Phishing prevention in mobile messaging platforms by the Dutch banking sector

Bachelor thesis

August 5th, 2021

Author:
Valentijn Bieger

Supervisors:
Dr. G.J. Ramackers
Drs. P.M. Kwantes

Universiteit Leiden

Abstract

After a previously declining trend, innovation in mobile phishing attacks has resulted in fraud rising from 3,81 million euro in 2018 to 7.94 million euro in 2019 in the Netherlands. This research focuses on phishing prevention methods for mobile messaging platforms. On the basis of literature study and a survey of mobile platform users, a number of technical and psychological anti-phishing measures are identified in the form of phishing detection software and subject areas for user training, respectively. Both kind of measures are essential to reduce the level of successful phishing attacks.

These anti-phishing measures must be provided by an institution that people trust. Results from the survey show people consider the bank as both trustworthy, as well as accountable for any resulting damages. Two technical anti-phishing measures appear to offer the best accuracy to detect and remove phishing messages: 'Dendritic Cell algorithm based approach' and 'spam detection using content based features'. Such technology could be incorporated within a mobile banking application or as a separate mobile application that checks messages for phishing activities based on embedded links, suspicious numbers or content. We furthermore recommend that bank institutions provide training on the following subjects: i) The manner in which the bank interacts with customers through mobile platforms ii) The methods through which phishing methods are applied. iii) How phishing messages can be detected.

Acknowledgements

This thesis is part of the bachelor study Computer science and Economics. This bachelor program is a study at the Leiden University. My two mentors for this thesis are dr. G.J. Ramackers and drs. P.M. Kwantes. I would like to thank them for the feedback during this period. An industry expert and employee of a Dutch bank, Rabobank, was willing to review my thesis and sent feedback. Therefore, a special thanks to E. Ruts. l would also like to thank the respondents of the survey.

Index

1. Introduction

This research focusses on mobile phishing in messaging platforms and how to prevent it for banking customers. Phishing is defined as: “phishing is a scalable act of deception whereby impersonation is used to obtain information from a target” (Lastdrager, 2014).
People get tricked into thinking they preform acts for someone they trust e.g. a bank. They transfer money, give personal information or download malicious software (Jansen and Leukfeldt, 2015). This results mostly in financial damage. Anti-phishing measures should be used to stop these phishing attacks.
This research focusses on mobile phishing where mobile phones and messaging platforms are used for phishing attacks. The banking sector and the government are using security measures and campaigns to raise phishing awareness. The problem is both with securing the data, but also preventing people to comply with phishing methods. This research will be about what anti-phishing measures should be used to reduce phishing victimization and which institution should implement these measures.

1.1 Social relevance

The various ways to conduct phishing results in multiple ways to counter these phishing methods. In the last few years financial damage due to mobile phishing showed an increase of 3,81 million euro in 2018 to 7,94 million euro in 2019 (Beugel, 2019). The years before that showed a decrease up to this point. This recent trend shows mobile phishing is rising and therefore better protection is needed.

Trends

Phishing techniques shifted over time from bulk spam emails to targeted email phishing, texting and/or using new apps such as “Tikkie” or payment requests. Attackers exploit trends such as the development of software like banking apps or f.e. the Covid-19 global pandemic. A research shows some recent trends about mobile phishing within our scope (Bhardwaj et al., 2020).

1. 60% of companies reported mobile phishing attacks through messaging platforms.
2. Every 20 seconds a new phishing portal is launched and these also include trends as Covid-19 related phishing. Between January and March 2020 5100 Covid-themed domains were registered globally.
3. 74% of the phishing attacks involved the HTTPS protocol. The use of this certification was 51% in 2019. HTTPS suggests that a link is secure, which attackers use to trick people.

4. Nearly 60% of all data breaches are due to human error. Even when people are trained they still fell prey to phishing attacks. This data included trained and untrained people.
5. 40% of the untrained employees at company's frequently failed phishing tests.

Phishers use trends to get people's attention and gain their trust to get what they want (Soymeal and Hammed, 2020). These attacks are not by "random" hackers. These people are skilled and know what they want and where to get it for financial gain, trade secrets, or anything else they want. There are many anti-phishing measures for SMS, but not yet for newer messaging platforms such as WhatsApp.

As mentioned above also payment request are being send by attackers. Recent development makes mobile money transfer easy. Attackers try to mislead people by sending them text or emails like fig. 1.

Fig. 1: Phishing payment request example (Nos, 2020)

1.2 Academic relevance

For this study, two perspectives are researched.

The first perspective is about security. People could use programs to detect and remove phishing messages. Even though there are programs to help people combat phishing, these are not frequently used. Research states: "Do customers in general and more specifically victims protect themselves adequately against online banking threats and how (awareness, skills, online safety cues, security software)?". They also show besides the possible anti-phishing programs their existence doesn't result in full prevention of phishing (Alsayed and Bilgrami, 2017).

This leads to the second perspective, human behaviour. Besides the offered protection there is also a need for phishing awareness. Research has shown that the ultimate protection of information is human behaviour (Rhee et al., 2008). To validate this statement in case of

phishing attacks research with elders was conducted. We see that trained people were able to detect and therefore prevent phishing (Alwanain, 2020). After this research, the question still remains whether younger age groups that have more digital knowledge would also perform better when being trained on awareness.

Research on the Dutch banking sector shows all types of people are targeted for phishing attacks. They also state: "Future research is needed to assess how customers can be trained to effectively mitigate phishing scams and whether customers are the right unit of analysis to target with interventions for combating malware attacks." (Leukfeldt and Jansen, 2016). This shows the lack of knowledge in how to improve human behaviour on this matter.

Another research shows various ways of phishing are used on mobile platforms and there are also many solutions (Goel and Jain 2018). They conclude that the current educational software or trainings are not sufficient. Therefore research is needed to assess how people should be helped to reduce phishing victimization.

Also research raises the question on who should counter phishing attacks (Leukfeldt and Jansen, 2016). They stated: "Furthermore, it is important to answer the question of whose responsibility it is" which referred to which party should counter phishing attacks.

In short as literature shows the importance of increased awareness, the lack of knowledge on how to counter message phishing and who should counter phishing attacks lay foundation for this research.

1.3 Research questions

As described in section 1.1 mobile phishing is rising and creates financial damage. Therefore anti-phishing measures have to be found and this paper focusses on mobile phishing in messaging platforms. By evaluating existing literature described in section 1.2 there were unanswered questions regarding phishing. Given these questions two research questions were formed in this paper.

The first research question states: "What anti-phishing measures should be used to reduce phishing victimization in the Dutch banking sector?". Prior research concluded further research should assess how to train people and what technical measures should be used to reduce phishing victimization.

The second research question states: "Which institution should implement anti-phishing measures in mobile messaging platforms?". The paper of Leukfeldt and Jansen shows this question is not answered yet.

These questions will result in recommendations for practical solutions on how to reduce phishing victimization.

1.4 Research methodology

The research methodology exists of literature study (desk research) in combination with a survey (field research).

The literature study will gather information about the following subjects: mobile limitations, messaging platforms, phishing within messaging platforms, human behaviour in phishing, phishing anti-phishing measures and legal.

A survey will be conducted to evaluate the aforementioned subjects and gain new insights. To answer the research questions the literature review is supplemented with additional information from the survey: Concerning the current awareness of people, what anti-phishing measures they already use, their willingness for anti-phishing measures and their trust in different parties e.g. the government or bank.

1.5 Thesis outline

This first section contains the introduction of this thesis, social and academic relevance, the research questions and the research methodology.

Section 2 contains the theoretical framework which includes:

1. Mobile limitations; mobile devices have their limitations that are exploited by phishing attackers. This section focusses on what limitations cause mobile phones to be targeted by phishing attacks.
2. Messaging platforms; to get messages on your mobile device applications are needed. This section discusses multiple messaging platforms, the usage and trust of users in these platforms.
3. Phishing within messaging platforms; information will be gathered about the types of phishing used at mobile messaging platforms. Mobile phishing will be examined. There are various techniques used for mobile phishing. This research needs to know which ones applies to messaging platforms.
4. Human behaviour in phishing; information is gathered about the human behaviour in phishing. The biases and methods used in phishing are researched. Knowing which methods occur the most and why people comply to these methods will give insights in the human thought process. This will help targeting the anti-phishing measures more precise.

5. Anti-phishing measures; information is gathered about anti-phishing measures in this section. For this research we want to find psychological and technical anti-phishing measures. By mapping out current anti-phishing measures we know how to reduce phishing victimization.
6. Legal side of phishing; the Netherlands has legislation on privacy and accountability. For this research we have accessed these in order to counter phishing within the legal boundaries. Also, the legal responsibility will be researched.

Section 3 describes the survey design:

1. At first the background of the participants is investigated. This includes age groups and gender.
2. In the second subsection, the message platform usage is questioned to find what the most used platforms are.
3. In the third subsection, participants are questioned whether they encountered phishing before and how this changed their behaviour.
4. This continues into the fourth subsection, where the way they analyse messages is questioned.
5. Banking procedure knowledge is tested in the fifth subsection. This results in knowledge about the clarity of the banking channels.
6. The sixth subsection tests willingness for anti-phishing measures. Whether participants are open for technical and training solutions.
7. The seventh subsection is about accountability and who participants think should be held accountable for preventing phishing.

Section 4 contains the results of the survey which is structured equally as the survey design. It also includes the survey's conclusion.

Based on the results of the research, section 5 contains recommendations about the research questions.

The last section, 6, contains the conclusion and the subsections:

1. Discussion; findings and recommendations are discussed which are taken to an elaborated scope.
2. Limitations; the research its limitations are discussed.
3. Future research; possible research is discussed.

2. Theoretical framework

In this section, the following subjects will be discussed: mobile limitations, messaging platforms, phishing within messaging platforms, human behaviour in phishing, anti-phishing measures and the legal side of phishing.

2.1 Mobile limitations

Smartphones have gained significantly more functionality over the past ten years. Due to their small size, long battery life and portability the use of smartphones is more prevalent (Foozy et al., 2013). The easy use and availability of smartphones also had its part. Due to its many functionalities not only young people but all age groups use smartphones. Phishing innovates and adepts all the time and also smartphones became a target. The attackers send messages on platforms containing links to webpages or applications that ask for personal information etc. (CAPEC, 2017). Due to the vulnerabilities of the smartphone attackers can easily send this to users. First, the screen size of a smartphone is small. The small screen makes it harder to check the legitimacy of a page or full URLs in a mobile browser. Second, a smartphone contains a significant amount of personal data. Due to the development of banking applications the mobile phone also contains banking information. Third, most mobile phones have an open source platform such as Android. Attackers can develop applications which trick users into giving or even steal information. Users can also download these apps for free. Attackers tend to trick users into making a legitimate application and modify the application to include malicious content. Fourth, mobile applications have simple login interfaces. Attackers can easily mimic these pages so users enter their credentials (Goel and Jain, 2018). Fifth, mobile users are less aware of security options or don't take them serious. If awareness is risen this could stop or prevent phishing attacks.
Due to the above mentioned, an attacker can easily target mobile users with phishing attacks (Tewari et al,. 2016).

2.2 Messaging platforms

The Netherlands has 13,7 million people active on one or more social media applications. The most used platform is WhatsApp with 12,4 million users. In figure 2, the top 10 social media applications are shown. These applications all have messaging functionalities.

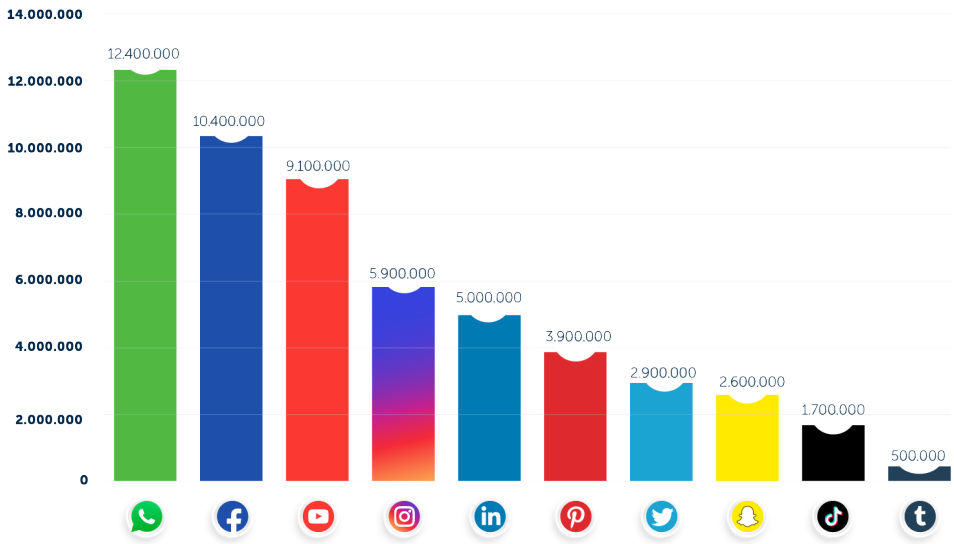

Fig. 2: Statistics of the amount of social media users in the Netherlands (Team Coosto, 2021)

Fig. 3: Statistics of trust level of user on various messaging platforms (Proofpoint, 2017)

Figure 3 shows the trust level of users on different messaging platforms. The most trustworthy channel is SMS according to 35% of the users. Followed by platforms such as WhatsApp and Instagram with 28%. WhatsApp is used by almost all mobile users in the Netherlands and with a high trust level this could indicate why message phishing is effective.

2.3 Phishing within messaging platforms

As shown, messaging platforms are used by many mobile users. Due to mobile limitations and the high trust level, it became target for phishing. 81% of the mobile phishing attacks used mobile applications, SMS, or websites (Wandera, 2017).

2.3.1 Smishing

One of the most popular methods at this moment are phishing attacks through SMS or other messaging platforms. This is called smishing and the goal is to steal personal and financial

information. These attacks have exponentially risen over the past few years. Smishing messages contain text with a link and when opened the user is forwarded to a fake website or a malicious program is installed (Choudhary and Jain, 2017). Through social engineering users are targeted and appealed to give information or follow the attacker's guiding. There is a significant amount of methods for detecting URLs in SMS but these URLs are changed frequently (Joo et al., 2017). Personalised phishing techniques are successful when the source of the message seems to be trustworthy, the information within the message seems valid and the request seems logical (Goel and Jain, 2018). Figure 4 shows an example of someone getting a phishing text.

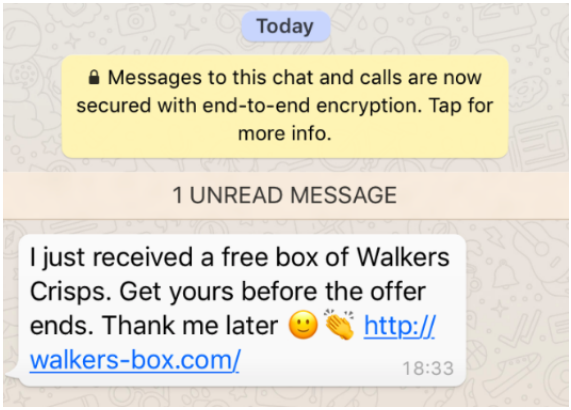

Fig. 4: WhatsApp phishing message example (Wandera, 2018)

2.3.2 Phishing links

Phishing links are links from attackers that redirect the users to a malicious website. When a link is send 90% of the users click within twenty-four hours (Proofpoint, 2017). The links are made to be appealing so they gain the user's trust. For social media providers, it is hard to counter these URLs because it is difficult to identify whether the link is legitimate or not. The URL brings you to a website that contains misleading information like an application, fake login page or fake products (Goel and Jain, 2018).

As an example, for phishing links, fig. 5 shows a message presumably send by the Rabobank. However, if you look at the full address used you can tell this is a malicious link. The sender is imitating the Rabobank where an action is needed in order to prevent your banking pass from declining. The user receives a link how to fix it, but the link directs you to a phishing website.

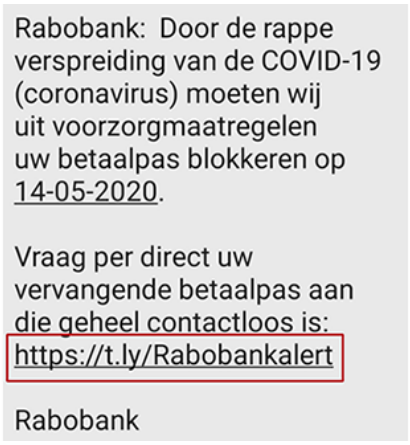

Fig. 5: Phishing link and smishing example (Rabobank, 2021)

2.3.3 Phishing through online social networks

Social networks are used for professional as well as personal communication. Millions of people around the world use social networks and due to these large numbers attackers see opportunities. They are exploiting trust of users to gain information (Goel and Jain, 2018). 24% of the users click on fake connecting requests and half of these users even share their credentials (Wandera, 2017). Research shows that it is easy to trick the people on social networking sites (Goel and Jain, 2018). They found when a user thinks he is somehow related to a person he is four times more likely to become victim to phishing. Attackers tend to be claiming to be an old friend. Next the attacker asks for private information. Also, attackers tend to create fake groups. They name themselves after a well-known organisation and invite employees in order to gain secret information.

2.3.4 Ransomware and malware

Phishing messages can also contain links to download malicious software. There are two types that are called ransomware and malware. Users are tricked into downloading software through links or attachments. Ransomware encrypts the data and infects the system so the attacker can decrypt it in exchange for money. Ransomware is effective on both computer as smartphones. The ransomware changes the PIN of the device and locks it till ransom is paid. The Netherlands is in the top ten of ransom attacks in the world (Richardson and north, 2017). Malware is software that enters the data of the user without his consent. It steals or damages the data on the device or is made to annoy the user. It sends personal data to the attacker which he can use for his own benefit (Goel and Jain, 2018).

2.4 Human behaviour in phishing

In section 2.3, various methods of message phishing are discussed relevant for this research. Also, it shows attackers tend to aim for user's trust. This section focusses on the human behaviour in message phishing. The process of smishing is shown in fig. 6.

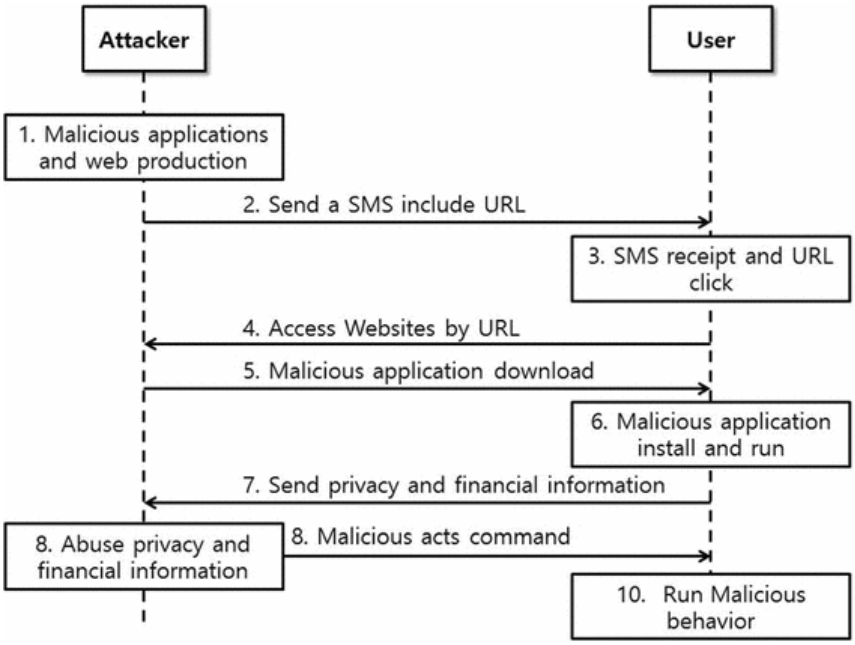

Fig. 6: Smishing process (Joo et al., 2017)

In the first step, the attacker makes the malicious application and website to distribute the software. Secondly, the attacker sends a text with an URL to direct the user to the phishing website. Thirdly, the user receives the message and clicks the URL. Fourthly, the user gets forwarded the URL to the phishing website. Fifthly, the application gets downloaded through the URL. Sixthly, the application gets installed and executed. Seventhly, the application sends the users' data, e.g. personal and financial information from their mobile device. Eighthly, the attacker uses the information for his benefits. The last two steps are a repeated cycle where the attacker can redo the attack while the software is installed (Joo et al., 2017).

A research had findings about human behaviour in 150 online phishing cases in the Dutch banking sector (Jansen and Leukfeldt, 2015). Within these cases there were findings about message related cases. The phishing victims appeared to trust the messages the attackers send them. So early in the phishing process, step 3 in fig 6., users get tricked. Attackers mimic the bank and the content of the message corresponds to the usual style of the bank. Three methods are the most effective: testing the security of online banking, information regarding their bank account or customer verification. These topics made people feel obligated to help and enter personal information such as credentials. Attackers also use recent events in their messages; e.g. introduction of IBAN, the banking app or flaws in newly developed features.

Also, people did not suspect something was wrong. The messages, safety signs, closed padlock or the answers of the attacker via phone gave them enough trust to give them what they wanted. Users also mentioned they cooperated with attackers because they had life events, such as passing of a family member, or did not read the message or page well (Jansen and Leukfeldt, 2015).

That is also the reason why victims give credentials to fake websites. In step four of fig. 6 users enter the URL of the attacker. Users perceive the fake website as trustworthy because the colours, fonts and logos resemble the bank's corporate identity. Attackers also let people download malware through these links as shown in step six in fig. 6. These apps obtain data in the background while the user enters credentials.

People tend to participate in phishing schemes because attackers use their trust. Psychological literature shows that individuals cannot be expected to judge messages to find fraud indicators. People are likely to rely on judgmental heuristics in evaluating the content and authenticity of messages (Chang and Chong, 2010). When an attacker shows someone a bank styled message or a link to a page which seems to resemble the bank people will easily cooperate under the assumption he is using a bank tool (Claessens et al,. 2002). As said, people are expected to rely on judgmental heuristics and are therefore easily misled. Attackers also fake real authenticity signs, so even if people check the validity they almost stand no chance (Downs et al., 2006). Attackers make the lay-out and the content of the message as accurate as possible and people comply because they are appealed to trust and authority of the bank.

2.5 Anti-phishing measures

In the previous sections the human behaviour of phishing is examined. This shows how attackers trick people. To reduce phishing victimization anti-phishing measures have to be used. These measures could be both psychological and technical.

In the United States 26 billion dollar was lost over phishing in 2019. 90% of the phishing mails were caught and verified by security measures but the 10% remaining still managed to get over 170.000 victims inside organisations (Bhardwaj et al., 2020). Technical measures can help detect phishing messages, but does not remove all phishing messages. In order to reduce phishing victimization also psychological measures are needed.

2.5.1 Technical measures

There are many applications and methods to counter mobile phishing cases. Here we discuss anti-phishing measures that can detect fraudulent messages. To detect these messages

multiple anti-phishing software are suggested. The solution methods discussed are S-detector, Dendritic Cell algorithm based approach, Spam detection using content based features, Smishing defender, and Detecting smishing in cloud computing environments. These apps have to comply with the legal requirements discussed in the section 2.6.

S-detector

This is a model for detecting and blocking smishing messages (Joo et al., 2017). It uses the data mining classifier "Naïve Bayesian classifier" to differentiate smishing and normal messages. Messages will be viewed and words are extracted and compared with words most used in smishing messages. Also, it checks URL's and if an APK file, which indicates fraudulent software, is downloaded the messages is regarded as a smishing message.

Dendritic Cell Algorithm based approach

This a technique to filter multimodal textual messages (El-Alfy and Alhasan, 2016). It uses machine learning methods. The program needs messages to learn to recognize them and filter them. This approach could be used to counter phishing if phishing messages are learned. This method was created for spam and could also identify phishing messages. The approximate accuracy for spam is 100%. However, since phishing is different from standard spam the accuracy could be lower.

Spam detection using content based features

This is an approach based on content and uses semantic group of words as features (Karami and Zhou, 2014). Using this multiple phishing messages could be identified and through a machine learning algorithm these can be detected. The accuracy of the system lies from 92% to 98%.

Smishing defender

This application detects and blocks phishing messages on android smartphones (Goel and Jain, 2018). The application identifies the text messages received and when a smishing message is recognized the app notifies the user.

Detecting smishing in cloud computing environments

This technique detects smishing messages using a cloud virtual environment (Lee et al., 2016). For corporate employees, this technique could be real useful. This technique looks at the source, content and location of the server of the message. The user has to judge the risk in a virtual environment. Because it is a virtual environment de user can test if it is a smishing case. Because it is a verification test in a cloud environment the user is safe from possible

risks and damage. The program generates a report and the user can determine whether it is smishing.

2.5.2 Psychological measures

Technical anti-phishing measures do detect and remove the majority of the phishing messages, but not all. As shown in the introduction of this section, some messages pass the filter and this results in phishing victimization. Next to technical also psychological anti-phishing measures should be taken. Psychological means methods or training that are directed to users to help them understand the dangers of phishing attacks. These measures are focused to protect people from fraudulent messages. Psychological anti-phishing measures are needed and as stated by a researcher: "It doesn't matter how many firewalls, encryption software, certificates, or two-factor authentication mechanisms an organization has if the person behind the keyboard falls for a phish" (Hong, 2012). There has already been literature on educating users about phishing and helping them make better decision. These are trainings developed to identify phishing emails, messages or URL's. They found security measures are the first line of defence and should be used. User education offers a complementary approach to help people better recognize fraudulent e-mails and web sites (Kumaraguru et al., 2010). Also, another research found educated people's tendency to enter information into phishing web pages was reduced by 40% and also reduced the tendency to click on links (Sheng et al., 2010). These trainings could be modified for message phishing cases. There has also been a test about awareness. It shows when users suspect phishing they were significantly better in discriminating it from normal cases (Kathryn et al., 2015). People do get warnings when clicking links or entering pages but these are mostly passive. Kathryns et al.' research shows when users are notified they react better. Other research states that users do not pay attention to passive warnings so active warnings should be used. Passive warnings only show an indicator and does not require action from the user. Users do not pay attention to passive warnings. Active warnings block content and require a certain action from the user. Therefore active warnings are more effective compared to passive warnings (Goel and Jain, 2018). As shown attackers can mimic banking messages easily, therefore banks should not send messages via email or text applications and make people click hyperlinks or attachments. The bank already has an online environment with an app and portal. They should use their portal instead and let people only enter there and not through detours. People shouldn't click on these links and cannot be held responsible for making these errors. Still, people could use technical anti-phishing measures and some form of training to minimize the risk of clicking or complying with phishing (Jansen and Leukfeldt, 2015). Next to the visual fraud, attackers also

present themselves as banking personnel, who gains trust (Chang and Chong, 2010). Next to that, these attackers already know some personal information. These personal details also create trust (Jakobsson, 2007). The people should be trained about these methods and more specifically about the use of security codes (Jansen and Leukfeldt, 2015).
Also embedded training within the banking environment can effectively teach individuals how to avoid phishing attacks (Kumaraguru, 2010). User awareness among people about phishing is important during this training (Goel and Jain, 2018).
However, a recent study shows that groups trained for phishing did not result in reduced incidents (Back & Guerette, 2021). They were also more likely to engage in clicking links or submitting personal data. This research shows a contradiction against earlier research. They also found that the more time spent online the higher the likelihood of experiencing phishing. The higher online presence could have been the reason why the number of incidents did not decrease due to the increased exposure to phishing messages. Despite their conclusion they also stated that the significance of awareness training cannot be overlooked. Technological anti-phishing measures cannot be the only remedy to mitigate phishing attacks.

Training

People could use training to minimize the risk of complying with phishing. This training should be about the online banking environment and avoiding phishing attacks. People should also be trained on the various phishing methods and the use of security codes.
One way to do training is via a gaming app. This app can train people to correctly identify phishing and legitimate cases. Various games are being developed to train app users in identifying these cases. A game has been developed for seeing legitimate emails and URL's (Arachchilage et al., 2012). Also, a game has been developed that integrates "self-efficiency" so the user's behaviour to avoid phishing attacks is enhanced (Arachchilage and Hameed, 2017). These training games could also be made for mobile cases such as texting.
They also showed another way of training was simulating phishing attacks together with embedded training. This showed the users who do this reduce the risk of becoming victim to phishing attacks. Embedded training means warning screens, notification messages and the option to participate in the online training program. One contributing factor to the reduced risk may have been because the users influenced each other and got more awareness. Also, the content matters for users. Users comply because some content seems trustworthy or does not make them think something is wrong. After seeing what they did wrong the next time they did not fall for it (Jansson and von Solms, 2013). These simulations can also be done with messaging phishing cases.

So, training could help people make better decisions when clicking on links or complying to a phishing message.

2.6 Legal

In the Netherlands, there are also regulations about app development and privacy. For message phishing, we discuss privacy, procedures and accountability.

2.6.1 Laws

The government has multiple laws to convict a phishing attacker, but due to their anonymous character they are hard to find. Our law has multiple articles where phishing cases are punishable (Ejure, 2015).

1. Article 326 states scam is punishable. In 2009 the law was adjusted so it was better applicable on phishing cases. Not only money but also personal information can't be taken without permission.
2. Article 138ab shows that computer trespassing by for example malicious software is illegal. If the attacker doesn't just trespass but also takes information the punishment will be more severe.
3. Article 350a states that destroying or manipulating information is illegal and also the spreading of a virus.
4. Article 2.20 states that attackers are not allowed to copy sites of companies and take their identity.

2.6.2 Privacy

An application needs to ask the user for permission to use personal information on the device. Also, the application needs to ask which data it needs so the user is more informed what data is used. The application needs to have clear and understandable goals why the app needs this data and the goal of use cannot change without the user having to accept these conditions. Data used by the app are only for the purpose of its goals, after the goal is reached the data has to be deleted. The app can also be deleted with all its gathered data. Next to the usage of the data the information needs to be well secured, e.g. encryption and who has access to the data. At last, there has to be a readable, understandable and accessible privacy statement. After following these rules, the app can use the personal information for its usage (Autoriteit Persoonsgegevens, 2021).

As stated, security is a legal requirement when using data in an application. European law states that when an application is hacked the user's needs to be notified (AVG, 2021).

2.6.3 Procedures

When someone becomes victim of phishing they can claim reimbursement from the bank and follow the following procedure (Rabobank, 2021). The phishing attacker has twenty-one days to transfer the money back. When the attacker does not repay the victim, the bank will try to find the name and address of the attackers. The victim can go to court with the name, address and charge for the attacker. To start this procedure there are conditions to be met. There are differences between internet fraud and other forms of non-banking fraud. Non-banking fraud is transferring money but under false terms. Internet fraud will be handled by the LMIO (Politie, 2021). This is the "Landelijk Meldpunt Internetoplichting". The LMIO has a register of prior phishing cases. Data is stored such as bank account numbers, mailing addresses, phone numbers and website URL's.

When an attacker cannot be identified the bank has to judge the case whether they reimburse the victim.

2.6.4 Accountability

The possible parties involved that can be held accountable are the messaging platform provider, bank, government or the phishing victims. All parties involved have a different role and therefore accountability. In 2014 politics passed a notion about online fraud which states banks should reimburse the money. However, this is when the money is unwillingly transferred (Radar, 2020).

Message platform provider

The most used messaging platform at this moment is WhatsApp. Their terms of usage and responsibility is only the service they offer. Not the way others use the platform. So, if someone text a phishing message WhatsApp denies accountability (Whatsapp, 2021). Because this is a legal construction any other messaging platform has the same type of terms of use.

Bank

The bank has a role in the phishing process because phishers get money from banking customers. In some cases of phishing, money gets transferred back to phishing victims by the phisher when caught, see section 2.6.3 above. If it's not, the money may be reimbursed by the bank. They judge your case and determine whether your money is reimbursed. Most of the time the bank does not reimburse when money is willingly transferred. If people are scammed by an imitation of banking staff, software or a malicious link after evaluation of the bank the money gets reimbursed (Maxvandaag, 2020).

So, the bank does refund money if someone was victim of phishing, but if someone transfers money willingly to a phisher their money is not likely to get reimbursed. The bank judges these cases. For message phishing people get tricked into transferring money and law does not state this has to be reimbursed (Radar, 2020).

Government

The laws mentioned above show phishing is illegal. The accountability of phishing is partly stated in a law. Banks should reimburse money when, in case of online fraud, money is unwillingly transferred. With message phishing people are often tricked into transferring money and these cases have no legal accountability yet. The government do try to catch phishers, but they have no role in the responsibility of phishing. The minister of finance is looking into a government fund for phishing cases so money can be refunded to phishing victims when the bank did not reimburse the money. For now, this is not the case and their focus is on preventing/countering phishing (De Nationale Adviesbalie, 2020).

Phishing victims

People who willingly transfer money in phishing schemes do usually not get their money back. However, if money gets transferred from their account without people knowing the bank reimburses the money. People can report phishing cases to the police, but the accountability mostly lies with themselves.

3. Survey design

This section shows the survey design. The survey will have quantitative and qualitative questions. The program used to make the survey is Qualtrics. This is a program developed for making surveys. The participants were selected through the student population, family circle and social network (n=58). This research hasn't been conducted earlier so there are no similar surveys. Due to this, the questionnaire is based on the literature research and the research questions of the thesis. The survey will result in information about the current awareness of people, what anti-phishing measures they already use, their willingness for anti-phishing measures and their trust in different parties e.g. the government and bank. This will validate the literature research and gives additional information to answer the research questions. The survey has the following structure.

Background

To get a feeling about our sample group the following questions were asked:
"What is your gender? and "What is your age group?". Because there is no specific targeted group targeted by phishers the distribution doesn't really matter other than the fact multiple groups are supported (Alwanain, M. I. 2020). This is done by gender and age categories.

Messaging platforms

People use multiple messaging platforms and therefore we need to know the distribution of the used messaging platforms and also the most used platform. The follow questions were asked about messaging platforms: "Which messaging platforms do you use?" and "Which one do you use the most?". This concludes where the help is most needed and where the solution should be aimed at.

Phishing encounters

Some people have already encountered or were even victim of phishing. To know if people encountered or were victim of phishing the following questions were asked: "Have you ever heard of phishing yourself?". Do you have experience in being phished or do you know people who got phished?" People who never had encountered phishing or were victim did not have the following question: "After this encounter, did you became more alert?" This question was to see if there was changed behaviour noticed by people and what this changed behaviour meant. If they said yes, they had the question: "What changed in your behaviour?" This was to research where people pay attention to regarding phishing. If people said no before they had the question: "Why didn't you become more alert?" to see why they did not become more alert for phishing.

Message analysis

People have some awareness when analysing a message. The way people make decisions regarding clicking links and complying with phishing messages is researched. At first, we wanted to see if they click hyperlinks and what they pay attentions to by asking the following questions: “Do you click on hyperlinks in messages?” and “Where do you pay attention with hyperlinks?”. Phishing links are used frequently and this is to research what people know about them. Also, attackers use new links such as a pay request. Therefore, also people are asked: “When u get a message from an acquaintance to pay a payment request, what do you pay attention to?”. This is to evaluate when they comply to paying someone. At last, in general is asked what they pay attention to prevent complying to phishing messages: “What do you pay attention to, to prevent message phishing?”.

Bank procedure knowledge

To see what people know about the bank procedures a few questions were asked about the way they inform people and how willing people are in giving information. The first two question are “Do you think the bank calls, messages or mails to provide information?” and “Do you think the bank messages or mails a with a link attached?”. These questions are regarding the way people think banks inform them. The follow three: “When do you trust a mail or message from the bank?”, “When trusted, would you share personal information?” and “When trusted, would you perform tasks given by the bank?” were to see how trust and willing people are towards giving information.

Willingness for solutions

Phishing solutions are available but people must be willing to use them. The first two questions regard training solutions and their willingness to attend them: “Are you willing to take a training against mobile phishing?” and “Would you have a problem with, before the first try of the bank application, following a quick training?”. The following two were to see if people are willing to download anti phishing apps and if these apps can use their data: “Would you download an anti-phishing application?” and “To prevent phishing an application, without saving, has to check messages and hyperlinks to check their validity, would you still download the application?”.

Accountability

Next to legal accountability there is also a perspective from people on who should help counter phishing. The following three questions were to see which institutions people trust and should help them: “Which party should counter phishing messaging according to you?”,

“Which party do you trust with your data, when its temporary and within legal boundaries” and “Which party has the highest chance for you to download an anti-phishing application?”.

4. Results

This section contains the results of the conducted survey.

4.1 Background

Our survey was conducted over 58 participants (n=58). For the background, participants gender and age categories were asked. The age distribution and gender representation is shown in figure 5 and 6.

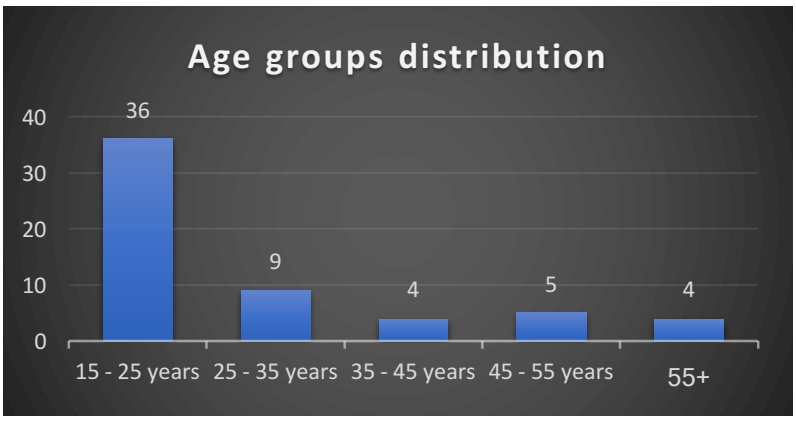

Fig. 7: Age distribution

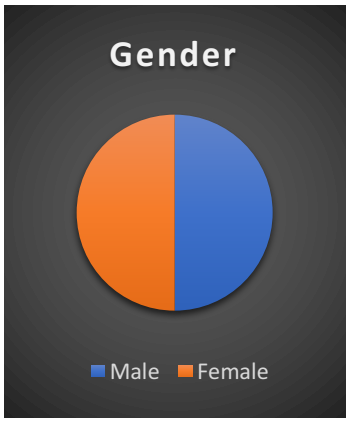

Fig. 8: Gender distribution

There is an even distribution man and woman shown in figure 8. The age distribution has a peak at 15 to 25 years old (n=36). All other groups are represented by at least 4 participants.

4.2 Messaging platforms

To know more about the messaging platforms and the distribution within our sample we asked the platform usage and the most used platform.

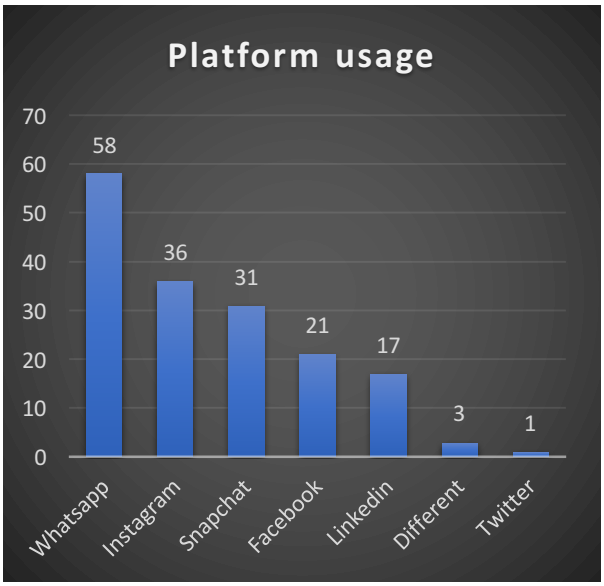

Fig. 9: Platform usage

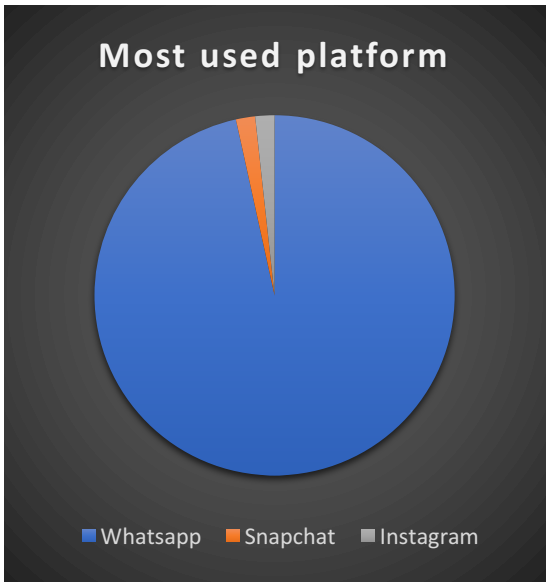

Fig. 10: Most used platform

Figure 9 shows the platform usage under the survey group. As expected from figure 1, everyone in our sample has WhatsApp. Also in figure 10 is shown that of all the platforms this one is used the most for messaging nowadays.

4.3 Phishing encounters

To test the awareness also the prior encounters with phishing were asked. Participants knew others who encountered phishing or got phished or even got attacked themselves. This is displayed in figure 11 and 12. Figure 13 shows if participants became more alert when encountering phishing in their environment.

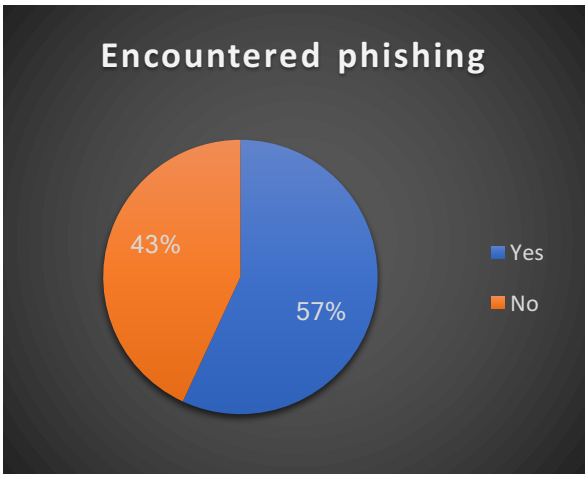

Fig. 11: encountered phishing

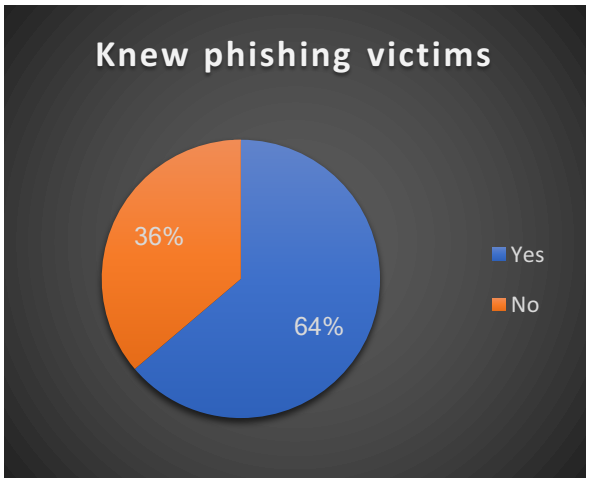

Fig. 12: Knew phishing victims

Figure 11 showed 43% encountered phishing themselves which means they already have seen phishing up close (n=25). Figure 12 showed 64% knew participants how had encountered phishing, so also participants who encountered phishing talk about their experience.

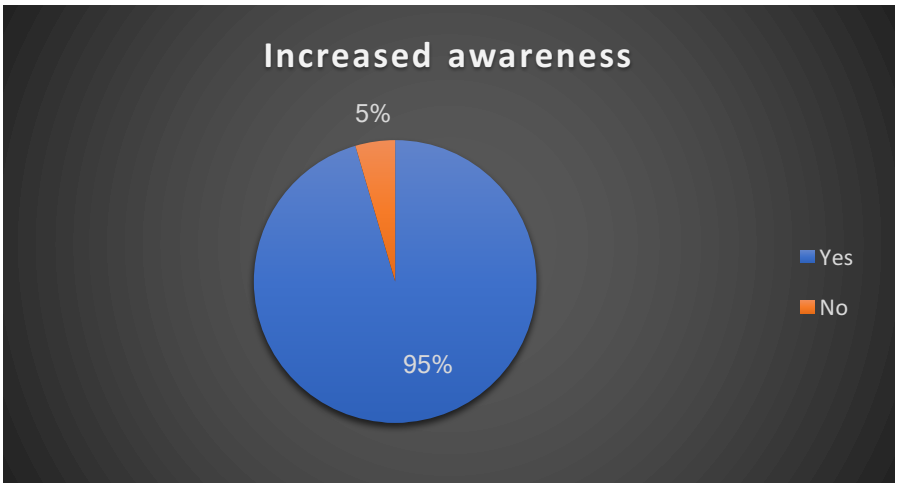

Fig. 13: Increased awareness

95% of the participants who became more alert had different visions (n=21). The most frequent named measure participants took was seeing who the sender was (n=8). Also, the style of the message is watched (n=7). Participants mentioned grammar, sentence structure

and language use. Next to the style, also the content was something participants were more cautious about (n= 6). Some participants mentioned they won't click links in e-mails (n=5). The remaining 5% who did not become more alert (n=1), said they already were aware about phishing so nothing changed.

4.4 Message analysis

Now we wanted to evaluate how all participants react to links or some type messages and what they pay attention to. In figure 14 is shown if participants click on hyperlinks.

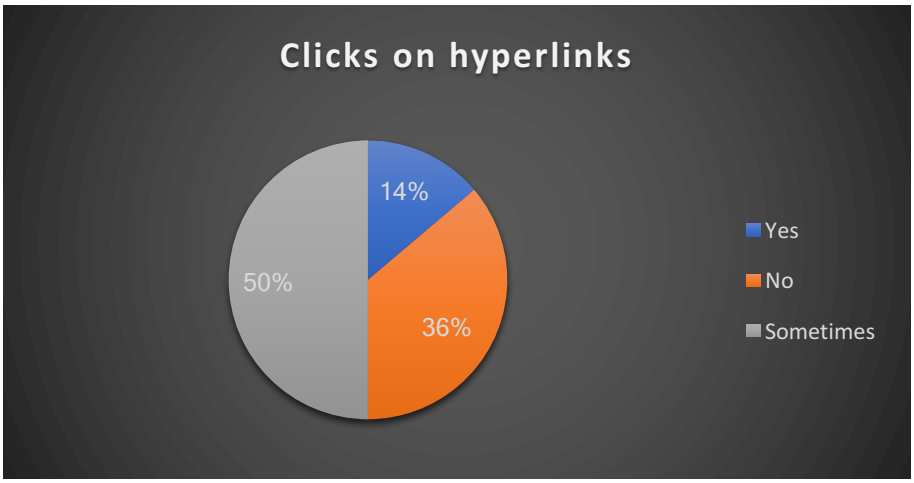

Fig. 14: Clicks on hyperlinks

Also, the caution is asked for hyperlinks. Most of the participants look at the address of the link to see if it is not a phishing link (n=34). Some participants never click on hyperlinks, because they don't trust them (n=4). There is also a group who always click links and also don't watch what the link is (n=6).

Also, the reaction to payment requests by a known individual is questioned. Participants pay the most attention to the reason of the request (n=33). When it corresponds with an event they can relate to they will pay. Participants questioned whether this individual is really the person he or she claimed to be (n=15). Others stated the amount of the payment request mattered, if they would pay (n=7). A few stated they would just pay because they knew this person (n=4).

At last, participants were asked where they pay attention to when trying to prevent phishing in general. Most participants pay attention to the sender of the message (n=33). Also, participants watch the style of the message and if it suits the sender (n=14). The content is also watched and if it appeals to them (n=12). Some participants mention they watch out for links and their validity (n=9). Only a few stated they don't really watch out for phishing (n=3).

4.5 Bank procedure knowledge

Participants have a perspective about the bank and how the bank contact them. In figure 15 is shown if participants think banks call, send texts or mail them for information. In figure 16 is shown if participants think banks send links with emails or texts.

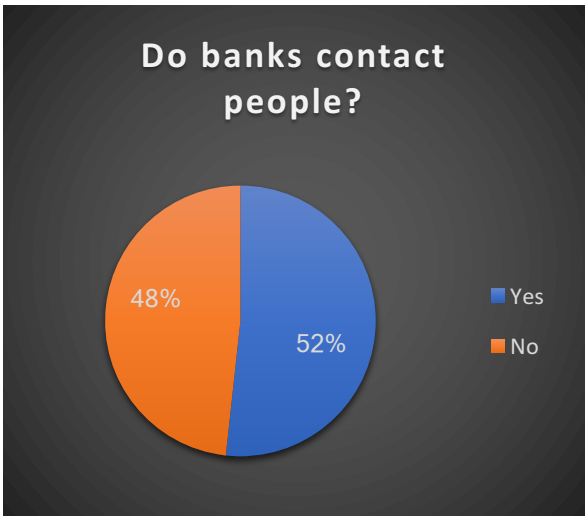

Fig. 15: Do banks contact people?

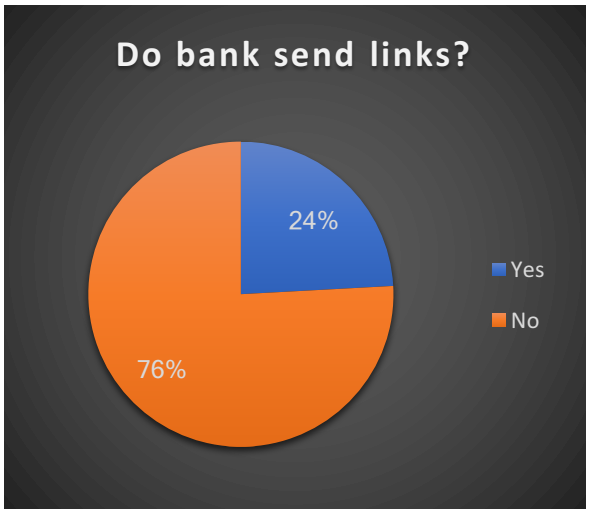

Fig. 16: Do bank send links?

The division between the 48% no and 52% yes in figure 15 shows there is no uniform understanding how the bank contacts their customers. When a bank sends someone a message 24% thinks this could include a link.

Also, when a message is trusted is asked and shown in figure 17.

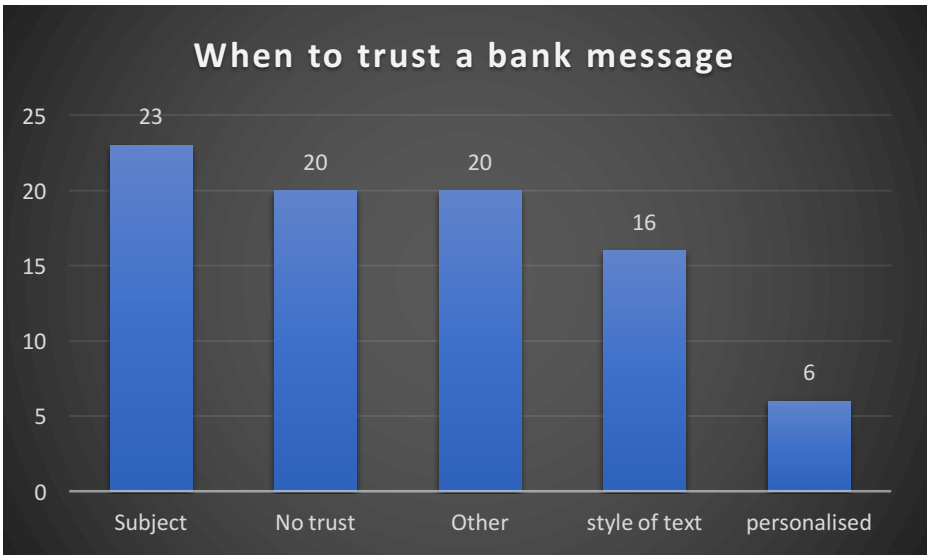

Fig. 17: When to trust a bank message

The most important thing participants pay attention to for trust is the subject (n =23). Also, a significant number of participants don't trust messages from the bank (n=20). For the other column participants mentioned they trust it when the message has no requests or call to actions (n= 8). A few also mentioned they only trust messages when they expect one because

they had prior contact or requests for the bank (n=3). Also, the style of the message participants creates trust (n=16). This means grammar, sentence structure and language use. The fact messages are personalized gains also trust but way less than the above mentioned (n=6).

Phishers have a way to make participants trust them. Therefor is questioned how they comply when trusted. In figure 18 is shown if participants share personal information with someone they trust.

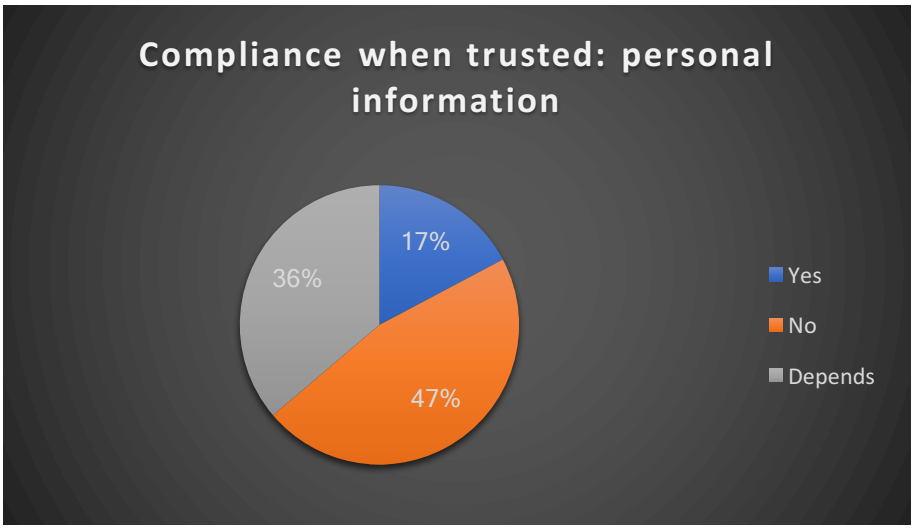

Fig. 18: compliance when trusted: personal information

As shown on the left 17% comply when they trust someone. 36% of the participants even when they trust someone don't share personal information. The remaining 47% had some conditions. Some said it depends on the personal information, but not bank credentials for example (n=8). Another frequently named item is participants only trust it when they themselves initiated the contact (n=6).

Phishers also make participants use their gateways by leading participants step by step. Mostly phishers want participants to put their credentials into their websites. In figure 19 is shown how compliant participants are when they trust someone.

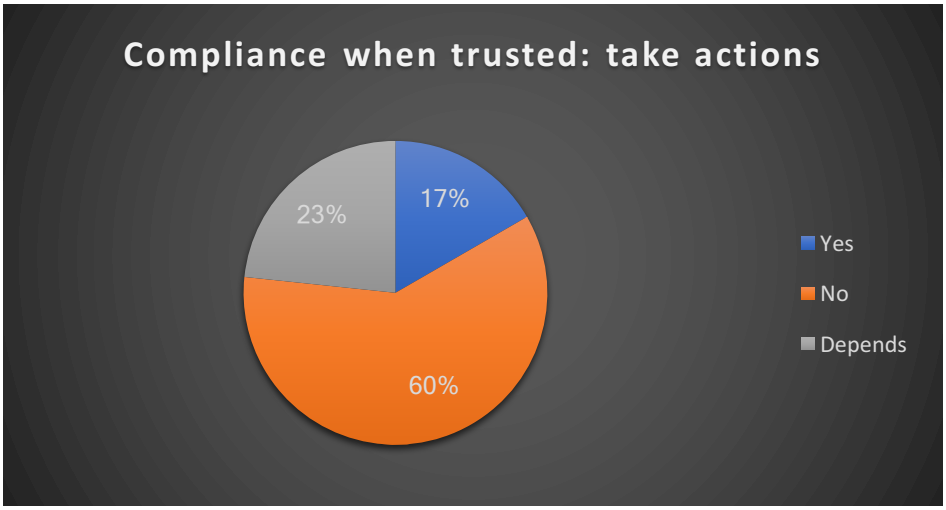

Fig. 19: Compliance when trusted: take actions

62% of the participants say they don't comply with someone they trust by logging in. 14% say they would comply when they trust someone. The remainder said it depends on mostly one condition. It really depended on the information they wanted (n=9). They would not give credentials or other important information.

4.6 Willingness for solutions

To prevent phishing, we need solutions but the willingness of people for training and technical solutions is crucial. At first, the willingness for a phishing training is shown in figure 20.

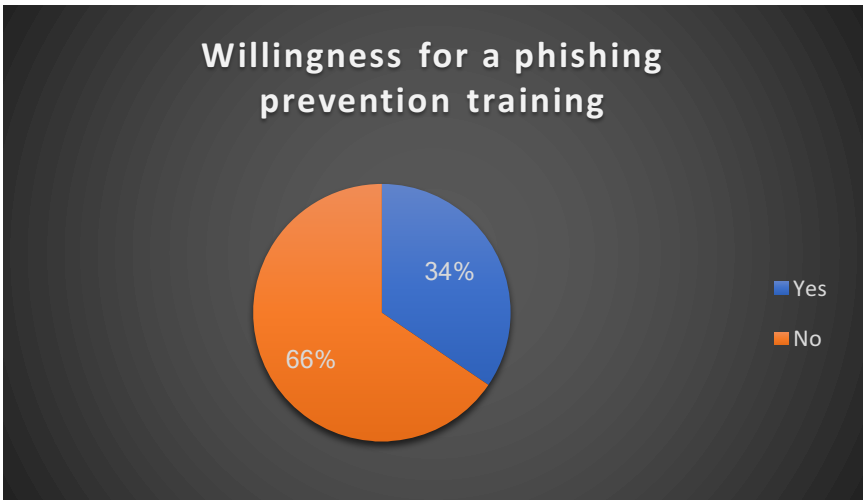

Fig. 20: Willingness for a phishing prevention training

Only 34% is willing to take a training to prevent phishing. The remaining 66% is not willing to take the training. Some gave their reasons (n=26). These all indicated they already had enough knowledge about phishing and did not need a training.

When the bank askes for a mandatory training before using the app for the first time a question was asked about their willingness in figure 21.

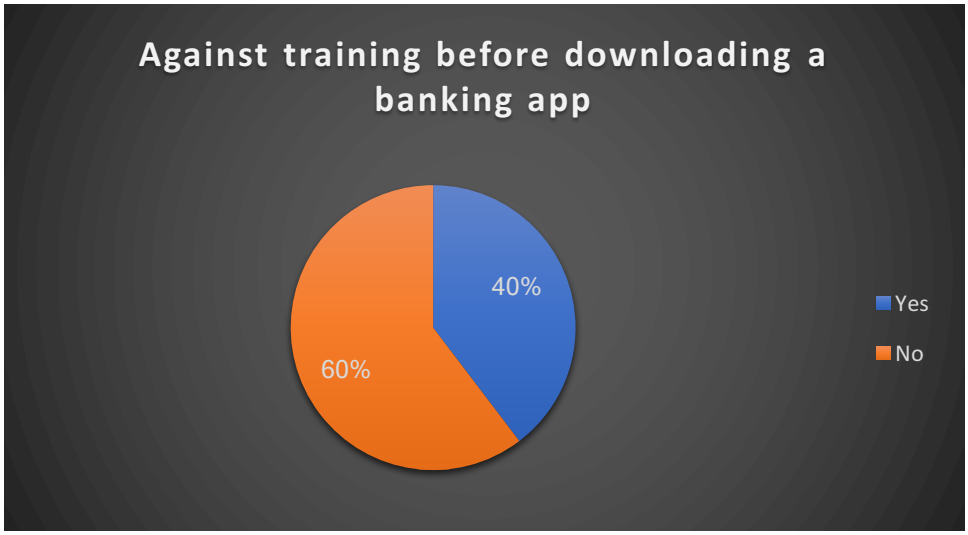

Fig. 21: Against training before downloading a banking app

60% was willing to do a short training about phishing before using the bank application. 40% had a problem with the fact this training was mandatory. Some gave a reason why they had a problem with the training. The training takes some time and some were not willing to invest some of their time in a short phishing prevention training (n=9). Some also thought they knew enough about phishing and they did not need this training (n=6).

There are also technical anti-phishing measures next to the training solutions. The willingness is questioned and for the app to work it needs to have access to the user their data. The willingness is shown in figure 22 and 23.

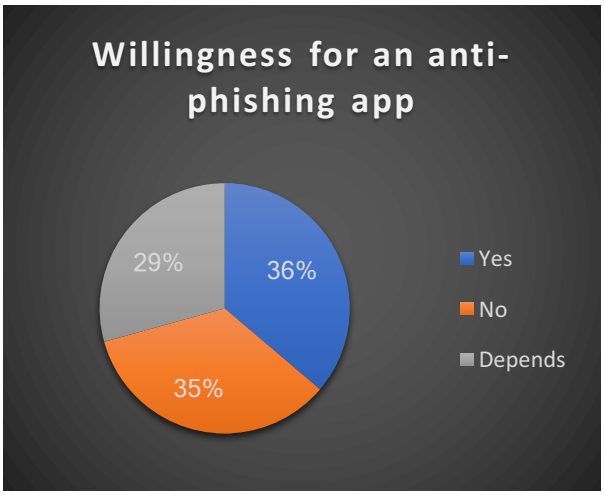

Fig. 22: willingness for an anti-phishing app

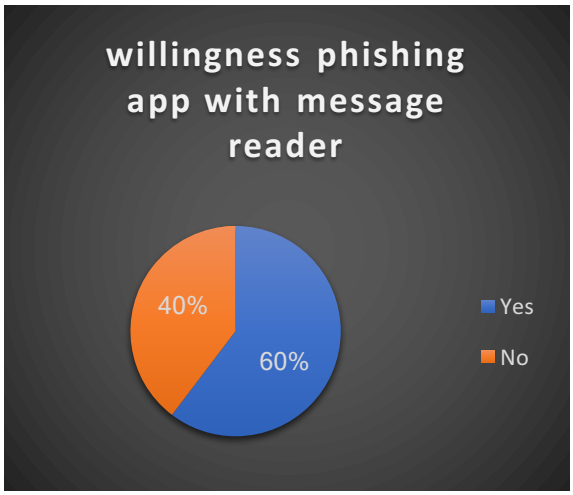

Fig. 23: Message reader willingness

A part of the participants shown in figure 21, 36%, are willing to download a phishing application. 35% of the participants were not willing to download a phishing application. The remainder had some conditions. Some had to know if the application was safe from hacking and if they can trust it (n=6).

The required extra performance of the application made some participants doubt it, due to a shorter battery life (n=3).

A phishing application needs data in order to work and as shown in figure 23 60% of the participants were willing to give the application permission. 40% of the participants were not willing to let the application check messages for validity.

4.7 Accountability

When the right solutions are found, there still is the question who should supply these solutions to the people. Therefore, the accountability and responsibility has to be determined. In figure 24 is shown who participants think should provide phishing solutions.

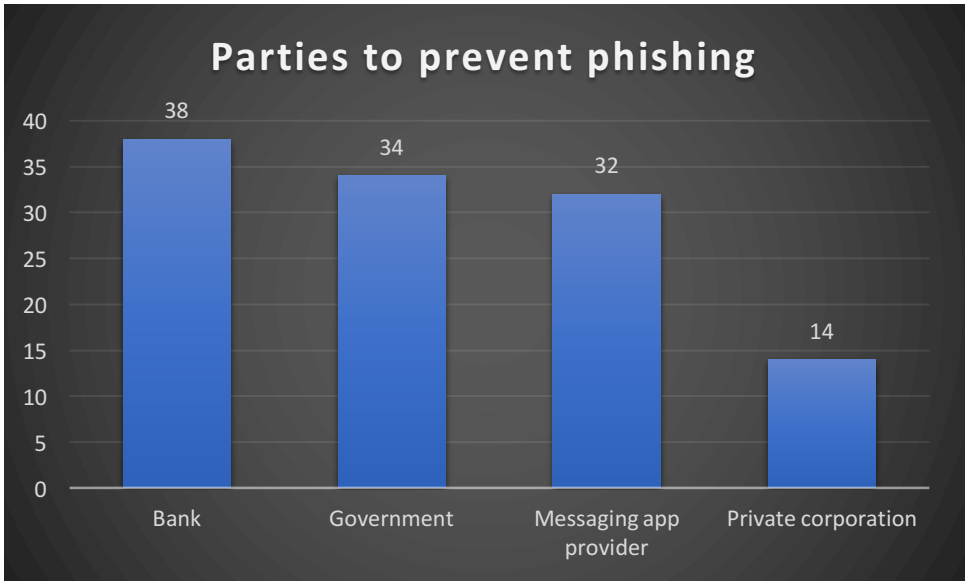

Fig. 24: Parties to prevent phishing

The bank has the most votes (n=38), but the distribution between government (n=34) messaging app provider (n=32) and bank is not far apart. Private corporations were the least favourite (n=14).

In order to prevent phishing data has to be used and people must be willing to give this data. In figure 25 is shown which parties people trust.

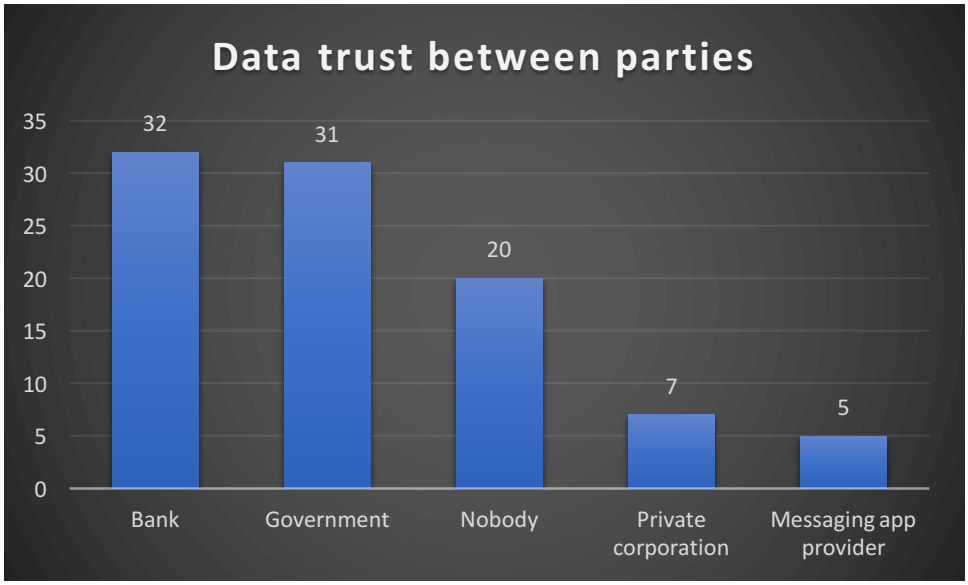

Fig. 25: Data trust between parties

Participants trust their data the most at the bank (n=32) and with the government (n=31). Some participants don't trust any institution with their data (n=20). Messaging app provider's (n=7) and private corporations (n=5) scored the lowest.

Also, an ultimatum has been asked, if a party were to help u counter phishing which one would this be. This party will be the one participants are most willing to download phishing applications. The distribution is shown in figure 26.

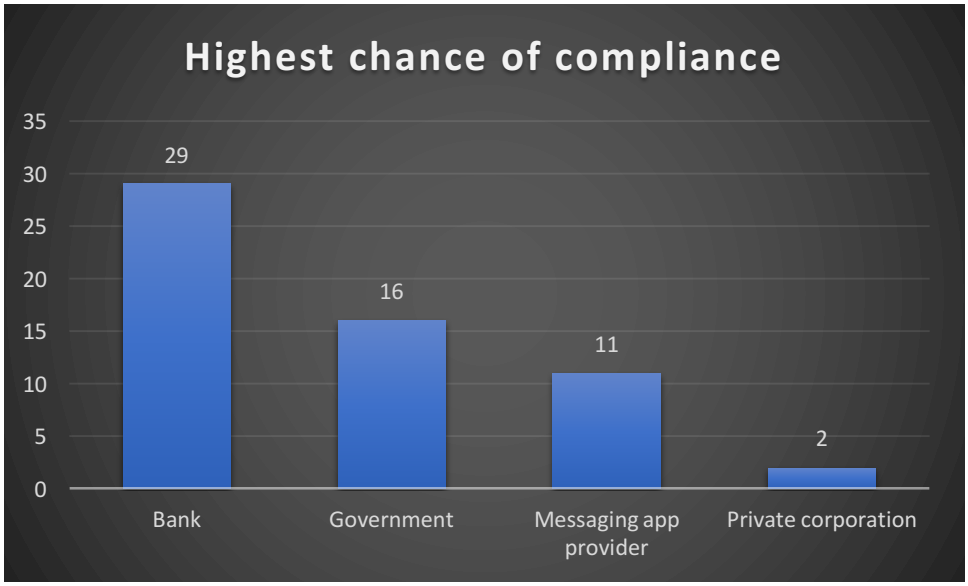

Fig. 25: Highest chance of compliance

The figure shows the bank has the highest chance for participants to download an anti-phishing application (n=29). The government (n=16), messaging app providers (n=11) and private corporations (n=2) were not picked as favourite.

4.8 Conclusion survey

The survey gives insights on how to answer the research questions: “What anti-phishing measures should be used to reduce phishing victimization in the Dutch banking sector?” and “Which institution should implement anti-phishing measures in mobile messaging platforms?”.

The first research question is about anti-phishing measures. These should be both psychological as technical. For psychological anti-phishing measures, training should contain how the bank communicates. The survey showed a confusion about which channels the bank uses for communication. Fig. 15 shows there is an even division about whether the bank contacts people or not. Fig. 16 shows 24% people think the bank does send hyperlinks and 76% doesn’t think so. The majority was not willing to do a phishing training, as shown in earlier figures and mentioned above, the majority has an increased awareness. Therefore, they don’t see the need for training. However, the majority was willing to do a quick training when using the banking application for the first time.

For the technical anti-phishing measures an interesting finding was technical measures seem to be more appealing. This could be because a training takes time and a technical solution just assist people and takes less time. If met some requirements for a technical solution the majority was willing to download one. 60% of these people, shown in fig 23, had no problem with a message reader in the application to detect and remove phishing messages. Anti-phishing measures could also be targeted only for the willing 60% to test its accuracy.

The second research question was mostly shown in fig 26, where the majority said they would download an anti-phishing application from the bank. They had the highest chance of compliance. Also fig. 24 and 25 shows the bank has the most trustworthy and accountable according to the participants. This implies the bank should provide a technical solution. At a second place the government should act on this matter.

Also, other interesting results were found. At first, shown in the age group distribution, in fig. 7, and their platform preference, fig. 10, WhatsApp is used by all age groups. More than half of the participants have not encountered phishing themselves, but the majority has heard of phishing through acquaintances. The people who encountered phishing in a way, 95% said they had an increased awareness, which is an interesting finding. 16% said they would just click on hyperlinks. Also, the compliance questions in fig. 18 and 19 show 17% and 14% would click malicious links, the remainder had multiple conditions to be met or would not comply. Not everyone will be victimized by phishing due to awareness, but approximately 16%, are easy targets for phishing. If compute this scale to the population of 12.4 milion

Whatsapp users 1,984 milion people are victimized. This could cause a lot of damage and therefore phishing has to be prevented. Also, fig. 17 shows what people trust in a banking message. This could be reviewed by the bank to see if these perspectives are appropriate to be assumed.

5. Recommendations

The literature research together with the survey resulted in recommendations.

Recommendations on research question 1: "What anti-phishing measures should be used to reduce phishing victimization in the Dutch banking sector?"

1. To reduce phishing victimization people should be informed about phishing methods and raise their awareness as shown in section 2.4.

   Therefore training is needed. In the survey we found that only 34%, shown in fig. 20, is willing to do this. On the other hand 60%, shown in fig. 21, is willing to do a short training when first using a banking app.

   We recommend that all banks provide such a short training before letting people use a new banking app. This will raise the awareness for phishing attacks.

   The training should contain the following items according to section 2.5.2:

   - Education about identification of phishing messages and hyperlinks.
   - Education about their tendency to enter information into phishing web pages.
   - Literature tells us banks should only contact people via their portal and educate users more in their use of information channels. The survey shows there is ambiguity regarding the information channels the bank uses.
   - People should be educated about the phishing methods used by attackers. This means e.g. an attacker mimicking banking personal.
   - At last, the use of security codes should be addressed.
2. Next to a training, also the willingness for technical anti-phishing measures was tested. In the survey, in fig. 22, was shown 35% was against an anti-phishing application and 36% was willing for such an app. The remainder had conditions but if these are met the majority, 65%, would use a phishing application. Also 60% claimed to have no problem with a message reader in the phishing app, shown in fig. 23. So, when executed right, the majority is willing for technical anti-phishing measures. Because not everyone is willing to download an anti-phishing application, we recommend the bank should beta-test the application on the willing part. When the test proves successful, it can be implement on the entire platform.
3. This paper showed a few algorithms which could be used to detect and remove phishing messages in section 2.5.1. Two had accuracy ratings and therefore these two are recommended when a company decides to create an anti-phishing application.

- Dendritic Cell Algorithm based approach, approx. 100% accuracy
- Spam detection using content based features, approx. 92 – 98% accuracy

4. As the survey showed, in fig. 10, 97% used WhatsApp as their main messaging platform and thus the anti-phishing application should focus on WhatsApp as messaging platform.
5. Also, the bank application should have active warnings about phishing. This proved to be way more effective compared to passive warnings in section 2.4.

Recommendations on research question 2: "Which institution should implement anti-phishing measures in mobile messaging platforms?"

1. Section 4.7 showed two parties were held most responsible for countering phishing victimization: the bank and the government. The bank according to the participants had the most responsibility, shown in fig. 24, and trust, shown in fig. 25. Section 2.6 shows the bank should reimburse money when money is unwillingly transferred or when someone imitates the bank and should therefore reimburse. Current regulations state no law regarding who should counter phishing. The bank already takes action and is recommended to keep going and add some extra measures discussed below. Because banking companies reimburse money this creates costs. Anti-phishing measures would decrease these costs. We recommend the bank should implement anti-phishing measures. They already help and are willing to implement more anti-phishing measures to decrease their financial damage.
2. Messaging platforms are not held accountable for phishing messages on their platforms, but there are technical features which could detect and remove the majority of phishing messages. We recommend these platforms should be legally obligated to use such features. Otherwise they can be held accountable. This could solve a significant amount of the message phishing attacks.
3. The government could also impact phishing by making better defined laws regarding accountability. As of this moment, the law only states bank should reimburse money when money is unwillingly transferred or if a someone imitates the bank, but not other kinds of trickery. We recommend these regulations should be adjusted to the recent message phishing cases where people are tricked to willingly transfer money to e.g. a fake friend. Adjusting this law would help the customers but would not take away the problem. Therefore the law should also mention parties should take anti-phishing measures.

6. Conclusion

Phishing has innovated over the last years and as shown attackers adapt to new situations and developments. Mobile phones are targeted by attackers due to their many limitations. Phones consists of a significant amount of data and due to their small screen and low security measures which makes it an appealing and easy target. This research focusses on message phishing and the most used platform for messaging is WhatsApp at the moment.
Malicious messages are being send by someone impersonation a close friend, family or for example a banking employee. These consist actions you have to do or hyperlinks you have to click. Transfer money or obtain data are the most common goals of attackers. People comply because attackers gain their trust by misleading them. People rely on judgmental heuristics while evaluating the content and authenticity of messages. People are also easily misled by judgmental heuristics. Psychological anti-phishing measures should help assist people making better decisions. Next to training also technical anti-phishing measures would reduce phishing victimization. There are multiple existing machine learning techniques to detect and remove phishing messages. Combining psychological and technical anti-phishing measures will result in less phishing victims. Psychological anti-phishing measures should aim on training or workshop which should focus on how the bank operates, phishing methods and phishing message detections. Technical anti-phishing measures should use an algorithm with a high accuracy to detect and remove phishing messages such as Dendritic Cell Algorithm based approach or Spam detection using content based features. This could be incorporated with the bank app or a separate app where messages containing links or strange numbers should be checked for phishing activities. Legally no party is responsible, but as shown by actions and by the survey the bank should be the party assisting people in phishing prevention. They already have the trust of people and they already reimburse part of the phishing cases where people did not willingly transfer money. Because the bank reimburses money phishing increases the bank their costs. Therefore, the bank is the right party to counter phishing and a well preformed anti-phishing plan would reduce phishing victimization and reduce the financial costs of the bank. The government could also impact phishing by making better defined laws regarding accountability. Regulations should be adjusted to the recent message phishing cases where people are tricked to willingly transfer money to e.g. a fake friend. Adjusting this law would help the customers but would not take away the problem. Therefore the law should also mention parties should take anti-phishing measures.

6.1 Discussion

This research focusses on phishing in messaging platforms. The recommended anti-phishing measures could also be used for other types of phishing such as whaling or spear phishing. Whaling is targeted phishing where attackers target high value companies or executives with valuable information. Spear phishing is a type of phishing where individuals, organisations or business groups are targeted with a personalized email (Goel & Jain, 2018).

This research also provides information for Dutch banking companies. In figure 14, 15 and 16 is shown how people perceive banking messages and how there is a divided and unclear knowledge in how the bank contacts people. The psychological side of people is also evaluated. How people comply when trusted, when a message is perceived trusted and what they notice when looking at a message. This could be used by banks to improve their security and communication channels.

People answered which party they trusted the most in fig. 23, 24 and 25 and the government had a second place. When developing applications this could be insightful. Also, people are being phished for personal information which includes the government e.g. DigiD. These government applications could also contain anti-phishing measures.

At last, for anti-phishing app developers this research gives insight in the peoples willingness to download these applications. The application would have to be made in cooperation with the bank or government otherwise people don't trust the application. Figure 24 and 25 shows the low compliance and trust in private corporations.

6.2 Limitations

There were a few limitations while conduction this research. The sample size of this research (n = 58) could be bigger to ensure the representability and reliability. There could be more samples added which possibly could lead to different answers. This survey had no participants who were victimized with phishing. Adding these to the sample could result in more recommendations. Also, the age distribution is a bit skewed at the younger ages. More samples could even out the distribution. This could result in different results because as research showed the likelihood of being phished is influenced by time spent online. Younger ages spent more time online than older age groups therefore the results are based on the group with the presumed highest risk. Therefore, not all risk groups might be fully represented. Phishing techniques alter every year and therefore not much research is conducted on this specific area. The trends and recent developments are not yet described and fully researched.

This research did get an industry expert his feedback, but more information from multiple banking companies could provide more findings.

6.3 Future research

For future research WhatsApp as messaging application needs anti-phishing software. Applications that work complementary with WhatsApp and their efficiency could be researched. Also, research into the training and how these in detail should be constructed could be researched. The topics are clear, but how to address them and in detail put into a training could be researched. The bank already has employees on phishing prevention. Also, a more detailed problem analysis could be done to see where attackers focus their attention. As shown in the results, the channels the bank uses to inform people is not clear to them. Research can be conducted in what is the most secure way and also how to create clarity to prevent confusion. At last, the recommendations could be implemented and monitored to see if and how much it reduces phishing victimization.

7. Bibliography

1. Autoriteit Persoonsgegevens. (z.d.). Smartphones en apps. https://autoriteitpersoonsgegevens.nl. accessed on 11 May 2021, from https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/smartphones-en-apps#welke-risico's-brengen-apps-met-zich-mee-voor-mijn-privacy-4750
2. Alsayed, A., & Bilgrami, A. (2017). E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. Int. J. Of Emerg. Techn. and Adv. Activ, 7(1), 109-115.
3. Alwanain, M. I. (2020). Phishing Awareness and Elderly Users in Social Media. IJCSNS, 20(9), 114.
4. Arachchilage, N., Love, S., & Scott, M. (2012). Designing a mobile game to teach conceptual knowledge of avoiding 'phishing attacks'. International Journal for e-Learning Security, 2(1), 127-132.
5. Arachchilage, N. A. G., & Hameed, M. A. (2017). Integrating self-efficacy into a gamified approach to thwart phishing attacks. arXiv preprint arXiv:1706.07748.
6. Ashford, W. (2014). Phishing Attacks Track Mobile Adoption, Research Shows.
7. Back, S., & Guerette, R. T. (2021). Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks. Journal of Contemporary Criminal Justice, 10439862211001628.
8. Beugel, J. B. (2019). Veel meer phishing en bankpasfraude in 2019. Betaalverenigingen & NVB
9. Bhardwaj, A., Sapra, V., Kumar, A., Kumar, N., & Arthi, S. (2020). Why is phishing still successful?. Computer Fraud & Security, 2020(9), 15-19.
10. Boddy, M. (2018). Phishing 2.0: the new evolution in cybercrime. Computer Fraud & Security, 2018(11), 8-10.
11. CAPEC. (2017), CAPEC-164: mobile phishing, https://capec.mitre.org/data/definitions/164.html (2017)
12. Chang, J.J. and Chong, M.D., "Psychological influences in e-mail fraud," Journal of Financial Crime, vol. 17, pp. 337-350, 2010.
13. Chang, J. J., & Chong, M. D. (2010). Psychological influences in e-mail fraud. Journal of Financial Crime.

14. Choudhary, N., & Jain, A. K. (2017, March). Towards filtering of SMS spam messages using machine learning based technique. In International Conference on Advanced Informatics for Computing Research (pp. 18-30). Springer, Singapore.
15. Claessens, J., Dem, V., De Cock, D., Preneel, B., & Vandewalle, J. (2002). On the security of today's online electronic banking systems. Computers & Security, 21(3), 253-265.
16. De Nationale Adviesbalie. (2020, 10 november). Wanneer krijg je compensatie van jouw bank bij fraude? https://laagsteadvocatentarief.nl/blog/wanneer-krijg-je-compensatie-van-jouw-bank-bij-fraude/
17. Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006, July). Decision strategies and susceptibility to phishing. In Proceedings of the second symposium on Usable privacy and security (pp. 79-90).
18. Ejure. (2015, 20 september). Phishing. http://www.ejure.nl/2015/10/phishing/
19. El-Alfy, E. S. M., & AlHasan, A. A. (2016). Spam filtering framework for multimodal mobile communication based on dendritic cell algorithm. Future Generation Computer Systems, 64, 98-107.
20. Felt, A. P., & Wagner, D. (2011). Phishing on mobile devices. na.
21. Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. Computers & Security, 73, 519-544.
22. Hong, J., "The state of phishing attacks", Contributed Articles in the Communication of the ACM. Vol 55 No 1, 2012
23. 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.
24. Jansen, J., & Leukfeldt, R. (2015, July). How people help fraudsters steal their money: An analysis of 600 online banking fraud cases. In 2015 workshop on socio-technical aspects in security and trust (pp. 24-31). IEEE.
25. Jansson, K. and von Solms, R., "Phishing for phishing awareness," Behaviour & Information Technology, vol. 32, pp. 584-593, 2013.
26. Jakobsson, M., "The human factor in phishing," Privacy & Security of Consumer Information, vol. 7, pp. 1-19, 2007.
27. Joo, J. W., Moon, S. Y., Singh, S., & Park, J. H. (2017). S-Detector: an enhanced security model for detecting Smishing attack for mobile computing. Telecommunication Systems, 66(1), 29-38.

28. Karami, A., & Zhou, L. (2014). Improving static SMS spam detection by using new content-based features.
29. Kathryn, P., Agata, M., Malcolm, P., Marcus, B., Jakobsson, J. G. and Myers, S., "The design of phishing studies: Challenges for researchers", Journal of Computers and Security, 2015.
30. Kumaraguru, P., Rhee, Y. W., Acquisti, A., Cranor, L. and Hong, J., "Protecting people from phishing: The design and evaluation of an embedded training email system", in Proceedings of CHI, 2010.
31. Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F., and Hong, J., "Teaching Johnny not to fall for phish," ACM Transactions on Internet Technology, vol. 10, pp. 1-31, 2010.
32. Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. Crime Science, 3(1), 1-10.
33. Lee, A., Kim, K., Lee, H., & Jun, M. (2016). A study on realtime detecting smishing on cloud computing environments. In Advanced multimedia and ubiquitous engineering (pp. 495-501). Springer, Berlin, Heidelberg.
34. MAX vandaag. (2020, 8 september). Hoe zit het? Krijgt u altijd uw geld terug als u online wordt opgelicht? https://www.maxvandaag.nl/sessies/themas/geld-werk-recht/hoe-zit-het-krijgt-u-altijd-uw-geld-terug-als-u-online-wordt-opgelicht/
35. Mohd Foozy, C. F., Ahmad, R., & Abdollah, M. F. (2013). Phishing detection taxonomy for mobile device. International Journal of Computer Science Issues, 10(1), 338-344.
36. NOS. (2020, 11 juni). Veel meer meldingen over phishing uit naam van de Belastingdienst. https://nos.nl/artikel/2336887-veel-meer-meldingen-over-phishing-uit-naam-van-de-belastingdienst
37. Politie. (z.d.). Controleer verkopergegevens. Geraadpleegd op 9 juni 2021, van https://www.politie.nl/aangifte-of-melding-doen/controleer-handelspartij.html
38. Proofpoint, 2017. Human factor. https://www.proofpoint.com/us/resources/threat-reports/human-factor
39. Rabobank. (z.d.). Geld terug na fraude. Geraadpleegd op 9 juni 2021, van https://www.rabobank.nl/particulieren/veiligbankieren/phishing-melden/geld-terug-na-fraude/
40. Rabobank. (2021). Phishingvoorbeelden. https://www.rabobank.nl/particulieren/veiligbankieren/phishingvoorbeelden/

41. Radar. (2020, 18 november). Tientallen miljoenen schade door bankfraude, wanneer krijg je compensatie? Radar – het consumentenprogramma van de AVROTROS. https://radar.avrotros.nl/uitzending/gemist/item/Tientallen-miljoenen-schade-door-bankfraude-wanneer-krijg-je-compensatie/
42. Rhee, H.-S., Kim, C., and Ryu, Y.U., "Self-efficacy in information security: Its influence on end users' information security practice behavior," Computers & Security, vol. 28, pp. 816-826, 2009.
43. Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10.
44. Shahriar, H., Klintic, T., & Clincy, V. (2015). Mobile phishing attacks and mitigation techniques. Journal of Information Security, 6(03), 206.
45. Sheng, S., Holbrook, M., Kumaraguru, P., L. F. and Downs, J., "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions", in Proceedings of the 28th International Conference on Human Factors in Computing Systems, USA, 2010.
46. Soyemi, J., & Hammed, M. (2020). AN ENHANCED AUTHENTICATION SCHEME FOR PREVENTING PHISHING ATTACKS ON WHATSAPP ACCOUNTS.
47. Team Coosto. (2021). Social media gebruik in 2021: cijfers & statistieken. Coosto. https://www.coosto.com/nl/blogs/social-media-gebruik-2021-cijfers-statistieken
48. Tewari, A., Jain, A. K., & Gupta, B. B. (2016). Recent survey of various defense mechanisms against phishing attacks. Journal of Information Privacy and Security, 12(1), 3-13.
49. Wandera, 2017. Mobile data report: focus on phishing. http://go.wandera.com/rs/988-EGM-040/images/Phishing%20%282%29.pdf
50. Wandera. (2019, 13 september). New family of mobile phishing attacks preying on WhatsApp users. https://www.wandera.com/malware-family-whatsapp/
51. Whatsapp. (2020, 29 september). Servicevoorwaarden van WhatsApp Business. https://www.whatsapp.com/legal/business-terms/?lang=nl