. By presenting examples of phishing emails he categorized phishers in two categories: posers and mongers. Posers are phishers that create phishing emails without putting much effort into it, resulting in emails that are easily detected by most people. Monger on the other hand use smart techniques to trick even semi-experienced users. They are responsible for the most of global financial losses caused by phishing. Berghel (2006) concluded that unfortunately even most silly phishing emails made by posers do occasionally catch phish.

Blythe et al. (2011) analyzed 100 phishing emails, collected in the span of five days from 26th to 31st October 2009. The results of this analysis show that only 11% of these email contained more than three spelling mistakes, 50% contained one or two and 38 % contained no spellings errors at all. 64% of the emails contained the logo of the spoofed company. Furthermore 82% spoofed financial organizations and 75% used “security updates” as pretext for contacting. In addition Blythe et al. (2011) conducted online phishing survey with 224 participants. The survey consisted of genuine spam and phishing email and the participants had to distinguish them, first based on subject line only then base on whole email. The results showed that participants were more accurate at correctly determining phishing emails base one whole email than just the subject line. Other important finding was that existence of a logo in phishing emails significantly lowered the accuracy for correctly detecting phishing email.

Publication	Summary of important findings / conclusions
Dhamija et al. (2006)	Education, age, sex, previous experience, hours of computer use had no effect on phishing susceptibility. Pop-up warnings in browsers proved ineffective.
Bose and Leung (2007)	Phishing attacks divided in four stages: preparation, mass broadcast, mature and account hijack. Anti-phishing framework is presented that highlights various techniques to disrupt four stages of phishing.
Jagatic et al. (2007)	Spear phishing attack proved very successfully, revealing the dangers of publicly disclosing personal information.
Vishwanath et al. (2011)	Analyzed susceptibility to phishing attacks, concluded that urgency cues, email load and habitual media use have positive effect on phishing susceptibility, while computer self-efficacy has none on susceptibility to phishing.
Hong (2012)	Presented overview of current state of phishing and predicted increase of spear phishing attacks.
Downs et al. (2006)	Defined strategies in determining credibility of emails used by users with low experience with computer security.
Berghel, H. (2006)	Categorized phishers in two categories.
Baker et al. (2007)	Revealed what public relation strategies are implemented by companies most affected by phishing.
Blythe et al. (2011)	Showed that spelling error aren’t a defining part of phishing emails. Found that logos increased susceptibility to phishing emails.
Bose and Leung (2013)	Adoption of anti-phishing measures by firm has proven to have positive effect on short term market value.

Table 2. Summary of major findings / conclusions in selected publications

2.3 Conclusion

The literature study has revealed several surprising findings (Table 2). Vishwanath et al. (2011) found that computer self-efficacy did not have any effect on phishing susceptibility. But Jagatic et al. (2007) noted that the students of computer science, informatics and cognitive science (technology majors) were least susceptible to phishing attack. This might suggests that very high computer self-efficacy can indeed have an effect on susceptibility to phishing, something that Vishwanath et al. (2011) might have missed. This apparent discrepancy in observations is the reason this thesis will also research the effect of self-efficacy on phishing susceptibility. Bose and Leung (2007) presented anti-phishing framework that helps to understand the place of certain anti-phishing measures in different phishing phases, while Hong (2012) and Vishwanath et al. (2011) presented the phishing phenomenon in a transparent fashion revealing its inner workings. Dhamija et al. (2006) conducted one of the earliest studies about phishing, investigating the ability of participants to detect phishing websites. The results showed that while the participants were stimulated to detect phishing websites, 90% of them failed to correctly detect the best phishing website. This result showed the dangers of phishing websites. Furthermore both Dhamija et al. (2006) and Downs et al. (2006) found that pop-up warning in browsers were ineffective. Additionally Blythe et al. (2011) revealed that spelling errors aren't necessary a defining part of phishing emails, and that logos in phishing emails can improve their success rate.

While most literature focused on individuals, two studies in this literature review focused on businesses. Bose and Leung (2013) discovered that financial advantage can be achieved by adopting anti phishing measures, while Baker et al. (2007) revealed which public relations strategies companies use to fight against phishing.

All journal articles covered in this review that conducted survey studies focused on detecting the phishing websites or emails. However none of them concentrated on the awareness of phishing amongst the participants. Therefore the exploratory survey performed in this thesis, researching awareness of phishing under the Dutch population, has evident scientific contribution. Furthermore based on finding and observations of Dhamija et al. (2006), Jagatic et al. (2007) and Vishwanath et al. (2011), gender, age, email load and previously mentioned computer self-efficacy are measured against phishing susceptibility to determine correlation. The inclusion of gender, age and email load measures in this study provides more insights into the possible effects on phishing susceptibility of Dutch people, moreover it serves as a link to prior research.

The next chapter provides insights in phishing and anti-phishing measures while chapter 4 presents exploratory survey and the results.

Chapter 3 Insight into phishing

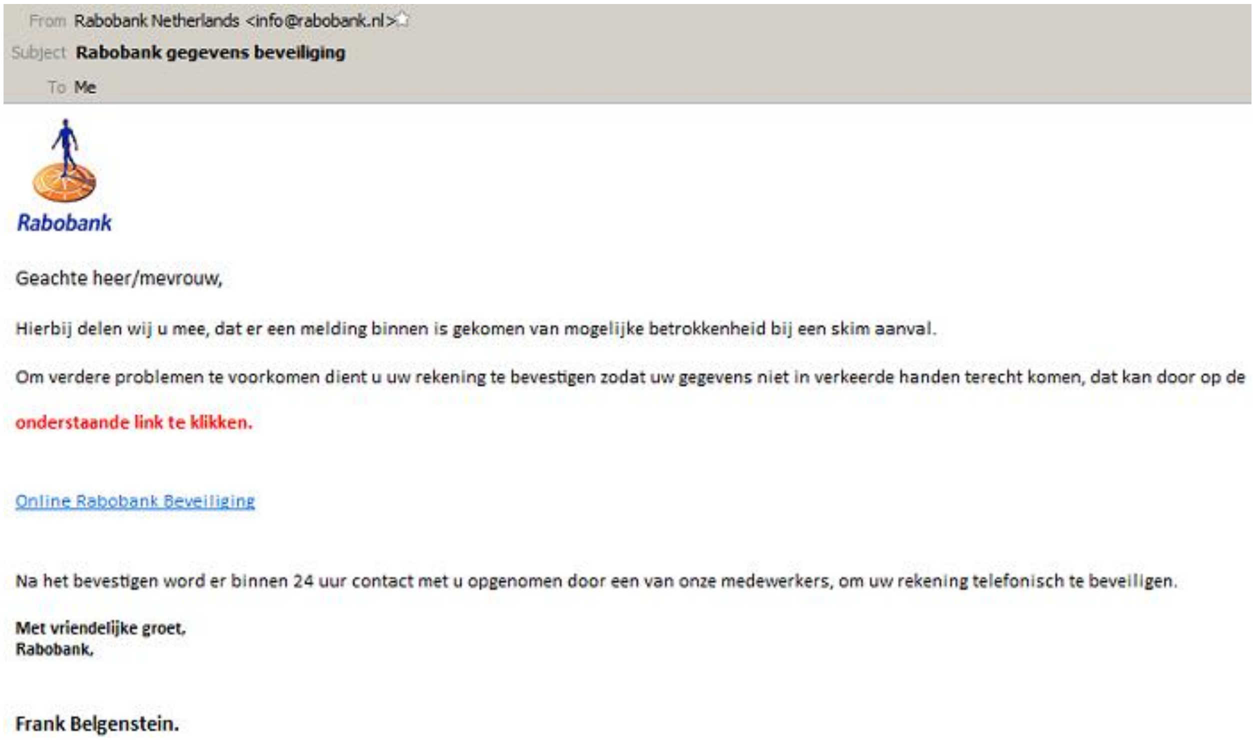
3.1 What is Phishing ?

The word "phishing" comes from the analogy that Internet scammers are using email lures to "fish" for passwords and financial data from the sea of Internet users.[4] The term was invented around 1996 by hackers who were stealing America On-Line accounts by tricking the AOL users to send their passwords. Phishing was first mentioned on the Internet on the alt.2600 hacker newsgroup in January 1996 but it was probably used earlier in the printed version of the hackers “2600” newsletter. The letters “ph” are commonly used by hackers as a replacement for the letter “f” and this stems from the word “phreaking” from the 70’s which was invented by the famous hacker John Draper (aka Captain Crunch). Phreaking meant hacking the telephone system so that it was possible to make free phone calls. By 1996, hacked accounts were referred to as “phish” and the year later phishes became hackers’ form of currency. Hacker would then for instance trade 10 phishes for hacking software that they needed.

3.2 Phishing attacks

In recent years the typical phishing attack take place through email, where the sender of the message is spoofed to an existing email that belongs to a real company, financial institution or other trustworthy source. (Fig. 2) The text of a phishing email always asks you to click on a link and usually contains urgency cues, words that invoke feelings of vulnerability or threat, to try to force the recipient to act impulsively. The embedded link is often disguised to look like a link to a genuine website but in reality it directs user to a fraudulent website. Fraudulent websites will try to make the victim believe that he’s on a familiar website, by copying the look and feel of the real website, in order to gain his trust and then persuading him to give away his personal information. The spear phishing attacks are phishing attacks that target specific (group of) users. Spear attacks are more dangerous because phishers use previously obtained personal information to make the phishing email appear more personal hence increasing the chance of gaining the trust of the recipient.

[4] Anti-Phishing Working Group (2013). Origins of the Word "Phishing" . Available At: http://docs.apwg.org/word_phish.html



From Rabobank Netherlands <info@rabobank.nl>

Subject **Rabobank gegevens beveiliging**

To Me

Rabobank

Geachte heer/mevrouw,

Hierbij delen wij u mee, dat er een melding binnen is gekomen van mogelijke betrokkenheid bij een skim aanval.

Om verdere problemen te voorkomen dient u uw rekening te bevestigen zodat uw gegevens niet in verkeerde handen terecht komen, dat kan door op de **onderstaande link te klikken.**

Online Rabobank Beveiliging

Na het bevestigen word er binnen 24 uur contact met u opgenomen door een van onze medewerkers, om uw rekening telefonisch te beveiligen.

Met vriendelijke groet,
Rabobank,

Frank Belgenstein.

Figure 2. Example of phishing email targeting customers of Rabobank

3.3 Detecting phishing

There are several techniques one can use to help detect phishing emails.
One is to check to email for spelling errors. Phishing emails often contain some obvious spelling mistakes, a respectable company or financial institution would not send emails without spell checking them first. It is usually a good indicator that something is phishy about an email.
As stated before, another big characteristic of a phishing email is that it often disguises the actual address of the URL. Phishers use html syntax in phishing emails to hide the true address of the link, the hyperlink displayed as “www.realbank.com” can be easily directed to www.fakebank.com. To detect this kind deception one has to look in the email source code for the actual URL or to move the mouse cursor over the link and see what URL appears in the status bar of the browser or email client. It’s also very important to not get deceived by the domains the phishers might use. Phishers often use visually similar domains to host their bogus website. In such cases the redirected URL might not be as obvious as “www.fakebank.com” but for instance “www.reallbank.com” (with double L’s).

3.4 Anti-Phishing measures

For combating phishing attack companies use various anti-phishing measures.
Email service providers (ESP), such as Google Gmail, Microsoft Outlook or Yahoo! Mail, make use of email filters to filter out phishing emails before they get into user’s inboxes. In an effort to make the email filters as accurate as possible, most ESP’s now allow users to report phishing emails if they detect one. After a reported email is verified as phishing by ESP it’s added to the email filter and from this moment this email will not land in other users inboxes.

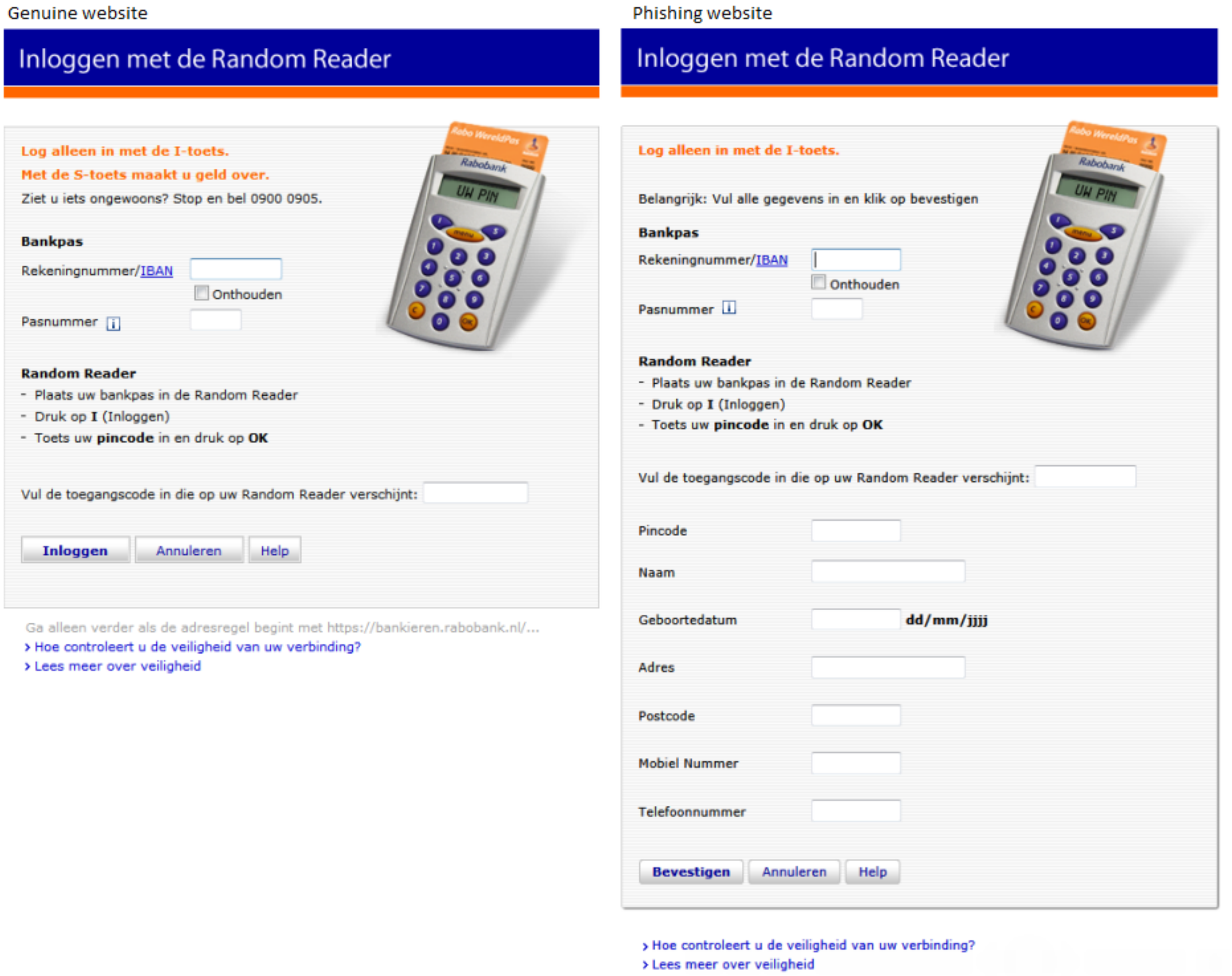
Banks on the other hand monitor and analyze the transaction logs of their customers. If an unusual transaction occurs, the account or the internet address in question will be suspended and bank will seek contact with the owner of the account in question. Unusual transaction include for instance wiring of large amounts of money from a location that wasn't previously associated with that account, or wiring money from multiple different accounts from one location. To improve security of authorization, for accepting a transaction for example, most banks now offer two-factor authentication (2FA) or one-time password (OTP). A single password login means that when it lands in the hands of a criminal it can be used to gain access to users account. With 2FA and OTP this is no longer possible as a user needs to input two passwords, one that he knows and one that is generated randomly for one transaction only. 2FA usually uses a hardware security device to generate a password and OTP is usually send by the bank to user in the form of a text message (SMS) to users mobile phone. Because randomly generated passwords are valid for one session, even if a criminal intercepts both passwords, the combination of the two will no longer be valid.

Security companies monitor newly registered domains and compare these newly created domains to the domains of their clients (other businesses). If the newly created domain is similar to the client's domain, further visual check will be carried out to spot phishing websites. If one is spotted they can ask the ISP to bring down the website and report the website to DNS providers like OpenDNS (PhishTank) and Google.

The individual users also have several tools at their disposal to guard themselves against phishing attacks. User can use password management tools to remember a password on a website. On the next visit the tool will automatically fill in password field. As the tool recognizes the websites by it's unique IP address it will not fill in the password on a phishing website, alerting the user this way that the shown website is not what he thought it was. Using an anti-virus software is also a valid method to protect yourself against phishing attacks. It guards against, already mentioned in the introduction, credential stealing malware that some phishing websites will try to install. Installing an anti-spam filter software is another valid option as such software will detect and delete suspicious mail before it reaches the user.

3.5 Modern phishing attacks

Today, phishing attacks have grown from simply stealing dialup accounts into much bigger criminal operation. Phishing attacks now target clients of online banks, online payment services such as PayPal and other e-commerce businesses such as Amazon or eBay. The number of phishing attacks is growing rapidly and to date most major banks in the world have already been targeted by phishers. In the Netherlands the recent attacks have targeted users of DigiD and Rabobank (Fig. 2). In both cases users were asked to verify their credential because of some unexpected circumstances by following the embedded link. Figure 3 illustrates the differences in login screens of Rabobank website. Visually both phishing and genuine versions appear the same; the only difference is the number of information fields to fill in. And naturally phishing website is trying to gather as many information as possible. These kinds of attacks are becoming more frequent in the Netherlands, following the global trend. According to Statistics Netherlands[5] (CBS) 58.000 Dutch people fell victim of phishing fraud in 2012 and according to Online Fraud Report of RSA[6], the Netherlands had 9th place globally in consistently hosting most phishing attacks over 2012.



Genuine website

Inloggen met de Random Reader

Log alleen in met de I-toets.
Met de S-toets maakt u geld over.
Ziet u iets ongewoons? Stop en bel 0900 0905.

Bankpas
Rekeningnummer/IBAN
□ Onthouden
Pasnummer

Random Reader
- Plaats uw bankpas in de Random Reader
- Druk op **I** (Inloggen)
- Toets uw **pincode** in en druk op **OK**

Vul de toegangscode in die op uw Random Reader verschijnt:

Inloggen | Annuleren | Help

Ga alleen verder als de adresregel begint met https://bankieren.rabobank.nl/...
› Hoe controleert u de veiligheid van uw verbinding?
› Lees meer over veiligheid

Phishing website

Inloggen met de Random Reader

Log alleen in met de I-toets.

Belangrijk: Vul alle gegevens in en klik op bevestigen

Bankpas
Rekeningnummer/IBAN
□ Onthouden
Pasnummer

Random Reader
- Plaats uw bankpas in de Random Reader
- Druk op **I** (Inloggen)
- Toets uw **pincode** in en druk op **OK**

Vul de toegangscode in die op uw Random Reader verschijnt:

Pincode
Naam
Geboortedatum **dd/mm/jjjj**
Adres
Postcode
Mobiel Nummer
Telefoonnummer

Bevestigen | Annuleren | Help

› Hoe controleert u de veiligheid van uw verbinding?
› Lees meer over veiligheid

Figure 3. Phishing website example. Genuine Rabobank login on the left, phishing version on the right

Chapter 4 of this thesis presents the exploratory survey performed to provide more insight into the awareness of phishing in the Netherlands.

Chapter 4 Survey and results

4.1 Introduction

[5] Statistics Netherlands (2013). “More than 200 thousand victims of skimming or phishing” Available At: http://www.cbs.nl/en-GB/menu/themas/veiligheid-recht/publicaties/artikelen/archief/2013/2013-3912-wm.htm

[6] EMC Corporation (2013). RSA Monthly Online Fraud Report -- January 2013. Available At: http://www.emc.com/collateral/fraud-report/online-rsa-fraud-report-012013.pdf

To be able to answer the research question, *“To what extent are people in the Netherlands aware of phishing and the risks of phishing ?”* and the related sub-question, a web-based survey is conducted. This survey has as objectives firstly to find out if people in the Netherlands are aware of phishing, secondly whether they have a clear understanding of the phishing phenomenon and if they were affected or not (financially) by phishing scams. The first objective is thus answering the research question and supporting sub-questions. Second objective is to test a number of findings which emerged from the literature review, more specifically in the context of the Netherlands. In doing so, this research links up with prior studies.

4.2 Development of measures

The important variables that need to be defined in order to develop hypothesis and understand the reasoning behind survey question are: susceptibility to phishing, phishing awareness, computer self-efficacy and email load.

Susceptibility to phishing is the likelihood that a person is going to get phished. Four questions were used to determine its value, first a question was asked after a participant was shown a crafty phishing email *(Fig.4)*, it is formulated as ‘*If I was a client of this company, I would click on the embedded link in this email’ with answers being on 5 point Likert scale where 1 = Strongly disagree,* second, third and fourth, a simple yes and no questions, ‘*Have you ever clicked on a link in a phishing email ?*’ , ‘ Have you ever fallen for a phishing scam ?’ and *‘Did you know email sender of any email can be falsified ?’* respectively. The value of *susceptibility to phishing was* calculated by summing all of the questions together, where yes = 1, no = 0 and scale points keep their value. The values for the fourth questions had to be inverted to reflect the same direction of relationship. Thus the levels of phishing susceptibility can be from 1 to 8, with 1 meaning not susceptible and 8 meaning very susceptible to phishing.

Phishing awareness is the knowledge a person has about the existence of phishing phenomenon and the correctness of this knowledge. To determine the value of phishing awareness 3 yes or no questions were asked. First question was ‘*Have you ever heard the term phishing before ?’* and second *‘Do you know what the term means ?*’. The third question came after the correct definition of phishing along with an example was presented to the user, it was formulated as ‘*Is the above explanation what you thought phishing was?*’. The value of phishing awareness was accordingly defined as the summation of all 3 questions where yes = 2, yes, but not sure = 1 and no = 0. Thus the levels of phishing awareness can be from 0 to 6, with 0 meaning not aware of phishing at all and 6 meaning very aware of phishing.

Email load is defined by the question *‘Estimate how many emails do you receive daily’,* which was developed and used in study by Vishwanath et al. (2011). The number of estimated daily emails is thus the measure of the *email load.*

Computer self-efficacy is a judgment of one's capability to use a computer. This measure is computed using the computer self-efficacy measure developed by Compeau & Higgins (1995), it consists of 10 questions about the confidence to complete a specific task on a 10 point scale where 1 = not at all confident, 5 = moderately confident and 10 = totally confident. The task used for this study is 'I could set up and start using a new email program'. An example of one question for *computer self-efficacy* measure would be *'I could set up and start using a new email program if someone showed me how to do it first.'* , and the measure is calculated by summing all scale points together. If the answer is 'no' then value of 0 will be assigned to the answer. The measure is calculated by summing all values together resulting in a measure scaling from 0 to 100.

4.3 Hypotheses development

It is expected that *phishing awareness* will have negative effect phishing susceptibility. The reasoning is that the more people know about phishing the less likely it is for them to fall for a phishing scam.
The hypothesis that is based on the previous argument and deductive logic is formulated as follows:

H0: 'phishing awareness has a negative effect on phishing susceptibility'

It is expected that *computer self-efficacy* will have a negative effect on phishing susceptibility. Similarly to phishing awareness, the reasoning is that the more computer know-how people have the less likely it is for them to fall for a phishing scam. It is also expected that most participants will have high computer self-efficacy because almost everybody in the Netherlands has access to a PC (95% of the households according Statistics Netherlands, 2013).The hypothesis that follows from this reasoning is:

H1a: 'computer self-efficacy has a negative effect on phishing susceptibility'

In line with Vishwanath et al. (2011), who found that computer self-efficacy has no effect on phishing susceptibility, the hypothesis H1b is formulated as follows:

H1b: *'computer self-efficacy has no effect on phishing susceptibility"*

It is expected that *email load* will have a positive effect on phishing susceptibility. The reasoning being that the more daily emails a person receives the more likely it is he will take less time to view an email, possibly missing cues about the authenticity of the email. This reasoning is in line with findings of Vishwanath et al. (2011), hence the hypothesis in the context of email load is formulated as follows:

H2: *'email load has a positive effect on phishing susceptibility'*

Dhamija et al. (2006) showed that gender have no effect susceptibility to phishing. The expectation is that this finding will also be valid in the context of the Netherlands, based on the relatively high score on the Gender Empowerment Measure (GEM)[7] of the Netherlands. The hypothesis for gender and its effect on susceptibility to phishing is thus as follows:

H3: *'gender has no effect on phishing susceptibility'*

The age is expected to have positive effect on susceptibility to phishing, based on that reasoning that older people are expected to be less knowledgeable about technological developments than younger people. The hypothesis that follows from this expectation is thus:

H4a: *'age has a positive effect on phishing susceptibility'*

In line with Dhamija et al. (2006), who also concluded that age has no effect on phishing susceptibility, the hypothesis H4b is formulated as follows:

H4b: *'age has no effect on phishing susceptibility'*

4.4 Survey set-up

The following sections provide the argumentation that forms the base for the questions used within the survey. These questions are used to ultimately test the previously formulated hypotheses and answer the research question.

4.4.1 Measurement validity

For each construct different questions are used.

To be able to answer research question *"To what extent are people in the Netherlands aware of phishing and the risks of phishing ?"*, the following survey questions are used 3, 4, 5, 6, 10, 11

To be able to answer the first sub-question "*To what degree do the people in the Netherlands know how to protect themselves against phishing"* , questions 8, 9, 12, 13, 14 are used

To be able to answer the second sub-question "*Does phishing awareness, computer self-efficacy ,email load, gender or age have effect on susceptibility to phishing in the Netherlands?*", questions 1, 2, 3, 4, 5, 7, 10, 15, 16, 19 are utilized.

Finally questions 17 and 18 determine whether the participant is located in the Netherlands or has the Dutch nationality, assuring that the results focused only on the Netherlands and Dutch

[7] Statistics Netherlands (2009) 'Dutch women among the most emancipated in Europe' Available At: http://www.cbs.nl/en-GB/menu/themas/dossiers/vrouwen-en-mannen/publicaties/artikelen/archief/2009/2009-2811-wm.htm

people. Thus if the answer to both these questions was ‘Other’, the answers of this participant would not be included in the results.

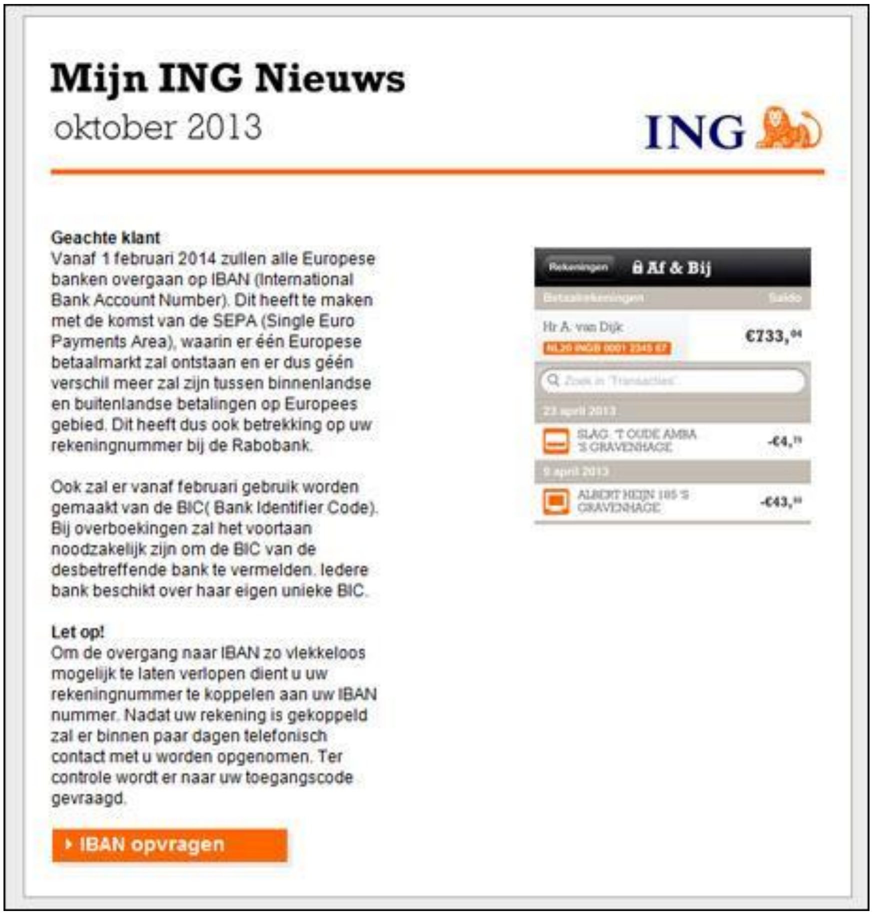
4.4.2 The survey

Survey was distributed using social sites such as facebook and twitter to gather a representative sample of responses.

The survey is constructed as follows:
First an image with a crafty phishing email is shown to the user. (Fig 4.) Then the questions follow.
1. If I was a client of this company, I would click on the embedded link in this email (IBAN aanvragen). [strongly agree / agree / neutral / disagree / strongly disagree]
Then the questions continue on the next page.
2. Estimate how many emails you receive daily. [number of emails]
3. Have you ever heard the term phishing before ? [Yes / No]
4. Do you know what the term means ? [Yes / Yes, but not sure / No]
Then follows a brief explanation of phishing with an example followed by question 5.
5. Is the above explanation what you thought phishing is ? [Yes / No]
6. Have you received phishing emails before ? [Yes / No]
    If answer to 6 is yes.
    7. Have you ever clicked on a link in a phishing email ? [Yes / No]
8. Did you know email sender of any email can be falsified ? [Yes / No]
9. Did you know you can report phishing emails to you email provider ? [Yes / No]
10. Have you ever fallen for a phishing scam ? [Yes / No]
11. Do you know anybody who fell for a phishing scam ? [Yes / No]
12. Have you ever reported phishing scam to the police ? [Yes / No]
13. Have you ever had any financial loss as a result of a phishing scam ? [Yes / No]
14. Which of the following tools do you use specifically with phishing in mind ? (Select at least one) [OpenDNS, Anti-Virus Software, Anti-spam filter, Other, None]
15. For measuring computer self-efficacy participants need to answer the question and rate his confidence; [for Yes 10 point scale where 1 = not at all confident, 5 = moderately confident and 10 = totally confident, for No, value = 0]:
    I could set up and start using a new email program ...
    Q1. ...if there was no one around to tell me what to do as I go.
    Q2. ...if I had never used a program like it before.
    Q3. ...if I had only the software manuals for reference.
    Q4. ...if I had seen someone else using it before trying it myself.
    Q5. ...if I could call someone for help if I got stuck.
    Q6. ...if someone else had helped me get started.
    Q7. ...if I had a lot of time to complete the job for which the software was provided.
    Q8. ...if I had just the built-in help facility for assistance.
    Q9. ...if someone showed me how to do it first.
    Q10.. if I had used similar packages before this one to do the same job.

Then follow multiple choice demographic questions
16. Gender [Male / Female]
17. Location [Netherlands / Other]
18. Nationality [Dutch / Other]
19. Age [0 - 11 / 12 - 17 / 18 - 24 / 25 - 34 / 35 - 44 / 45 - 54 / 55 - 64 / 65 +]

At the end of the survey the participant is offered and link with further information about phishing.



Mijn ING Nieuws
oktober 2013

ING

Geachte klant
Vanaf 1 februari 2014 zullen alle Europese banken overgaan op IBAN (International Bank Account Number). Dit heeft te maken met de komst van de SEPA (Single Euro Payments Area), waarin er één Europese betaalmarkt zal ontstaan en er dus géén verschil meer zal zijn tussen binnenlandse en buitenlandse betalingen op Europees gebied. Dit heeft dus ook betrekking op uw rekeningnummer bij de Rabobank.

Ook zal er vanaf februari gebruik worden gemaakt van de BIC(Bank Identifier Code). Bij overboekingen zal het voortaan noodzakelijk zijn om de BIC van de desbetreffende bank te vermelden. Iedere bank beschikt over haar eigen unieke BIC.

Let op!
Om de overgang naar IBAN zo vlekkeloos mogelijk te laten verlopen dient u uw rekeningnummer te koppelen aan uw IBAN nummer. Nadat uw rekening is gekoppeld zal er binnen paar dagen telefonisch contact met u worden opgenomen. Ter controle wordt er naar uw toegangscode gevraagd.

▸ IBAN opvragen

Figure 4. Phishing email included in the survey.

4.5 Results and findings

The end result is that 78 participants have completed the survey, 24 participants were excluded because of not fully completing the survey and none were excluded based on location or nationality. In fact all participants declared they were currently in the Netherlands, which was the target group for this survey. The participants were 48.7 % male (38 participants) and 51.3 % female (40 participants). All participants but one were 18 years or older, see table 3. Email load ranged from 2 to 120 (M=16.87,s.d.=18.9,var=358.6). 62 of the participants (79.5%) said they would not click on the link in the included phishing email, while 8 (10.3%) were undecided (neutral) and other 8 said they would actually click on it. Out of 78 participants, 91% (9 participants) said they heard about phishing before and 9% (7 participants) responded negatively, additionally 2 participants that heard the term phishing before didn't know what it meant. After reading the explanation about phishing, 73 participants (93.6%) confirmed that it was exactly what they thought phishing was, suggesting that a couple of the participants correctly guessed what phishing was without hearing the term before.

Age group	Frequency	Percent
12 - 17	1	1.3
18 - 24	15	19.2
25 - 34	16	20.5
35 - 44	14	17.9
45 - 54	16	20.5
55 - 64	9	11.5
65+	7	9.0
Total	78	100.0

Table 3. Ages of survey participants

Surprisingly, 30 participants (38.5%) have indicated that they have never received phishing email before (after it was explained what phishing emails are), which can be an indication that modern email filters used by ESP's are doing a decent job in stopping the phishing emails before they reach the end user. 4 participants have ever clicked click on an embedded link in a phishing email before, while 3 participants (3,8%) have stated that they have been victims of phishing scams. It is worth noting that only 1 participant out of those 3, said he clicked on a link in a phishing email suggesting that the other 2 participant were targeted using other medium than email, possibly the telephone or instant messaging. Also 3 participants have stated that they have reported a phishing scam to the police in the past. Interesting is that fact that 24 participants (30.8%) said they knew somebody who fell for the phishing scam, a much lower number than the number of victims amongst the participants. Giving the low number of phishing victims amongst the participants it's not surprising that none of the participants have suffered any financial loss as a result of phishing.

Participants proved to be relatively knowledgeable about the technical aspects of emailing as 65 participants (83.3%) are aware of the fact that a sender of any email can easily be falsified. Furthermore 43 of those who participated (55.1%) stated that they did know that phishing emails can be reported to the email service providers. Ask about the tools they used specifically with phishing in mind, 20 participants (25.6%) chose 'None', while other 30 and 20 participants chose 'Anti virus software' and 'Anti-spam filter' respectively. Nobody used 'OpenDNS' service as an anti-phishing measure, while 8 other participants chose 'Other' and all them specified what can be condensed as 'common sense'.

Phishing susceptibility level ranged from 1 to 5 (s.d.=1.90, s.d.=1.223, var=1.496) while phishing awareness value ranged from 0 to 6 (M=5.28, s.d.=1.395, var=1.945). To test H0 hypothesis that posited that phishing awareness has a negative effect on phishing susceptibility Pearson's correlation was calculated for phishing susceptibility and awareness (r = -0.127, p=0.266, N=78). It indicated the existence of weak negative relationship but no significance was achieved. Additional linear regression analysis with phishing susceptibility as dependent variable (DP) and phishing awareness as independent variable (IV) resulted in ß = -0.127 and p = 0.266 (R^2 = 0.016, SE = 1.221, DP = -0.112 * IV + 2.488). Hence, H0 was not supported by the data.

Computer self-efficacy value (calculated on basis on questions specified in 4.4.2) ranged from 0 to 100. However as it was predicted, the average computer self-efficacy value amongst the participants was relatively high, it amounted to 62.71 (s.d.=27.66, var=765.38). To test H1a and H1b, Pearson correlation coefficient for computer self-efficacy and susceptibility was computed, it equaled to 0.070 (P=0.544, N = 78). Additional linear regression analysis with phishing susceptibility as DP and computer self-efficacy as IV resulted in ß = -0.070 and p = 0.544 (R^2=0.005, SE = 1.228, DP = 0.003 * IV + 1.704) which was in line with Pearson's r. Correlation coefficient is indicating a weak relationship between without significance, hence H1a was rejected and H1b was supported by the data.

As stated before email load ranged from 0 to 120. To test hypothesis H2 that posited that email load has a positive effect on phishing susceptibility Pearson's correlation was calculated for phishing susceptibility and email load (r = -0.146, p=0.203, N=78). Additional linear regression analysis with phishing susceptibility as DP and email load as IV resulted in ß = -0.146 and p = 0.203 (R^2 = 0.021, SE = 1.218, DP = -0.009 * IV + 2.056). Coefficients indicated the existence of weak negative relationship and no significance was achieved. Hence, H2 was not supported by the data.

To test H3 that posited that gender (M=1.51, s.d.=0.503, var=0.253) has no effect on phishing susceptibility Pearson's correlation was calculated for gender and susceptibility (r = 0.129, p=0.261, N=78). Linear regression analysis with phishing susceptibility as DP and gender as IV resulted in ß = 0.129 and p = 0.261 (R^2 = 0.017, SE = 1.221, DP = 0.313 * IV + 1.424). No significance was achieved thus H3 is supported by the data.

To test H4a and H4b than posited that age has a positive (H4a) or no (H4b) effect on phishing susceptibility Pearson's correlation and linear regression analysis was used. Pearson's correlation computed for age and phishing susceptibility resulted in r = -0.154, p=0.178, N=78 while linear regression analysis with phishing susceptibility as DP and age as IV resulted in ß = -0.154 and p = 0.178 (R^2 = 0.024, SE = 1.226, DP = -0.117 * IV + 2.492). The correlation coefficient showed a weak negative relationship and no significance was achieved. Hence H4a was rejected and H4b was supported by the data.

The results of the survey illustrate that the awareness of phishing in the Netherlands is surprisingly high; almost everybody who participated in this survey was already familiar with phishing. People know they can report phishing to the police and that senders in emails can be spoofed, the latter can perhaps be explained by the high computer self-efficacy level in the Netherlands. As for susceptibility to phishing, it is unexpected to see that the participants seem ‘immune’ to phishing scams. A relatively small number of participants were fooled by the phishing email included in the survey and even fewer participants have said to have fallen for phishing scams before. Hence, unsurprising is the fact that none of the participants experienced any loss in finance as results of phishing. Unexpected discovery however was that more than half of participants did not realize that phishing emails can be reported to emails service providers, it is something that needs to be addressed in ordered to better deal with phishing targeted at people in the Netherlands. Email load has proven to have no significant effect on phishing susceptibility, this in contrast to findings of Vishwanath et al. (2011). The findings of Dhamija et al. (2006) about age and gender not having the effect on susceptibility to phishing have been tested and validated. In fact, based on the tested hypotheses, results show that none of the measures used in this survey study have had any significant effect of phishing susceptibility.

Chapter 5 Conclusion

The main goal of this thesis was to investigate phishing awareness amongst people in the context of the Netherlands and to assess the current state of knowledge with regard to phishing by performing a literature review. The latter revealed that a lacuna exist in research about phishing. None of the prior research focused on the awareness of phishing but instead almost every study directed a great deal of attention to exploring phishing detection and anti-phishing measures in different aspects. Some of the findings from prior research were tested in this thesis and rejected or supported accordingly. Two conclusions that stood out were the ones involving computer self-efficacy and email load. Computer self-efficacy, the strength of one’s beliefs in his computer abilities, was expected to be negatively related to the level of one’s susceptibility to phishing scams. Remarkably computer self-efficacy proved to have no effect on phishing susceptibility, which is in line with findings of Vishwanath et al. (2011). The possible reason for this lack of correlation could be that some people overestimate their abilities with regards to computers, which in return increased their computer self-efficacy levels and by doing so neutralizes the effects of computer self-efficacy on phishing susceptibility. Email load on the other hand was expected to have a positive effect on one’s phishing susceptibility but the results of conducted exploratory survey found that email load, like computer self-efficacy, does not affect the susceptibility to phishing. This conclusion was directly contrary to findings of Vishwanath et al. (2011) and can possibly be explained by the differences in average and standard deviation of email loads between this study (M=16.87,s.d.=18.9) and Vishwanath et al. (2011) (M=19.28,s.d.=33.26). It would seem that people in the Netherlands receive far less emails than in the US, which can be an explanation for the undetectable effect of the email load on phishing susceptibility.

The exploratory survey provided enough data to be able to assess the levels of phishing awareness in the Netherlands. The calculated levels of phishing awareness were very high; on a 7 point scale (0-6) 67.9% of participants had the highest level of phishing awareness while 16.7% had the second highest. The higher the phishing awareness level the more accurate people knew about phishing scams. Almost every participant knew what phishing was or had a correct assumption of what it is. The possible explanation for the high awareness could be increase of phishing attacks in the Netherlands, which resulted in more extensive media coverage of this phenomenon. The survey did not manage to provide an insight in the financial losses for the Dutch population, as none of the participants reported any financial losses as a result of phishing scams. In fact only 3 people said they have fallen for a phishing scam. The reason for apparent absence of financial loss under participant could be that the stolen personal information was not yet used to hijack user's account. If this should be the case, then the same survey with same participants could provide meaningful results about the financial aspect if repeated after couple of month from now.

The results of the survey have also shown that people in the Netherland are very aware of the different measures against phishing. Most are aware that the sender of any email can be falsified and that one can use anti-virus and anti-spam software as an effective tool against phishing, some even specified that they use 'common sense' as a tool to detect phishing. As stated before, very surprising finding was that more than half of people weren't aware of the fact that they could report phishing email to their email service providers. Given the presumption that Dutch people are very good at detecting phishing email, based on high levels of phishing awareness and low levels of phishing susceptibility, it is a one thing that people in the Netherlands could do in order contribute to the fight against phishing.

As mentioned previously neither gender, age, email load nor phishing awareness has proven to have any significant effect on phishing susceptibility. This can possibly be attributed to the low level of phishing susceptibility amongst survey participants.

5.1 Future research & Limitations

From the review it became clear that there is still a great deal to learn with regard to phishing. Some studies point to email load and computer self efficacy as explanatory variables for phishing susceptibility. This study however shows that these variables do only provide a limited insight into phishing susceptibility. One limitation of the study may be the sample size, which leads to the presented findings. However, that only partially explains the limited results. It seems that awareness of the actual problem plays a major role in explaining susceptibility. An agenda for future research may be in choosing other variables to measure and explain susceptibility to fishing and taking awareness of the actual problem into account when performing studies on this subject. Another suggestion is of course increasing the sample size and controlling for age, to see whether age is related to susceptibility.

5.2 Practical use of the acquired knowledge

Increasing awareness of the problem may prove beneficial. The findings of this study clearly show that awareness of - the risks involved in - phishing clearly affect susceptibility. From an economics perspective, different organizations could benefit from creating policies that create awareness of the risk involved in phishing, and therefore limiting the risks of exposure.

References

- ❏ Association for Information System. MIS Journal Rankings. Available At: http://start.aisnet.org/?JournalRankings
- ❏ Anti-Phishing Working Group (2013). Origins of the Word "Phishing". Available At: http://docs.apwg.org/word_phish.html
- ❏ Anti-Phishing Working Group (2013). Phishing Activity Trends Report 2nd Quarter 2013. Available At: http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf
- ❏ Bose, I. and A. C. M. Leung (2007). "Unveiling the Mask of Phishing:Threats, Preventive Measures, and Responsibilities." Communications of the Association for Information Systems 19: 544-566.
- ❏ Bose, I. and A. C. M. Leung (2013). "The impact of adoption of identity theft countermeasures on firm value." Decision Support Systems 55(3): 753-763.
- ❏ Berghel, H. (2006). "Phishing Mongers and Posers." Communications of the ACM 49(4): 21-25.
- ❏ Baker, E., et al. (2007). "Organizations Respond to Phishing: Exploring the Public Relations Tackle Box." Communication Research Reports 24(4): 327-339.
- ❏ Blythe, M., et al. (2011). F for fake: four studies on how we fall for phish. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Vancouver, BC, Canada, ACM: 3469-3478.
- ❏ Compeau, D. R. and C. A. Higgins (1995). "Computer self-efficacy: Development of a measure and initial test." MIS Quarterly 19(2): 189-211.
- ❏ EMC Corporation (2013). RSA Monthly Online Fraud Report -- January 2013. Available At: http://www.emc.com/collateral/fraud-report/online-rsa-fraud-report-012013.pdf
- ❏ Dhamija, R., et al. (2006). Why phishing works. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Montréal, Québec, Canada, ACM: 581-590.
- ❏ Downs, J. S., et al. (2006). Decision strategies and susceptibility to phishing. Proceedings of the second symposium on Usable privacy and security. Pittsburgh, Pennsylvania, ACM: 79-90.
- ❏ Hong, J. (2012). "The State of Phishing Attacks." Communications of the ACM 55(1): 74-81.
- ❏ Jagatic, T. N., et al. (2007). "Social Phishing." Communications of the ACM 50(10): 94-100.
- ❏ Statistics Netherlands (2013). “More than 200 thousand victims of skimming or phishing”. Available At: http://www.cbs.nl/en-GB/menu/themas/veiligheid-recht/publicaties/artikelen/archief/2013/2013-3912-wm.htm
- ❏ Vishwanath, A., et al. (2011). "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model." Decision Support Systems 51(3): 576-586.

Appendix.

Gender	Age	EmailLoad	SelfEfficacy	Awareness	Susceptibility	Q1	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14
1	4	2	83	5	1	5	1	2	1	2	2	1	2	2	2	2	2	5
2	3	4	90	6	2	4	1	1	1	2	2	1	1	2	2	2	2	5
1	4	4	72	4	4	2	1	1	2	2	2	1	2	2	2	2	2	5
2	7	20	47	6	1	5	1	1	1	1	2	1	1	2	1	2	2	3
2	6	8	23	2	1	5	2	3	1	2	2	1	2	2	2	2	2	2
2	5	7	57	6	1	5	1	1	1	1	2	1	1	2	2	1	2	2
1	5	120	60	6	1	5	1	1	1	1	2	1	1	2	2	2	2	4
1	4	5	100	6	1	5	1	1	1	1	2	1	2	2	2	2	2	5
1	6	40	100	6	1	5	1	1	1	1	2	1	1	2	1	2	2	3
2	3	10	44	4	3	3	1	3	1	1	2	1	2	2	2	2	2	5
1	5	25	74	6	1	5	1	1	1	2	2	1	1	2	2	2	2	5
1	5	6	73	6	2	5	1	1	1	1	2	1	1	1	1	2	2	2
1	5	7	62	6	1	5	1	1	1	2	2	1	2	2	2	2	2	3
2	5	100	75	6	1	5	1	1	1	1	2	1	2	2	2	2	2	5
2	7	20	60	2	1	5	2	3	1	1	2	1	2	2	2	2	2	4
2	5	25	38	6	1	5	1	1	1	1	2	1	1	2	2	2	2	5
1	4	3	10	6	1	5	1	1	1	2	2	1	2	2	1	2	2	3
1	4	5	0	6	2	4	1	1	1	1	2	1	1	2	2	2	2	3
2	8	15	100	6	3	3	1	1	1	1	2	1	2	2	2	2	2	2
2	3	6	55	6	5	2	1	1	1	2	2	2	2	2	2	2	2	5
2	3	3	49	6	1	5	1	1	1	2	2	1	1	2	2	2	2	5
2	7	8	78	2	4	2	2	3	1	2	2	1	2	2	2	2	2	3
1	5	5	52	5	1	5	1	2	1	1	2	1	1	2	2	2	2	2
2	5	10	63	6	2	5	1	1	1	1	1	1	2	2	2	2	2	3
2	6	30	61	5	2	5	1	2	1	1	2	2	2	2	1	2	2	4
2	3	4	78	6	3	4	1	1	1	2	2	2	1	2	2	2	2	5
1	7	10	49	6	5	2	1	1	1	1	2	2	2	2	2	2	2	2
1	7	25	35	5	2	5	1	2	1	1	2	2	2	2	2	2	2	2
2	4	8	100	5	4	2	1	2	1	2	2	1	1	2	2	2	2	2
1	3	7	0	6	4	3	1	1	1	1	2	2	2	2	1	2	2	2
1	5	20	68	5	2	4	1	2	1	2	2	1	1	2	2	2	2	4
2	8	3	5	5	1	5	1	2	1	2	2	1	1	2	2	2	2	2
2	6	25	21	6	1	5	1	1	1	1	2	1	2	2	2	2	2	2
2	6	8	45	6	3	4	1	1	1	2	2	2	1	2	1	2	2	2
2	8	15	26	2	1	5	2	3	1	1	2	1	1	2	2	2	2	5
2	7	25	100	6	1	5	1	1	1	1	2	1	1	2	1	2	2	4
1	6	25	65	6	1	5	1	1	1	2	2	1	1	2	1	2	2	2
2	6	6	93	6	2	4	1	1	1	1	2	1	1	2	1	2	2	3
2	3	5	71	0	4	2	2	3	2	2	2	1	2	2	2	2	2	2
1	5	50	98	6	1	5	1	1	1	1	2	1	2	2	2	2	2	3
1	3	3	85	5	1	5	1	2	1	2	2	1	1	2	2	2	2	5
2	4	12	50	0	2	4	2	3	2	1	2	1	2	2	1	2	2	5
2	5	10	61	4	5	2	1	3	1	2	2	2	2	2	2	2	2	3
2	8	10	55	3	1	5	1	2	2	2	2	1	2	2	2	2	2	3
1	3	5	100	6	1	5	1	1	1	1	2	1	1	2	1	2	2	4
1	4	30	55	6	1	5	1	1	1	1	2	1	1	2	1	2	2	3
1	3	15	100	6	1	5	1	1	1	1	2	1	1	2	1	2	2	3
1	6	10	50	6	1	5	1	1	1	1	2	1	1	2	1	2	2	2
2	4	20	65	6	1	5	1	1	1	1	2	1	1	2	2	2	2	5
1	4	18	79	6	1	5	1	1	1	1	2	1	1	2	2	2	2	4
2	3	10	0	2	1	5	2	3	1	2	2	1	2	2	2	2	2	4
2	4	6	65	5	1	5	1	2	1	1	2	1	1	2	2	2	2	2
2	6	25	45	6	1	5	1	1	1	2	2	1	1	2	2	2	2	2
2	5	20	60	4	2	5	1	1	2	1	2	2	1	2	2	2	2	2
1	8	20	60	6	3	4	1	1	1	1	1	1	1	2	1	1	2	3
1	4	29	50	6	3	3	1	1	1	1	2	1	2	2	1	2	2	5
2	4	8	100	6	1	5	1	1	1	2	2	1	2	2	1	2	2	2
1	7	5	86	5	2	5	1	2	1	1	2	2	2	2	1	2	2	2
1	6	7	71	6	1	5	1	1	1	1	2	1	1	2	2	2	2	3
2	6	35	57	6	1	5	1	1	1	2	2	1	1	2	2	2	2	3
2	3	5	100	5	1	5	1	2	1	2	2	1	1	2	2	2	2	5
2	6	35	57	6	3	3	1	1	1	2	2	1	1	2	2	2	2	3
1	6	6	100	6	1	5	1	1	1	1	2	1	1	2	2	2	2	2
2	3	10	94	6	2	4	1	1	1	2	2	1	2	2	2	2	2	2
1	7	20	50	6	2	5	1	1	1	1	2	1	1	1	1	1	2	2
1	2	10	86	6	3	3	1	1	1	2	2	1	1	2	1	2	2	2
2	3	7	84	6	4	3	1	1	1	1	2	2	2	2	2	2	2	3
1	7	15	76	6	1	5	1	1	1	1	2	1	2	2	2	2	2	2
1	4	4	80	6	1	5	1	1	1	1	2	1	2	2	2	2	2	2
2	6	25	71	5	5	4	1	2	1	1	1	2	2	1	2	2	2	2
1	8	20	0	5	1	5	1	2	1	1	2	1	2	2	2	2	2	2
1	8	10	15	6	1	5	1	1	1	1	2	1	2	2	1	2	2	5
2	6	2	36	6	1	5	1	1	1	1	2	1	1	2	2	2	2	3
2	6	10	37	6	2	5	1	1	1	2	2	2	2	2	2	2	2	3
1	4	40	100	6	2	5	1	1	1	1	1	1	1	2	2	2	2	5
1	4	20	62	6	1	5	1	1	1	1	2	1	1	2	1	2	2	5
1	3	5	74	6	4	2	1	1	1	2	2	1	1	2	2	2	2	2
1	5	50	95	6	3	3	1	1	1	1	2	1	1	2	1	2	2	2

Survey data of 78 participants.