Bachelor’s thesis in Software Engineering
Comparison of Security and Risk awareness between different age groups
Blekinge Institute of technology

Amanda Björneskog
Nima Goniband Shoshtari

June 20, 2017
This thesis is submitted to the Faculty of Computing at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Bachelor in Software Engineering.

Contact Information:

Author(s):
Amanda Björneskog, amanda bjorneskog@outlook.com
Nima Goniband Shoshtari, n goniband@gmail.com

External advisor:
Bengt Aspvall
Bengt.Aspvall@bth.se

University advisor:
Conny Johansson, Conny.Johansson@bth.se
Assistant Professor
Blekinge Institute of Technology

Faculty of Computing
Blekinge Institute of Technology
SE-371 79 Karlskrona, Sweden

Internet: www.bth.se
Phone: +46 455 38 50 00
Fax: +46 455 38 50 57
Foreword

This thesis is called ‘Comparison of Security and Risk awareness between different age groups’, the basis of which is several interviews with the age groups within our scope and general surveys. It has been written to fulfill the graduation requirements of the Software Engineering education at Blekinge Institute of Technology (BTH). We have been engaged in researching and writing this thesis from January to June, 2017, in a 50% study, which is equivalent to 300 work hours.

We would like to thank everybody who participated in the interviews, everyone who answered our survey and we'd like to thank Rosenfeldtsskolan in Karlskrona for allowing us to interview their second grade students.
A special thanks goes out to our mentor Bengt Aspvall that helped us in the process of making this thesis.

Amanda Björneskog and Nima Goniband Shoshtari

Keywords

Cyber security, Security, Risk, Awareness, Social engineering, Age groups

1 Abstract

The Internet have become a 'necessity' in the everyday life of just below 50% of the world population. With the growth of the Internet and it creating a great platform to help people and making life easier, it has also brought a lot of malicious situations. Now a days people hack or uses social engineering on other people for a living, scamming and fraud is part of their daily life. Therefore security awareness is truly important and sometimes vital. We wanted to look at the difference in security awareness depending on which year you were born, in relation to the IT-boom and growth of the Internet. Does it matter if you lived through the earlier stages of the Internet or not? We found that the security awareness did increase with age, but if it was due to the candidates growing up before or after the IT-boom or due to the fact that younger people tend to be more inattentive is hard to tell. Our result is that the age group, 16-19, were more prone to security risks, due to an indifferent mindset regarding their data and information.

2 Introduction

A receptionist working in a big IT-corporation got a flower delivery one day at work, but instead of a card she got a USB-drive. Happy with the flowers and curious to who had sent these beautiful flowers she plugged in the drive to her work computer, and that is the story of how that corporation got hacked.

This story was told during a lecture with Combitech and Carolin Solskär. Due to confidentiality and security reasons she couldn’t tell us which corporation.

There are a lot of different stories and most of them are just that stories, but some are serious and down right scary. Those stories are also an example of Social Engineering. A very important part of security risks and a risk not a lot of people think about.

After reading different types of stories and listening to numerous TED talks we both found social engineering fascinating, it was something we would like to study a bit more. One day while discussing this we got to thinking, what is the difference in awareness between different age groups? Are kids who grew up after the Internet-boom as aware as the people who grew up before. But to figure this out we had to read more into the different types of security risks online. This lead us to OWASP top ten [14].

2.1 Background

The number of users on the Internet has since 1995 grown rapidly, going from approximately 0.4% of the world population to just below 50% [21]. With this increase, The Internet has grown from a non-necessity to a necessary tool for everyday tasks and a place to store personal information, both locally and online, making Internet one of the most valuable inventions of mankind. When we chose to write this thesis, we were concerned with the growth rate of the Internet compared to our perception of the level of knowledge that the user has about IT security. What interested us the most was to see how big of a difference there was between the younger generation, who has only used the Internet as we know it today, and older generation who has experienced
Internet in its earlier stages.

2.2 Scope

Our research for this study covers the topics of the online habits and security awareness of our participants. We’ve decided to divide the generations into smaller groups;

- Age group 1: 7-10
- Age group 2: 11-15
- Age group 3: 16-19
- Age group 4: 20-25
- Age group 5: 45-69

When looking at these groups you will notice the absence of people in the ages between 25 and 45. We decided to exclude this age group from our interviews because of various reasons, some being that we wanted to concentrate on the younger groups. It is also a complex generation, they have seen both life without Internet as a ‘necessity’ and Internet as a big part of society. All our other groups have either lived a large part of their lives without Internet or just had Internet their entire lives. But to get a somewhat clear picture of their mindset we did a separate survey. We will return to this matter in chapters 3 and 4.

We will not discuss the technical destruction of malware in a system in greater detail in the end, as our research focuses on the amount of risk of being affected.

2.3 Outline

This thesis is divided into two parts; The Contextual part and the Research contribution. The Contextual part is designed to give you as the reader some background and necessary information regarding Social Engineering and malicious intent which is needed to understand the result of our research. This part is mostly based on Martin Boldt’s definitions and materials from his dissertation from 2006; 'Privacy-invasive Software' [4]. The second part describes our approach to the research questions, our motivation, methods and results. The appendix contains all of our collected data, sorted by age group and the emails used for the phishing experiment.
3 Social Engineering and Malicious Intent

When writing this thesis, we have relied heavily on the definitions of Spyware presented by Martin Boldt in his 2006 dissertation 'Privacy-Invasive Software' [4]. This section has the purpose of defining and explaining principles and technical terms used in our research and some history.

3.1 Retrospective

The general public's interest for the Internet rapidly grew during the 1990's, speeding up the development. Boldt mentions the release of the first browser which was called 'Mosaic' in 1993 as a big factor as it marked the birth of the graphical perspective of the Internet. With this growth companies soon understood the potential of the Internet as an electronic platform of commerce.

A table which internetworldstats.com[9] provides shows how many connected users the Internet currently consists of, and can show us statistics as far back as 1995. At the first measurement back in 1995 the active users were 16 million, which was roughly 0.4% of the then current world population. Today in 2017 that number is 3.7 billion users, which is close to 50% of the world population.

As the population of the Internet grew, the e-commerce companies revenue grew making the Internet handling large amount of transactions. The competition over customers intensified and some companies turned to some less-ethical methods in their desire to secure more transactions from the growing customer base. Boldt mentions this as the gateway for illegitimate actors to push the boundaries of methods used to collect personal information or push commercial advertisements. Companies could get an advantage over their competitors by using unwanted commercial messages sent by the bulk to users, which is what we today know as spam and which also mutated into adware (3.3.2).

Boldt goes on to mention the Advertisers desire to be more effective and that they soon realized the potential of targeted ads. This was the start of the early versions of spyware, which collected users' interests through browsing habits. This phenomenon quickly evolved to a threat to connected devices by reducing system security and performance. The data that was gathered was used to construct user profiles including interests and information.

Malwares has been around since before the boom of Internet, making their first entrance in the mid-80’s [12]. At that time, the systems at biggest risk was located in universities due to the amount of computers and the public access to them, and the general intention of the hackers was to test and try to break the system out of sheer curiosity and entertainment. The main type of distribution during this time were by floppy disks. As mention earlier, by the mid-90’s the Internet had grown into a platform for commerce and distribution had moved on to the network. This created a transition in the intentions of the hackers to a more profit-driven one and gave rise to different hackers; blackhats, grayhats and whitehats. The blackhats always had the intention of destruction, while the grayhats had the intention of finding weaknesses and releasing this information for a small fee to the companies of the product or, if they are not interested, to the public. The whitehats are very similar to the black hats in their ways of working but the difference is that they do it with
the owners permission, and are often employed to do this task. This transition also made the ill-intended hackers to target businesses instead of private home users as the profits were larger. The practice of Social Engineering is older than the era of digitalization as the information desired does not have to be digital. The Internet provided a safe and fast way to distribute these scams, but before that regular mail and faxes were widely used.

Today there are a magnitude of different variation that stems from these examples, the most common ones are mentioned later on under the section of definitions (3.3), but they still have the same intention of profit as they did back in the 90’s. The malware has become more complex, and the countermeasures have a hard time keeping up as they work retroactively and can’t foresee the malware evolution.

3.2 OWASP Top Ten

The OWASP foundation first came online in 2001 and states on their website that their core purpose is to drive the visibility and evolution of security and safety in software. OWASP has released documents known as the ‘OWASP Top 10 Most Critical Web Application Security Risks’ or for short; OWASP top ten. The latest official list was released in 2013, and they have another one planned for release in august 2017. The reason for the four year gap between the document from 2013 and the planned one is because the order of the list has not changed. Each entry in the OWASP top ten includes:

- A short description.
- Example vulnerabilities.
- Example attacks.
- Countermeasures.
- References to OWASP and other related resources.

This is the list we have used in our research since these entries are the most common, and shaped our research after the nature of the vulnerabilities on the list.

**OWASP Top Ten Online Vulnerabilities 2013**

1. Injections
2. Broken Authentication and Session Management
3. XSS
4. Insecure Direct Object References
5. Security Misconfiguration
6. Sensitive data exposure
7. Missing Function Level Access Control
8. Cross-Site Request Forgery (CSRF)
9. Using Components with Known Vulnerabilities
10. Unvalidated Redirects and Forwards

Every entry in the OWASP top ten is not relevant as they describe vulnerabilities in webpages and servers, which does not always entitle direct attacks towards the end user. We will be looking closer into the risks of XSS attacks, Security Misconfiguration and unvalidated redirects in our research as they compose a direct risk for the users in their online habits. While vulnerability exploits like the injection is a risk for the users privacy, this is not part of the malwares distributed by the ways of social engineering.
Vulnerability definitions according to OWASP Top Ten [14]

**XSS**  
"XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim’s browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites."

**Security Misconfiguration**  
"Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date."

**Unvalidated Redirects and Forwards**  
"Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages."

### 3.3 Concept Definitions

#### 3.3.1 Privacy

Boldt refers to Simone Fischer-Hübner when he defines the word *privacy* [5]. She presents three principles which together make an individual’s privacy. They are as follows;

- **territorial privacy**: Focuses on the protection of the area around the person, like the office or a school.
- **privacy of the person**: Protects the individual from undue interference (constituting for example, physical searches and drug tests)
- **informational privacy**: This aspect is concerned with how personal information (information related to an identifiable person) is being gathered, stored, processed, and further disseminated.

The most relevant aspect in our research is the last one, *Informational privacy*, as almost every service has to handle their users personal data, and the users has to protect themselves from illegal spyware (3.3.2).

#### 3.3.2 Malware Types

*Malware* is a concatenation of the words *Malicious* and *Software* and is entitled to any type of software with malicious intent [21][4]. Historically, malware has gone from standalone processes to malicious executable code inside data that once was considered pure, such as image files and word documents.

- **Adware**: Not a true malware in the traditional sense as it does not disturb the operations of a computer. The goal of the adware is to populate your online habits with ads. Sometimes adwares work together with Spywares to give you ads based on information it has stored on your person. Often downloads malicious code when clicked on.

- **Spyware**: Software that monitors your computers and reveals the collected information for an interested third party. There are legal ways, as
Google who keeps it transparent, or it can be very invasive as it can track your mouse and keyboard actions.

**Ransomware**: This has become a very popular way for Internet criminals to make money. This type of malware alters your system in a way that it becomes unusable until you pay the attacker a sum of money, often in bitcoins. The attacker basically keeps your computer hostage and releases it for a ransom, as the name suggest. In the spring of 2017, the world was hit by a Ransomware called Wannacry. This affected big parts of Europe, Russia and the US, causing big damage across a lot of sectors. Wannacry entered your computer and encrypted all your files, to get them decrypted you had to pay a ransom in Bitcoins. The exploited computers could be infected because they had not updated their OS. Windows released an update in March that could’ve prevented this.

**Scareware**: Software that gives the illusion of being non-malicious and acts as something else, usually as a tool to help fix your computer. Gives error messages in a way that’s meant to frighten you into doing something.

### 3.3.3 Malware distribution

There are several ways to distribute Malware. Below you will find the most commons ways to infect a system.

**Virus**: The most generic term in cyber-security. Used to mean malware generally but has now gone to define software that self-replicates after hooking onto something in Windows specifically.

**Worm**: Like the Virus, the worm self-replicates but does not need a Windows-process to latch on to. Generally small programs that run in the background of your system.

**Trojan**: Named after the legend of the ancient Greek trojan horse. Disguised as one thing, but actually contains other intents.

**Drive-by download**: The most common way to insert Malware into a system. Usually happens when visiting a bad web page. By exploiting a weakness in your browser, they can cause your system to be infected. This is done by an automatic download of malicious files when visiting a bad url.

**Phishing**: These attacks are a prime example of Social Engineering. Often by posing as someone else, they ask you questions regarding the domain they are posing as. This could be a bank or other services or maybe just posing as someone famous; like the famous Nigerian prince scam.

### 3.3.4 Social Engineering

Social Engineering in the context of cybersecurity can be defined as techniques used by ill-intended hackers designed to lure at trick users into giving up confidential data, infecting their systems with malware or making them click links to infected sites. Although there are several ways to gain access to someone’s system or information, like a worm through an email attachment (like the Loveletter worm in 2000), the aspect they all have in common is the fact that the user has to be tricked into clicking a link or attachment.

### 3.3.5 Password Security

According to the SANS institute, which is an organization established in 1989 and specializes
in training staff in cyber security, the base criterion for a secure password is as follows:

- Contains at least 12 alphanumeric characters.
- Contains both upper and lower case letters.
- Contains at least one number (for example, 0-9).
- Contains at least one special character

On the contrary, a weak password has the following characteristics:

- Contains less than eight characters.
- A substring can be found in a Dictionary, including foreign languages.
- Contains personal information, such as a birthday or the name of a pet.
- Work-related phrases on a password inside the domain of the office.

This document is aimed towards staff members at Cisco[7] and their affiliated third party members, which makes us confident in the credibility of the criterion for a strong password as Cisco is one of the world leading network hardware providers. This is also the standard to which we will compare the results from our research.
4 Research

4.1 Motivation and Research Questions

When looking at the history of the Internet we can see that there has been several stages of evolution. The first phases was mainly located in the universities and in scientific purposes to develop this means of communication. The Internet soon became a platform for commerce, making shopping faster and easier. With the entrance of the personal computer somewhere in the mid-90’s the number of users grew rapidly over the coming decade and the technological accomplishments of the computer became more frequent and more astonishing. Only twenty years later we now have smaller computers in our pockets which outranks computers that were made only ten years prior, and the Internet is embedded in almost every service that we use. We have also seen the threat of malicious intent grow and together with the aspect of commerce, change goals from trying to break a system and prove one’s own skills to pursue the goal of profit. When considering all of these phases during the Internet’s history we started to wonder how much of an impact it has on one’s cyber-security awareness when someone was born. Therefore we have formulated these questions, hoping to be able to find out the answers.

RQ1: How does different age groups perform compared to each other concerning IT security knowledge and awareness?

RQ2: Are any of the age groups extra vulnerable to certain exploits?

4.2 Methods

This section covers how we have conducted our research. We will explain where we got our inspiration for designing the interviews, we will formulate our hypothesis and refer to relevant literature that we have used.

4.2.1 Hypothesis

When starting with this thesis we were interested in the difference in age groups and we defined the age groups accordingly to when they were born in relation with the birth of the Internet and the IT-boom. Our hypothesis is that the people born before the IT-boom and were old enough to remember it, and are more careful online of the sole reason that they’ve always been told to be careful. The age group born during the development and start of the Internet (ages 20-25) we believe will be aware of the risks, though they have been raised by the previous generation, but will take more risks because they are comfortable using the Internet. Age group 3 (16-19) we had a hard time setting into perspective, but our hypothesis is that they will be similar to the previous age group (ages 20-25). This age group have not experienced life without Internet, but they were born in the very early stages of Internet. However, we believe that this group will be aware of risks and follow them to some extent. The remaining two age groups, 7-10 and 11-15, are the age groups we as researches have the hardest to identify with. The age group 7-10 were born after the smartphone became a common necessity, that means they might have gotten a smartphone early in their life or have used a smartphone early on in their life. We think that this effects the awareness online. The age group 11-15 were born just before or right at the
launch of the smartphones, which means they also have gotten an interaction with the smartphones early on in their lives. As with the previous age group we believe that this effects the awareness online. Something that also could effect the security awareness is their parents. As mentioned before the age group born during the IT-boom were raised by the age group we think will be careful and promote to be aware online. The younger age groups might have been (more often) raised by the generation that were still very young during the IT-boom and have had access to internet during most parts of their lives. We believe this also will effect the awareness in the younger generations.

4.2.2 Empirical Study

- **Interview:** We conducted interviews with candidates from all of the age groups, with questions regarding their online behavior and knowledge about IT security. The size of each age group was 5-8 candidates each.

  **Ages 7-10** We interviewed six students from a second grade class at Rosenfeldtsskolan. We sent a document for the parents to sign, in which we declared our intentions with the interviews and the purpose of our study.

  **Ages 11-15** This group was the hardest to find candidates for. We had emailed Rosenfeldtsskolan and we wanted two classes, but at the time only the second grade were available. There was also the issues with parental agreement and shyness. What we did to solve this issue was to go to the first author’s old neighborhood and ask kids and parents there. Some kids were so shy that we made a special survey that could substitute an interview. It was an emergency thing and we got five answers for the interview through the survey and two real life interviews. One of the five kids who answered the survey we know the background of, the rest were anonymous.

  **Ages 16-18** We interviewed eight (8) students at Chapman a secondary school in Karlskrona, here we got a green light to question the students from the school Principal.

  **Ages 20-25** For this age group we had five candidates. All of them were our friends, that means we know their background. But we still asked the same questions as decided and we will evaluate them exactly as the rest of the candidates.

  **Ages 45-69** Here we interviewed our parents but also friends parents. We had many different ages for this age group to get a better understanding if more time spent before the IT-boom and birth of the Internet had any effect on their security awareness.

- **Survey:** The purpose of the surveys was to collect secondary data from a wider, more general, audience that we can use to compare against the interviews.

- **Phishing experiment:** We conducted an experiment with all the age groups, besides the two youngest. The purpose of the experiment was to find out how the interviewees reacted to certain types of emails, and asked them to tell us if they thought it was a scam and why. We had 11 emails, 5 of which were actual phishing attempts towards the first author’s email address. The rest were commercials and regular emails.
4.3 Validity Threats

First of all, the number of candidates in each group might not be enough to get a full representation of each age group. Also the candidates in age group 4, 20-25, were mostly our friends. Which could be a validity threat that we surround ourselves with similar people, even though we tried to pick friends with different backgrounds. The same applies to the age group 5, where we interviewed the first author’s parents and friends of parents.

Another threat is the survey, were we accidentally stated the wrong age groups. We do take special caution when using the data from the surveys and the data received in the survey is not used in the conclusions.

4.3.1 Literature Study

We had a hard time finding literature, the section 2.6 goes through the information we choose to use while writing questions and while conducting interviews. This information is strictly technology based and its purpose was for us to know what to look out for in the candidates answers and behavior.

At first we wanted to find other scientific sources related to our topic, but found mostly research about social networks or research with one specific age group in mind. This made our work a bit harder but also more rewarding knowing that not a lot of people had our point of view. The sources we have chosen for the later part of the study takes age into consideration when researching their online habits and the security awareness. We did not only want to find sources of the subject we had in mind though, we had to understand the risks online for children and on social networks. Much of the research other people have done on children stays within the scope of the risks of being tricked into a social encounter with people that has the desire to acquire pictures of, or meet, the children, and less on the technical aspect of the risks towards the systems that children uses. We will compare our findings of the younger groups with a dissertation called 'A survey on internet usage and cybersecurity awareness in students'[18] written by S S Tirumala, Abdolhossein Sarrafzadeh and Paul Pang at the Unitec Institute of Technology in Auckland, New Zealand. This dissertation focuses on the younger age groups and their security awareness after the introduction of the principle 'Bring your own device’ into the school system in the Oceania. Their finding are relevant as they are not western European as we could classify our participants as and they have asked similar questions to figure out the technical habits of the generation. The sources we found was also from 2009-2011, which was a bit out of date, and focused mainly on the eastern part of the world. This comparison will be made together with Boldt’s[4] technical definitions of security risks and the OWASP top ten online vulnerabilities[14] found in the chapter 'Social Engineering and Malicious intent’[3].

4.4 Analysis and Result

The analysis we will structure like the following:

We’re going to start of by analyzing the interviews and then summarize the whole groups security awareness, along the way we will get to certain conclusions, for example with the phishing emails we can get a better picture of the age groups security awareness.

After going through the interviews there is
some further knowledge in the surveys that is going to help us credit or discredit our hypothesis. With the help of the surveys we can also extract answers from the age group that is missing, 25-45.

4.4.1 Interviews

Age Group 5 The first set of interviews to analyze is the age group 5. Here we have the ages 45 to 69 and this is the people that were born and grew up entirely without the Internet. In the statistics we see that the older generation (55-69) spend less time online than the younger (45-49). This is an interesting observation, although not that surprising because we did expect that while making our hypothesis. Does this make the older generation more cautious while online, because they aren’t used to the online environment as much as the younger?

We asked about their passwords and what principles they followed while creating one. Many of the candidates followed a good set of rules for creating a password, even though many said their password was a reflection of their everyday life. This leads to a risk of social engineering [3.3.4] and many of the candidates said they had the same password on many different sites and half of the candidates told their password to family and friends, which could make them more open to social engineering and the fact that they use the same password on many sites makes it easier for the hacker/social engineer to access all of their accounts and information. None of the candidates had their credit card information saved online or in their browser.

When it comes to the older generation being more cautious online; when asking what determines if a site is secure according to them, all the people who spent less then five hours a day said they were very cautious with which sites they visited. They also said they only visited sites that they had been recommended or had previous knowledge about. While the people who spent more than five hours online a day trusted their guts and someone wasn’t quite sure what the meaning ‘secure’ meant while talking about a website.

After the interviews with age group 5 we summarized their online behavior to that they’re cautious while online, they might not understand why but they do have aspects like layout and sources in mind. Two of our candidates in this group have been hacked previously, but this made them more aware not to visit some sites and to choose their password wisely.

Age Group 4 Continuing on with age group 4, ages 20-25. Here a majority spent more than five hours online a day. The only person who didn’t wasn’t able because of work, but did say that during the weekend the hours were significantly increased. We asked this age group about passwords and half of the group had passwords that were related to their own lives. But many, almost all of them, did add numbers to their passwords and one candidate just had something completely randomized for their password. We were pleasantly surprised with how aware they were while creating a password, because we didn’t expect them to be in our hypothesis [4.2.1], but then we asked if they had the same password on many sites and if they told friends and family their password, all of the candidates had the same password on different
sites and all except one told other people their password. This was alarming, especially since 40% of the candidates saved their credit card information in their browser or online. However, when asking what made a page secure they all had very valid and knowledgeable answers. One candidate looked for HTTPS protocols and others trusted their virus softwares Internet plugin. The candidates that wasn’t sure what a secure website meant answered that they were cautious to what pages they visited, they looked at the layouts and watched out for pages with pop-ups. While shopping online they looked for pages that had reliable payment systems, e.g Klarna [10].

Result Group 4:

We would like to summarize the age group 4 to be cautious while online, somewhat lazy and that leads to their indifferent attitude, but they are aware of the risks.

Age Group 3 Next age group is number 3, 16-18. Here we started to see a change in thoughts and online behavior. The majority spent more than five hours online a day, but most of the candidates spent those hours on their phone on applications like Snapchat etc. When it comes to password security 7 of the 8 candidates had passwords that related to themselves and one of the seven even told us the substance of their password. The remaining candidate had a randomized password. The same statistics (7 out of 8) occurred while asking if they had the same password on several pages and 4 of those 7 has told their password to a friend or family member. When it comes to saving credit card information online, many of the candidates didn’t have a card that had the option to shop online. But two candidates had their information saved online or in the browser. When asking what determines if a website is secure or feels secure there were mixed answers, most of them relied on Google search and some just assumed the pages they visited were secure. A majority knew that they should research and how to research, but did admit that they rarely did any research at all and trusted the pages they were on.

Result Group 3:

We were a bit shocked after this age group, they knew some aspects of how to stay secure but chose not to follow them. Our hypothesis was that they would be aware of the risks and follow them to some extent [4.2.1]. Only they were somewhat unaware of most of the risks, the ones they were aware of was not relevant to them, since they didn’t see themselves as a reasonable target. Just as we continued on with the phishing part of the interview we got more alarmed over their understanding of emails and their behavior in phishing situations.

Phishing Email - Age Group 3-5 For the phishing part of the interview all of the candidates in age group 5 had all correct answers and even added some aspects in the form of stories from the early days of Internet. The information we got while asking about phishing and fraud/scam emails were stories about it existing before emails existed, but at that time in the form of letters and fax.

Age group 4, most of the candidates were aware
of which emails were phishing and if they were uncertain they would access the page by typing in the page which the mail comes from in the browser instead of the link in the email.

Then on to the age group we were concerned about, age group 3. All of the candidates were aware of fraud/scam emails, e.g Nigerian Prince[2], but a majority did fall for some phishing emails containing company logos. They trusted that they came from the companies and did not check the sender, which all the previous age groups had done. It was alarming, but we did ask what they would have done if they received an email like said phishing mail and their answers was to check with their parents or go via browser.

We did not conduct the phishing part of the interview with the younger age groups (1 and 2). We did ask if they had an email and none of the candidates had one, or didn’t have access to it. We asked if they would click a link sent to them and most of the candidates would, not knowing what that really meant.

For age groups 2 and 1 we had to arrange the interviews a bit different. The kids would have had a hard time understanding the questions we asked the older age groups and those questions wouldn’t had been relevant for their age.

**Age Group 2** Age group 2 are the ages 11-15 and was the hardest to get candidates to. We got two candidates that had the courage and time to meet us for an interview. Both the candidates had older parents that had an eye on their online activity. They were restricted when it came to social networks and their computer activity. But when it came to smartphone usage both of the candidates had free access to what they wanted with the restriction of not being able to buy applications for actual money.

Not many kids wanted to meet us or didn’t have time, that lead to us making a survey for this age group that answered the same questions as the ones being asked in a real life interviews. Five kids answered our survey, so we had a total of 7 kids for age group 2. Everyone in the group had their own smart phone and almost everyone had their own tablet and computer, except one candidate. They all had a pretty wide selection of units.

When it comes to time spent online we decided to divide it into how much time spent on each device. Look at Appendix for more detailed information. [6.2 fig. 2]. In this age group there were no specific device that were more popular then the other, as said before everyone had a smart phone which made that more popular in that aspect, but the usage was divided pretty evenly throughout devices. Also when it came to where they used the devices everyone answered at their spare time, except for the tablet and computer that was used in school for two candidates [6.2 fig. 3]. While online the candidates did pretty harmless stuff, like chatting with friends, social networks etc. But one candidate, 13 years old, watched pirate streamed films, and those sites are more often than not filled with pop-ups and viruses.

When it comes to password the 50% of the candidates would create easy passwords that they would remember, 12,5% would have something
personal, 25% randomized characters and the
remaining 12.5% had the principle to just have
a very long password. [6.2 fig. 4].

We asked them a bit about passwords and buy-
ing applications. 57.5% had at one point told
someone their password, but out of those 57.5%
only one candidate had access to their parents
password. So we weren’t worried about that
statistics, most of the kids didn’t have access to
their parents password and therefore couldn’t
tell it anyone else. While buying applications,
57.5% had done it and all except one had used
their parents account.

**Result Group 2:**

To summarize this age group, the statistics
show that they have a wide variety of devices
they can use for a lot of hours during the day.
Most of candidates had older parents (over 45)
except for the ones who were 13-15, who also
were the ones who tended to be more indiffer-
ent. This is according to our hypothesis, but
to strengthen it more we have to look through
the age group 1 as well.

**Age Group 1** The last age group we’re going to
analyze is age group 1, ages 7-10. We only got
the ages 8 to 9 in our investigation but since
we had trouble finding candidates we were satis-
ified with getting six candidates inside of our
decided spectrum. Our hypothesis is that most
of the candidates in age group 2 and 1 had ac-
cess to a smartphones and that was very much
ture. As mentioned before, everyone in age
group 2 had an own smart phone. In age group
1 four out of six (4 out of 6) candidates had
their own smart phone, the remaining two (2)
either borrowed or didn’t use a smart phone.
The person who didn’t use a smart phone said
if she wanted to she could borrow her moms
phone and didn’t feel the need because she had
her own tablet. The statistics for the ownership
in tablets were different. 50% of the candidates
had their own and 50% borrowed or shared one
with their siblings. [6.1 fig. 1]

When it comes to computer usage many of the
candidates expressed that they didn’t use a
computer that often, 2 out of 6 had their own
computer and the rest borrowed or didn’t use
one. That is also visible in the hours of usage
statistics [6.1 2]. The people who had their
own computer spent five to ten hours on the
computer a day, while the remaining candidates
expressed that if they used a computer it was
only for an hour or two. Which is interesting,
we see a trend in both age group 1 and 2 of the
computer being used less.

The usage of smart phone and tablet was more
frequent. All the candidates said they used
their phone for less than five hours a day, they
also expressed that it depended if it was a
weekday or not. But the usage of a tablet was
significantly more frequent. When we asked
some of the candidates when they used their
tablets they answered that they sit with them
before breakfast in the morning, after school
and after dinner. The only time spent away
from the tablet was during school and if they
were with friends. That we see in the statistics
when we asked were they used their devices, all
of the candidates answered on their spare time.

Now that we know the usage and what devices
their on we want to know what they do during all that time spent. The majority were playing games on their devices and chatting with friends. Pretty harmless usage, even though they expressed that they used social networks and that puts them at risks for hackers, malicious people online and pedophilia. We asked the candidates how they keep themselves safe online and some didn’t know, because they didn’t think about it, but many of them had locked profiles and didn’t allow just anyone to look at their profile. We noticed while asking after their parents age that there was a tenancy for kids with younger parents to have space to roam around on the Internet, their parents didn’t set that many restrictions. However, some kids with younger parents had heard from friends to be careful and even knew about pedophilia. We think that they were indeed careful online, but had a bit of a indifferent attitude towards Internet usage.

Result Group 1:

This group was not aware of risks. But due to the restrictions of their parents, they did not do much online. Which made the small amount of time spent online secure. The candidates were young in this group and that made it hard for them to have any sort of experience.

4.4.2 Surveys

Now that we’ve analyzed all the interviews in the different age groups we have one stage of data collection left, the surveys. We had one in Swedish which should be easier for kids to answer and one in English for adolescents and adults. Our goal was to get over 22 answers to make it valid, and we were blown away when just during our first day we reached well above that, and ended up with 67 answers. That was very fortunate and we were happy with that, but also when it comes to surveys we can only see it as secondary source of information. Often while answering a survey you get time to think and there is no one there to monitor you which could lead to some answers not being 100% true. For the survey we had a different set of questions, because all of the age groups had the same survey. So to analyze this data we will first go through the information collected in the surveys and then compare that to the interviews.

Age Group 1

Four candidates answered the survey who were under the age of ten. They all spent different amount of time online, we did not ask for a separation in time on different devices, just amount spent online. We had one candidate that spent more than five hours online, and that person stood out to us because of its way of online usage. The candidate spent time on torrent sites, pirate streaming sites and had a different choice in both search engine and browser. The search engine was DuckDuckGo [1] which is a search engine that doesn’t track what you do and they prioritize integrity. Browser choice was Microsoft Edge, which has a tendency to track you. However, Microsoft Edge is also known for being a secure browser. We were very confused with this entry. It did not sound like a person under the age of 10. Regardless, while asking the chain of thoughts while creating a password the person answered ’Something simple, easy to remember’ and ’My pet’, with a spelling error on pet. So the situation might be that they have parents with an interest in IT and the kid itself is also interested. Also the person was the only one who answered yes to the question ’If some-
one were to send you a link without any text would you click?'. The rest of the candidates had pretty similar behavior while online, their answers show a sense of carefulness, but at the same time a sense of insecurity.

Connecting the survey data with the interviews here is a bit hard. The understanding we got of the age group while interviewing is sharper than the answers in the survey. We would say the awareness of security shows in the surveys as well as the indifferent mindset mentioned in the analysis of the interviews.

**Age Group 2** Unfortunately we had no entries from this age group, which also was the hardest to hold interviews for. However, while doing the analysis we have had a tendency to add age group 1 and 2 together, and with the data collected from each age group we can make a good and accurate conclusion later on.

**Age Group 3-5** Here we had a bit of a mishap, while entering the ages we accidentally merged the age groups together by have answers like 15-20, which is both in the age group 3 and 4. Therefore the usage of the survey is a bit limited. We’re are going to divide into new age groups in the analysis only and see if we can get any useful information.

**Age 20-30** Most of our answers were in the ages 20-30, which is the age group 4 and a bit over. We are going to use them as age group 4, but the data can’t be taken as seriously as the data collected in the interviews. The group is active online, 59,2% is online more than five hours a day, 38,8 up to five hours a day and the remaining 2% up to one hour a day. Most of the candidates related their password to their everyday life and wanted it to be easy to remember and a majority of 85,7% would not tell a friend or family their password, but there were still 14,3% who would. We asked if they were careful with what pages they visited and a majority of 73,5% answered sometimes, which is a bit alarming. A interesting question for this group was if one of their accounts ever been hacked, here 36,7% said yes, 16,3% said maybe and the remaining 46,9% said no. A lot of people were unsure and a big amount had been hacked. Out of all the age groups participating in the survey it was only the one between 20 and 30 that had been hacked. The cause to this could be a several amount of reasons. It could be that this group is overrepresented and there were more likely to be someone in that group who had been hacked, or it could be that the younger generation is more reckless and when they get older they have more risk, because they have more responsibility. But we can’t really tell due to the lack of participants in the remaining groups.

**Age 15-20** This group we are going to count into the age group 3, 16-18. This group were also very active online with a majority of 85,7% spending more than five hours online each day. The rest of the participants spent less than five hours but more than one hour online a day. Their online activity were pretty harmless, mostly social networks and official streaming sites. Although, one participant did use pirate streaming. When it comes to passwords this group were very much aware. Only 14,3% had something that related to themselves, and 57,1% said they had a different password for each platform they used. 28,6% had something random for their password. With that in mind this group sounds cautious. The survey shows a more positive trend in the age group than the
interviews, which were more concerning than the survey.

Age 31-60 Only two participants in this group, both very similar in their answers. Both spent more than five hours online a day and while online they were on social network sites and official stream sites. Where the two candidates start to disagree is in questions about updates, anti-virus software, handling of credit card information and of personal information. One of the participants shops on a wholesale website and has a bit more relaxed mindset when it comes to saving information online. It is hard to summarize and compare to the interview because of the lack of participants in this group.

4.4.3 The Missing Age Group

In chapter 2.2 Scope we talk about a missing age group, 25-45. In the beginning of the Empirical study we thought we had a good understanding of this group and therefore excluded them from the interviews. We did have a good understanding, but to credit our speculations we conducted a second survey, more structured and specific than the first one. This survey was only for the age group 25-45.

Analysis: This group spends a lot of time online, 57.9% more than five hours a day and 42.1% less than five but more than one hour a day. What they did online was not age related, all the different ages used the same sort of sites and programs. We saw a lot of similarities between the missing age group and age group 3 and 4. The statistics for if they tell other people their password was almost identical to the statistics for the same question in age group 3. The age group we were a bit worried about.

However, while creating a password the age 25-45 were cautious and had many guidelines. If someone were to send a link without any text explaining only 5.3% would click, which is a very good statistics. When it comes to updates and anti-virus software the group was very divided. 52.6% had anti-virus software.

In this age group we also had some participants that had been hacked. Three participants had been hacked in the ages 25-30 and one participant in the ages 31-35. No one above the age of 40 had been hacked.

This survey didn’t show us anything that we didn’t expect already.

4.5 Discussion

In this section we’re going to go thorough all of the age group once again and use the data collected to evaluate what vulnerabilities the age groups expose themselves to. As mentioned earlier, we’re going to use the OWASP top ten list of vulnerabilities as they are the most common ones and they provide a comprehensive explanation to how something becomes vulnerable to a specific entry and general countermeasures that one can take.

Age group 1 As mentioned in the analysis 4.4.1 most participant in this age group owned their own smart phones but relies heavily on borrowing or sharing when it comes to both the tablet and computer, but what the devices have in common is that they are almost exclusively used in their spare time 6.1 fig. 3. From their answers in the interview we can see that the common activities associated with each device are all the same, mainly playing games. There are some time spent on social media and browsing but to a much lesser extent. Many of the
participants told us that both teachers, friends and parents has warned them about online activities, especially social ones as they can never be sure of who it is behind the other screen which has made them quite aware of the fact that there are people with bad intent.

As these devices are mostly used for entertainment we judge the risk of being targeted as low, because most of their time is spent in-game but there are some tendencies that we consider as risky behavior. During the interviews we found out that even though the participant owned a device, they mostly did not have administrative privileges but more often than not it is a parents account that is connected to the device which can be an easy way for a social engineer to acquire some information by taking advantage of the na"ive nature of children. While children are aware that they should be careful when chatting, they do not have the same caution when playing games, often interacting with other players. By befriending them online posing as another player, trust can be gained and information can be leaked. If we look at the charts showing how many that has access to their parents passwords [6.1, fig. 3] and the one showing how many that has given out their password [6.1, fig. 6] we can see that in both questions that half the participant answered yes, showing us that information could be extracted from the participants if one successfully tricks them.

None of the participants had bought applications in their respective application store (Google Play or Apple’s Appstore), meaning that all of their games are free for the participants but gains revenue by advertisements. This exposes this age group to adware and could easily target younger audiences and make them click.

We noticed that even though the participants were used to handling the devices, they had trouble doing tasks outside of their comfort zone, namely gaming and using their favorite applications. This trait is interesting because this makes children harder to target for Social Engineers because the effort of tricking them into doing a task becomes much harder.

The traits mentioned above make them less eligible to some extent to several exploits presented by OWASP as they often require some more knowledge about the system which the participants did not have. The aspect of drive-by download or unvalidated redirects and forwards as mentioned by OWASP[15] is always relevant as links are often presented when using a device connected to the Internet. As mentioned above, adware are present in many free-to-play games that exists in the different application stores available. We consider the participants in the age groups less prone to be subjected to this kind of intent as they don’t use the Internet as a source of information to the same extent as the other age groups.

Participants and their online activities in this group were under supervision by their parents which limits their online freedom but also limits the risks of malicious intent. We noticed that participants with generally younger parents had more online freedom, while other with older parents had more strict limitations. Examples of this is that the older parents often had to approve which applications that they wanted to download and limited the time the participant could use the devices while the younger parents did not put much effort into these kind of limitations. Another form of limitation is actually the age of the participants. Many on-
line services, like social media and other services where you register an account, require you to be 13 years or older. This limitation is not hard to bypass but many of the participant mentioned that their parents did not allow accounts on these services because of this age limit. Even though their age is somewhat a safety net their attitude and mindset is still to some extent reckless. That makes us wonder if their security mindset will affect their online experiences when they grow up and with that get less restrictions.

**Age group 2** While this group is similar in many ways to the prior one, there are some differences that stand out which are relevant for us to look into. Compared to the prior group, these participants tend to use the computer to a wider extent and for longer periods of time and a larger percentage own their own devices. There is a bigger variety of online activities in this group as well. For instance, we can see that general browsing and time spent on social networks has increased while the time spent playing games has decreased. This increases the risk of exposing themselves to malicious intent as their personal presence on the web is greater. Streaming video is also something that is quite popular in this group, and although streaming at sites like Netflix or YouTube is harmless there were some that used illegal pirate streaming sites (e.g. Dreamfilm) that often is infected with malicious adware, validated redirects, validated forwards and JavaScript adbombs.

Similar to the prior group, most of the devices are used in their spare time, but unlike them the computer has taken a bigger part in their education. Depending on how the school uses filters and such to prevent malicious intent to enter the domain, the participants could be a potential threat to the school’s system by becoming the exploits way into the domain.

When talking to the participants we got the impression that they were aware of the risks of online usage but generally did not care as they thought the risk of it happening to themselves were small because of the low value of their information. What they don’t consider is that malicious intent often is targeted against a wide range of people and not towards one specific individual.

**Age group 3** Compared to the previous groups, the time spent by the computer in general has increased since the computer has gone from being mainly a medium for entertainment to a tool for projects in school, browsing and personal errands. The most time online is spent on their smartphones and looking at the figure we can see that the time spent on social media is notably higher than the previous groups and compared to other online activities.

When it comes to their passwords and password security the answers were generally below our expectations. Comparing to the standard for a strong password which were mentioned in the section ‘Software Engineering and Malicious Intent’ the participants in this group mostly had a password that was easy to remember and was related to themselves. Some of them tried to make them more secure by auto generating their passwords but did also write them down which drags down the level of security.

This is the youngest group that was conducted to do the phishing experiment and while they did not trust the obvious scam and fraud emails, e.g the ones that are similar to the
Nigerian scam emails[^2], they did hesitate and sometimes fell for the phishing emails that included well-known brands and companies such as Swedbank or Paypal. When asked what signs they looked for when analyzing the authenticity of the e-mail the most common answer was that they looked at the design of the email, spelling errors and how it related to themselves, for e.g. there were few who fell for the scam which claimed that they had won a gift card from a well-known Swedish retailer since they would not sign up for online competitions and raffles. None of the participants looked at the sender which is a huge sign in most cases and many did not know that banks don’t send emails because of the risk of being posed as. On the other side, many participants told us that they wouldn’t click on links in an email if they were unsure about the content. If they did they would manually type it into the URL bar of their browser because then they can see the details of the URL.

In relation to the OWASP top ten there are obvious risks concerning unvalidated redirect, the risk is even bigger than the previous groups as their online presence is quite bigger and the number of pages they visit has also increased.

**Age group 4** By the data collected for this age group we could tell that the security awareness had increased as their passwords were stronger[^6, fig. 3] and we could see more cautious behavior like a bigger percentage having an antivirus software installed and were aware of the criterion’s of a secure website. Some were aware of the HTTPS protocol which is knowledge that previous groups did not show.

Many answered that they try to keep a relative long password (Minimum of 8 characters) with a combination of numbers and being complex (Upper- and lower case and Special characters) but still tried to keep it self-related to a reasonable extent. Some used variations of a password by changing some characters.

Almost everyone in this group has used the same password on multiple logins which is a risk but they mentioned that accounts which contain vital information often had a more secure and unique password. All but one answered that they had told their password to someone else, but mostly to accounts which does not contain said vital information[^6, fig. 4].

Many of the participants have stored their credit card information online or in the browser which is a quite a risk since the account connected to the browser is widely used for multiple services[^6, fig. 2]. The most common browser is Google’s browser Chrome. Google has implemented verifications that has greatly reduced the risk of credit card fraud by not storing the CVC number that’s on the back of the card. Instead they asks for it explicitly and thus making it a requirement to have access to the physical card.

When it comes to online activities the variations has grown and legal streaming has become the most dominant activity[^6, fig. 9]. There are still some tendencies to visit illegal pirate streaming sites and as mentioned earlier the risks of malicious adware and unverified forwards are big if sites like this are visited. However, many answered that a site feels insecure if it is full of ads and if the design is poor, which shows that they are aware of the risk but know that they can avoid the exploit by not clicking on ads and using browser extensions like ad-block[17].
Age group 5 On to the group who grew up without the Internet as a big part of their life, we noticed that they generally spend less time online and uses the Internet more as a tool for errands, socializing or as a source of information [6.5, fig. 6]. Their principles when it comes to password are quite similar to the previous group (group 4), if not even more secure as fewer has told their password to other people [6.5, fig. 4]. During the interviews, we got the impression that privacy is quite a important part of their online presence, which is not the impression that we got from the younger generations. This is based on this groups expressed concern around the information posted on social networking sites e.g Facebook. While the other groups has a bigger knowledge of how to limit the software that tracks them (e.g Google search) or uses software that doesn’t track at all (e.g DuckDuckGo), this group simply limited the information that they posted online. We would argue that the younger generations doesn’t value information as highly as the older ones, considering some data not to matter if it is posted which makes them seem more reckless in comparison to the older group.

During the time we wrote our thesis the virus *Wanna Cry* surfaced. It made it more important to make sure you updated your computer. This was very interesting, because in our survey we asked our participants how often they updated their computer etc. The answers we got were varying. We had three different surveys, one in English with the most participants, one in Swedish with the least participants and the last was for the ages 25-45. In the bigger survey the 43,3% answered *Yes, I try to do it as often as possible* and 23,3% answered *Yes, as soon as the update occurs*. The rest of the participants answered *Sometimes, when I have time, No, I postpone them, I don’t have time for updates* or *I tend to forget.*

The Swedish survey had different statistics, 54,5% answered that they don’t think about updates or believed they occurred automatically. 18,2% updated as soon as the update is released and the same amount (18,2%) avoids to update if it isn’t necessary. The remaining 9,1% tends to forget to update.

On to the ages 25-45, the statistics were a bit different here as well. 31,6% answered *Sometimes, when I have time,* 21,1% answered *I tend to forget* and same (21,2%) for *Yes, as soon as the update occurs*. 10,5% answered *Yes, I try to do it as often as possible* and the remaining 15,8% answered *No, I postpone them, I don’t have time for updates.*

It tends to vary if the participants update often or not at all. We would say that the numbers are a bit alarming, after *Wanna Cry* happened. In the case of *Wanna Cry* the majority of hacked systems were Windows machines that hadn’t been updated or old versions of the system. These versions still had a security hole which was fixed in March 2017 by Microsoft. With that said, updating your operating system is crucial. [6]
5 Conclusion

We notice some obvious and big differences in the various age groups. When looking into the security aspects, the candidates seemed to get more aware or cautious of risk the older they got. It is difficult to determine whether this reduced risk depends on the age of the candidates or because of their level of maturity.

It is arguable that information is considered less valuable to the younger groups, and it might have to do with the fact that information has always been available to them. The younger age groups generally run a smaller risk of exploitation than the older groups, not because of their lower level of knowledge and awareness but because of the restrictions imposed by parents or the services that the users used. All of the participants of the youngest group had some kind of limit on their activities and time spent on devices, which is a factor that reduces risk greatly. Another factor is that the amount of information that the younger groups have access to can be considered less valuable, as their personal email often are account made solely to register for accounts (e.g Games) and they do not have their own bank accounts which makes it almost impossible to make a profit of their information. We did consider age group 1 and 2 as the most vulnerable groups, but due to the facts stated above we decided otherwise.

The answer to our first question is that the group we feel is the most vulnerable and at risk according to their awareness and behavior is the age group 3 (16-18), born around the year 2000. These candidate shows a lack of understanding of what makes a password secure and were indifferent to the risks as they felt that they were not personally relevant to hackers. Most of the participants showed a great deal of insecurities during both the interview and phishing experiment. They were also prone to Social Engineering, e.g one of the candidates even told us the substance of their password without us even asking.

To answer the second question, all of the age groups are vulnerable to unvalidated redirects and bad links, some to a bigger extent than the others.

As mentioned above, the scope of activities limits the younger age groups. Age group 3 are more vulnerable, because of their increased activities on social sites like forums and social networks. This group is also the first one to show vulnerability to XSS attacks as they often have accounts registered on a large number of sites and mentioned that they did not think of the authenticity of the links that were sent, as long as they trust the source which sent it. The older age groups performed well in their awareness which clearly reduced their risk but unvalidated links are still a small concern. Their e-mail accounts are often strictly used professionally and thus keep the number of spam emails down, but there are still some influx.

We noticed that all of the age groups had an inapprehensive view on updates. Most of the participants knew to update and did so, but as rarely as possible. Wanna Cry is over but that doesn’t stop new similar viruses to show up, update your software!

Future Work

As mentioned earlier, we didn’t find sources that was up-to-date or relevant in this problem area, and our conclusion might be a red flag for the schools. When asking the younger age groups
how they learned how to act online, most answered through friends and learning by doing. We believe that the schools should place some focus on risk of online activities. Our thesis can help get an understanding of what the different age groups are more prone to be exposed to and indicate where they can continue the investigation further on.

You should not have to be hacked to learn the importance of online security, which might happen if we continue the course of trial-and-error.
References


6 Appendix

6.1 Appendix 1 - Statistics for age group 1

Figure 1: Device usage

Figure 2: Time spent at each device
Figure 3: Password Principles

Online Activities

Figure 4: Main Activities
Figure 5: Access to their parents password

Do you have access to your parents password?

- Yes: 50%
- No: 50%

Figure 6: Has told their password to someone else.

Have you ever told your password to someone?

- Yes: 50%
- No: 50%
Figure 7: Password Principles

Principles when creating a new password?

- Easy to remember: 45.5%
- Personal: 27.3%
- Random Sequence of characters: 18.2%
- Many numbers: 9.1%

Figure 8: Connection to public Wifi

Do you connect to public wifi connections?

- Yes: 50%
- No: 50%
6.2 Appendix 2 - Statistics for age group 2

Figure 1: Device usage

Figure 2: Device usage
Figure 3: Where each device is most used

**Principles when creating a new password?**

- **Easy to remember**: 50%
- **Personal**: 12.5%
- **Random Sequence of characters**: 25%
- **Long (Min. 8 char)**: 12.5%

Figure 4: Password principles
Figure 5: How many that have told their password

Have you ever told your password to someone?

- Yes: 42.9%
- No: 57.1%

Figure 6: Access to their parents password

Do you have access to your parents password?

- Yes: 14.3%
- No: 85.7%

Figure 6: Access to their parents password
Figure 7: Connection to public wifi

Do you have access to your parents password?

- Yes: 85.7%
- No: 14.3%

Figure 8: Main Activities

Online Activities

- Chat & Social Media: 38.5%
- Gaming: 23.1%
- Browsing: 30.8%
- Pirate streaming: 7.7%
6.3 Appendix 3 - Statistics for age group 3

Figure 1: Time spent by the computer each day

How much time do you spend by the computer each day?

- 75% up to 5 hours
- 25% 5 to 10 hours

Figure 2: Time spent online each day

How much time do you spend online?

- 62.5% up to 5 hours
- 25% 5 to 10 hours
- 12.5% more than 15 hours
Figure 3: Creditcard information stored online

Figure 4: Password Principles
Figure 5: Password Principles cont.

Same password on multiple accounts

- Yes: 87.5%
- No: 12.5%

Figure 6: Do you connect to public WiFi spots?

Do you tell your password to others?

- Yes: 62.5%
- No: 37.5%
Figure 7: main activities online
6.4 Appendix 4 - Statistics for age group 4

Figure 1: Time spent by the computer each day

Figure 2: Time spent online each day
Figure 3: Creditcard information stored online

Figure 4: Password Principles
Figure 5: Password Principles cont.

Figure 6: Do you connect to public WiFi spots?
Main activities online?

- Gaming: 13.3%
- Streaming: 33.3%
- Pirate streaming: 13.3%
- Social Media: 33.3%
- Information seeking: 6.7%

Figure 7: main activities online
6.5 Appendix 5 - Statistics for age group 5

Figure 1: Time spent by the computer each day

Figure 2: Time spent online each day
Do you have a password on your smartphone?

- Yes: 83.3%
- No: 16.7%

Figure 3: Smartphone password

Password principles

- Variation of an earlier password: 25%
- Self related: 20%
- Easy to remember: 20%
- Long (min. 8 characters): 20%
- Upper- and Lowercase: 10%
- Numbers: 5%

Figure 4: Password Principles
Figure 5: Password Principles cont.

Figure 6: Do you connect to public wifi spots?
Figure 7: main activities online

Main online activities?

- Social Media: 31.3%
- News: 12.5%
- Banking: 6.3%
- Business: 6.3%
- Gaming: 18.8%
- Streaming: 25%

Figure 8: Stored credit card information online

Do you save your creditcard information online?

- No: 100%
6.6 Appendix 6 - Emails used in the Phishing experiment

Figure 1: Swedbank phishing email
Don't recognize this activity? Review your recently used devices now. Why are we sending this? We take security very seriously and we want to keep you in the loop on important actions in your account.

We were unable to determine whether you have used this browser or you have used this browser or device with your account before. This can happen when you sign in for the first time on a new computer, phone or browser, when you use your browser's incognito or private browsing mode or clear your cookies, or when somebody else is accessing your account.

Log In

Do not reply to this email. To contact us, click on Help & Contact.
Från: Mitchell D. Chester <mitchellchester@doe.mass.edu>
Skickat: den 25 februari 2017 06:49
Till: Me
Ämne: Confidential Message About Your Fund ($4,100,000.00)

Hello my dear friend,

I am Dr. Mitchell Chester. I am a US citizen, 64 year Old. I reside here in Massachusetts US. My office address is as follows. 75 Pleasant Street Malden, MA 02148 USA.

I am one of those that fall victim to scammers in Africa two years ago. I have lost over US$74,000 for the past years. I was trying to get my payment all to no avail and they always stopped. I decided to travel with my son to WASHINGTON, D.C. with all documents, there the (FBI) was amazed and contacted the Nigeria Embassy in the US and after some hours in that office, I was able to get all the required documents.

When I did, the FBI officer gave me the contact of Mr. Godwin Emefiele who is the Governor of the Central Bank of Nigeria. When I contacted him, he explained everything and said that we should fly down to Nigeria to see things for myself, which I did and he took me to the paying bank for the claim of my compensation fund.

This was paid to me successfully and right now, I am the happiest man on earth because I have finally received my compensation fund of ($4,100,000.00) Moreover, Mr. Godwin Emefiele informed me that I am yet to receive their compensation fund and this was how I came across your email address and your full name.

The only money I paid after I met with Mr. Godwin Emefiele was just $275 for the demurrage charge. So I am advising you to contact Mr. Godwin Emefiele through his email address (godwinemefiele@gmail.com) including the money you lost to those scammers. You can as well call him on his direct telephone number (+2349079857244) please take it very serious. Contact him right now and send your address to him so that he can release your own money to you.

Thank you & God bless you.

Mitchell D. Chester
Commissioner of Elementary and Secondary Education Massachusetts Department
75 Pleasant Street Malden, MA 02148

Figure 3: Mitchell D. Chester fraud email
Hej Amanda Björneskog!

Du har fått ett nytt brev från Pensionsmyndigheten i Kivra.

Tipa dina vänner om Kivra! Ju fler som använder Kivra desto bättre för miljön. Nu skänker vi dessutom 20kr till Barncancerfonden för varje person som registrerar sig på kivra抗癌cancer.se
Frågor om Kivra? Kontakta oss på support@kivra.com

Majoriteten av Sveriges största företag och myndigheter skickar post via Kivra. Se fler

Figure 4: Kivra real email

Från: Briony Briony <Briony.Gore@glos-care.nhs.uk>
Skickat: den 14 mars 2017 13:10
Till: Briony Briony
Ämne: RE: Grant

I write this email to you on behalf of Qatar Foundation. Contact them for more details on (donationredeemoffice12@gmail.com) about funds.
Figure 5: Gore Briony fraud email

From: IKEA FAMILY KALMAR <noreply@ikeafamily.anpdm.com>
Sent: March 23, 2017 08:19
To: mandolina_95@hotmail.com
Subject: Premier tomorrow!

IKEA FAMILY
Detta händer i ditt varuhus

Se mer av KRYDDAD – ny tillfällig kollektion!
Omr du inte kan läsa detta mail klicka här »

NY TILLfällig KOLLEKtION!
PREMIÄR 24/3

INGET GÅR TILL SPILLO!
KRYDDAD är skapad i samarbete med sociala entreprenörer i Indien. Produkterna i kollektionen är
handgjorda av hållbara traditionella material. Bland annat används bananfiber, ett material som blir över
efter att bananerna skördat. I KRYDDAD har färorna bland annat använts för att göra korgar, väskor och
sittväddar.

Figure 6: IKEA Family real email
Alzheimersforskning som gör skillnad redan idag


En blick från insidan av Alzheimers sjukdom


Läs mer här

---

Figure 7: Hjärnfonden real email
Grattis, [mandolina_95] du är en vinnare
Klicka Här

Vinna ett Presentkort!
Din e-postadress har blivit utvald att vinna detta
Lindex Presentkort vårt 5000 kr!
Valda e-postadress:
mandolina_95@hotmail.com
Gå med nu, detta erbjudande slutar snart!
Fortsätt

Vinna ett Presentkort!

Du får detta e-brev eftersom du prenumererat på erbjudanden från oss.
Om du inte längre vill få erbjudanden från oss, klicka här.

Figure 8: Win a gift card scam email
Från: CANADIAN PHARMACY <nxhaepeivsabsuxoj@pharmaa.can>
Skickat: den 30 mars 2017 16:00
Till: rasmusholm11@hotmail.com; petter_1520@hotmail.com; piliprex@hotmail.com; mandolina_95@hotmail.com; peace3002@hotmail.com; parisspp1@hotmail.com; melanie
Åmne: DISCOUNT 67%

Click Here [US Pharmacy Online]

==> www.mdsrece.webrale.su

SALE TODAY:
Viagra | Price: $0.81
Cialis | Price: $0.84
Viagra Professional | Price: $2.64
Cialis Professional | Price: $3.55
Levitra | Price: $1.04

Payment: VISA, MasterCard

Copyright 2007-2017. All Rights Reserved!

(If the link does not work then click - It's not spam Or Copy and Paste this Safe redirect Url into your browser)

Figure 9: Canadian pharmacy scam email
Från: Rosenboms Nation <curatelet@rosenboms.se>
Skickat: den 21 mars 2017 22:19
Till: 
Ämne: Kallelse valmöte

Hej kära medlem,

Varmt välkommen till Rosenboms Nations valmöte fredagen den 31 mars klockan 17:15. Mötet kommer äga rum på Campus Gräsvik, Blekinge Tekniska hemsidan.

Ur stadgan:

-----

§ 6. Ordinarie nationsmöten
Nationsmöten sammankallas av styrelsen. Ordinarie nationsmöten äger rum i april och oktober samt udda är även i mars. Kallelse ska vara medlemmarna tillhanda senast 18 dagar före mötet. Föredragslistan med bilagor fastställs av styrelsen och ska vara medlemmarna tillhanda 8 dagar innan mötet.

§ 7. Valmöte

Vid valmöte ska nationen:
- Välja curatorer på en mandatperiod om två år

-----

Medtag medlemskort och giltig fotovalidering.

Vi uppskattar att ni attenta på facebook eftersom vi kommer bjuda på fika under mötet. Rumsnummer meddelas via facebook.

Öppen utfrågning av kandidater

Valberedningen välkomnar dig till en öppen utfrågning av curatorskandidaterna torsdagen den 23 mars klockan 12.

Ur stadgan:

-----

§ 2. Attaganden

Valberedningen ska sammanställa ett förslag med kandidater till samtliga valbara poster. Inför val av curatorer ska valberedningen sammanställa nationens medlemmar till en öppen utfrågning av kandidaterna. Den öppna utfrågningen ska äga rum minst 7 dagar innan nationsmötet.

-----

Vänligen / Best regards,

Curatelet | Rosenboms Nation
Mail: info@rosenboms.se
Facebook | Web | Instagram | Linkedin

Figure 10: Rosenbom real email