

Phishing susceptibility: Differences Across Generations

A qualitative comparative case study assessing the phishing detection abilities in young and elderly people

ESPEN THORSEN FRANK

SUPERVISOR

Marko Ilmari Niemimaa

University of Agder, 2022

Faculty of Engineering and Science
Department of Information systems

ABSTRACT

During the last couple of years organised cybercrime have gotten substantially worse, especially the method known as phishing. This is a comparative case study that investigated how well we as users detect this type of cyberattack by analysing the participants thought process as well as their ability to verify incoming emails and text messages. The data collection process was done through semi-structured interviews with seventeen participants, where nine were young adults and eight elderlies. Firstly, the interview procedure consisted of questions regarding their occupation, education, internet activity, and phishing knowledge. Secondly, they went through ten phishing examples while explaining why they thought it was legitimate or phishing. My results showed a clear distinction between the two groups, such as the elderly were much more careful and sceptical compared to the younger group. Thus, it can be suggested that age has a clear impact on how we deal with the phishing threat.

ACKNOWLEDGMENT

Finishing this master thesis could not have been done without the help from several generous people. Firstly, my supervisor Marko, who throughout this entire process provided me with his expert insight on the topic as well as guidance meeting bi-weekly from start to finish. Secondly, I would like to thank all the participants who were kind enough to open themselves up for me while being under the “magnifying glass”. Lastly, I would like to thank my mom, dad and brother who all pushed me to keep going when motivation was wavering.

TABLE OF CONTENTS

1	INTRODUCTION.....	10
	1.1 Research Motivation.....	11
	1.2 Research Questions and Gap.....	11
	1.3 Research Activities.....	11
2	LITERATURE REVIEW.....	14
	2.1 Key Concepts:.....	16
	2.1.1 Stage Theory and Personalised Recommendations.....	16
	2.1.2 Cognisant Study Bias.....	16
	2.1.3 Kill Chain.....	17
	2.1.4 Attack Tree.....	19
	2.1.5 Attack Trends.....	20
	2.1.6 Opportunistic COVID Exploiters.....	20
3	METHODOLOGY.....	22
	3.1 Literature Review.....	22
	3.2 Problem Formulation.....	22
	3.3 Protocol Development.....	22
	3.4 Literature Search.....	23
	3.5 Screening.....	24
	3.6 Quality Appraisal.....	24
	3.7 Data Extraction.....	25
	3.8 Comparative Case Study.....	25
	3.8.1 Case study pros & cons.....	26
	3.9 Case selection and definition.....	26
	3.10 Data collection.....	27
	3.11 Methodology Limitations.....	28
	3.12 Ethics.....	28
	3.13 COVID Complications.....	28
	3.14 Interview Process.....	29
	3.14.1 Phishing Detection and Process.....	29
	3.14.2 Phishing Assessment.....	29
	3.15 Qualitative Analysis Process.....	33
4	FINDINGS.....	34
	4.1 Case: Young.....	34
	4.1.1 Descriptive Themes Uncovered.....	34

4.1.2	Detection Analysis	34
4.1.3	Young Participants Message Content.....	35
4.1.4	Young Participants Message Context.....	36
4.1.5	Accuracy Young.....	37
4.2	Case: Elderly	38
4.2.1	Descriptive Themes Uncovered	38
4.2.2	Elderly Participants Message Content.....	39
4.2.3	Elderly Participants Message Context.....	39
4.2.4	Accuracy Elderly.....	39
4.3	Secondary findings	40
4.3.1	Attack Trends.....	40
4.3.2	Phishing Victims	40
4.3.3	Training	41
4.3.4	Cognizant Bias.....	41
4.3.5	Outside Factors	41
5	DISCUSSION.....	42
5.1	Limitations.....	44
5.2	Future research.....	45
6	CONCLUSION	46
7	REFERENCES.....	47
7.1	Appendix 1: Interview guide.....	51
7.2	Appendix 2: Phishing assessment	52

List of tables

Table 1	PICO table.....	23
Table 2	Case descriptions.....	27
Table 3	Phishing assessment accuracy young participants (P)	38
Table 4	Phishing assessment accuracy elderly participants.....	40
Table 5	Message content comparison.....	43
Table 6	Message context comparison.....	44

List of figures

Figure 1	Kill chain depiction.....	17
Figure 2	Attack tree module.....	19
Figure 3	Convergence behaviours in disasters.....	20
Figure 4	Phishing example: Contextual relevance	30
Figure 5	Phishing example: Unreasonable Request	31
Figure 6	Phishing example: Grey area.....	32
Figure 7	Young participants thought process, Message content	35
Figure 8	Young participants thought process, Message context	37

1 INTRODUCTION

As technology continues to develop and improve our day to day lives, threats have also become more rampant. With the globalisation and increase in accessibility, the internet has become increasingly dangerous for unaware individuals. The fact that the barrier of entry into the digital world is close to non-existent, results in hundreds of millions of people yearly being affected by cybercrime (Lazic, 2021).

Phishing is a criminal tactic that threat-actors use to fool and exploit innocent people for their own benefit. The act of phishing revolves around convincing the target to reveal personal identifiable data (PII), which they then use to gain access to accounts, with banking or credit card details stored. The phishers also deploy strategically planned out attacks to specific individuals, a spear-phishing attack, who often are the start of advanced persistent threats (APT) (Singer & Friedman, 2014). The damage globally is in the billions of dollars, whereas a single data breach caused by phishing on average cost four and a half million dollars according to IBM (Brecht, 2019). The damage affects many aspects of the day-to-day business such as loss of work hours, a drop in the stock price and trust from customers are lost as a result of their reputation being tarnished by cyber criminals and mishandling of their personal data.

Phishing also comes in many variances and has always followed the digital innovation trend. Over the years, the threat actors have gone from social engineering over the phone (vishing) to text messages (smishing) (Yeboah-Boateng & Amanor, 2014). Usually accompanying whatever technology the population uses the most at a given time. During COVID-19 pandemic, opportunistic threat actors saw the massive surge in home-office working employees with little to no security training and promptly tried to abuse the situation. Up to 220% increased phishing incidents were recorded compared to the usual average (Warburton, 2020). Phishing is also a very subjective threat, meaning that different people will react to it differently (Hassandoust, Singh & Williams, 2019). Which is the main motivation for this thesis.

In my master thesis I will be studying young adults and elderly people in their relation to phishing attacks. My goal is to get a deeper understanding on their rationale for identifying a fraudulent email from a legitimate one. I will be doing this through a qualitative study with relevant interview subjects and quantifying the data through the usage of a phishing detection assessment. Lastly, I will compare the results and do a comparison analysis between the young adults and elderly to

see if there are any differences in their cyber awareness, success rate of phishing frauds and if any of the two demographics are more susceptible than the other.

1.1 Research Motivation

The phishing threat is an ever-increasing method utilised by black hat hackers today and has seen an exponential growth during the COVID-pandemic (Johnson, 2021). Statistics shows that in Q3 2013 the amount of detected phishing sites was in the 140,000 whereas in Q1 2021 the numbers were as high as 637,302 sites. The fact that this is a world-wide current problem motivates me as my research can be beneficial in decreasing the number of successful attacks and helping unfortunate people who are taken advantage of.

1.2 Research Questions and Gap

In my research, I will be studying young adults (age 18-26) and elderly people (age 60-80) to see if there are any specific differences in their susceptibility towards phishing attacks. I will also be looking at how they verify an illegitimate email to see if there is any correlation between age and reasoning skills or if it comes down to technical skills. To execute this research, I will therefore try to answer the following research questions to explain my findings:

- Are the young or old generation more susceptible to phishing frauds?
- How do they identify a phishing email from a legitimate one?
- Are there any differences in their verification skills?

What separates my thesis from the other published articles regarding phishing susceptibility is the chosen demographic and the focus of the study. The main focus of my study is to portray the individual thoughts when processing a phishing email.

1.3 Research Activities

To conduct my research, I completed several different research activities. In the following order they are represented in the thesis.

Literature review: The literature review follows the Systematic Literature Review method (SLR) which consists of several steps to help reduce the amount of literature down to the most beneficial for my own study and research questions (Kitchenham et al., 2009).

Data gathering methods (Qualitative interviews): For information gathering I will be collecting data through both interviews and a phishing assessment process. The interviews will be semi-structured, and the participants will be asked about their relationship with phishing frauds as well as their rationale when identifying illegitimate messages. I will also show examples from real life phishing attacks which they will attempt to distinguish from genuine emails. These interviews will be conducted either virtually through Zoom, Microsoft Teams or phone call or physically at Campus and elder homes.

The goal of the phishing assessment process is to get more quantifiable data, where the participants will go through a ten phishing examples and label them genuine or fraud.

Analysis of the data gathered: The data from the interviews and the phishing assessment will then be analysed to see how the results may differ based on age.

2 LITERATURE REVIEW

One way to gain a more overall understanding of the situation is to study both the victims as well as the perpetrators (Tambe, 2017). This is done to figure out why they end up as scammers, which in itself can have many variables such as personal experiences. It is revealed in the study "*Toward a rational choice process theory of internet scamming: the offender's perspective*," that many of the older perpetrators do it out of revenge as they could not obtain lawful employment by factors out of their control. Alas, they are justifying their criminal methods because they were cut short the legitimate way. While the younger perpetrators tend to join the activity through inspiration of the luxurious lifestyle the older generation portray or through societal connections.

The act of phishing is also extremely cost efficient which can seem very tempting to many people with less opportunities, hence why they are often situated in areas with low quality of life.

Essentially, phishing is "stealing" sensitive information, and therefore shares some similarities with burglary. However, burglars often choose their targets randomly as suggested by street crime offenders (de Haan & Vos, 2003), on the contrary, phishing threat actors plan out their angle of attack meticulously from start to finish to maximise their success rate and yield. Phishers chose their target based on the victims' interests or position. Often are executive employees targeted through spear-phishing attacks which are planned specifically for chosen individuals. Their motive being espionage on the company's trade secrets or exfiltrating internal data such as customer records or employee credentials to further extend their grasp on the internal systems by moving laterally undetected (Ghafir et al., 2018).

Another important aspect of phishing is to examine if there are any demographics that are more susceptible than others. The reason for this being that if we know who are more exposed, we can focus on improving our recommendations towards those that suffer the most.

One way that we can specifically tailor recommendations between many skill levels and cybersecurity awareness is by using stage theory (Tambe, 2017). Stage theory is a concept taken from health and psychology communication which aims to separate people into distinct stages and apply the corresponding recommendation based on their prior knowledge on the subject. Thus, it is proposed three stages to include all varieties of skill levels. In stage 1 we have people described as having zero awareness training as well as being completely naive that their online actions

can have serious repercussions if exploited by malicious hackers. These people need to be informed on what existing threats are on the internet as well as overall increase their awareness. Stage 2 people are described as having some prior knowledge; however, they do not actively seek out new information on the subject, leaving them unaware of scams they are unfamiliar with. Hence why they should be trained more sophisticated, such as simulated phishing attacks and how to verify the authenticity of emails by identifying the most common cues on fraud attempts. Lastly, the people in stage 3 have continuous security training and high self-efficacy. Compared to the people in the earlier stages, stage 3 individuals are already aware of existing frauds and should therefore be cautious not to be overconfident. Recommendations for these individuals should also be to discourage complacency.

These examples highlight that by applying stage theory when giving out recommendations we reach all skill levels and we do not enforce completely unfitting knowledge on certain individuals, which will always happen when the recommendations are generic. Now that we know that we should give recommendations based on the individual's skill levels, figuring out who is most susceptible is the next step.

Sheng et al., (2010) says that the younger generation have less experience, lower education level and less rationale financially, making them increasingly reckless on the internet. Compared to the older generation who are more reserved. The study also showed that participants who took an anti-phishing course improved their detection skills by 40%, an interesting side effect accompanied the training which made them overly cautious hence a reduction on identifying legitimate emails.

More direct studies have been conducted regarding phishing detection between the younger and older generations, where they tested how well they could sort legitimate emails from the scams (Sarno, Lewis, Bohil & Neider, 2020). The most notable result from this study was that overall, the accuracy was surprisingly low where on average half of the phishing emails went unnoticed. This is very alarming as only one undetected phishing email can be extremely costly.

Grilli et al., (2021) shows that in their study of eighty individuals, older age does not necessarily mean their perception or email safety was reduced but their perceived suspiciousness made them worse at identifying legit from phishing emails. This result was similar to the Sheng et al., (2010) study where they theorise that when people are made aware of a threat, their increased suspicion negatively impacts their critical thinking leading to a reduction in their identification process.

Hakim et al., (2019) conducted a study where the 158 participants (young and old) were unaware that they partook in an experiment and received simulated phishing attacks daily over the course of 21 days. Their findings showed that while being unaware of the situation they were in, forty-three percent of the participants got phished whereas older people reported lower susceptibility awareness. Further

enforcing the notion that study bias impacts the results, as their results differed from the studies where participants were cognisant. It also shows us that personalised recommendations should be the norm in security solutions for the coming generation.

Pattinson et al., (2011) also investigated whether personal characteristics impacted the user's response to phishing emails. The study showed that familiarity with computers and cognitive impulsivity have significant effect when analysing phishing emails.

2.1 Key Concepts:

While developing my literature review, these key concepts were often brought up in several research articles.

2.1.1 Stage Theory and Personalised Recommendations

Most articles discuss their recommendations for minimising the effects of phishing emails in the future. Tambe (2017) and Lin et al. (2019) both recommend that personalised security training and recommendations should be the staple security solution going forward. Tambe (2017) showcases this by separating people into "stages" built on their preconceived knowledge of internet threats. The study by Lin et al. (2019) exacted the same conclusion based on their results where age and gender might have impacted their verification and validation skills. Hence why instead of a universal overall safety recommendation, recommendations should be tailored towards the individual's needs.

2.1.2 Cognisant Study Bias

After reading several papers performing a type of phishing test, it is clear that when the participants were cognisant about their task, they became overly cautious. Therefore, the results shown by Lin et al. (2019) are more authentic to how people would act in a natural setting, distracted by other variables while being exposed to phishing threats.

2.1.3 Kill Chain

One way to think about a cybersecurity attack is as a kill chain. The definition originates from military operations, where it is used as a model to display the stages of an attack. (Greenert, 2013) To differentiate the military definition and information security definition, the latter is often referred to as the cyber kill chain. The first description of a cyber kill chain was in 2011, by scientists at Lockheed-Martin. (Hutchins, Cloppert & Amin, 2011) They initially called it an “intrusion kill chain” and was used as a model for defending computer networks. Today, the cyber kill chain is a framework consisting of seven different phases: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, Actions on Objective. One of the primary concepts with the kill chain framework is that the phases must happen in order. As such, stopping an attacker during any one phase will break the chain and prevent them from further advancing their attack, essentially giving a defender seven opportunities to halt the attack. (Lockheed, 2015) Lockheed-Martin presents malware defenders with defence options for each phase of the attack, which includes defences involving humans, technologies, and protocols. Phishing and social engineering is typically used in the first four phases. I will provide a summary of the first four phases and how to defend against each step.



Figure 1 Kill chain depiction

Phase 1 - Reconnaissance

The first phase is when an attacker gathers information and plans the attack. Information gathered could be email addresses or other accounts connected to employees, or about the discovery of other potential entry points for an attack, like an internet-facing server or scouting which employees are potentially more susceptible.

Successfully detecting reconnaissance in real time is difficult, but carefully logging traffic can be very useful to have after an attack or during later phases of the attack. If one is able to recognise patterns from the logs it can be used to implement rules and detectors that may in the future alert a defender of a potential reconnaissance project. Training both humans and computers to know what to look out for

are viable options, so the optimal defence strategy involves both human and technological concepts.

Phase 2 - Weaponization

In the second phase the attacker will design their weapon used in the attack. They will use the information gained from the first phase to make sure their weapon can get through the target system's defences, and package all the components together. There can be many different items involved, both physical and digital, such as files, emails, social media profiles or USB sticks.

Defending against weaponization in real time is practically impossible, as the attacker isn't directly interacting with the defender. It is still possible to hinder or slow down the progress of an attacker. The primary method is to analyse how the malware is built, whenever they get detected in the system. Effective analysis can lead to recognising patterns of malware artefacts, in turn being able to recognise the artefacts of future malware and stop it in its tracks. In this phase the defence options are primarily technological.

Phase 3 - Delivery

For the third phase, the attacker will have to bring their malware to the target. This can be an adversary-controlled delivery, which focuses on a direct attack on a web server or similar, or an adversary released delivery, which goes through employees through malicious emails, watering holes or similar. The delivery can be performed physically, like with a USB stick, but generally attacks are digital at the moment due to more delivery options and a higher number of potential targets.

In this phase it becomes possible for a defender to stop attacks as they happen. By constantly analysing malware that gets successfully delivered, it is possible to learn how they infiltrate the security of the system and update it so those loopholes or exploits no longer work. This makes each subsequent attack harder to pull off than the previous one. An effective countermeasure for this phase would also be to make sure employees are up to date on how to safely traverse the web, and what steps need to be taken in case they spot something suspicious. In this phase it is important to combine human and technological defence mechanisms.

Phase 4 - Exploitation

In phase four is where any exploit is started and used to gain some sort of access to a system or a user. Zero-day exploits, server based vulnerabilities or a victim triggered exploit (like a user clicking a malicious link or opening a malware attachment from an email) is typically used in this phase.

Defence in this phase can also be done through training the employees, both with awareness and secure coding. Successfully employing both of these means an employee can't be tricked into starting the exploit, and it is harder to do it through

the web servers. Another way is to make use of scanning and penetration testing tools frequently.

For phases 5-7, an attacker would already have some sort of access to a system and gains no notable advantage from further phishing

While the Lockheed-Martin kill chain framework leaves potential entryways for an attacker that does not require any use of phishing, it is still likely to be used. It is potentially easier for an attacker to use a general model for their phishing purpose and change some variables depending on the target, than to have a general model for attacking a web server. While humans have fairly similar weaknesses that can be exploited, different types of servers could have a wide variety of weaknesses that work in very different ways.

2.1.4 Attack Tree

Software gets infiltrated all the time. No matter how robust it might seem, every system has flaws. Attack trees were designed with that context in mind, seeing the system from the threat actor's point of view and mapping out all possible ways they might take to exploit and infiltrate the software.

Highlighting the attack process can be done through the usage of attack tree modules. It is done to further analyse digital threats and their different outcomes. The root node represents the threat actor's goal, while the sub-trees are the different paths the perpetrator can take to reach the goal.

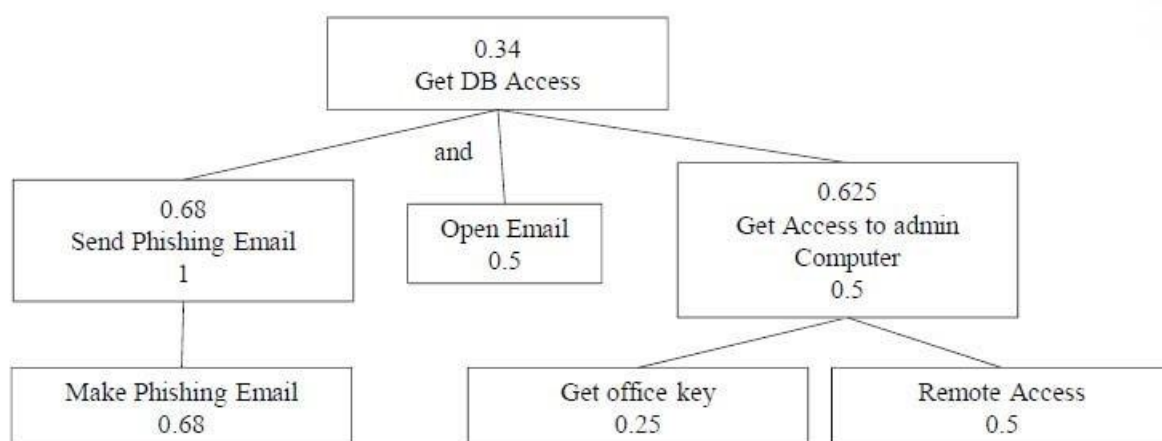


Figure 2 Attack tree module

In this diagram, the threat actor can accomplish their goal [Get DB Access] by either following the right or left path (Torkura et al., 2018). The paths begin at the bottom, where the perpetrator can either follow the digital left path, or the more physical right path.

2.1.5 Attack Trends

As cyberspace becomes more interconnected, shifting towards mobility and accessibility, malicious actors will always follow suit. In a report by McKinsey; *Cybersecurity trends: Looking over the horizon* published March 2022, three trends were identified as growing with large-scale implications. Especially has the massive increase in collection of personal data soared to new heights, such as political views, interests and transactions are gathered to better personalise ads and to influence their purchasing behaviour. As well as gathering more information, most of the data can be access by cloud services making them also more centralised. Threat actors have taken notice of this trend and aim to harvest login credentials from employees with access to the data sets.

2.1.6 Opportunistic COVID Exploiters

The framework made by Fritz and Mathewson can be used to study and prepare for how exploiters will adapt to new crises such as the pandemic that began around 2020 (Fritz & Mathewson, 2957). To a great degree, convergence behaviour in cyberspace can be observed with the massive increase of cyberattacks and shift of attack trends during this period. The exploiters are opportunistic people, who are looking to take advantage of the vulnerable people who are even more susceptible to threats as they find themselves in a completely new setting.

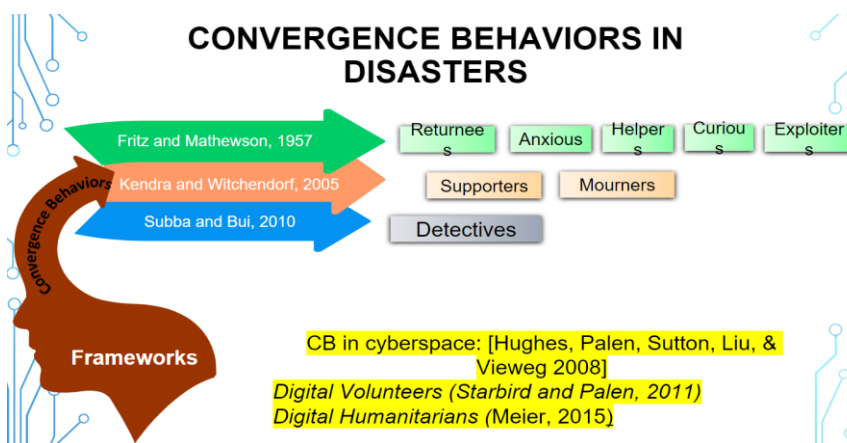


Figure 3 Convergence behaviours in disasters

In this picture we can see all the groups of people that are affected and those who respond during an incident. The Anxious demographic are often the group of people who get taken advantage of, as they are more emotionally invested in the situation which the exploiters see as an entry point. In the COVID case this can be perceived particularly in two situations. The first being the global shutdown incident which promptly sparked a massive resurgence of interest in online shopping. Exploiters would then take notice of this trend and employ tailored cyberattacks accordingly.

One of the more common cyberattacks they initialised was phishing emails masked as shipping emails. Such as

“There was a problem during shipment, visit [link] to pay a fee for it to be sent”

which is a clear attempt to exploit the people who are insecure about how shipping is handled and if additional costs may occur during the process. However, fortunately during an incident we can also observe The Helpers, who in this case will report to officials that there is a new cyberattack trend going on. IT providers and media outlets will then rapidly issue a warning, reducing the effectiveness of the new attack trend.

The second attack trend, spear-phishing attacks, rose in popularity as much as 220% according to Warburton in his 2020 Phishing and Fraud Report (Warburton, 2020). The primary objectives of these phishing emails were to capitalise on the pandemic, such as threat actors creating fake charities asking for financial support. As well as impersonating several of the most popular brands such as Amazon, WhatsApp, and Netflix. As much as 52% of phishing sites were using said brands to lure victims in. Paired with a fake name, phishing domains also started to follow encryption standards to appear as genuine as possible. 72% of the sites were utilising the standard encryption protocol HTTPS to further sell the image of a legitimate site.

3 METHODOLOGY

3.1 Literature Review

The research regarding phishing is already quite heavily documented and studied upon. Many of the articles however have different limitations and goals which makes for a perfect read as no two articles conclude or share the same results.

In my literature review, I will use the method known as Systematic Literature Review (SLR) to help answer my research questions (Kitchenham et al., 2009). The method consists of eight steps to define my research and find corresponding relevant data through systematic research of current literature on the subject.

3.2 Problem Formulation

Through the usage of SLR, I will further investigate and aim to answer my thesis research questions:

- Are the young or old generation more susceptible to phishing frauds?
- How do they identify a phishing email from a legitimate one?
- Are there any differences in their verification skills?

By looking through existing literature, I can begin to understand what types of studies have already been conducted and build upon my own study through their experiences. By limiting my research questions to phishing susceptibility and age, the review process becomes much more manageable as the topic of phishing is already covered quite extensively in many areas.

3.3 Protocol Development

By developing a protocol for me as a reviewer, I will set up criteria for inclusion and exclusion so that my literature search stays cohesive throughout the whole process (Shamseer et al., 2015).

- Rationale & Objective

Through the tool PICO, I will describe my qualitative and quantitative research goals.

Table 1 PICO table

P	I	C	O
Population/Problem	Intervention/Exposure	Comparison	Outcome
Young vs old, Increased susceptibility with age and their rationale	Observe their identifying and awareness skills	Compared with baseless recommendation	Decrease the amount of successful attacks, by understanding their skill level

- Inclusion & Exclusion

Limiting the raw amount of published articles will help narrow down my search to match exactly what I am looking for. My criteria were research included: phishing, phishing & susceptibility, phishing & age, and phishing & recommendations.

By starting broad with phishing in general I aimed to gain a better general understanding, before narrowing it down to my desired topics within phishing.

- Search

Most of my search will be on online databases through the usage of Google.Scholar and the tool SCOPUS.

3.4 Literature Search

In my literature search I mostly used two of the methods suggested by Petticrew and Roberts in the *Systematic Reviews in the Social Sciences: A Practical Guide*, database search and backward search. Primarily I used Google Scholar as my chosen database collection of literature as well as SCOPUS. Using more than one type of database can also be beneficial in my search as some articles may have only been published in one of them.

Backward and forward search proved also to be quite useful as some publishers had several relevant articles published prior to the one I originally found. This creates a snowball effect throughout my search, where additional research is found for every article that I read through. Google Scholar also allows the usage of advanced search which further narrows the number of articles down to exactly match

my pre-established criteria, only displaying articles with exact phrases, authors, keywords and exclude certain keywords. Such keywords were phishing, phishing detection, phishing recommendations, phishing+age, phishing+age+susceptibility.

3.5 Screening

The amount of literature remained rather large even after applying several criteria and would therefore need further screening to ensure only the most relevant literature is included. The screening process aims to exclude any literature that does not have any relation to my research question by applying a few criteria. The following criteria were made:

- **Source:** All the information should be from scientific articles in journals who are seen as a lot more trustworthy unlike websites with blog posts or Wikipedia who are prone to bias and incorrect information.
- **Setting:** The literature should be in the Information Technology & Security setting and conducted similar studies regarding phishing prevention and susceptibility.
- **Content:** The content of the chosen literature should be closely related to my own research questions and include new information on the topic. This is to exclude very similar articles.
- **Language:** The language in the chosen literature must be in either English or Norwegian.

3.6 Quality Appraisal

This step builds further upon the quality of the chosen literature. In order to validate the literature in my study, an appraisal of their characteristics is necessary to examine their trustworthiness and relevance to my own research questions. I did this by validating the individual articles towards more criteria:

Relevance: Similar study type with similar goals to my own (PICO analysis)

Results: Were their results statistically significant?

Applicable to my own study: Does the literature contribute an answer to my own research? Do they have different study demographics or similar?

Quality: To check for the quality of the literature I followed the proposed method in *Evidence-based practice workbook: Bridging the gap between health care research and practice*, known as RAMMbo (Salisbury, Glasziou & Del Marc, 2007).

- **Recruitment:** who did they enlist in the study and do they represent a population at large.
- **Allocation:** Study groups should be comparable
- **Maintenance:** how was the study group treated during the data gathering process.
- **Measurement, Blinding & Objective:** Were the measurements done objectively and without bias?

3.7 Data Extraction

Data from all the relevant literature remaining after several screening and appraisal processes were then extracted. The findings from the literature review were presented in chapter 2 and below.

3.8 Comparative Case Study

To accurately study my research questions, I developed a case study as it was appropriate for my “why” and “how” investigative approach. As my goal of the study is to understand the actions taken by the individuals and shed light on the decisions they take, why they did it and what was the result, a case study as research method is applicable, as suggested by Yin (2019). I also wanted to study the *real-life phenomenon* between human behaviour and their ability to perceive fraudulent emails, which is closely related to social science where case studies are popularly used.

Case studies are separated into three different types and while all of them have similarities, choosing the one most suited to my study will help data collection and synthesis substantially. **Explanatory** research leaves little to interpretation as it aims to explain a question, such as studies heavily focused on numbers ($1+1=2$) which is not up for debate (Universalclass, 2022). Hence why it would not be applicable to my study, as human behaviour is always affected by variables. **Descriptive** research aims to reveal connections within the theoretical constructs, which is why it is often referred to as an *intensive* case study (Mills, Durepos & Wiebe, 2010).

All the different types of case studies however can easily overlap, as the goal remains relatively the same across all studies, such as giving a coherent display of a phenomena or development on a pre-established concept. For that reason, **Exploratory** research is a more appropriate study design. It is a method designed to help determine which events are the causes for the outcome I am investigating, being increased phishing susceptibility with age. The objective is to get a deeper

understanding about phishing susceptibility and if age has any significance in the matter.

3.8.1 Case study pros & cons

Following the path of exploratory case study, my opinions drive the study forward as the goal of my study is to seek out information related to my research questions (Gaille, 2018). Hence, having predetermined hypotheses will help reveal data as they are generated.

As the case study researcher and participants are working so closely together, both parties have something to gain from the relationship. The participants get to test their own knowledge on the given subject as well as gain further knowledge based on the outcome of the study. The problem that I am investigating is also very relevant in the current cyber threats, and recommendations to ward off phishing attacks will also be expanded upon in the discussion section. Given the current pandemic situation, case study can also be done very effectively remotely as meeting people physically became increasingly more difficult during this time period. All the interviews were carried out over phone and Zoom calls.

One of the major downsides with a qualitative case study is that there are no clear rules and guides on how to correctly synthesise and analyse the data. Contrary to quantitative studies where specific formulas are followed to generate your R and T-values. Therefore, the qualitative researcher must be a lot more “creative” when analysing the raw data to accurately reveal the themes within the dataset. The same process is also very time-consuming. Sifting through the transcribed interviews is a tedious process and the accuracy of the participants' answers must be verified as they can partially impact the study by withholding or giving incomplete answers during the interview process.

3.9 Case selection and definition

The cases represent each of the demographic groups that I wanted to investigate, which were young adults and elderly people. The reason I chose these two groups was because I wanted to investigate whether there are clear distinctions in their perceived susceptibility. I also wanted to clear up the misconception about elderly people being naturally targeted because of their unfamiliarity with technology, and rather look at what specifically they do different regarding phishing email. Lastly, by comparing them to the “tech-savvy” generation, I can get tangible results and uncover their differences.

Elderly:

Going by official definitions provided by the United Nations (UN Refugee Agency, 2022) and multiple law definitions (Law Insider, 2022), humans in the range 60-65 years are considered to be of old age and soon to reach retirement age. I believe aiming for this range would be most beneficial regarding availability of interview subjects especially in covid times where visitors are not so easily accepted into caring homes. The participants also vary between having some prior knowledge about phishing attacks, which can affect the results from the interview. Most likely will the participants that have fallen victim in the past or those who are educated on the subject can give deeper explanation of how they identify phishing emails.

Young adults:

The young adults that I interviewed were in the age range from 18-27 and mostly served as a counterpart to the elderly to see if there were any significant differences in how they perceive phishing emails.

My hypothesis is that these young adults might be slightly more familiar with technology than the older people as many of them are IT-graduates and spend many hours daily on the internet.

Table 2 Case descriptions

Case	Size	Occupation	Location
Young adults 18-26	9	Students	Norway
Elderly 60-80	8	Retired, some working	Norway

3.10 Data collection

Data collection is often done through either qualitative interviews or quantitative surveys/questionnaires. Initially my plan was to do both at the start, however an unmotivated questionnaire was not warranted, and it should rather seek to quantify the results that were gathered in the interviews. Hence why my main source of data will be through semi-structured interviews as rich text would provide a much more in-depth insight into their rationale rather than through quantitative means.

As for my sampling strategy, I went for a non-randomized approach (Crossley, 2021). The recruitment process was mainly done through my own network of friends, colleagues, and students. Mainly because some of the questions might

make random interview subjects withheld information that they find embarrassing such as “have you been phished before?” whereas people that trust and know me will naturally feel more comfortable with sharing such information. Ease of access was also a major factor as time-constraints would make it hard to go for a probability sampling strategy with random people.

3.11 Methodology Limitations

When it comes to my method of collecting data and the analysis process, there are some shortcomings. The most obvious is the time constraint and especially when working alone everything takes a little while longer. This also ties into my interview process where about 60% of the participants were recruited through my own network and the rest were distant “friends of friends”. Therefore, my participants cannot be truly representative as some selection bias has gone into the recruitment process. However, as discussed in 3.10 this was a good thing.

3.12 Ethics

To begin my data collection, there were ethical aspects that had to be done such as getting approval from the NSD. This was to ensure that the data collection process followed a certain approved standard of storage and deletion throughout the whole thesis. Participants had to be informed what they were partaking in and their rights concerning data retention, collection, and deletion. However, for my thesis the only PII data that I gathered was their age, education, and voice, which cannot be directly linked to anyone as their names were never disclosed in the interview process.

All the interviews were stored on an offline phone without a SIM-card provided by the institution. This was done to ensure that only myself had initial access to the recordings and they remained secure until transcription and deletion.

3.13 COVID Complications

The interview process also got slightly more complicated due to different regulations arising during the pandemic. Especially interviewing older people got significantly harder as visiting them would be a lot easier than relying on that everyone had a pc and knew how to join and set up a Microsoft Teams meeting. Therefore, most of the interviews had to be carried out over the phone which worked out fine.

3.14 Interview Process

In the preliminary interview process, questions regarding the participants relation to phishing and some of their descriptive data was asked. The descriptive data consisted of their current age, to group them into one of the two study groups, and their level of education to see if there was any correlation between phishing knowledge and education.

The data that I gathered are somewhat prone to changing over time like opinions and experiences, which would be considered a longitudinal methodology, however, what I was interested in was their current knowledge and experiences and therefore I adopted a cross-sectional method. This means that all the data were gathered at one point in time. All of my interviews were carried out in the period of March-April 2022.

3.14.1 Phishing Detection and Process

During the interviews I also ran a phishing assessment process which consisted of ten images of real-life phishing examples, where the participants were asked to explain their thought process on how they identify the email to be legitimate and their conclusion if the mail was legitimate or phishing. This was done to gain further understanding of the different demographics analysis of the phishing examples and I could observe in real-time how quickly they could discern a phishing email from a legitimate one.

3.14.2 Phishing Assessment

The examples used in the phishing assessment were chosen with a couple of criteria. The criteria were based upon the attack trends discussed earlier as well as the most common types of phishing techniques threat actors use.

A) Contextual relevance:

To see if the participants were following the emergence of post fraud emails, one of the examples was this:

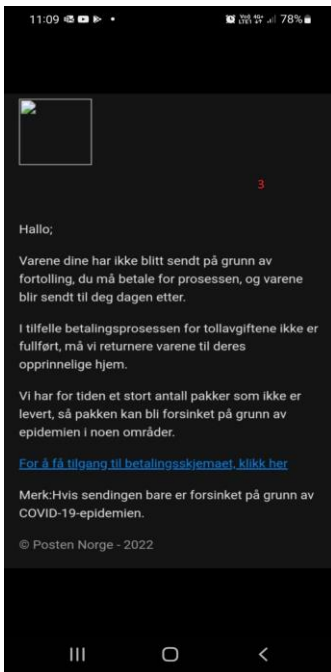


Figure 4 Phishing example: Contextual relevance

This example highlights how they have adapted to the increase in shipment since the pandemic and trying to capitalise on gullible individuals who does not know any better.

B) Unreasonable request:

The second most common tactic is to provoke an action from the receivers. Either by scaring them or by offering a deal which is too good to be true. The example below is riddled with errors such as spelling errors, senderID completely wrong and lastly asking for your banking credentials. Official banks would never ask for this through an unsuspecting email, yet people still fall for it.

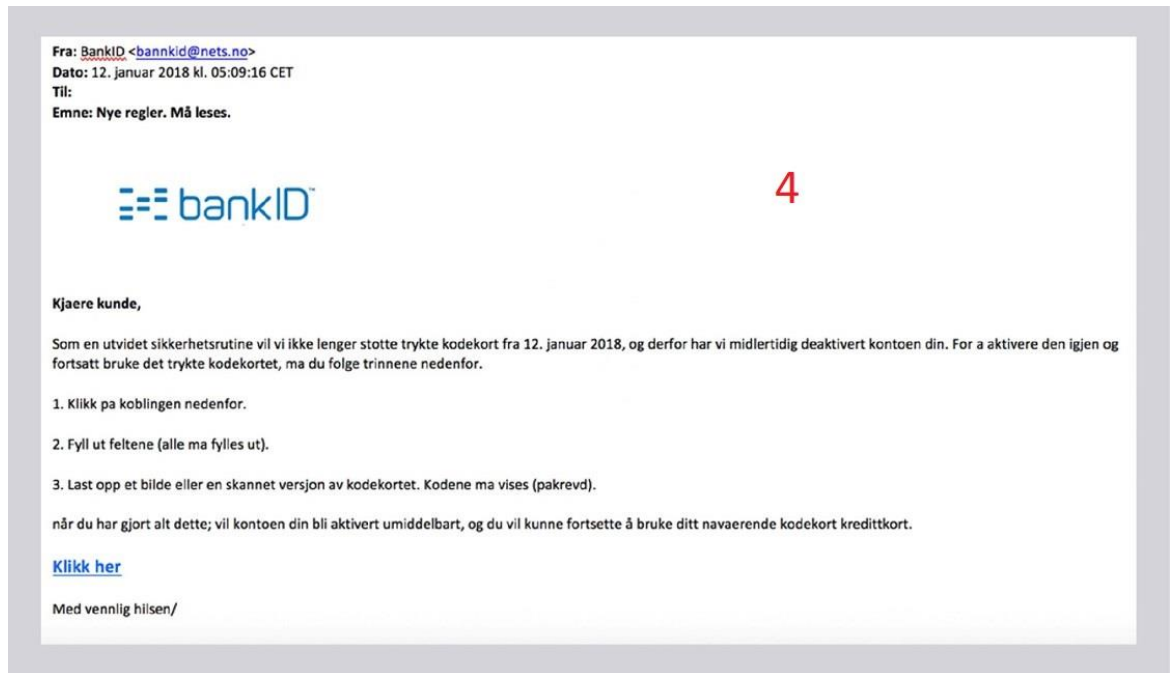


Figure 5 Phishing example: Unreasonable Request

C) Grey area:

Lastly, I wanted to see how they responded when represented with a more ambiguous example, which could be difficult to discern between phishing or legitimate.



Figure 6 Phishing example: Grey area

This email can be easily initially written off as phishing as the senderID seems a little fishy coming from Netflix, as well as attempting to provoke a reaction from the receiver. Therefore, I included this type of mail to observe what the participants would do when uncertain if they could trust the sender or not. What I was looking for was, would they seek out the information on their own and disregard the email entirely or would they look at earlier received emails from Netflix to see if they have mails from the corresponding senderID. The rest of the emails used in the phishing assessment process can be located in the appendix.

3.15 Qualitative Analysis Process

Analysing qualitative data can be done in several ways and mine will be done thematically (Crossley, 2021). This means that excerpts from the interviews will be presented in the findings chapter, and I will be trying to find the common and the uncommon themes that were gathered in the interviews. By finding the concepts that are repeatedly brought up, the dataset can be more easily read. I will therefore focus on my own research questions when doing thematic analysis, as not all data from the data set can be placed into topics. Subjective data such as opinions and experiences can be more easily digested when placed into categories. Approaching the data set can be done in different ways such as inductive, where the researcher has no preconception of what themes that might emerge. In my case however, deductive approach is a way better fit as I already have a set of themes that will most likely be present within the data which also ties back to findings from my literature review.

The themes that I will be analysing are

- Education
- Prior phishing
- Age and prior phishing
- Phishing detection process
- Phishing attack trends
- Detection accuracy

4 FINDINGS

To present the findings from the qualitative interview process, I transcribed the interviews and conducted the thematic analysis of the data collected. The different themes uncovered from that analysis will be presented in their respective case study.

4.1 Case: Young

The initial findings that will be presented here, are the themes uncovered by analysing the data provided by the young participants. Such as their descriptive characteristics, their thought process and how accurate their phishing assessment process were.

4.1.1 *Descriptive Themes Uncovered*

The younger participants spent on average eleven hours daily on the internet, and some of them reported to spend up to fourteen hours. Education varied quite heavily between the two cases. Eight out of the ten young participants had either acquired a bachelor's or master's degree.

4.1.2 *Detection Analysis*

The biggest part of the interview was spent on understanding the participants' detection skills when presented with phishing emails. Two major factors were present when they were tasked with verifying email examples: *message content* and *message context*. Message content refers to everything included in the actual email such as senderID, content, spelling mistakes and hyperlinks. While message context refers to everything “outside” of the email such as knowledge on current cyber threat trends, situational and logical awareness.

4.1.3 Young Participants Message Content

All of the young participants gave detailed descriptions when uncovering the many mistakes within a phishing email. Using Figure 5 as an example, all of the participants instantly noticed that this was indeed a phishing email. The senderID being completely wrong in relation to the company it is posing as, bannkID != bankID. Even though that was already enough to expose the sender, they also noticed the many spelling errors which often occur when the threat actor has glossed over the usage of ÆØÅ characters when attempting to phish Norwegian recipients. Lastly, they took notice of the unreasonable request within the email, which was sending a picture of your credit card, something they would never ask of their customers. Their detection process can therefore be represented like this:



Figure 7 Young participants thought process, Message content

This procedure was the most common thought process the participants went through when presented with the phishing examples. This way of thinking will in almost all cases be enough to detect whether the email is fraudulent or legitimate. Nevertheless, only scrutinising the message content might not be enough to take notice of the more well-crafted phishing emails.

4.1.4 Young Participants Message Context

The young participants were also very good at applying contextual variables to the phishing assessment. Almost all of them were quick to deduce that the account creation examples were legit if they were initially requested by the user. It can be referred to as *expected response*, which they applied to the examples where it would make sense that such a request was sent to their inbox. The same logic was also applied on the examples where *unexpected responses* made sense, such as receiving an email regarding shipping costs when not expecting any products. They were also aware of current trends within the phishing space, such as the shipping example where many of them had received themselves recently. Lastly, the majority of the participants also came to the conclusion that instead of clicking any links they would rather search up the official website and not take any risks if there was a shred of doubt.

Participant nr 5 taken from appendix 2 summarises the process clearly with “*If I am expecting an email I would have considered it, but I am very sceptical so I would not have pressed the link but rather logged onto their website*”.

Their contextual thought process can be summarised with this module.

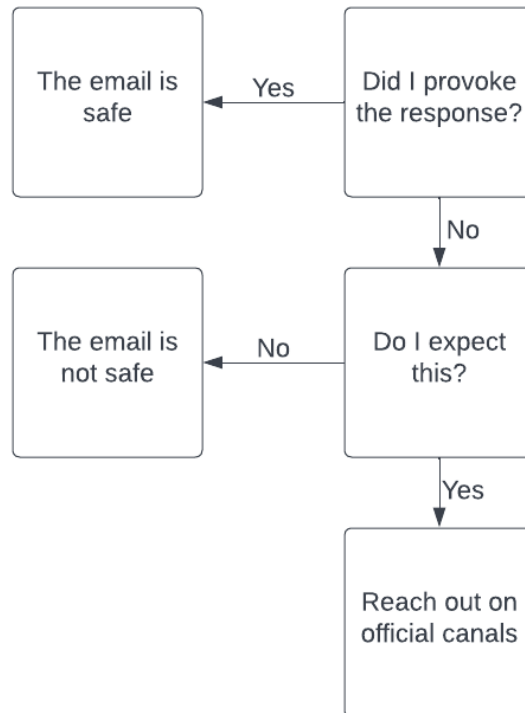


Figure 8 Young participants thought process, Message context

By following the three steps, the participants could safely assume that they made an informed and correct decision on whether to trust it or not.

4.1.5 Accuracy Young

The accuracy when judging the phishing examples varied quite a lot between the young and old. In the figure below we can observe the accuracy among the younger participants.

Table 3 Phishing assessment accuracy young participants (P)

	P1	P2	P3	P4	P5	P6	P7	P8	P9
Phishing example 1	Correct	Wrong	Wrong	Correct	Correct	Correct	Wrong	Correct	Correct
Phishing example 2	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct
Phishing example 3	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct
Phishing example 4	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct
Phishing example 5	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct
Phishing example 6	Correct	Correct	Wrong	Correct	Correct	Correct	Correct	Correct	Correct
Phishing example 7	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct
Phishing example 8	Correct	Wrong	Wrong	Correct	Correct	Wrong	Correct	Wrong	Correct
Phishing example 9	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct
Phishing example 10	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct

In the left most column are the examples listed, green meaning they were legit while the red ones were real phishing examples. We can instantly note that none of them branded a phishing email as a legit one. While a few of them did report legit ones as phishing, the majority correctly identified most of the examples. Most of the falsely reported examples was the same image, meaning that it might have been particularly hard to identify compared to the other ones. None of them wrongfully identified a phishing email which obviously is the most important factor to consider.

4.2 Case: Elderly

The data collected from the elderly participants showed clear differences when compared to their counterparts.

4.2.1 Descriptive Themes Uncovered

In clear contrast to the younger participants were including work hours, ten hours was the maximum amount, while on average they spent three hours on the internet daily. While few of the older participants had any formal education after finishing the normal mandatory requirements in Norway being Videregående skole that you

finish at the age of 18/19. Most of the older participants were currently working IT jobs or at least interacting with information-technology on a daily basis.

4.2.2 Elderly Participants Message Content

The older participants were much quicker to judge the examples and they all showed truly little trust towards any email who inhabited a link. One of the elderlies stated the following when questioned about how they spot phishing attempts, “*I see it instantly, credit, and free money or anything of that kind I just delete at once, and I never click links as it frightens me*”. Therefore, very few of them concluded that; if they provoked the email, the link could be trusted. This might cause some implications for them which will be talked more about in the discussion. All things considered they exhibited more or less the same reasoning when looking through the message content, such as spelling errors, the message itself and the senders’ ID.

4.2.3 Elderly Participants Message Context

All of the older participants were quite aware of the current threats that take place over email and SMS. None of them had any prior incidents with phishing which signifies that they are good at applying situational context to the emails they receive to deduce whether it is safe or not. Many of them however were overly cautious during the phishing assessment as they gave a lot more false positives compared to the younger participants, meaning they were sceptical to many of the legit emails as well.

4.2.4 Accuracy Elderly

In the table below (4) we can observe the accuracy portrayed by the older participants. As discussed, they were a lot more sceptical which consequently made them report many more false positives. We can also notice a trend within the table as to which of the examples they struggled with. In example 1 and 8, six out of eight participants mis flagged it as phishing. Whereas in example 6, seven reported it as phishing. Lastly example 9 also showed clear signs of distrust even though it was a legitimate email. We can also see that there was a singular phishing email that went undetected by one of the participants which could result in a successful attack.

Table 4 Phishing assessment accuracy elderly participants

	P1	P2	P3	P4	P5	P6	P7	P8
Phishing example 1	Wrong	Wrong	Correct	Wrong	Correct	Wrong	Wrong	Wrong
Phishing example 2	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct
Phishing example 3	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct
Phishing example 4	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Wrong
Phishing example 5	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct
Phishing example 6	Wrong	Wrong	Wrong	Wrong	Wrong	Wrong	Correct	Wrong
Phishing example 7	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct
Phishing example 8	Wrong	Wrong	Wrong	Wrong	Correct	Wrong	Correct	Wrong
Phishing example 9	Wrong	Wrong	Wrong	Correct	Correct	Correct	Wrong	Wrong
Phishing example 10	Correct	Correct	Correct	Correct	Correct	Correct	Correct	Correct

4.3 Secondary findings

In addition to the phishing assessment, these were the secondary themes that the participants portrayed.

4.3.1 Attack Trends

Attack trends were discussed during the interviews and if the participants were subjected to any phishing attack recently. A vast majority of the participants had received several phishing emails and SMS and particularly among all of them was the typical toll and shipping fraud that is trending in the current cyber threat space.

4.3.2 Phishing Victims

When asked about if any of them had been a victim of a successful phishing attack, none of the older generation said yes while several of the younger ones had been successfully phished. All of the victims reported that they were tricked at a young age through the gaming platform Steam. The attack was also similar among all the cases, where a fake version of their website was used to harvest login credentials.

4.3.3 Training

Very few among the participants had received official training to improve their resilience towards phishing attacks. However, many mentioned that they regularly at least received some rules to follow when dealing with suspicious emails. Moreover, all of the working participants mentioned that their work-mail remained untainted with spam emails and stated that they had good spam filters. As many of them also worked IT-jobs, to have a basic knowledge of safety and how to manage such threats was expected by all of the co-workers. One of the participants said the following about phishing training, “*No actually nothing, where I work we only got warnings every months, but when you work in IT it is kinda expected that you have basic knowledge about security*”, which encapsulates what the majority also said.

4.3.4 Cognizant Bias

Many of the participants got overly cautious when presented with the phishing examples as they did not want to appear oblivious and take any risks. This also came up during the literature review, that participants who knew they were under the looking glass got increasingly suspicious and looked for phishing signs even though the email looked completely normal. However, their thought process was what I was most interested in, but it was affected second handily nonetheless.

4.3.5 Outside Factors

All of the participants were asked if they had any stress related issues at their workplace, such as working in a high intensity environment. A collective no was said among all of them, meaning they all did their due diligence when reading emails.

5 DISCUSSION

The results from the qualitative interviews were quite interesting albeit expected results. The number of hours the separate groups spent on the internet; I would say worked in both their favours. The young people spent on average spent more time, meaning they were to a much higher degree exposed to digital threats. Which will not necessarily put them at greater risk but rather more resilient and knowledgeable over time on the issue. The young people were also the only group that had several prior incidents, which correlates with what was mentioned in the literature review were younger people had a tendency to be more reckless due to the lack of experience and threat awareness (Sheng et al., 2010). Although, it is possible that more of the participants had been a victim without realising it. While the elderly participants who hardly spent any time on the internet besides a couple of hours, would naturally be a lot less exposed to phishing threats. However, during the phishing test they showed a much greater distrust towards all the examples. While initially being cautious is a good thing, overly cautious can have some implications down the line. Most notably in a working environment, distrusting all the incoming emails will drastically slow down the internal processes making everything more time-consuming.

When it comes to their different rationales, the younger participants showed a much greater acceptance towards the examples regarding account creation and verification. The logical reason being that they have seen this type of email hundreds of times before during their many hours on the internet when creating gaming and social media accounts. Whereas the elderly participants showed extraordinarily little trust towards the same examples, which would make sense as they mentioned they only used internet for reading news or similar activities.

The accuracy among the groups also varied greatly. The elderly participants did flag around 50% correct on the test. That being said, being overly cautious meant they would naturally get that score as five out of the ten examples were phishing. This is a direct correlation to the study mentioned in the literature review by Grilli et al., (2021) who reported that the older people were worse at identifying legitimate emails apart from the phishing ones due to increased suspiciousness during the test. Relative to the younger people who were much more open minded to the same examples, reporting a substantial higher accuracy when discerning the emails.

The reason this research matters is that people will always be seen as a weak link and entry point into digital systems. Therefore, it is in everyone's best interest that we are aware of current threats and how to appropriately respond to them. As

mentioned in the literature review, by applying stage theory we can provide much more tailored recommendations based on their previous knowledge on the subject.

The majority of the young participants showed great reasoning during the phishing assessment, meaning they are above basic understanding of the threat. Which is why their recommendations should be focused around how to take their understanding to the next level, such as keeping up with current threat trends. Learning more about new emerging trends will be much more beneficial for the already tech-savvy individuals.

In the tables below, are the most significant differences between the two study groups. In table 5 Message content, three main aspects from each of the groups were present in most of the interviews. The young people tended to be much more open minded and deductive, which can be a result of having more experience on the subject. They were also a lot better at following through on their thought process when presented with each of the examples. Meaning that they would always look at the senderID, spelling errors, the content itself and if they provoke the email themselves. Compared to the elderly participants who were much quicker to judge instantly when they saw a link.

Table 5 Message content comparison

Message content	
Young	Elderly
More open minded	Quicker to judge
Applied the tree deductive steps more often	Discarded emails with links
Deductive	Suspicious

As for the message context, the young participants were quite aware of the current threats and would often come to the correct conclusion that they might as well reach out on the official websites instead of taking any risks. The elderly however, had a more practical approach, and applied situational context to the phishing examples. Most of them also explained that spam filters played a big part to maintain distance from the threat altogether.

Table 6 Message context comparison

Message context	
Young	Elderly
Aware of current trends	Pragmatic/Practical
More familiar with account creation	Situational awareness
Reach out on official channels	Rely on spam filters

The findings from this study can be beneficial for people that provide IT recommendations such as government officials, or security experts tasked with training their fellow employees. The study shows that there are clear differences in how we deal with phishing, and it comes down to how well we can apply contextual awareness as well as being familiar with the most common giveaways present in phishing attacks.

5.1 Limitations

The study examined individuals in Norway and therefore cannot be taken as a globally accepted result. My targeted demographic are also students with higher education (university level), hence, they do not represent as generic young adults as education level can potentially have a significant impact on the results. The study also has cognizant observation bias, meaning that the participants are aware of the task beforehand as opposed to when an attack happens in real life where they might be affected by more variables such as stress and focus. Other studies have shown that biases are present when the participants are informed versus uninformed (Hakim et al., 2019).

5.2 Future research

In light of my own research, I have come across several aspects of the study which could have been done differently that future researchers definitely can benefit from. The first being the phishing detection process. As explained, the participants quickly turned into detectives rather than approaching the examples in a more natural way. Hence why incorporating some biometric assisted tools for eye tracking would be interesting. This can uncover what they are really looking at when opening an email, as most of us execute the verification process subconsciously we could get an even more exact answer to my research question. Secondly, I would have engaged with a larger number of participants to see if the results that I got were truly quantifiable. In my results there are clear differences already between the groups, however they were not chosen at random apart from a few of the elders, and many of them shared the same education and hobbies. Thus, it could be interesting to see if the same results would be replicated in a much larger scale with greater variance among the participants. Different demographics could also be studied such as even younger individuals. As technology becomes increasingly more accessible, children are already surfing the internet independently at the age of eight (Microsoft, 2013). Which would put them at a notable risk without proper protection and boundaries set by their parents.

6 CONCLUSION

The aim of the study was to inspect and compare how we deal with phishing threats differently with age. The results I gathered was quite comparable to the study done by Grilli et al., (2021), which emphasizes the necessity for increasing cyber threat awareness among all age groups. As for the differences between their phishing detection processes, both study groups conveyed equivalent answers, although the phishing assessment process showed a clear disparity between the two study groups. Namely the distrust the elderly showed towards emails with links. From this it can be assumed that most people have some knowledge on what to look for, but when actively engaged in a phishing scenario more external factors prevent them from making an informed decision. Thus, future research paired with eye tracking technology can determine what exactly happens in that scenario.

Although there has been a rapid increase in phishing threats over the last years, and since the technology still heavily relies on human interaction, it is my belief that with training and proper recommendation based on the users pre-existing knowledge the threat can be greatly mitigated. The case study done in this report also showcases that both study groups share similar level of susceptibility, which signifies that the individual's comprehension of the threat is a greater factor than their age.

7 REFERENCES

- Aberdeen, T. (2013). Yin, RK (2009). Case study research: Design and methods. Thousand Oaks, CA: Sage. *The Canadian Journal of Action Research*, 14(1), 69-71.
- Brecht, D. (2019). Phishing: Who Is Being Targeted By Phishers? Retrieved from: <https://resources.infosecinstitute.com/topic/who-is-being-targeted-by-phishers/>
- Crossley, J. (2021). How to Write the Methodology Chapter. Retrieved from: <https://gradcoach.com/how-to-write-the-methodology-chapter/>
- Crossley, J. (2021). What Exactly is Thematic Analysis? Retrieved from: <https://gradcoach.com/what-is-thematic-analysis/>
- David Warburton. (2020). Phishing Attacks Soar 220% During COVID-19 Peak as Cybercriminal Opportunism Intensifies. Retrieved from: <https://www.f5.com/company/news/features/phishing-attacks-soar-220--during-covid-19-peak-as-cybercriminal>
- De Haan, W., & Vos, J. (2003). A crying shame: The over-rationalized conception of man in the rational choice perspective. *Theoretical Criminology*, 7(1), 29-54.
- Fritz, C. E., & Mathewson, J. H. (1957). Convergent behavior: A disaster control problem. *Special report for the committee on Disaster Studies. Disaster Study*, 9, 1-102.
- Gaille, B. (2018, July 11). 12 Case Study Method Advantages and Disadvantages. Retrieved from: <https://brandongaille.com/12-case-study-method-advantages-and-disadvantages/>

- Ghafir, I., Prenosil, V., Hammoudeh, M., Aparicio-Navarro, F. J., Rabie, K., & Jabban, A. (2018, June). Disguised executable files in spear-phishing emails: Detecting the point of entry in advanced persistent threat. In *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems* (pp. 1-5).
- Greenert, J. (2013). Kill Chain Approach. Chief of Naval Operations. <https://web.archive.org/web/20130613233413/http://cno.navy.mil/2013/04/23/kill-chain-approach-4/>
- Grilli, M. D., McVeigh, K. S., Hakim, Z. M., Wank, A. A., Getz, S. J., Levin, B. E., Ebner, N. C., & Wilson, R. C. (2021). Is This Phishing? Older Age Is Associated With Greater Difficulty Discriminating Between Safe and Malicious Emails. *The journals of gerontology. Series B, Psychological sciences and social sciences*, 76(9), 1711–1715. <https://doi.org/10.1093/geronb/gbaa228>
- Hakim, Z. M., Ebner, N. C., Oliveira, D., Getz, S. J., Levin, B., Lin, T., ... & Wilson, R. (2019). Evaluating the cognitive mechanisms of phishing detection with PEST, an ecologically valid lab-based measure of phishing susceptibility.
- Hassandoust, F., Singh, H., & Williams, J. (2019). How contextualisation affects the vulnerability of individuals to phishing attempts.
- Hutchins, E. M., Cloppert, M. J., Amin, R. M. (2011). “Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.” <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>
- Johnson, J. (2021). Number of global phishing sites as of Q1 2021. Retrieved from: <https://www.statista.com/statistics/266155/number-of-phishing-domain-names-worldwide/>
- Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering—a systematic literature review. *Information and software technology*, 51(1), 7-15.

- Law Insider. Elderly person definition. Retrieved from:
<https://www.lawinsider.com/dictionary/elderly-person>
- Lazic, M. (2021). 39 Worrying Cyber Crime Statistics[Updated for 2022]. Retrieved from: <https://legaljobs.io/blog/cyber-crime-statistics/>
- Lockheed, M. (2015). “Gaining the advantage” Applying Cyber Kill Chain
https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf
- Microsoft Corporate Blogs. (2013). How old is too young to go online? Retrieved from: <https://blogs.microsoft.com/on-the-issues/2013/10/14/how-old-is-too-young-to-go-online/>
- Mills, A. J., Durepos, G., & Wiebe, E. (2010). *Encyclopedia of case study research* (Vols. 1-0). Thousand Oaks, CA: SAGE Publications, Inc. doi: 10.4135/9781412957397
- Pattinson, M. R., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. A. (2011). Managing Phishing Emails: A Scenario-Based Experiment. In *HAlSA* (pp. 74-85).
- Salisbury, J., Glasziou, P., & Del Mar, C. (2007). Evidence-based practice workbook: Bridging the gap between health care research and practice (2nd ed.). Oxford: Blackwell/BMJ Books
- Sarno, D. M., Lewis, J. E., Bohil, C. J., & Neider, M. B. (2020). Which Phish Is on the Hook? Phishing Vulnerability for Older Versus Younger Adults. *Human factors*, 62(5), 704–717.
<https://doi.org/10.1177/0018720819855570>
- Shamseer, L., Moher, D., Clarke, M., Gherzi, D., Liberati, A., Petticrew, M., ... & Stewart, L. A. (2015). Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015: elaboration and explanation. *Bmj*, 349.

- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '10). Association for Computing Machinery, New York, NY, USA, 373–382. <https://doi.org/10.1145/1753326.1753383>
- Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. oup usa.
- Tambe Ebot, A. C. (2017). Explaining two forms of internet crime from two perspectives: toward stage theories for phishing and internet scamming. *Jyväskylä studies in computing*, (259).
- The UN Refugee Agency. (2022). Older persons. Retrieved from: <https://emergency.unhcr.org/entry/43935/older-persons>
- Torkura, K. A., Sukmana, M. I., Meinig, M., Kayem, A. V., Cheng, F., Graupner, H., & Meinel, C. (2018, May). Securing cloud storage brokerage systems through threat models. In *2018 IEEE 32nd international conference on advanced information networking and applications (AINA)* (pp. 759-768). IEEE.
- Universal Class. (2022). Understanding the Different Types of Case Studies. Retrieved from: <https://www.universalclass.com/articles/business/case-studies-types.html>
- Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vish-ing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, 5(4), 297-307.

7.1 Appendix 1: Interview guide

- How old are you?
- What form of education do you have?
 - o Highschool
 - o University
- Approximately how much time do you spend on the internet daily?
- Do you know what a phishing attack is?
 - o If no, explanation will be given.
- Do you often receive phishing emails?
 - o Personal or work mail?
- Have you been a victim of a phishing attack?
 - o What type?
- What signs do you look for when identifying a fraudulent/phishing email?
- Do you often answer/open emails hastily because of stress level at your work-place or home?
- Have you received any training in regards to phishing?

7.2 Appendix 2: Phishing assessment

Endre passord

1

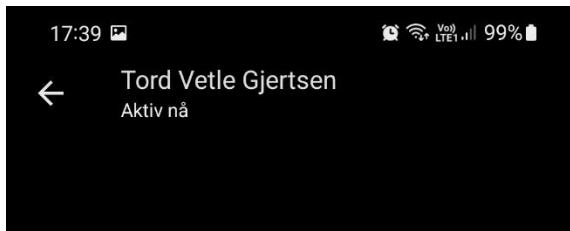


ice@ice.no <ice@ice.no>

16.10.2021 15:02

Til: frankthorsenespen@hotmail.com

Her kan du endre passordet ditt for Min Side: [Endre passord](#)



2

Dear customer,

The security of your MetaMask is a top priority for us and we are happy to work together to protect your account.

We need your help resolving a problem with your wallet. To protect your crypto, log in to your MetaMask with the personal link below and complete the steps to confirm your identity and recent wallet activity.

Your wallet has been restricted temporarily

In order to remove your restriction, we must ensure that your account is validated by its rightful owner. Please click below to verify your MetaMask wallet.

[Verify your wallet](#)

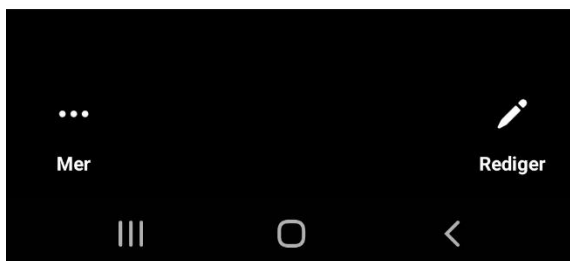
In case of inactivity we will suspend your account on Sunday, February 13, 2022. We're sorry for any inconvenience we cause with this, but please keep in mind that our intention is to keep our customers safe and happy.

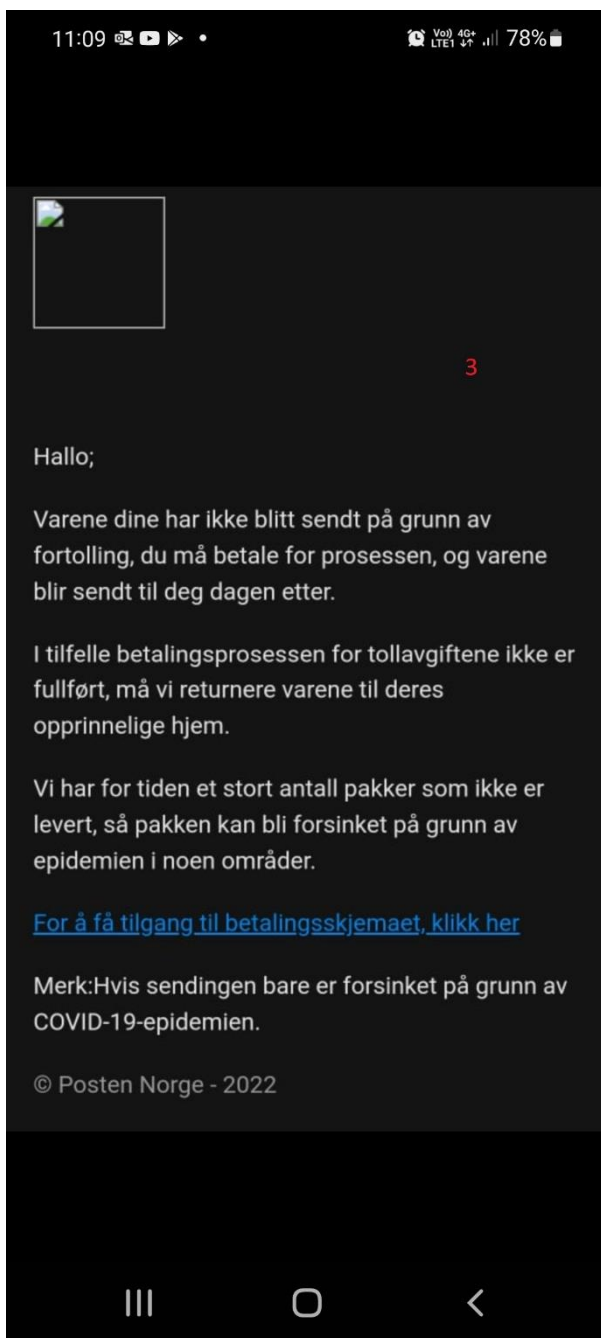
Thank you for your understanding.

<https://metamask.io/accounts/wallet-validation=585939438456c45e305ca87a65ab9107a1eca7e00>

For further assistance with this issue, please contact our support team [here](#)

[Metamask](#)





Fra: [BankID <bankid@nets.no>](mailto:bankid@nets.no)
 Dato: 12. januar 2018 kl. 05:09:16 CET
 Til:
 Emne: Nye regler. Må leses.



4

Kjære kunde,

Som en utvidet sikkerhetsrutine vil vi ikke lenger støtte trykte kodekort fra 12. januar 2018, og derfor har vi midlertidig deaktivert kontoen din. For å aktivere den igjen og fortsatt bruke det trykte kodekortet, må du følge trinnene nedenfor.

1. Klikk på koblingen nedenfor.
2. Fyll ut feltene (alle må fylles ut).
3. Last opp et bilde eller en skannet versjon av kodekortet. Kodene må vises (pakrevd).

når du har gjort alt dette; vil kontoen din bli aktivert umiddelbart, og du vil kunne fortsette å bruke ditt navaerende kodekort kredittkort.

[Klikk her](#)

Med vennlig hilsen/



Mrs. bill Chantal <etimbukudo345@gmail.com>

16.21

5

DEAR FRIEND

You have been compensated with the sum of \$5.4 million dollars in this united nation,The payment will be Issue into ATM visa card and send to you from the bank,We need your Address, Passport and your WhatsApp Number.

Thanks

Mrs.Bill Chantal



Kattis <bounces@kattis.com>

07.05.2021 18.38



6

Til: Espen Thorsen Frank

Dear Espen Thorsen Frank

There has been a request to register the address frankthorsenespen@hotmail.com with the user espen-thorsen-frank on the Kattis judge. In order to complete the address registration you need to go to the following link in a web browser: <https://open.kattis.com/email?email=frankthorsenespen%40hotmail.com&authcode=dhpnsnnwdbk>

Best regards from Kattis



Lånekassen <ikkesvar@lanekassen.no>

11.01.2021 18.23



Til: frankthorsenespen@hotmail.com

7



Hei

Du har fått et brev fra oss med viktig informasjon.

Logg inn på Dine sider på lanekassen.no for å lese det vi har sendt til deg. Informasjonen blir ikke sendt i posten.

Vennlig hilsen

Lånekassen

Dette er en automatisk utsendt e-post, du kan ikke svare på den.

[Logg inn - DINE SIDER](#)

VI GJØR UTDANNING MULIG



Netflix <info@mailier.netflix.com>

25.07.2021 04.09

Til: frankthorsenespen@hotmail.com

N

8

Det er alltid trist å ta farvel


Hei, Espen


Beklageligvis har vi ikke klart å løse problemet med betalingen din så vi har avsluttet medlemskapet ditt.

Selvfølgelig vil vi gjerne ha deg tilbake. Du trenger bare starte medlemskapet på nytt.

[Start medlemskapet på nytt](#)Vi er her om du trenger det. Gå til [brukerstøtten](#) for mer informasjon, eller [ta kontakt](#).

Netflix-teamet

 no-reply@mail.sumango.no
fr. 11.02.2022 08:09
Til: Oscar Ram Kalia

 INNTEKTSSKJEMA.pdf
172 kB

9

This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.



