A CITIZEN PERSPECTIVE OF PHISHING IN HONG KONG

Bachelor Degree Project in Network and Administration
Spring term 2016

a15jeska
Jesper Karlsson

Supervisor: Erik Bergström
Examiner: Rose-Mharia
Åhfeldt
Abstract

In the world of today, Internet is a part of everything we do. Almost all appliances, from the cell phone to in some cases even freezers, are getting options to connect up to the Internet. But in this great, new world lurks dangers, as new threats are developed and sent out on the Internet at the same rate with which they are resolved.

The people in charge of managing their networks, be it a parent in a household or an employee at a corporation, needs knowledge of how to tackle these threats in a productive manner. Where do these people gain their knowledge and what does the public – who are joining the connected world at a rapid rate – think about having to gain this knowledge by themselves? Perhaps only a few need the knowledge of cybersecurity, or perhaps it should be covered as part of the school curriculum? This work strives to find the general opinion on this problem in one of the world’s most technologically advanced cities: Hong Kong.

Data of the citizens’ opinion on the subject was collected using a questionnaire handed out to citizens in multiple public places in Hong Kong. This research could greatly benefit governments or corporations who are in the pipeline of starting up courses for cybersecurity education or businesses in need of people with that knowledge.

The result was then compiled and analysed at which point the results then showed that the citizens of Hong Kong feel exposed to the threats that phishing poses. However, the majority also believed themselves capable of defending against phishing attempts. The result also showed the citizens claimed to have an understanding of phishing and a general awareness about most of the threats. The majority of the participants also thought that the responsibility to educate the populace about phishing should lie with the school system.

Future work based on this study could, for example, broaden the perspective of the survey and include different types of cybersecurity threats or use the same concept, only changing the focused threat to another.
# Table of contents

Table of contents.................................................................................................................................................. 2

1. Introduction .................................................................................................................................................. 4

2. Background ................................................................................................................................................. 5
   2.1. Cybersecurity and Hong Kong ........................................................................................................... 5
   2.2. Lack of knowledge ............................................................................................................................. 6
   2.3. Related work ........................................................................................................................................ 6

3. Problem description .................................................................................................................................... 7
   3.1. Aim ..................................................................................................................................................... 7
   3.2. Research questions ............................................................................................................................ 7
   3.3. Motivation .......................................................................................................................................... 7
   3.4. Delimitations ...................................................................................................................................... 8

4. Method ....................................................................................................................................................... 8
   4.1. Choice of method ............................................................................................................................... 8
   4.2. Quantitative survey ........................................................................................................................... 9
   4.3. Target group ....................................................................................................................................... 9
   4.4. Validity .............................................................................................................................................. 9
      4.4.1. Construct validity ....................................................................................................................... 10
      4.4.2. Internal validity .......................................................................................................................... 10
      4.4.3. External validity .......................................................................................................................... 10
      4.4.4. Reliability .................................................................................................................................. 10
   4.5. Ethics ............................................................................................................................................... 10

5. Implementation ........................................................................................................................................... 11
   5.1. Survey questions .............................................................................................................................. 11
      5.1.1. Separation questions ................................................................................................................. 11
      5.1.2. Understanding of phishing ...................................................................................................... 11
      5.1.3. Perceived exposure when it comes to cyber-crime ............................................................... 11
1. Introduction

Cybersecurity and the threats against it are something we now face daily. As the world’s connectivity grows, so does the number of malicious codes, software, and their creators who are trying to make a living in the darker side of the Internet. There is a large amount of malicious content on the Internet, phishing among the numerous threats to cybersecurity. However, the general populace tends not to know more than the basics when it comes to protecting themselves against the ever growing number of threats (Ben-Asher & Gonzalez, 2015).

Today in Hong Kong, phishing is the largest threat to cybersecurity and unaware users (Hong Kong Police Force, 2016a). The skills needed to avoid those problems should be common knowledge in the city, considering that the Hong Kong Police Force lists it as the biggest threat. Yet somehow, it seems that the only ones learning about cybersecurity are mostly professionals in the area, or those who actively search for the information themselves.

One thing that can counter network threats are firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). IDS are systems that check traffic, looking for harmful code (Ben-Asher & Gonzalez, 2015), and IPS are systems which automatically sift through the network and prevent entry for some malicious code. However, the most prevalent protection against network threats and their effects is knowledge. And according to research (Herley, 2009), even people with light knowledge reject security advice.

Perhaps learning about cybersecurity should be taught on a larger scale, maybe even in schools as part of regular education. This work aims to investigate the level at which the common citizen in Hong Kong perceives their education on cybersecurity, but also to whom they think cybersecurity and its threats should be taught.
2. Background

This chapter introduces the concepts surrounding cybersecurity, and also some ways of learning about it and why it's imperative to build knowledge about cybersecurity.

2.1. Cybersecurity and Hong Kong

Information security is a concept involving protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability (Kissel, 2013). Cybersecurity is a subset of information security and is a concept involving the technologies used to protect networks, data and computers from different attacks. The biggest issue with cybersecurity, but also its greatest feature, is that it needs to be ever evolving as the world of technology is rapidly renewing itself (Rouse, 2010). This work will use the term cybersecurity in all instances since it is the subset that this work will focus on.

*Phishing* is a cyber threat wherein perpetrators trick users into sharing personal information through deceptive computer-based means (Kissel, 2013). There are many different forms of phishing and one of them is social media deception in which perpetrators use social media sites to befriend people and then ask to borrow money and items with the intent of stealing them (Hong Kong Police Force, 2016b). Another scenario is that the perpetrator uses illegally gained login information to use an already existing account to ask for money or items from friends linked to that account (Hong Kong Police Force, 2016b). There have also been accounts of people using social media sites to gain acquaintances which the genuine user will try to meet, but upon agreeing for a meeting the perpetrator asks the user for some kind of deposit to guarantee their safety during the meeting and as soon as this is paid, the perpetrator is never heard from again (Hong Kong Police Force, 2016b).

*Email scams* are phishing crimes in which a genuine user or corporation is tricked into either paying money or revealing sensitive information via email to someone who has something to gain from the fraud (Hong Kong Police Force, 2016d). Once considered part of the simpler mischief known as SPA where emails with little or commercial content gets sent out in massive numbers to undesiring recipients, phishing type email scams have outgrown that category (Granova and Eloff, 2005). A corporate example would be receiving emails with false account information to which they should pay for another corporation’s services. Using stolen emails or inside information, the perpetrators know that a transaction soon will take place so they pretend to be one of the businesses in order to make the company pay the wrong people (Hong Kong Police Force, 2016d). Another common occurrence is individuals getting appeals to help relatives both near and far away by sending them money due to an accident or other event. The perpetrators often use hacked email accounts to send these emails to improve the illusion of authenticity, only when the relative in question is in fact contacted in other ways than emails is the scam revealed (Hong Kong Police Force, 2016d).

The phishing attacks have as of late become harder to detect as well as more technically advanced. Computers can be infected with advanced malware or spyware, just by opening the wrong email (Hong, 2012). One example is E-banking frauds which occur when a genuine user, who has received malicious software from, for example, an e-mail, tries to log in to their Internet banks (Hong Kong Police Force, 2016c). The perpetrators detect this and send the user false interfaces and pages which prompt the user to input sensitive information such as login names, password and even one-time passwords used by authentication.
The fact that phishing is prevalent in Hong Kong is not only discussed by the police force, but the Anti-Phishing Working Group or APWG as well. In a study conducted in 2015, they found out that not only is the Hong Kong populace being actively targeted, but the region hosts many phishing type pages as well (APWG, 2015).

2.2. Lack of knowledge

"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). As written in the previous section, more and more risks are associated with going online, not only with computers but with each online device. To not have some basic knowledge about these threats, increases the risks of becoming an easy target (Furnell, 2007). In an article written by Furnell (2007), the author gauges the level of security awareness amongst home users. His conclusion is that a widespread confidence lies on the surface of what the users believe they know, but when digging deeper they realize that there are many areas of their knowledge that is, in fact, lacking. One could argue that the problems lie with new and inexperienced users, but Furnell’s findings suggest that even those who considered themselves advanced users have shortcomings.

In a report written by Furman (2012), they link lack of education about cybersecurity, in this case phishing, with actually becoming vulnerable to it. The results show that even though a large number of users claimed to be aware of the threats, there was still a large part that couldn’t correctly define what a specific threat actually was. This supports Furnell’s (2007) findings and Furman’s (2012) report further states that by providing education that gives users knowledge of cyber threats and how to behave online to avoid them, the Internet would be a safer place for everyone. In other words, lack of knowledge is dangerous and puts a user at risk; it is only by learning more that one can be able to protect oneself properly.

2.3. Related work

There are some related works to what this work is trying to achieve, however most of them are more inclined to research the self-efficacy of users or how they perceive themselves to be able to fulfill the requirements of a safe network at home or at work.

Herley (2009), touches on the subject that people do in fact know a great deal about cybersecurity but due to it being obtuse or time consuming discard the risks and often ignore advice or configuration altogether. In the paper he describes it in a comical manner with the quote “given the choice between dancing pigs and security, the users will pick dancing pigs every time”. He then explains that security nowadays is not what the user is presented with, but instead an ever-growing list of policies, regulations and network threats.

Furnell (2007), writes in his work that users on the internet are increasingly exposed to network threats, and that users claim with a high degree of confidence that they are secure and aware, but after some inspection it can be suggested that much of the desired knowledge is lacking. He also states that this problem is more prevalent with newer users, but even more experienced users lacked in some areas.
Further research brings the subject of need, and supplying of knowledge regarding information security to the table. One of the results was that the citizen’s general knowledge needed to both be improved and perhaps introduced at a younger age and the authors discuss different channels for introducing this knowledge (Åhlfeldt, Andersén, Eriksson, Nohlberg, Bergström, Fischer-Hübner, 2015).

The fourth paper which correlates to this study, delves deeper into how people act when it comes to the network threat phishing. In that paper they test the susceptibility to phishing attempts of participants aged 18-25, and came to the conclusion that more knowledge equals better protection from the network threat that is phishing (Arachchilage & Love, 2014).

The common factor among these reports is that they bring up the knowledge that the end user has regarding cybersecurity; they focus mostly on security but one paper also has its main focus on how complicated the security efforts really are. This paper is designed to concentrate on the opinion of the target group and perceived knowledge regarding the cybersecurity threat phishing, instead of focusing on the actual knowledge of the target group.

**3. Problem description**
This chapter presents the aim, research questions, motivation, objectives and delimitations.

**3.1. Aim**
The aim of this work is to gain a basic understanding of how exposed the Hong Kong population perceives themselves to be when it comes to the cyber threat phishing. This work also aims to create an understanding of how knowledgeable the populace in Hong Kong is when it comes to common phishing attacks, but also who the general public think is responsible for sharing knowledge of cybersecurity and phishing avoidance.

**3.2. Research questions**
According to the Hong Kong police force, the largest cybersecurity threat for the citizens in this town is as stated above, phishing. It has indeed many forms and ways and encompasses many different smaller threats, but in large, phishing is the main “crime”. The research questions within this work are thus regarding phishing and its education.

- How exposed do the citizens of Hong Kong feel when it comes to the cyber threat phishing?
- How knowledgeable are the citizens of Hong Kong when it comes to common phishing types?
- Who do the citizens of Hong Kong think should have the responsibility to inform about phishing?

**3.3. Motivation**
Hong Kong is often thought of as one of the most advanced cities in the world when it comes to technology. A survey measuring the citizen’s general knowledge when it comes to phishing, the largest cybersecurity threat (Hong Kong Police Force 2016a), as well as where they think the responsibility to educate people about cybersecurity lies, provides valuable
data to the general public as well as government bodies. Especially considering the amount of difference it would make to have public schools teach children perhaps even at an early age how easily technology can be used maliciously.

Hong Kong is one of the top targets (Lee, Lee, Juan, Chen & Tseng, 2014), and sources, of phishing (APWG, 2015). The citizens there would be most interesting to interview about their opinions on the matter because of their target status. There is also an interest from the author to do the survey in Hong Kong seeing as it is going to be conducted during an exchange study period within the city.

When it comes to contributing, one thought is that this work might contribute a collection of opinions on how the general public wishes cybersecurity to be taught. This can be used to motivate, for example, schools to implement cybersecurity education within curriculums and subsequently lower the risk of people being affected by network threats such as this work’s main target; phishing.

3.4. Delimitations

This work is concerned with how aware the citizens are of phishing, and also to some extent who is responsible for teaching people about cybersecurity, but not how the information is gained. Therefore, it will not delve into where the general public thinks new threats should be announced. It will not look into what people use for protection against cyber threats. Gender differences are not something that this work will take in consideration, instead age and education level will be considered.

4. Method

This chapter deals with the methods used to create this work and its conclusions.

4.1. Choice of method

This work will start off with a literature review to collect information about what has been done earlier in this area of research, but also to learn about different terms surrounding the research subject. This is going to be done using systematic literature reviews and snowballing (Wohlin, 2012) to find relevant material.

An experiment in this type of survey is not particularly feasible, as experiments usually subject the same groups of targets to new differing methods in order to find their conclusions and due to that nature, experiments were not chosen. Neither were qualitative studies with interviews chosen. Granted, a qualitative study would lead to more explanatory answers where the citizens could answer what they truly thought of the presented subjects, but due to the fact that the target group for this work is the population of Hong Kong, the amount of interviews that would be needed in order to get a broad enough perspective would probably need to be very large, and due to time limits this too was omitted.

For this particular work, a quantitative method will be chosen since it collects more relevant data from a larger group of people than can be done quickly with a qualitative method. The quantitative method chosen is that of a questionnaire survey which can be passed out and answered almost everywhere to capture the broadest possible range of people and not a small select group. This is important because the survey is aimed at the citizens of Hong
Kong, which means the survey needs a large pool of different participants from all walks of life.

4.2. Quantitative survey

A survey with quantitative nature, especially questionnaires, is created to get a generalized result out of many participants, often the survey places people in different groups to get images of different relations within, for example, different age groups (Atlas, 2016). The quantitative approach puts numbers on data which makes it easier to compile the results into conclusions (Atlas, 2016). With the many responses collected from a quantitative survey, a generalized view of the opinion of the public can be compiled, in this case that data will be crucial to the eventual conclusion of this work. It is however important to note that the answers, being numbered and not free text, tend to become less deep (Atlas, 2016).

To make sure that the answers of the questionnaire will be usable and unbiased, it must be planned accordingly. Due to the research questions’ opinionated nature, no real yes or no questions can be present on the questionnaire since that would lead to absolutes which in the later stages of the work can become a validity threat when it comes to opinions (Wohlin et al., 2012). What is going to be done instead is to use the Likert scale, which consists of five-point answers where a respondent could answer either “absolutely not” or “very low” with the contrast of “absolutely yes” and “very high” as well as a “not sure” option. Due to the fact that the range thus will have an even number of squares between them – if you count out the not sure – it allows people to align themselves in one direction, rather than staying in a comfortable middle (Chandler & Munday, 2014).

4.3. Target group

The target group of this work will be ordinary citizens living in Hong Kong. To accurately represent the population a broad group of participants will get the chance to answer. This work will not differentiate citizens by their gender, instead as stated above, age and education levels will be the deciding factor when it comes to separating groups of people in the respondent pool. This is due to gender not being a relevant factor for this research. Age and education will be the separating factor since cybersecurity is important for everyone in today’s world regardless of gender.

Since Hong Kong is the target area, and this work will try to limit itself to its citizens, people without citizenship will not be included in the final conclusion. All surveys will be printed and done out in the field, handed out and answered at the same time. Convenience sampling will be used since time is limited and a great number of people pass by locally each day, thus eliminating all need to search for citizens elsewhere.

To get a well distributed answer pool, the survey needs to take some answer quotas into consideration, if one particular group becomes overrepresented then it can become both a threat to the validity of the work, but also damage the status of citizen, since the definition encompass all kinds of people living in Hong Kong.

4.4. Validity

The main validity threats are listed below. They are fetched from Wohlin (2012). A complete list of validity threats can be found in appendix A.
4.4.1. Construct validity
Construct validity deals with the issues surrounding misinterpretation between researcher and subjects. For example, a question that means one thing to you could mean something completely different (Wohlin et al., 2012).

Due to the questionnaire being the same for everyone, construct validity is more or less achieved. Misinterpretations can still occur, but due to the human factor this cannot be avoided.

4.4.2. Internal validity
Internal validity deals with issues that stem from researchers failing to see part C of an equation while examining the correlation between A and B. This can happen due to the researcher not knowing about the third factor or that he underestimates its value (Wohlin et al., 2012).

Internal validity is a big threat to this survey because it is hard to see it from another angle when working alone. The study strives to counter this by often asking for second opinions from parties not involved, this might lead to a smaller risk of missing critical information regarding both the foundation of the theory but also the local area.

4.4.3. External validity
External validity is all about whether the research can be released in such a way that it is still interesting to external stakeholders. This threat exists due to researchers not generalizing data enough and thus a non-relatable compilation is released (Wohlin et al., 2012)

This work will try to avoid this type of threat by careful analysis and compilation in order to get the best results in an easy to understand fashion.

4.4.4. Reliability
Reliability is a validity threat concerning how the single researcher handles their work. Examples in this area include researchers compiling poor documentation so that no external party could ever replicate the experiment (Wohlin et al., 2012).

Currently the knowledge surrounding cybersecurity is not very widespread, the biggest threat to this validity is that this may very well change in the future. Asking the same opinionated questions about whether or not it should be taught could then be obsolete.

4.5. Ethics
According to Wohlin et al. (2012) empirical research that involves people must take some ethical aspects into account, such as things prohibited by either law or social standards. Four points in particular are in need of discussion:

- People who partake in the survey must give “informed consent” meaning that they must all be aware and informed with access to relevant information before the decision of partaking is made.
- The study should be done in a way that gives “scientific value” so that even though the risks are minimal, people who partake in the survey are accepting of the risks.
- The study must be made in such a way that confidentiality of data and sensitive information are kept.

- The study need to see to it that the beneficence always is larger than the possible risk of harm to the people partaking.

This work will make sure to follow those points by firstly passing the questionnaire out in public places where people can ask relevant questions before venturing into the survey and also give their consent for the data to be used in this work. Everyone who answers the questionnaire will be guaranteed anonymity so that they can answer without repercussions.

5. Implementation

Presented below is the implementation of the chosen method and how the questionnaire will be formed. The questions in the survey needs to be formed in such a way that they answer the research questions. There must also be some consideration to whom the questionnaire will be passed out to, and can thus be answered by as many people as possible without difficulty. The survey questions can be found as they were on the questionnaire in appendix B.

5.1. Survey questions

This segment details the questions found in the survey. Each question with the exception of the first three separation questions will have its own headline detailing its motivation and reasoning. The research questions that needs to be answered are about how exposed to and how knowledgeable about phishing the citizens are as well with whom they feel that the responsibility to inform about phishing lies.

5.1.1. Separation questions

The first four questions in the survey serve as a mean to categorize the participants so that they can be divided in groups which leads to more accurate correlations and a more accurate representation of the different citizens. There are four factors here. First comes the question of citizenship, if the answer is no, then the results cannot be used in the final conclusions, this is due to the survey being targeted towards the citizens of Hong Kong. Then comes age, then education level and also if they had completed a cybersecurity course of any kind. The second (age) and third (education) questions are tied together. These were chosen as separators because it’s possible to see correlations between the opinions when it comes to age and education, as well as if it would make participants feel differently towards their exposure to the threats.

5.1.2. Understanding of phishing

The fourth question in the questionnaire asks if the respondent has an understanding when it comes towards phishing. This will be used together with the question regarding perceived awareness to determine correlations between exposure and education, in turn answering the research question regarding how knowledgeable they feel towards the subject.

5.1.3. Perceived exposure when it comes to cyber-crime

The aim of the fifth question will be gathering data about the users’ perceived exposure and is based on the phishing chapter of the Statistics Sweden report regarding the use of
computers and the internet by private persons (2015). This question will gauge the level of
fear the individual has for some of the more usual phishing types, it also helps introduce
phishing to the answerer which will be vital to the coming questions. Together with the
question regarding ability to protect oneself, it will also answer the research question
regarding perceived exposure to phishing attacks.

5.1.4. Perceived awareness of different phishing types
The sixth question asks for the respondent’s awareness when it comes to some of the more
usual phishing types in Hong Kong. The types selected are all based on the most common
from the Hong Kong Police Force (2016) webpage, where they state some of the crimes
plaguing the city currently. This, together with the question regarding understanding of
phishing, will determine their perceived knowledge of phishing types and thus answer the
research question regarding knowledge.

5.1.5. Perceived knowledge of how to defend against or avoid phishing
attempts
This question, together with the question of perceived exposure, aims to answer the research
question of how aware they feel towards phishing, and also to help correlate if previous
knowledge and feeling of exposure affects their ability to protect themselves. As Furman
(2012) and Furnell (2007) states in their respective reports, more knowledge leads to better
ability to protect oneself.

5.1.6. Opinion of who is responsible for teaching online security,

The aim of the eighth question will be to find out who the participants think should be
responsible for teaching the populace about cybersecurity. This question was formed with
the help of a study by Åhfeldt et al. (2015). One of the things addressed in that discussion is
that the citizens should perhaps gain some more competence within information technology
earlier in life, perhaps even in schools. This work also tries to find out where the citizens think
the responsibility lies, and since the other study was done in Sweden, there might be a
completely different result from a study conducted in Hong Kong.

There is also a free-text field on this question, if anyone feels that the answers provided are
not enough. This question will answer this work’s final research question of with whom the
responsibility to teach cybersecurity lies.

5.1.7. How has answering this questionnaire changed their perspective of
security?
The ninth and final question has the aim of making the answerer reflect on phishing as an
issue. With this a correlation between those who know a lot and don’t want to know more and
vice versa can be shown. It is based on a similar question in a questionnaire written for the
report assessing the security perceptions of personal Internet users by Furnell (2007). The
motivation behind this question is to see if this survey has been eye-opening for the
participants to the different threats within phishing and cybersecurity and if it has led to them
wanting to learn more about this subject. This in turn will not help answer a single research
question, but all of them.
5.2. Passing out the questionnaires

There was a need to ensure that a large amount of participants would be able to answer the survey in the short time frame that was available, and to get a varied group of participants so that the citizen of Hong Kong could more closely be represented. With this in mind a plan was formed to pass copies of the questionnaire to three groups of assistants, which were handed 100 copies each and instructed to what the questions mean so that they could more easily translate if needed. The groups then sat up answering booths in strategic locations around Hong Kong. The survey was to be filled out behind a screen as to protect the anonymity of the participant. The locations that was chosen were outside the Hong Kong Polytechnic University, outside the IFC shopping mall and next to a supermarket near Nathan road. These locations were chosen due to the large number of people who pass through these places every day. The booth next to the Hong Kong Polytechnic University was also close to a big bus station where people from all walks of life pass through to catch their commutes. Ideally to get a good representation it would need more than the 300 copies to get an accurate description of reality, but within the time frame a goal of 200 was set.
6. Results

In this section, the results and analysis of the responses collected from the survey are presented. The result is presented in different sections, divided after the different types of questions in the survey and is finished with a collective summary and analysis of these parts. All questions were answered by all participants.

6.1. Background questions

The survey received answers from a total of 178 participants, out of which nine replied that they were not in fact citizens of Hong Kong, and thus these were excluded since they were outside of the intended target group, leaving 169 as the counted total of participants. Out of these there were 122 in the ages 18-30, 40 who were in the ages 31-50 and seven who were over 50 years old. The third separation through the background questions was about education. 29 of the total participants replied that they had completed less than high school education, 75 responded that they had completed high school education and 65 responded that they had completed higher education.

The fourth and last of the background questions was about whether or not the respondent had attended a course in cybersecurity. Out of the 169 total, there were three who had done so in their spare time, 56 who had done so through work and 34 who had done so through school. On the other hand, there were 57 who had not attended a course in cybersecurity, but they would like to do so and 14 who had not attended a course and did not want to at all. Finally, there were five participants who weren’t sure if they had attended a course in cybersecurity.

The participants could after these background questions get separated into different groups, the first separation was by age and education. In the 18-30 age bracket there was a total of 122 participants, out of which 24 had less than high school education, 46 had high school education and 52 had higher education. In the 31-50 age bracket there was a total of 40 participants, out of which three had less than high school education, 25 had high school education and twelve had higher education. In the last age group which was 50+, there were a total of seven participants out of which two had less than high school education, four had high school education and one had higher education. For complete distribution, see figure 1.
The second separation was decided by whether or not the participants had completed a course in cybersecurity. This separation doesn’t take either age or education into consideration and only goes on what the participants responded in question three b, which was presented above but is clarified through figure 2 below.

Figure 2 If citizens have attended course in cybersecurity

6.2. Phishing

Below follows the presentation of the results from the phishing section of the questionnaire

6.2.1. Understanding

The phishing section of the questionnaire started off with a basic “yes or no” question, asking for the participants understanding towards phishing as a threat. Out of the 169 total responses, 116 perceive themselves to have an understanding of the cyber threat phishing, whilst the remaining 53 do not.
When going deeper and separating the numbers, it shows that the majority of the ones with less than high school education answered that they did not have an understanding of the cyber threat phishing. There were 24 participants in the 18-30 age bracket and they responded with ten yes, versus 14 noes while the 3 participants from the 31-50 age bracket answered with one yes versus two noes, and the two participants in the 50+ age bracket with less than high school educated both answered no.

The 46 participants who had completed a high school education in the 18-30 age bracket responded with 34 yes and 12 noes, the 31-50 age bracket had 25 participants and they answered with 13 yes, 12 noes, whilst the four 50+ answered one yes and three noes.

Among the participants with higher education, there were 52 in the 18-30 age bracket and they responded with 49 yes and 3 noes. In the 31-50 age bracket there were 12 participants out of whom 7 answered yes while 5 answered no and in the higher educated 50+ age bracket, there was only a single respondent who answered yes. For a complete view of the distribution of answers, see figure 3.

Further separation of the groups reveals that the participants who answered that they have undergone a previous course in cybersecurity, had an understanding of the cyber threat phishing. Out of the total of 93 participants who had previously undergone a course there were a total of 90 yes and three noes, while the group who had not previously undertaken a course had 71 participants and they answered 26 yes and 45 noes. The group who was not sure of whether or not they had attended a previous course, replied with zero yes and five noes.

6.2.2. Exposedness to phishing

The question about how exposed the citizens felt when it came to frequently phishing threats, was formulated in such a way that there were three statements portraying different scenarios to which the participants would mark the option on a Likert scale that closest represented
how much they agreed with the statement. The different statements were about them feeling exposed to receiving fraudulent emails through respected sources, being the target of a false URL leading to a fake website, and their accounts on frequently used webpages being compromised due to keylogging.

Amongst the less than high school educated 18-30 age bracket, the statements were rated with emails having six “absolutely yes” I feel exposed, ten “yes”, eight “no”, I do not feel exposed, zero “absolutely not”, and zero “not sure”. Fake URLs were rated with four absolutely yes, 14 yes, three noes, zero absolutely not and three not sure. Keylogging was rated with six absolutely yes, nine yes, eight noes, one absolutely not and zero not sure.

For the same three questions the less than high school 31-50 age bracket rated emails with two yes, one no, no one choosing either absolutely yes, absolutely not or not sure. Fake URLs were rated one yes, one no, one not sure and none in either absolutely yes or absolutely not. Keylogging had the rating of one yes, two not sure and none in absolutely yes, no or absolutely not.

The less than high school 50+ age bracket only had two participants and rated emails with one absolutely yes, one no and no one choosing yes, absolutely not or not sure. The fake URLs were rated with one absolutely yes, one yes and nothing in no, absolutely or not sure. The keylogging statement had one absolutely yes, one not sure and no one choosing yes, no or absolutely not. A total for all the answers can be found in figure 4 below.

The participants who had completed a high school education in the 18-30 bracket rated their statements for email with one absolutely yes, 31 yes, eight noes, six not sure and none choosing absolutely not. Fake URLs were rated with four absolutely yes, 30 yes, eight noes, four not sure and no choices of absolutely not. Keylogging was ranked five yes, 33 noes, seven absolutely not, eleven not sure and no one answered absolutely yes.

Coming up to the 31-50 high school educated age bracket, they rated emails with ten absolutely yes, three yes, seven noes, five not sure and no absolutely not. The exposure to fake URLs got the rating of six absolutely yes, twelve yes, four noes, two absolutely not and
one not sure. Keylogging exposure received the rating five absolutely yes, six yes, nine noes, one absolutely not and four not sure.

In the high school educated 50+ age bracket, the fraudulent email exposure was rated with two absolutely yes, one no, one not sure and no choices of yes or absolutely not. The false URL exposure was rated with one absolutely yes, three not sure and no one chose yes, no or absolutely not. Keylogging exposure was rated with one absolutely yes, three not sure and nothing in yes, no or absolutely not. A total for all the answers can be found in figure 5 below.

![Figure 5](image)

**Figure 5** Exposure felt by participants with high school education

The higher educated participants in the 18-30 age bracket rated their exposure when it came to fraudulent emails with 34 absolutely yes, eleven yes, four noes, three not sure and no one choosing absolutely not. The exposure towards fake URLs was rated with 13 absolutely yes, 28 yes, eight noes, three absolutely not and no one responded not sure. Keylogging exposure was rated with eight absolutely yes, seven yes, 21 noes, 16 absolutely not and no answers on not sure.

In the higher education 31-50 age bracket the rate for email exposure was rated with five absolutely yes, two yes, four noes, one absolutely not and no one was not sure. Fake URLs were rated with one absolutely yes, seven yes, one no, two absolutely not and one was not sure. Keylogging was rated with zero absolutely yes, five yes, four noes, one absolutely not and two were not sure.

The higher educated 50+ bracket consisted of only one participant who rated the feeling of exposure to fraudulent emails as absolutely not, the feeling of exposure towards fake URLs was rated as no and the feeling of keylogging exposure was rated as yes. A total of the answers can be seen in figure 6 below.
When looking at another separating question, namely if the participant had taken a previous course in information technology, it’s shown that the ones who previously had taken a course rated their perceived exposure towards fraudulent emails as 36 absolutely yes, 27 yes, 20 noes, two absolutely not and ten not sure. They rated their exposure towards fake URLs as 17 absolutely yes, 41 yes, 23 noes, four absolutely not and eight not sure. When it came to keylogging they rated their exposure with six absolutely yes, 21 yes, 58 noes, three absolutely not and five not sure.

Those who had not completed a course earlier answered their perceived exposure to the emails with 22 absolutely yes, 31 yes, twelve noes, zero absolutely not and five not sure. Towards fake URLs, their perceived exposure was ranked with twelve absolutely yes, 50 yes, three noes, three absolutely not and three not sure. Keylogging exposure was ranked with 13 absolutely yes, eleven yes, 14 noes, 23 absolutely not and seven not sure.

Those who were not sure whether or not they had taken a course ranked their exposure to the emails with one absolutely yes, three yes, one no and nothing in absolutely not or not sure. They ranked false URLs as one absolutely yes, one yes, one no, zero absolutely not and two not sure. On keylogging exposure, they rated it with two absolutely yes, two yes, zero noes, zero absolutely not and one not sure.

6.2.3. Awareness

The question about how aware the citizens felt they were to different phishing types was formulated in the same way as the one about exposure; here there were four different phishing threats listed and the participants would mark the option on a Likert scale that most closely represented how much they were aware of the threat. The different threats were social media deception, e-banking fraud, email scamming, and online blackmailing.

Amongst the participants with less than high school education, there were a total of 24 participants in the 18-30 age bracket, out of which three claimed to be very aware of the threat of social media deception, five somewhat aware, 14 not very aware and two not aware at all. When it came to the threat of e-banking fraud, there were none that claimed to be very
aware, two who were somewhat aware, 13 who were not very aware, six not aware at all and three chose not sure. When it came to the threat of email scamming, there were five who claimed to be very aware, seven somewhat aware, six not very aware, three not aware at all and three chose not sure. When it came to the threat of online blackmailing, there were none who claimed to be very aware, one who was somewhat aware, eleven who were not very aware, seven who were not aware at all and five chose not sure.

Figure 7 shows a complete distribution of answers in which it shows that the majority of the participants are not very aware of the different types of phishing threats at all. It is only when it comes to email scamming that there are more who are aware of the threat than there are participants who are unaware.

![Figure 7](image)

**Figure 7** Threat awareness, less than high school, ages 18-30

In the 31-50 age bracket, there were a total of three participants, out of which one was somewhat aware of the threat of social media deception, one not very aware and one not aware at all, while none were very aware at all. When it came to the threat of e-banking fraud, there were none that claimed to be very aware, somewhat aware or not aware at all, but two who were not very aware and one chose not sure. When it came to the threat of email scamming there was one who claimed to be very aware, one somewhat aware and one not very aware. None chose not aware at all. When it came to the threat of online blackmailing, there were none who claimed to be very aware or somewhat aware, one who was not very aware, none who were not aware at all and two chose not sure. Here too there is a majority who are not aware of the different threats, and it is only when it comes to email scamming that there are more of the participants that are aware than there are those who are not.

In the 50+ age bracket, there were only a total of two participants. They both chose not sure when it came to social media deception and e-banking fraud, but on email scamming and online blackmailing, there was one who chose not very aware on both and the other chose not sure on both. Here, there is a very uneven distribution between being aware and not being aware of the threats as all of the answers fall in the unaware of the threats’ section.
It is thus easy to see that the participants that have less than high school education in most cases are unaware of the different phishing threats they might face. There are, of course, those who are very aware, but in the end these present an overall minority.

Amongst the participants with high school education, there were a total of 46 participants in the 18-30 age bracket, out of which eight claimed to be very aware of the threat of social media deception, 26 somewhat aware, nine not very aware, one not aware at all and two chose not sure. When it came to the threat of e-banking fraud, there were two who claimed to be very aware, four who were somewhat aware, 33 who were not very aware and seven not aware at all. When it came to the threat of email scamming, there were three who claimed to be very aware, 24 somewhat aware, eight not very aware, nine not aware at all and two chose not sure. When it came to the threat of online blackmailing, there were two who claimed to be very aware, 15 who were somewhat aware, six who were not very aware, 16 who were not aware at all and seven chose not sure.

Figure 8 shows a complete distribution of the answers, and it shows that there is a majority that is aware of the threats of email scamming and social media deception. There are, however, not many who are aware of the threat of e-banking fraud, and only 36% that are aware of online blackmailing.

In the 31-50 age bracket, there were a total of 25 participants, out of which two claimed to be very aware of the threat of social media deception, 16 somewhat aware, four not very aware and three not aware at all. When it came to the threat of e-banking fraud, there were none who claimed to be very aware, 13 who were somewhat aware, six who were not very aware, four not aware at all and two chose not sure. When it came to the threat of email scamming, there was one who claimed to be very aware, ten somewhat aware, eleven not very aware, two not aware at all and one chose not sure. When it came to the threat of online blackmailing, there was one who claimed to be very aware, nine who were somewhat aware, three who were not very aware, eight who were not aware at all and four chose not sure.

Figure 9 shows a complete distribution of the answers, and it shows that there is a majority that is aware of the threats of e-banking fraud and social media deception. There are,
however, close to 40 and 45% respectively of the participants that are aware of the threats online blackmailing and email scamming.

![Figure 9 Threat awareness, high school, ages 31-50]

In the 50+ brackets, there were a total of four participants, out of which two were somewhat aware of the threat of social media deception, one not very aware and one chose not sure. When it came to the threat of e-banking fraud, there were two who claimed to be very aware, one who was somewhat aware and one not aware at all. When it came to the threat of email scamming, there were two who were somewhat aware, one not very aware and one not aware at all. When it came to the threat of online blackmailing, there was one who was not very aware, one who was not aware at all and two chose not sure. This results in the majority being aware of social media deception and e-banking fraud, whereas email scamming has an even distribution and none were aware of online blackmailing.

This shows that the majority of those with high school education are aware of the threat social media deception, but there is a great minority who are aware of the threat online blackmailing.

Amongst the participants with higher education, there were a total of 52 participants in the 18-30 age bracket, out of which six claimed to be very aware of the threat of social media deception, eight somewhat aware, 32 not very aware, five not aware at all and one chose not sure. When it came to the threat of e-banking fraud, there were eleven that claimed to be very aware, eight who were somewhat aware, 22 who were not very aware, three not aware at all and eight chose not sure. When it came to the threat of email scamming, there were nine who claimed to be very aware, 21 somewhat aware, seven not very aware, twelve not aware at all and three chose not sure. When it came to the threat of online blackmailing, there were 19 who claimed to be very aware, 13 who were somewhat aware, 15 who were not very aware and five who were not aware at all.

Figure 10 shows that a majority is unaware of both social media deception and e-banking fraud, but a clear majority is aware of online blackmailing and e-mail scamming.
In the 31-50 age bracket, there were a total of 12 participants, out of which none claimed to be very aware of the threat of social media deception, two somewhat aware, two not very aware, seven not aware at all and one chose not sure. When it came to the threat of e-banking fraud, there was one who claimed to be very aware, eight who were somewhat aware, two who were not very aware and one not aware at all. When it came to the threat of email scamming, there were four who claimed to be very aware, five somewhat aware, three not very aware and none not aware at all. When it came to the threat of online blackmailing, there were six who claimed to be very aware, three who was somewhat aware, one who were not very aware and two who were not aware at all. This shows that there is a great minority that is aware of social media deception, and a great majority that is aware e-banking fraud, email scamming and online blackmailing.

In the 50+ age bracket, there was only one respondent. They were somewhat aware of the social media deception, very aware of the e-banking fraud, very aware of email scamming and somewhat aware of the online blackmailing.

This shows that the majority of those with higher education are unaware of the threat of social media deception and a great majority are aware of online blackmailing and e-mail scamming, with e-banking fraud landing somewhere in the middle.

Using the second separation, there were a total of three participants who had taken a cybersecurity course in their free time and they were all very aware of the threat of social media deception. One was somewhat aware of e-banking fraud and two not very aware, while all three were very aware of email scamming. When it comes to online blackmailing, there was one who was very aware, one who was somewhat aware and one was not aware at all.

There were a total of 56 participants who had taken a course through work, and out of these, there were eight who were very aware of social media deception, 23 who were somewhat aware, 19 who were not very aware, two who were not aware at all and one who was not sure. When it comes to e-banking fraud, there were 14 who were very aware, 23 who were somewhat aware, 15 who were not very aware, two who were not aware at all and two who
were not sure. When it comes to email scamming, there were 16 who were very aware, 27 who were somewhat aware, ten who were not very aware and three who were not aware at all. When it comes to online blackmailing, there were 23 who were very aware, 26 who were somewhat aware, four who were not very aware and three who were not aware at all.

There were a total of 34 participants who had taken a course through school and out of these, there were five who were very aware of social media deception, ten who were somewhat aware, 14 who were not very aware, four who were not aware at all and one who was not sure. When it comes to e-banking fraud, there were three who were very aware, nine who were somewhat aware, 17 who were not very aware, none who were not aware at all and five who were not sure. When it comes to email scamming, there were two who were very aware, eleven who were somewhat aware, one who were not very aware, fourteen who were not aware at all and six who were not sure. When it comes to online blackmailing, there were three who were very aware, twelve who were somewhat aware, four who were not very aware, three who were not aware at all and twelve who were not sure. A complete distribution of the answers in can be seen in figure 11.

![Figure 11 Awareness of those who had previously taken a course](image)

There were a total of 57 participants who had not taken a course at all and out of these, there were none who were very aware of any of the threats. There were however 20 who were somewhat aware of social media deception, 29 who were not very aware and eight who were not aware at all. When it comes to e-banking fraud, there were none who were somewhat aware either, 41 who were not very aware, twelve who were not aware at all and four who were not sure. When it comes to email scamming, there were 30 who were somewhat aware, 22 who were not very aware and five who were not aware at all. When it comes to online blackmailing, there were none who were somewhat aware either, 26 who were not very aware, 29 who were not aware at all and two who were not sure.

There were a total of 14 participants who had not taken a course and also did not want to, and out of these, there were three who were very aware of social media deception, seven who were somewhat aware, one who was not very aware, one who was not aware at all and
two who were not sure. When it comes to e-banking fraud, there were none who were very aware, three who were somewhat aware, four who were not very aware, four who were not aware at all and three who were not sure. When it comes to email scamming, there were three who were very aware, none who were somewhat aware, four who were not very aware, four who were not aware at all and three who were not sure. When it comes to online blackmailing, there was one who was very aware, three who were somewhat aware, three who were not very aware, two who were not aware at all and five who were not sure. A complete distribution of the answers in can be seen in figure 12.

Figure 12 Awareness of those who had not previously taken a course

There were a total of five participants that replied that they were not sure whether or not they had taken a course in cybersecurity, and out of them there were none who were very aware of any of the threats. There was however one who was somewhat aware of social media deception, none that were not very aware, one who was not aware at all and three who wasn’t sure. When it comes to e-banking fraud, there was one who was somewhat aware, none who were not very aware, two who were not aware at all and two who were not sure. When it comes to email scamming, there were two who were somewhat aware, one who was not very aware, one who was not aware at all and one who was not sure. When it comes to online blackmailing, there were none who were somewhat aware either, two who were not very aware, one who was not aware at all and two who were not sure. A complete distribution of the answers in can be seen in figure 13.
6.2.4. Perceived ability to defend oneself from phishing

In this question the participant was asked whether or not they thought themselves to be able to defend themselves against phishing attempts, the available responses were yes, no or not sure. Out of the 169 total participations, 97 responded yes, 68 responded no and four participants responded that they were not sure.

When categorizing the participants in groups, it’s shown that the less than high school educated in the 18-30 age bracket had responded with 17 yes, seven noes and zero not sure. The participants from the 31-50 age bracket answered one yes, two noes and zero not sure. In the 50+ age bracket, responded with zero yes, one no and one not sure.

In the group with participants who had completed a high school education, the 18-30 age bracket answered 25 yes, 21 noes and zero not sure. The participants from the 31-50 age bracket responded 15 yes, nine noes, and one not sure. Finally, the 50+ age bracket responded with one yes, two noes and one who was not sure.

Out of the participants with higher education, the 18-30 age bracket answered 30 yes, 21 noes and 1 not sure. The 31-50 age bracket within the higher education group answered seven yes, five noes and zero not sure. In the 50+ age bracket the single participant answered yes. A complete distribution of the answers in can be seen in figure 14.

Figure 13 Awareness of those who were not sure if they had previously taken a course
To see whether or not previously taking a course has made any difference, it’s noted that the participants who had previously taken a course in cybersecurity responded with 63 yes, 30 noes and zero not sure. The participants who had not previously attended a course answered with 33 yes, 36 noes and two not sure. Out of the participants who were not sure, the answers were one yes, two noes and two not sure.

6.2.5. Responsibility

The eighth question of the questionnaire was about who the participant thought was responsible for distributing knowledge about cybersecurity so that people could protect themselves from cybersecurity threats such as phishing. The options they could choose were that the responsibility lies with themselves, with the school system, with the Internet service provider, with the government, and that they didn’t think the current cybersecurity education was a problem. There was also a free-text answer labelled “other” in which the participants could specify if they had other thoughts.

Amongst the participants with less than high school education, there were a total of 24 responses in the 18-30 age bracket, out of which 5 said that it was their own responsibility, 10 that it lay with the school system, 3 with the ISP, 6 with the government and no one thought it was neither a problem or had any other thoughts about it.

In the 31-50 age bracket there were a total of three participants, out of which one thought it lay with the school system, one with the government, and none who thought it was neither their own responsibility, the ISP’s or thought that it wasn’t a problem. The last one, however, used the “other”-option and filled in another thought, namely that “if you work with a computer, then they [the company] should teach you, otherwise, there is no problem”.

In the 50+ age bracket, there were only two participants that had less than high school education. One of them thought that the responsibility of distributing the knowledge was their own and the other thought it lay with the government. Thus, there was no one who thought that it lay with the school system, the ISP, or thought it wasn’t a problem.
Amongst the participants with high school education, there were a total of 46 participants in the 18-30 age bracket, out of which nine thought that it was their own responsibility, 13 thought that it lay with the school system, and 23 with the government. One thought that it wasn’t a problem, but none thought that it lay with the ISP.

In the 30-50 age bracket there were a total of 25 participants, out of which two thought that it was their own responsibility, 18 who thought that the responsibility lay with the school system, and five with the government. None thought that it lay with the ISP or that it wasn’t a problem.

Amongst the participants with high school education, there were a total of 46 participants in the 18-30 age brackets, out of which nine thought that it was their own responsibility, 13 thought that it lay with the school system, and 23 with the government. One thought that it wasn’t a problem, but none thought that it lay with the ISP.

In the 30-50 age brackets there were a total of 25 participants, out of which two thought that it was their own responsibility, 18 who thought that the responsibility lay with the school system, and five with the government. None thought that it lay with the ISP or that it wasn’t a problem.

In the 50+ age bracket there were a total of four participants, out of which one thought that the responsibility lay with the school system, one with the government and one thought that it wasn’t a problem. None thought that it was their own responsibility or that it lay with the ISP, but there was one who used the “other”-option to write “I think there is too much focus on [the] Internet, more people should go back to using secure papers”.

Amongst the participants with higher education, in the 18-30 age bracket there were a total of 52 participants out of which 21 thought that it was their own responsibility, 26 thought that it lay with the school system, and three who thought that it lay with the government. Two thought that it wasn’t a problem, but none thought that it lay with the ISP.

In the 31-50 age brackets, there were a total of twelve participants out of which five thought that the responsibility lay with the school system and seven with the government. None thought that it was their own responsibility, that it lay with the ISP or that it wasn’t a problem.

In the 50+ age bracket that had higher education, there was only one respondent and they thought that the responsibility lay with the school system. For the complete distribution of answers put in context, see figure 15.
Using the second separation, there were a total of three participants who had taken a course in cybersecurity in their spare time, and out of these there were two who thought the responsibility was their own and one that thought it lay with the school system. Out of the total 56 participants who had taken a course through work, there were 15 who thought it was their own responsibility, 23 who thought it lay with the school system, one who thought it lay with the ISP, and 17 who thought that it lay with the government. None thought that it wasn’t a problem.

A total of 34 participants had taken a course through school, and out of these, two thought it was their own responsibility, 16 thought it lay with the school, one thought it lay with the ISP, 14 with the government and one thought that it wasn’t a problem. Out of the 57 participants that had not taken a course but would like to, there were 15 who thought that it was their own responsibility, 28 who thought it lay with the school system, and 14 who thought it lay with the government. None thought that it was the ISP’s responsibility or that it wasn’t a problem.

From the 14 participants that hadn’t taken a course and didn’t want to take one, three thought that it was their own responsibility, six thought it lay with the school system, one that it lay with the ISP, and one with the government. Two thought that it wasn’t a problem and one used the “other”-option to write “if you work with a computer, then they [the company] should teach you, otherwise, there is no problem”.

Out of the five participants that weren’t sure if they had taken a course in cybersecurity or not, there was one that thought it was their own responsibility, one that thought it lay with the school system, and one with the government. None thought that it lay with the ISP, but one thought that it wasn’t a problem and one used the “other”-option to write “I think there is too much focus on [the] Internet, more people should go back to using secure papers”.

6.3. Concluding question

The last question in the questionnaire was about how the questionnaire might have changed the citizen’s perspective of phishing. This question was formulated much like the ones about exposure and awareness, using statements and a Likert scale on which the participants
would mark the option that closest represented how much they agreed with the statement. The different statements were that answering the questionnaire has made them more worried about the threats, increased their awareness of security as an issue, and made them realize that they want to know more about phishing.

For this question, the earlier separations are ignored as they are not judged as relevant for this type of question. Instead, all of the 169 participants’ answers are presented together, see figure 16.

![Figure 16 Changed perspective](image)

As can be seen in the figure above, there is a large majority who haven’t changed their perspective of phishing at all when it comes to awareness and wanting to know more. There were, however 58% of the participants who are more worried about the threats than they were before answering the questionnaire.

### 6.4. Analysis

Already in this first question it is possible to see that younger and more educated individuals perceive themselves to understand phishing more often than those who are older or less educated. The overall majority claimed to have an understanding of phishing, but when breaking it down by the separators it was possible to see that those who had taken a course in internet security through school or hadn’t but would like to didn’t have an understanding. What was interesting here was that those who had not and also didn’t want to take a course claimed to have an understanding of phishing. Using the age separator, it was possible to see that the older the participants got, the less percentage of them claimed to have an understanding of phishing. Looking at the education separation, there was a similar pattern where participants with higher education generally claimed to have an understanding of phishing while those with lower did not.

Combining the age and education separators, it was possible to see that regardless of age, those with higher education generally claimed to have an understanding of phishing while those with lower did not.
The overall result regarding responsibility was that the majority of the citizens thought that the responsibility lay with the school system with very few thinking it lay with the ISP or wasn’t a problem at all. What was interesting to see was that regardless of education, there was still a majority that thought that the responsibility lay with the school. It was only when looking at age and if they had taken a course in cybersecurity in their free time that the answers differed.

When combining the age and education separators, it was interesting to see that the older the participants were, the more they thought that the responsibility should lay with the government and the more educated they were, the more they thought the responsibility lay with the school system. This resulted in the participants in the younger age bracket with higher education thinking that the responsibility should lay with the school system. As age increased and education decreased, they thought that the responsibility should lay with the government.

The higher educated were more likely to have undergone previous courses or researched the subject themselves and thus their answers tend to lean towards feeling more exposed and more aware, but also that they understand phishing, however only about half of the respondents perceive themselves to be able to protect themselves from phishing attempts, which is interesting considering their high level of understanding. Even the higher educated 50+ age bracket answered with high awareness and understanding, however this might be influenced by the low number of participants in that particular group. According to the last question, the higher educated were also the ones who were most interested in learning more about phishing after the survey, another point from the last question was that they seemed to be confident in their beliefs and other than some wanting to know more, most chose the “middle answers” with tendencies to not being changed at all.

The high school educated participants have answered pretty evenly across the board, they rate themselves as mostly somewhat exposed and aware, but there is also a large amount (40%) of the participants who believe themselves unable to protect themselves from phishing. When sorting by age groups, the participants with high school education differed quite a bit, the younger 18-30 age bracket answered with confidence that most of them (70%) had an understanding of phishing, compared with 52% in the 31-50 bracket and 20% in the 50+.

The less than high school participants answered with mostly “middle” answers, but tended to steer more to the exposed and unaware route. They also had a majority of 60% saying that they did not understand phishing which also is interesting considering more than half of them answered that they were able to protect themselves from phishing attempts. Splitting the less than high school educated group up by age as well, reveals some differences but it seems to follow the overarching theme with oldest participants answering that they do not know or understand phishing.
7. Discussion

The study conducted was a quantitative study with the aim of getting a basic understanding of how exposed the citizens of Hong Kong felt when it came to the cyber threat phishing. Since the target group was the general public, a quantitative study in the form of questionnaires was preferred in order to be able to collect as many replies as possible. The usage of Likert scales on some of the questions in order to give the answerers a wider range of options when replying worked very well and should have helped to get the result to be as accurate to the participants’ opinions as possible.

There were however some problems when distributing the questionnaire. Since there was only a limited amount of time for the work to be completed, it was only possible to distribute the questionnaires on the streets for so long. In the end, there were a total of 178 participants, but there were a large portion of these that were in the 18-30 age bracket and very few in the 50+ bracket. This could be because of the time of day that was chosen to distribute the questionnaire, or simply because the questionnaire was only distributed in a few different places in the city. There were also a number of citizens who did not want to participate, many who looked to fit in the higher age brackets, so this probably influenced the distribution of age in the participants as well.

Another interesting point with the result is that even though an online survey was not chosen due to the chance of attracting younger more computer experienced participants, which would tip the result heavily, the printed out survey did so still. This is probably due to the human factor of not wanting to answer something which the individual knows nothing about thus turning people who feel disconnected from the field of computers and cyberspace away.

In hindsight, it might have been easier to get a lot of participants if the target group was different, perhaps only using the 18-30 age bracket since they were over represented in this study and some had to be turned away because of the uneven distribution. Using this target group instead, it might have been better to use occupation as a separator instead of education.

Regardless of the uneven distribution, the result is still very clear and is easy to draw conclusions from, which indicates that the result can be trusted (Berndtsson, 2008). However, the amount of participants in the survey cannot reasonably be applied over the entirety of the population but can provide a small snapshot of the citizens of Hong Kong’s attitude towards the cybersecurity threat phishing.

7.1. Comparison with related work

As previously mentioned in the section about related work, there are works which resembles this study. When comparing the results gained in this study with for example Furnell (2007), who in his research found novice users to be confident in their awareness of security issues, but lacked deeper knowledge and understanding when being asked relevant questions we can see a similar pattern. In general, the citizens feel exposed and aware, but after the final question they’ve become increasingly worried, suggesting towards some of the threats being news, or perhaps the presence of the survey making phishing feel even more common. It is important to note that Furnell (2007), did his survey online and one could argue that an online survey would attract participants with more experience in the computing field, whereas
this study was aiming to gain answers from the citizens of Hong Kong, whatever their previous computing experience might have been.

In the study made by Arachchilage (2014), it was discovered that users who gain sufficient education beforehand have a higher self-efficacy to thwart phishing threats. This correlates with the results gained in this study, with nearly 70% of the participants who had previously attended a course in cybersecurity saying that they would be able to defend themselves from phishing threats.

7.2. Social aspects
This work was done due to the increasing accessibility humans have when it comes to the Internet, and as the access becomes more widespread, so does the threats that comes with it. The largest social aspect that this work touches on is the question regarding with who the responsibility to educate citizens about cybersecurity lies. The three major answers chosen by the respondents was that it should be their own responsibility, that it’s the responsibility of the school system or that the responsibility lay with the government.

One could argue that the school system (which was the most common answer) would be the best alternative since the increasing accessibility exposes increasingly more young people to the Internet, and thus learning about cybersecurity could be essential. But this also comes at a cost; new teachers would have to be hired and an already cramped school schedule would gain another course.

The second most common answer, that it was the responsibility of the government, could also be both a blessing and a curse. More consultants would have to be hired to educate people, and a medium of education would also need to be thought out. Perhaps this would lead right back to it being taught in school.

To have cybersecurity solely relying on one self to learn is tricky since finding information and actively self-learning is something that perhaps do not entice many. However, with this outlook, the ones who educated themselves would gain information about what they perceived themselves to need.

7.3. Ethics
The four most important points about ethics in research that involve people according to Wohlin et al. (2012) have all been treated during this study. The first point regarding the fact that people who partake in the survey must give informed consent before the decision of partaking is made has been handled by first introducing the researcher to a potential respondent and informing them who they are, what the survey is about and what the results can be used for before they had to choose if they wanted to participate. This information was also written at the beginning of the survey.

The second point is that the study should be done in a way that gives scientific value so that the people who partake in the survey are willing to accept the potential risks. This too was handled by initially informing the participants of what the results could be used for after the study was completed. The third point regarding the fact that the study must be made in such a way that confidentiality of data and sensitive information are kept was handled by keeping all of the participants anonymous and deleting any data not in the report after the study is finished.
The fourth and final point is about the fact that the study needs to see to it that the beneficence is always larger than the possible risk of harm to the people partaking and this is also handled by promising anonymity as well as keeping the questions from being too private and prying.

7.4. Validity threats
The validity threats that were regarded to be the most serious against this study, and which were obtained from the list featured in Wohlin et al. (2012), have all been handled in one way or another during the study.

One of the more serious threats was reliability of measures, in other words that the questions were badly constructed and therefore didn't result in usable answers. This was handled by revising the questions numerous times to ensure their quality, although in the end this threat is not completely avoidable because of the fact that misinterpretations still can occur.

Another serious threat was fishing and the error rate which includes questions being asked in a certain way to generate a specific type of result. This too was handled by revising the questionnaire and keeping the questions opinion-based since opinions often is hard to change.

The third, and perhaps the threat with most impact, was interaction of history and treatment. Since news and happenings that can affect the participants' answers are impossible to foresee, it is almost impossible to handle this type of threat completely. What was done in this study was to distribute the surveys only during a short period of time. This way, if any major events were to happen that might have influenced the answers, all of the participants would most likely have the same conditions when answering the questionnaire.
8. Conclusions

Based on the result from the questionnaires it can be concluded that the citizens of Hong Kong feel exposed to the threats that phishing poses, but also that the majority believe themselves capable of defending themselves against it. They also claim to understand phishing and have a general awareness of most of the threats.

A very interesting point that could be seen after the analysis was that those who had taken a course through school generally claimed to not have an understanding of phishing and yet the majority thought that the school system should be responsible for distributing knowledge about the threats.

According to the responses on the last question of the questionnaire regarding whether or not answering the questionnaire had changed their perspective of phishing, the citizens’ replied that their views had generally not been affected, but only made them more worried, something which was not intended by this study.

8.1. Answering the research questions

The first question “How exposed do the citizens of Hong Kong feel when it comes to the cyber threat phishing?” was answered by the fifth and seventh questions which were about how exposed they felt to some threats and if they felt that they knew how to defend themselves against phishing attempts respectively.

In general, the citizens felt exposed to all the threats, the one with which people felt most exposed to was fraudulent emails, which is understandable considering how commonplace spam emails have become today. As with the overall trend of the survey, larger percentages of youth felt exposed to the threats than the older participants.

The second question “How knowledgeable are the citizens of Hong Kong when it comes to common phishing types?” was answered by the fourth and sixth questions which were about whether or not the participant had an understanding of phishing and how aware they were to different threats respectively. The overall majority claimed to have an understanding of phishing, but looking closer it could be seen that the education level seemed to be the deciding factor, regardless of age. What was interesting, however, was that those who had taken a course in internet security generally claimed to have an understanding except for those who had taken it through school.

The awareness of citizens in Hong Kong when it comes to phishing is varied according to the data, even though the majority of participants fell into one of the differing groups, the trend was clearly visible throughout the survey that lower educated or older participants were less aware, and higher educated younger participants were more aware. The participants who felt most aware belonged in the higher education category.

The third and final question “Who do the citizens of Hong Kong think should have the responsibility to inform about phishing?” was answered immediately by the eighth question which asked this directly. The overall majority thought that the responsibility lay with the
school system with only a few separating groups that thought differently, but the older the participants were, the more they thought the responsibility lay with the government.

8.2. Contributions

This study contributes with a mapping of the citizens’ general knowledge and opinions when it comes to the cybersecurity threat phishing. The mapping consists of three major parts; how exposed do the citizens feel to the threat, how knowledgeable are they about it and who do they think should have the responsibility of spreading information regarding the threats.

These three parts could either be used as a material for comparison when conducting further studies with other target groups or other cybersecurity threats. It could also be used as a slight guidance when it comes to designing, for example, information pamphlets or courses as it shows how the citizens feel about the subject and how knowledgeable they perceive themselves to be in the area and thus show which parts are of the highest importance for further teaching.

8.3. Future work

A future work based on this study could do a more thorough survey where the questions are more focused on what the citizens’ knowledge really is when it comes to phishing and from where they have learned about the threat. Another version could be to add in gender to see if there was any difference between the two, something which was intentionally not done in this study, or compare the results of this study with the result of a similar one conducted in another country to see if the citizens think differently.

A very interesting alternative would also be to broaden the perspective and include different types of cybersecurity threats, instead of keeping the questions about phishing. Granted, this would most likely be a very extensive study and would probably require more time than this study. Another version of this would be to focus entirely on one other type of cybersecurity threat and keep the questionnaire template the same but with the new focus.

It would also be interesting to perhaps observe in an experiment how different people from different ages and working classes would handle being faced with the types of threats directly in an experimental setting. In such an experiment, it could also be interesting to see if they could differentiate the threats from legitimate sources and record how they made their choices.
References


• Kissel, R. (2013). Glossary of key information security terms. DOI: 10.6028/NIST.IR.7298r2


Appendix

Appendix A: Validity threats

Appendix B: Questionnaire
Appendix A: Validity Threats

<table>
<thead>
<tr>
<th>Validity threat</th>
<th>Is it a relevant threat for this work?</th>
<th>Is a solution possible?</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low statistical power</td>
<td>Yes</td>
<td>No</td>
<td>Due to the paper having a questionnaire type survey, the frequency of answers cannot be controlled</td>
</tr>
<tr>
<td>Violated assumptions of statistical tests</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Fishing and the error rate</td>
<td>Yes</td>
<td>Yes</td>
<td>This can happen, but knowing about the threat hopefully reduces the risk.</td>
</tr>
<tr>
<td>Reliability of measures</td>
<td>Yes</td>
<td>No</td>
<td>This is entirely up to the participants and is therefore a very hard threat to counter with this study.</td>
</tr>
<tr>
<td>Reliability of treatment implementation</td>
<td>Yes</td>
<td>Yes</td>
<td>This threat might exist, but should be largely countered considering that the questionnaire is the same.</td>
</tr>
<tr>
<td>Random irrelevancies in experimental setting</td>
<td>Yes</td>
<td>Yes</td>
<td>The questionnaire will be passed out in public places where, sadly the area is out of the researcher’s control, thus making this an acknowledged threat.</td>
</tr>
<tr>
<td>Random heterogeneity of subjects</td>
<td>Yes</td>
<td>Yes</td>
<td>It is hard to predict who will answer the questionnaire, controlling this is hard since one group from the different citizen pools may be overrepresented.</td>
</tr>
</tbody>
</table>

Conclusion Validity

Internal Validity

Single group threats
<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
<th>-</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maturation</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Testing</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Instrumentation</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Statistical regression</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Selection</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Mortality</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Ambiguity about direction of causal influence</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

**Multiple groups threats**

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
<th>-</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interactions with selection</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

**Social threats**

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
<th>-</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diffusion or imitation of treatments</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Compensatory equalization of treatments</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Compensatory rivalry</td>
<td>Resentful demoralization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Construct validity**

**Design threats**

<table>
<thead>
<tr>
<th></th>
<th>Inadequate preoperational explication of constructs</th>
<th>Mono-operation bias</th>
<th>Mono-method bias</th>
<th>Confounding constructs and levels of constructs</th>
<th>Interaction of different treatments</th>
<th>Interaction of testing and treatment</th>
<th>Restricted generalizability across constructs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>By deciding all the factors regarding the experiment beforehand, this threat is significantly lowered.</td>
<td></td>
<td>The questionnaire will be handed out to multiple participants, thus eliminating this threat.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Social threats to construct validity**

<table>
<thead>
<tr>
<th></th>
<th>Hypothesis guessing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Yet again, it is up to the participants to answer truthfully.</td>
</tr>
<tr>
<td>Evaluation apprehension</td>
<td>Yes</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>Experimenter expectancies</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**External validity**

<table>
<thead>
<tr>
<th>Interaction of selection and treatment</th>
<th>Yes</th>
<th>Yes</th>
<th>This survey wants to ask the citizens perspective, possible low respondent rates can make this a possible threat.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interaction of setting and treatment</td>
<td>No</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Interaction of history and treatment</td>
<td>No</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>
Appendix B: Questionnaire

Cybersecurity & Phishing Knowledge and Opinions

My name is Jesper Karlsson, I am an exchange student from Sweden where I attend a program called Network and System Administration at the University of Skövde. This survey is a part of my final year project, which is to gauge the citizen opinion of how and where cybersecurity should be taught, as well as the citizens' knowledge of phishing which is the largest cyber threat in Hong Kong. The survey is composed of a few single choice questions, followed by scaled questions where you are supposed to answer how much you agree with the statement.

Terms of participation:

Your participation is completely voluntary and can be aborted at any time. Your participation is also completely anonymous and no connections will be made between the survey and you as an individual. The result will only be presented in my research as well as in front of other students of the University of Skövde. If the work is passed and accepted it will be published in academic databases, such as DiVA, which is reachable from www.his.se/en

Q1: Are you a citizen of Hong Kong?
- Yes
- No

Q2: How old are you?
- 18-30
- 31-50
- 50+

Q3: What is the highest level of education you have completed?
- Less than high school degree
- High school degree
- Higher education (University, college etc.)

Q4: Have you taken a course in cybersecurity?
- Yes, in my free time
- Yes, through work
- Yes, through school
- No, but I would like to
- No, and I do not want to
- Not sure

Q5: Your perceived exposedness when it comes to phishing

These statements are about how exposed you feel to some often occurring cyber-crimes. These statements are all types of the cyber-crime phishing, which are crimes where the
perpetrator tries to steal online accounts or other personal information. (Mark the option that closest represents how much you agree with the statement.)

5.a. I fear that someone will send me fraudulent emails through respected sources (stolen e-mail addresses of friends and family)
5.b. I fear that I will be the target of a false URL leading me unto a false website
5.c. I fear that accounts on webpages I frequently use online will be compromised due to key-logging technology (program that records login credentials)

Q6: Awareness of phishing types
How is your awareness to these following phishing types?

6.a. Social Media Deception
6.b. E-Banking Fraud
6.c. Email Scamming
6.d. Online

Q7: Knowledge of how to defend yourself against phishing attempts
Would you say that you know how to defend yourself against phishing attempts?

- Yes
- No
- Not sure

Q8: Your opinion of who is responsible for teaching online security
Who do you think is responsible for distributing cyber security knowledge so that people can protect themselves against cyber-threats such as phishing?

- I think it is my own responsibility.
- I think the responsibility lies within the school system.
- I think the responsibility lies with internet service providers
- I think the responsibility lies with the government
- Other (please specify)

Q9: Have the questionnaire changed your perception of phishing?
How have answering this questionnaire changed your perspective of phishing? (Mark the option that closest represents how much you agree with the statement.)

9.a. It has made me more worried about the threats.
9.b. It has increased my awareness of security as an issue.
9.c. It has made me realize that I want to know more about phishing.