Why phishing attacks remain a threat for organizations with a robust cyber security

Thesis written by Axel Rynjus Wahl

Under the supervision of Peter Rajsingh

Dissertation submitted in partial fulfilment of requirements for the MSc in International Management with Specialization in Strategy and Consulting, at the Universidade Católica Portuguesa, January 2022.

Table of Contents

Abstract ***3***

Resumo ***4***

Acknowledgment ***5***

Introduction 1.0 ..... ***6***

Thesis outline 1.1 ..... **8**

Literature review 2.0 ..... ***8***

Theoretical background 2.1 ..... **9**

Social engineering 2.2 ..... **9**

Email phishing 2.3 ..... **10**

Persuasion 2.4 ..... **11**

Cyber Security 2.5 ..... **12**

Multi-layer defense strategy 2.6 ..... **13**

The Human factor of Cyber Security 2.7 ..... **14**

Systematic mistakes 2.8 ..... **15**

Insider threats 2.9 ..... **16**

Data and methological issues 3.0 ..... ***16***

Scope of the study 3.1 ..... **16**

Primary data collection 3.2 ..... **17**

Interviews 3.3 ..... **17**

Questionnaire 3.4 ..... **19**

Secondary data collection 3.5 ..... **20**

Findings and analysis 4.0 ..... ***20***

Semi-structured interviews 4.1 ..... **20**

Questionnaire 4.2 ..... **26**

Final discussion 5.0 ..... ***31***

Conclusion 6.0 ..... ***32***

Future research 6.1 ..... **33**

Limitations 6.2 ..... **34**

Bibliography: ***36***

Appendix: ***40***

Abstract

Title: *Why phishing attacks remain a threat to organizations with a robust cyber security*

Over the last decade, there has been a substantial rise in the number of phishing attacks that harm organizations and individuals. Organizations are investing heavily in cyber security to minimize the risk of becoming a victim of a cyberattack, such as phishing attacks. Paradoxically, with cyber security budgets of organizations continuously increasing each year, the number of attacks that are successful is also increasing.

In this thesis, we investigate how organizations with cyber security become victims of phishing attacks, drawing upon academic literature and empirical data collection. We examine the critical factors for why phishing attacks are effective. We then look into how organizations can reduce the risks of becoming a victim of these attacks. We suggest that current measures used to educate employees on cyber security and phishing emails may lack efficacy, since current training and education often fail to adapt to individual variabilities.

This implies the need for more adapted training initiatives to increase the effectiveness of measures and hence reduce the probability of loss events. The other factor that leads to organizations and their employees failing to protect themselves from phishing attacks may be the human proclivity towards making unintentional mistakes. However, we argue that organizations need to be careful simply to blame human error as the root cause for phishing attacks becoming a larger threat.

Keywords: Cyber Security, Phishing, Social engineering, Cyber security training, Human error

Author: Axel R. Wahl

Resumo

Título: Porque é que os ataques de phishing continuam a ser uma ameaça para organizações com uma segurança cibernética robusta

Durante a última década, tem havido um aumento substancial do número de ataques de phishing que prejudicam organizações e indivíduos. As organizações estão a investir fortemente na segurança cibernética para minimizar o risco de se tornarem vítimas de um ataque desta natureza, tais como os ataques de phishing. Paradoxalmente, com os orçamentos de segurança cibernética das organizações a aumentar continuamente todos os anos, o número de ataques bem-sucedidos está também a aumentar.

Nesta tese, investigamos como as organizações com segurança cibernética se tornam vítimas de ataques de phishing, recorrendo à literatura académica e à recolha de dados empíricos. Examinamos os fatores críticos para a eficácia dos ataques de phishing. Seguidamente, analisamos de que forma as organizações podem reduzir os riscos de se tornarem vítimas destes ataques. Sugerimos que as medidas atuais utilizadas para instruir os funcionários sobre segurança cibernética e e-mails de phishing podem não ser eficazes, uma vez que a formação e educação atuais muitas vezes não se adaptam às variabilidades individuais.

Isto implica a necessidade de iniciativas de formação mais adaptadas para aumentar a eficácia das medidas e, consequentemente, reduzir a probabilidade de eventos de perda. O outro fator que leva as organizações e os seus empregados a não se protegerem dos ataques de phishing pode ser a propensão humana para cometer erros não intencionais. No entanto, argumentamos que as organizações precisam de ter o cuidado de não culparem o erro humano como a única causa dos ataques de phishing.

Keywords: Cyber Security, Phishing, Social engineering, Cyber security training, Human error

Autor: Axel R. Wahl

Acknowledgment

I am deeply grateful that I got the chance to work with Peter Rajsingh on this thesis, who is among the greatest teachers I have been lucky to meet. He is a true role model, with a personality and intelligence that has inspired me in so many ways. I am thankful for him always being helpful and for his contribution to this work. But most of all, I am thankful that I got the chance to work with a man of his caliber.

I want to thank every person who has contributed to this study, especially the people I interviewed, who were generous with their time. And to all those who took part in the questionnaire. This study would not have been possible without the help of these people. It has truly been an amazing time working with this thesis and talking to so many interesting people in the field within cyber security. Thank you, Vasileios Mavroeidis, Olav Østbye, Timothy Rohrbaugh, Nuno Loreiro, Micheal Standfield and all those who remain anonymous.

I also want to thank the people who I am lucky to have in life, my friends and family who have supported me and challenged me through my educational journey.

Introduction 1.0

An invisible enemy has become a significant threat to governments, organizations and individuals. The battle against cybercrimes is affecting every part of society. In 2017 Warren Buffet said, “I don't know that much about cyber (attacks), but I do think that it's the number one problem with mankind” (Berkshire annual shareholder meeting 2017). Data security is now a priority in firms’ technology budgets and a recent report from KPMG called on business leaders to ensure that cybersecurity specialists are part of the C-suite decision making process (KPMG, 2021). The global cybersecurity market is forecast to grow to US $345.4 billion by 2026 with a CAGR of 9.7% from 2021 to 2026 (Statista, 2021). Increasing awareness of cyber threats has led to rising investments in cybersecurity infrastructure worldwide. According to a survey conducted by the World Economic Forum on global risks, respondents voted cyberattacks as the fourth-most likely global risk to become a critical threat to the world (World Economic Forum, 2021). The future of industries will continue to be affected by this emerging threat and cyber security will progressively be a key topic as digitalization continues.

Colonial Pipeline, the largest fuel pipeline in the US that distributes almost 50% of the fuel consumed on the East-Coast, became a victim of a ransomware attack on the 29th of April 2021. According to open-source reporting, Darkside actors gained access to the corporate network through phishing techniques and exploiting remotely accessible accounts and systems (CISA, 2021). This led to Colonial Pipeline halting all of their pipeline operations to contain the attack, which caused people to panic buying fuel which resulted in 87% of stations to run out of fuel in Washington D.C and 71% in Charlotte. The shortage lasted for a total of six days and was felt across thousands of gas stations. President Joe Biden declared a state of emergency 10 days after the attack in an attempt to alleviate potential shortages (Bloomberg, 2021). Colonial Pipeline had to pay the hackers 75 bitcoin (5 million dollars) to restore their network. A few weeks after the cyberattack on Colonial Pipeline, JBS, a US meat supplier that processes roughly one-fifth of the US meat supply, suffered a ransomware attack that disabled its beef, lamb, chicken and pork slaughterhouse operations. The disruption caused a shortfall in meat production which increased meat prices for consumers across several geographical locations in North America and Australia. JBS had to pay the hackers 11 million dollars in bitcoin to restore their business operations (Bloomberg, 2021).

In November 2021, FBI become victim of a cyberattack (Wasington Post, 2021). FBI are planning to spend 458,4 million dollars on cyber security in 2022 (40 million increase from 2021) and they have 2,124 positions that are involved in cyber security (FBI FY 2022 Budget Request). These organizations are investing huge amount of money, however, they still become victim of cyberattacks.

In today's society we are moving everything online, putting the safety of personal credentials at risk. As we are networking almost all the data pertaining to our lives, digital societies are becoming more and more porous. Organizations tend to invest extensively in technical measures to fortify their assets against cyber threats. While these technical solutions are effective and useful, it is increasingly recognized that technology alone cannot guarantee a secure environment (Furnell and Clark, 2012). There is a substantial need for organizations to address the *human aspect* of cyber security, often times recognized as the "weakest link" in cyber security (Z Yan et al., 2018). Humans do not always act in a rational way and we occasionally do things we should not do. We fail to recognize the risks and consequences of the actions we do. Despite the best efforts of an organization to implement a proper standard of cyber hygiene, workers continue to click on phishing links and download malicious files. Kahneman and Tversky established theories on why human errors arise as a consequence of our predispositions towards heuristics and biases. Heuristics are mental short-cuts that we employ to solve problems and make judgements quickly and efficiently (Khaneman, 2011). These heuristics and biases make us vulnerable to those who know how to take advantage of them, for instance, social engineers (Mitnick, 2003).

Social Engineering

Social engineering is any act that manipulates human behavior into revealing confidential information that are detrimental to a specific person, or the security of a system/network without the victim being aware of it. There are various types of social engineering attacks, some uses technical tools, and some do not (Hadnagy, 2011). A research done by FBI finds an alarming jump in the most common social engineer-based attack, phishing. Phishing was by far the most prevalent cybercrime in the U.S in 2020 with 114.702 occurrences in 2019 and 241,324 incidents in 2020 (Internet Crime Report, 2020). Phishing attacks is considered to be one of the most frequent examples of cybercrime on the internet. McKinsey reports that it has been a near-sevenfold increases in spear-phishing attacks, since the beginning of the pandemic in 2020,

using social engineering techniques to gain sensitive information. Phishing has a quite simple approach – send an email, email sends victim to a website, site steal information.
Despite phishing attacks simple approach and the billions of dollars that have been invested to solve the problem, it is, and has been a major issue in our societies for a long time without a good solution in place. This thesis will seek to examine *why trained working professionals in organizations fail to protect themselves and their organization from email phishing attacks.*

Thesis outline 1.1

This thesis consists of six parts. The first part gives a background and context for the study, followed up by a literature review that covers significant themes in this research. The third part presents the methodology used to collect data. The fourth part introduce findings from interviews with experts in cyber security and quantitative data from a simulated phishing tested we performed on 134 participants. In the fifth part we present key findings and have a final discussion on our findings. In the last part we present our conclusion, suggestions for future research and limitations to our study.

Literature review 2.0

This research is within the field of information systems research. Cybersecurity has become a major consideration within information technology (IT) and information systems research (ISR) and practice over time (Zadeh et al., 2020). Information systems (IS) are composed of networks of hardware or software used by various actors within an organizational or social context to perform specific tasks. IS consists of four elements which are task, people, structure and technology (O'Hara et al., 1999). Moreover, it is an interdisciplinary field that encompasses multiple theories from a variety of fields (Webster and Watson 2002). Humans play a key role in the development, deployment and utilization of technology. In order to maximize the value which technology contributes to our society, we need to focus on how we can solve challenges that arise alongside it. In this context, the subject at hand will be to frame the challenges arising from the rising numbers of phishing attacks exploiting organizations.

As this thesis aims to tackle a relatively emerging field within IS research, inspiration has been drawn from the guide on "writing a literature review" by Webster and Watson (2002). The structure of the review will draw upon multiple fields of research and knowledge from various spheres, which will be synthesized with the intention of gaining greater insight on the topic.

Theoretical background 2.1

This literature review examines existing research on social engineering, phishing attacks, cyber security, cyber threats targeting humans, as well as measurements against phishing attacks.

Social engineering 2.2

Social engineering is the art of manipulating humans through various persuasion techniques to unknowingly infecting systems or releasing confidential information. Instead of technical attacks on systems, social engineers deploy tools and tactics to gain access to private and confidential information by exploiting human's cognitive limitations (Aldawood and Skinner, 2020). Social engineering attacks are one of the greatest threats facing cyber security, because they threaten all systems and networks (Lohani, 2019). The fundament of a social engineering attacks is to exploit "innocent" humans, rather than technological vulnerabilities. Humans are often referred to being the weakest link in cyber security (Lou, 2011). Victims of social engineering attacks are unaware of the destructive nature of their actions. Ransomware attacks are often a by-product of a clever social engineering scheme who uses open-source intelligence to trick employees into disclosing sensitive information.

Although social engineering attacks differ, they have similar approaches in their execution. The process usually begins with researching and gathering information about the target. Then a relationship with a key person is developed to exploit the target. In the exploitation phase, access to the system is gained and the final phase, the attack is implemented (Conteh and Schmick, 2016).

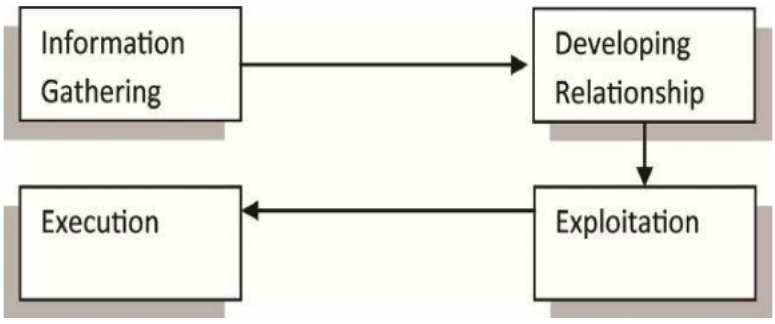


Figure 1: Phases of a targeted phishing attack

Email phishing 2.3

The most common type of social engineering attack is email phishing. Email phishing is aimed at obtaining sensitive information such as usernames, passwords and financial information from unsuspecting victims. Other phishing attacks implies masquerading malware such as worms or trojans in a document to compromise the victim's computer when downloaded (Vayanski and Kumar, 2018). People, organizations and even nation states can become victim of an email phishing attack. The attack methodology typically implies sending an email which appears to be legitimate in an attempt to deliver malware or obtain personally identifiable information. Phishing attacks are usually carried out via standard communication, such as email or instant messaging by masquerading as a familiar or and trustworthy entity. The challenge with phishing attacks is that attackers constantly look for new and creative ways to trick users into believing their action involve a legitimate website or email. Social engineers have become more skilled at developing emails, websites and documents to be identical to legitimate sources. These attacks lead to billions of dollars in damage each year. (Shashidhar and Chen, 2015). These attacks may also harm reputation of targeted brands by disrupting ecosystem and user trust (Oest et al., 2020).

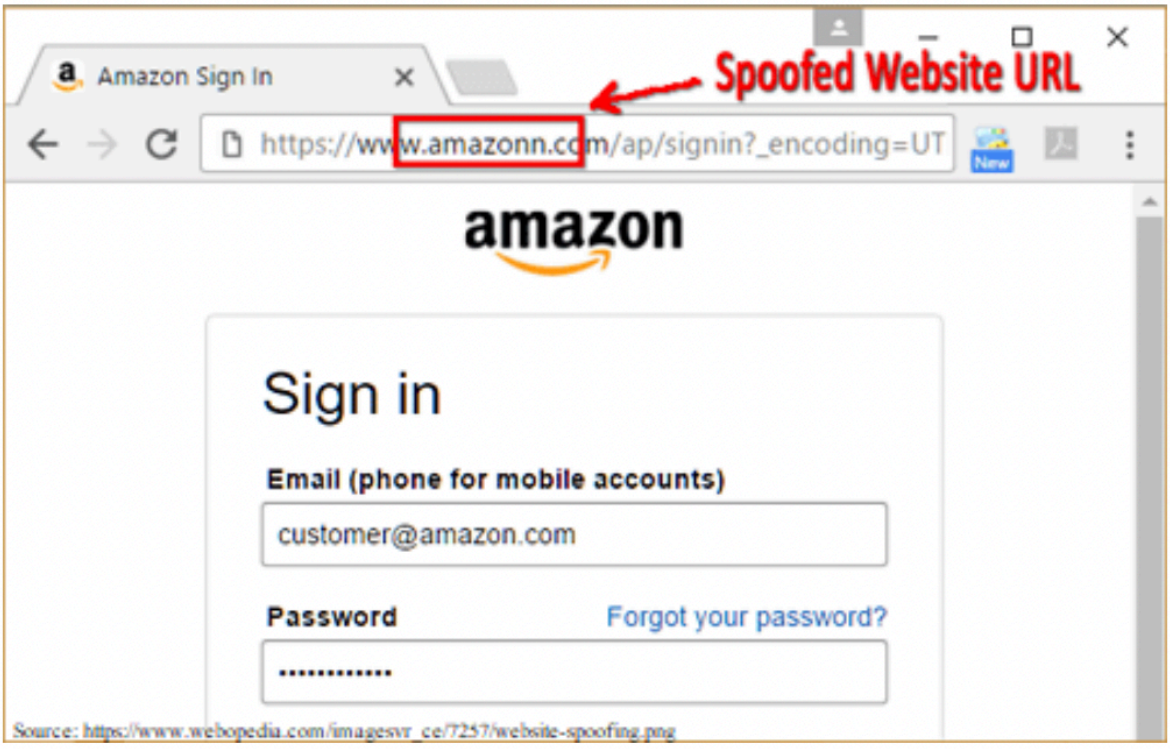


Figure 2: Example of a phishing website

Phishing attacks fall into two general categories: spear-phishing, which implies attacks that target specific high-value individuals or groups, and large-scale attacks, where attackers target multiple individuals or groups at the same time with volume. Spear-phishing requires information about the victim – where they work or what the person is involved with to execute an attack. Much of this information can easily be found over the internet. In spear-phishing attacks, social engineer works to gain trust or build a relationship with a targeted person. In some phishing attacks, the social engineers pretend to be someone that the victim knows. One study shows that victims are 4,5 times more likely to fall for a phishing attempt if it is from a person that they are familiar with (Vayanski and Kumar, 2018). Social engineers' uses different persuasion and psychological techniques in their phishing attacks to manipulate and successfully exploit victims.

Persuasion 2.4

In the literature about social engineering, we find in references to the work of Cialdini, an expert in the field of persuasion. Although Cialdini focuses on marketing, or on how executives may influence employees to act in certain ways, his principals are fundamental for anyone seeking to understand how social engineering works. Cialdini shows that persuasion works by preying upon a limited set of deeply rooted human drivers and desires, and it does so in predictable ways. Understanding the following six principals can help understand how and why these social engineering techniques work:

1. Liking

   People prefer to comply with those (they think) they know or like, or to whom they are similar or familiar with, as well as attracted to. If social engineers get their victim to like them through, for example, showing similarities and interest or giving compliments, it is according to Cialdini's research much more likely that the victim will comply with the social engineer's requests.
2. Reciprocity

   When people receive a favor from others, they develop a feeling of discordance until the favor is given in return (Hadnagy, 2010). A person will have the desire to give back to a person whenever the chance presents itself. Social engineers take advantage of the human automatic response to repay a favor.

3. Social Proof

   People tend to do what the majority of the people do or seem to be doing. It is common that people let down their guard when it appears that everyone else tends to share the same risks and behaviors (Ferreira et al., 2015).

4. Consistency

   Once committed to do something, people tend to follow through until the end. When a specific action is stated publicly, the odds of committing to something increases drastically. Most humans have a strong desire to appear consistent to others (Cialdini, 2001).

5. Authority

   In today's world, with the confusingly large amount of information that surrounds us, it is easy to rely on experts to navigate our day-to-day lives. In many environments people are also uncomfortable asking questions of people in authority. People therefore usually follow the request of an expert or authority.

6. Scarcity

   Scarcity is when there is a limited amount of a product, service, time or information available, which people perceive as increasing its value and attractiveness. Deploying scarcity as a marketing technique is something that is frequently used. Airline companies do it when selling plane tickets, "only 2 seats available for this price". Social engineers may use the scarcity technique when it comes to time, information or items being given away. Scarcity will create a perception that something is of higher value and may pressure someone to make a decision with little time to "think about it" (Hadnagy, 2010).

Cyber Security 2.5

Information security may be defined as protecting information assets from threats and vulnerabilities that may cause harm. Von Solms and Van Nierkerk (2013) argue that cyber security has another dimension in comparison to information security, namely, humans as potential targets of cyberattacks or even unknowingly participating in a cyberattack. This means that humans can be both a threat and a vulnerability within cyberspace. For that reason, cyber security is not necessarily only about protecting confidential information itself, but also entails defending those who function in cyberspace and any of their assets that can be reached through cyberspace. Furthermore, humans are a critical part of the assets that need to be shielded from

cyber threats. Regardless of how technically secure a system is, the human element will always be a vulnerability (Conteh and Schmick, 2016).

The international ISO/IEC 27032 standard (2012) defines cyber security as the "preservation of confidentiality, integrity, and availability of information in the Cyberspace." Confidentiality, Integrity and Availability is referred to as the CIA triad (Samonas and Coss, 2014). Together these three principals form the foundation of any organization's security infrastructure. Confidentiality refers to preventing disclosure of information to systems or individuals without authorized access. Encryption is a tool used to maintain confidentiality, which is the process of converting ordinary information into an unintelligible form. Integrity refers to preventing modification and alteration without proper authorization. Hashing is a cryptographic process used to validate the authenticity and integrity of various types of files. Availability refers to assuring that systems are accessible to those who need them and when they are needed (Jang-Jaccard and Nepal, 2014). The cyber security objectives of an organization should successfully implement all three components of the CIA triad for every security program. In other words, the goal of cyber security is anticipating different cyber-attacks and formulating a defense strategy that maintains the confidentiality, integrity, and availability of assets that can be reached through cyberspace.

Multi-layer defense strategy 2.6

The problem with phishing is that a holistic solution, that works to protect user's security from being phished, does not exist (Vayansky and Kumar, 2018). However, different strategies and tools for detecting and mitigate phishing attacks are widely used. Multi layers of defense is a common strategy used in organizations. This strategy implies using email filtering classification, crimeware and credential drop analytics, URL and content classification and blacklisting, malware and vulnerability scanning by web hosts, DNS, domain, user training, content take-down, and direct abuse report (Oest, 2020).

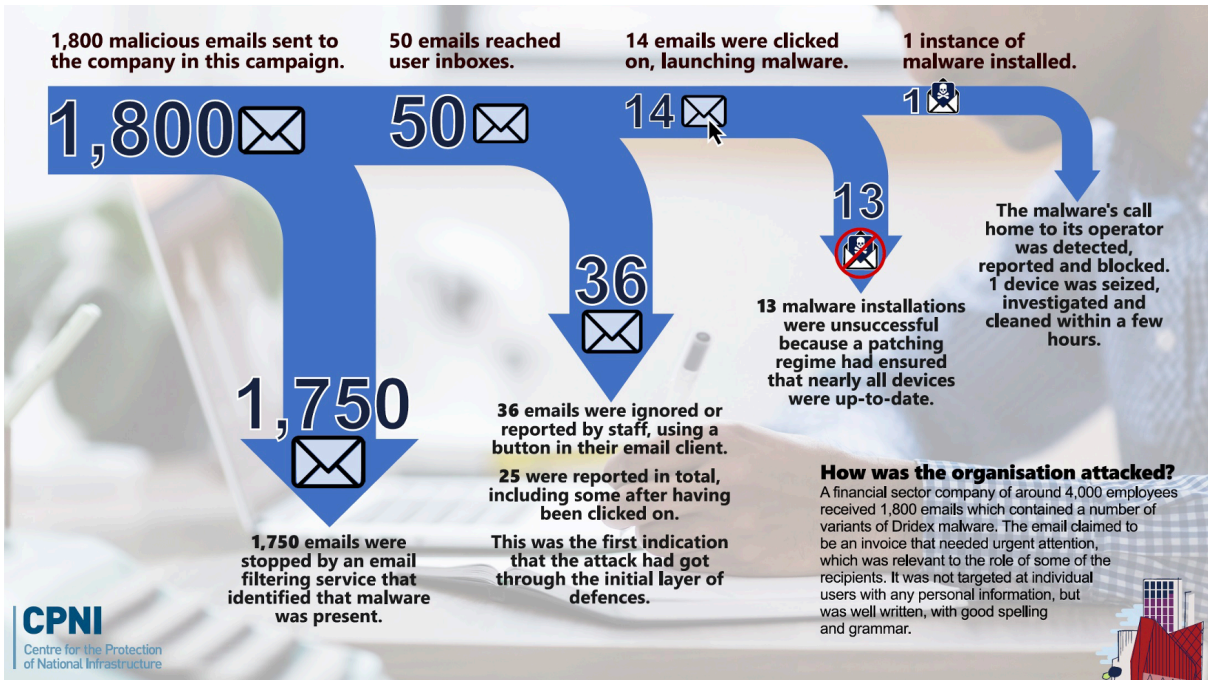


Figure 3: Multi-layer defense strategy for email phishing (Source: National Cyber Security Center, 2018)

The Human factor of Cyber Security 2.7

The number of layers of technological defenses can be as numerous and robust as is possible, but any cyber security defense is not stronger than its weakest link. Humans, therefore, are considered the most fragile link in cyber security. Having weak passwords or writing them down so they are available for others, opening unknown emails and attached files, downloading software online and leaving systems in login status while unattended are examples of common human mistakes. Focusing on the human aspect of cyber security is just as consequential as technical solutions, and is therefore paramount to decrease security threats due to human-related vulnerabilities and necessary for improving an organization's overall cyber security posture (Abawajy, 2014).

Research suggests that implementing countermeasures and training to increase cyber security awareness can reduce the uncertainties surrounding human behavior. Evidence shows that with the right security awareness personnel can become the organization's strongest defense against security threats (Kumaraguru et al., 2007). Therefore, organizations must implement training and programs for their employees in order to achieve an adequate level of cyber security awareness (Abawajy, 2014). Findings from a research conducted on 579 business professionals in the US, suggest that employees who are aware of their company´s information security

policies and procedures behave significantly more securely compared to ones who are unaware (Li et al., 2019). However, if the training and protocols consist of behaviors that no one in an organization adopts, then they are useless and ineffective. It is critical that an organization motivates employees to learn security policies and act securely (Li et al., 2019). Furthermore, what kind of training or procedures an organization chooses to use is key to whether these measures will be effective at minimizing cyber threats (Ergen et al., 2021). Games and simulations are some of the most effective and latest tools preventing social engineering attacks such as phishing (Aldawoord and Skinner, 2019).

Systematic mistakes 2.8

Despite the best efforts of organizations to minimize human error through cyber security awareness training and protocols, slips and mistakes still occur. To understand the human error phenomena, we need to look into the causes to why this is occurring. Kahneman and Tversky argue that deviations from behavior that is expected of an individual are too great to be ignored and too systematic to be dismissed as random errors (Kahneman and Tversky, 1979). Through multiple experiments they established that when humans are engaged in various domains of decision-making, they do not always act in the be most rational way. Furthermore, humans' cognitive capacities are limited, and we are often under time constraints whereby decisions need to be made quickly (Simon, 1952). To think faster we form mental models of the world based on meaning, description and knowledge (Laird, 1983). Mental models affect how we see problems and how we see people. In the context of cybercurity, unawareness of heuristics and cognitive biases can pose a threat when they short circuit previous security training and protocols. Heuristics are part of so-called "system 1" thinking – automatic judgements that stem from associations stored in memory that enable us to come to quick decisions based on limited information (Kahneman, 2011). System 1 is critical for humans to navigate key aspects of their lives. However, as previously pointed out from Kahneman and Tversky's experiments, system 1 is also a common source of cognitive biases that can result in poor decision making. System 2 thinking, that requires deliberate reasoning, also has it flaws. For instance, cognitive limitations and laziness may cause humans to focus on the wrong things or to exclude important factors in their considerations. Especially when we are fatigued, stressed or multitasking, we are at risk of becoming victims of such biases (HBR, 2015).

Insider threats 2.9

Most employees who give away confidential information do this unintentionally. However, an organization may also become victim of an insider threat, which is when a person who works or did work for or with an organization has ulterior motives. This threat is probably the most dangerous human factor threat to organizational security. Insider threats are insidious since they are hard to detect and can cause significant damage (Greitzer and Frincke, 2010).

Data and methological issues 3.0

This section will describe the sources of data that are used in this study to answer the problem statement. This thesis employs a qualitative and quantitative approach. There is both primary and secondary data collection.

Scope of the study 3.1

This study addresses why phishing attacks remain, according to signifciant statistical evidence, the most prominent cyberattack, year after year, and why trained professionals fail to protect their organization from these attacks. To look into this phenomenon, this study will examine two research questions where any chosen methodology must be sensitive to the characteristics of the questions:

1. Frist, we seek to understand **the critical factors as to why email phishing attacks are effective** on cyber security trained working professionals.
2. Next, we will explore **how organizations can reduce the risk of becoming victim of phishing attacks**.

Since this study aims to research an emerging and relatively unknown phenomenon, we have chosen an exploratory approach (Saunders et al., 2016). This approach allowed us to examine the research questions more openly, so that we could gain deeper insights into existing cyber security strategies aimed at preventing phishing attacks. An explanatory approach allowed flexibility and the opportunity to change direction during the study (Saunders et al., 2016). It can be challenging to have a rigid and solid research design in cases where one wants to investigate research questions through individuals' opinions, actions and experiences (Saunders et al., 2016). Needing to examine the research questions through the viewpoints of experts in

the field of cyber security, we avoided a rigid research design using an exploratory starting point.

There are multiple types of research methods which uses different tools for data collection. The literature presents three approaches to research: qualitative, quantitative and mixed methods. Since the nature of this phenomena may be described as a social or human challenge, which is complex, we are inclined to choose a qualitative research approach (Jack and Raturi, 2006). With this research method, we were able to explore the "whys" and "hows" which is vital to uncovering new information and better understanding of the topic. Qualitative research aims to gather data to explore and understand the opinion of an individual or a group, often on complex concepts, social interaction or cultural phenomena (University of Newcastle, 2020). A qualitative method is further suitable for studies where the purpose is to uncover and interpret experiences of individuals. Through qualitative methodology, non-numeric data was collected from sources such as secondary data, observations and interviews.

To provide empirical support for findings from the qualitative part of the study, a questionnaire was used to gather quantitative data for descriptive statistical analysis. Here it is important to note that the quantitative data did not meet the requirements for being a representative sample and was only used as support for findings from the literature and the qualitative data collection.

By using both qualitative and quantitative data, we used triangulation (Johannessen et al., 2016) to assess and investigate whether the findings supported each other (Saunders et al., 2016). In this way we could increase the quality of the findings. By combining multiple data sources, alternate methods, distinctly different theories we hoped to minimize the risk of intrinsic biases arising from single method, single-observer and single theory studies (Jack and Raturi, 2006).

Primary data collection 3.2

Primary data was obtained through two main sources: semi structured interviews with experts in the field of cyber security and a cyber security judgment questionnaire directed at working professionals.

Interviews 3.3

For the purpose of gaining in-depth knowledge the critical factors to why phishing attacks are effective on cyber security trained working professionals a qualitative approach using

interviews was performed (Johannessen et al., 2016). Due to the nature of the topic and the purpose of the research, interviews were the most appropriate data collection method. In this study we performed a total of 10 interviews. Interestingly, one of the interviews was with a manager running an organization that was a victim of a recent phishing attack and the nine others were cyber security experts in various rol

A semi-structured interview is a convenient data collection method where participants are allowed to express themselves relatively freely and constitute a selected expert group (Johannessen et al., 2016). The purpose of conducting these interviews was to understand the weaknesses with current strategies and why phishing attacks are so effective.

The advantages and disadvantages of performing interviews have been carefully considered. The interviews were planned thoughtfully to gain the information required and not take up too much time of the participants. This included creating an interview guide, performing general background research on participants, and creating a plan for execution. This sought to highlight what issues to raise in the conversations and establish credibility with participants while helping to record and assess the information provided.

Every interview began with a brief description of the topic and what the study aimed to achieve. Besides that, almost all interviews were different and context specific. Follow-up questions were asked based on information the informant provided. During the closing phase of the interviews, we prompted interviewees to clarify significant elements that had been discussed. We summarized our interpretations of what the interviewee had conveyed to correct any misunderstandings. Finally, we asked the interviewees if they had anything more on their minds that could be relevant to the study. Then we ended the interview and thanked subjects for participating. To document the interviews, we recorded the conversations if permission was granted by the interviewee and took personal notes during the interview. In the table below the roles of the interviewees, their organization type or the name organization are presented.

ID	Role	Organization type
Anonymous NA	Cyber Analyst	Multinational consultancy company
Vasileios Mavroeidis	Cyber security researcher	University of Oslo

Anonymous NB	Cyber security executive	Security Company operating in USA
Olav Østbye	Cyber security manager and host of largest cyber security podcast in Norway	Cloud Works
Anonymous NC	Cyber analyst	Multinational consultancy company
Anonymous ND	Security delivery Analyst	Multinational consultancy company
Anonymous NE	IT and security manager	Consultancy company operating in Norway
Timothy Rohrbaugh	CISO	Jetblue Airways
Nuno Loreiro	CEO	Probely
Anonymous NF	Manager of a company that became victim of a phishing attack	N/A

Questionnaire 3.4

The questionnaire was developed to test the effectiveness of phishing attacks. In the questionnaire, responders were asked to judge an email on whether they believed it was a secure email to interact with or if it was a phishing scam. There were 8 images in the questionnaire where 3 were categorized as a secure email and the other 5 were categorized as a phishing scam. The phishing scams used in the questionnaire were found online on different websites. Data was gathered online, using Facebook groups as well as direct messaging to gain responses. There was a total of 157 answers, where 23 was removed due to incomplete answers. The participants were from 13 different countries, Norway, Germany and Portugal being the most represented countries. The majority of the responders were in the age group of 16-29. Data was gathered from a questionnaire created in Qualtrics then exported to Excel to interpret and analyze the results.

Secondary data collection 3.5

A substantial part of the secondary data was from a review of the relevant literature. Secondary data was also used to complement data sources in the analysis and was collected from academic articles as well as materials and reports from consulting companies and other reputable entities.

Findings and analysis 4.0

This section is divided into three segments. Data gathered from the interviews with experts in the field is analyzed to gain insights into the research questions. Collected data identify key factors pertaining to the complexity of phishing attacks and why the problem of increasing attacks has yet not been solved, despite organizations investing millions of dollars to solve the crisis.

Interpretation of the qualitative data amplifies previously acquired knowledge and serves to substantiate the posited hypothesis about the effectiveness of phishing attacks. We compare demographic data to the score of the participants in the questionnaire and this is presented through graphical and correlation analysis. Findings from the quantitative research enable us to identify the most vulnerable demographic segment likely to become victims of a phishing attack.

The last section concludes by combing data from both sources and presents key findings. This will lay the foundation of knowledge that will be used for the concluding sections and suggestions on directions for future studies.

Semi-structured interviews 4.1

The first part of every interview was focused on understanding the critical factors as to why trained professionals working in organizations with a significant focus on cyber security nevertheless become victims of phishing attacks. Eventually, we explored how phishing attacks could be reduced using different strategies. The conversations led to different avenues of discussion based on the area of knowledge the expert had in the field.

Several variables were identified as casual factors why working professionals with cyber security training still become victim of phishing attacks. Below are the key identified factors:

1) Large organizations are increasingly targeted due to more potential gains for criminals
2) Phishing attacks are increasingly becoming more sophisticated
3) Lack of individual adaptability in current cyber security training modules may be a vulnerability to their cyber security
4) Humans may make mistakes
5) Organizations may lack a holistic cyber security perspective

The critical factors to why email phishing attacks are effective

The first remark points to the importance of emphasizing that organizations that usually have cyber security training for their employees, are often considered as high-value targets for cybercriminals. Furthermore, having cyber security training in an organization does not mean becoming less attacked. Often it means the opposite – that these organizations are being attacked more often. The more an organization is being attacked, the increasingly difficult it becomes for an organization to mitigate the threat. Criminals have often a greater incentive to attack "high-value" targets, and therefore are constantly looking for ways to get the "big fish". An increased number of attacks directed at a targeted organization makes the situation more complex from the defender's side.

In addition to the increasing frequency of these attacks, they have also become more sophisticated according to the interviewees. Cyber criminals are creating attacks with a lot more resources and effort than they used to deploy. Some of the attacks are backed by national authorities with unlimited resources. One of the interviewees who has been in the field of cyber security for a considerable time emphasized the significant evolution of the sophistication of these attacks. Olav Østbye explained that some of the attacks we see today are created by professionals – people that are so good at making it look real by spending a lot of work on preparing the attack to target a specific person, so-called spear-phishing. He explains that "There is a lot more context to the content we see in the targeted phishing attacks we see nowadays". A social engineer can pretend to be someone the person knows and personalize the message so it seems legitimate that the message actually is from that known person. The process of committing a spear-phishing attack or a targeted phishing attack can imply multiple phases and great preparation before that attack is actually executed. An example of this is hackers gaining information from a random company's client list and then later customizing an attack

by pretending to be from a company with which the targeted victim has a relationship. When hackers have information on the targets, it gives them the opportunity to create phishing attacks that seem legitimate using persuasion techniques described by Cialdini (2009). Interviewee ND explained that this is what makes some of these phishing attacks really hard to detect. The nature of human personal and business relationships is often based on selective trust. A user's amygdala is not primed to be susceptive of every email that enters his or her mailbox, especially not when an email comes from someone we trust. There are often no personal consequences to click on links or to download a software. The amygdala is the human's neural system for processing fearful and threat stimuli (Huberman, 2021). The social engineer may for instance use *liking* as persuasion technique, by pretending to be someone that the targeted person likes or trust. Research has found phishing attacks using *liking* as an influence technique to be the most effective (Wright, 2014). Another significant characteristic of phishing attacks is that it is always evolving. Hackers are seeking new mediums and new techniques in parallel with the evolution of cyber space. The internet ecosystem is constantly developing as applications running on the internet proliferate. Cyber criminals may use new techniques and new software that will not be detected by email protection filters. Organizations are trying to anticipate potential vulnerabilities, but sometimes they fail and fall one step behind.

How organizations can reduce the risk of becoming victim of phishing attacks

Having bulletproof cyber security is, according to the interviewees, impossible. There will be cyber criminals that have more resources who will manage to find a way to exploit a vulnerability. To minimize the risk of becoming victim of these attacks, some cyber security professionals use frameworks such as NIST or ISO 27001 as a fundament tool to build cyber security. These frameworks are standardized controls to systems, and guidelines to risks that arise. Timothy Rohrbaugh explained that "People believe cyber security is science, it is not, it is art." His argument was that there is not one solution to a given set of problem, to a given threat, or a specific technique. What matters depends on each situation, the nature of the organization and the threatened actors. Thus, he suggested that these frameworks have limitations.

Whether organizations choose to approach cyber security as an art or science, all informants were in agreement that there are two issues to focus on to minimize the risk of phishing attacks: 1) reduce the probability of a loss event

2) reduce the time it takes to discover the attack.
There are several ways one can go about doing that depending on the budget and situation of a given organization.

Technical protections such as web application security protocols are important to block phishing emails from entering the employee's mailbox. Email filtering is a tool that filters an organization inbound and outbound email traffic. There is a huge market for technical solutions that can protect organizations from receiving unwanted emails. These solutions use detection algorithms based on specific attributes of the email, whether it is unwanted or not. Although an organization is able to minimize the emails that workers receive through technical protection, there will still be emails that pass the filter and reach workers in an organization.

Awareness training and education is one of the most effective tools for mitigating the risks associated with phishing attacks. Previous research proposes that awareness training can reduce the uncertainties surrounding human behavior and risks of becoming victim of a cyberattack (Li et al., 2019). The interviewees stated that there are various training methods and strategies depending on the resources and risk appetites of organizations that are being implemented. It is common for organizations to test their employees with phishing attacks to train them for real world attacks. This kind of training is proven to be highly effective. Previous literature has found that participants who received phishing simulated training were significantly less likely to fall for subsequent simulated phishing attacks occurring a week later (Kumaraguru et al., 2008).

A factor the interviewees observed is that trainings often are too standardized. Training and educational tools being used are not adapted to the levels of technical knowledge of individuals in particular organizations and their specific vulnerabilities. They point out that people are different – some are technological savvy and may need another program than those less experience with technology. Another aspect is that people to do not learn at the same speed. Learning has many variables, people who are more motivated and interested in a specific topic tend to learn faster. The experts reported that there may be intellectual variability within an organization. Another challenge is that many employees find cyber security training exaggerated and boring. Getting everyone on board is crucial to have a strong cyber security. Previous research suggests that games and simulations are one of the most effective tools to

familiarize employees with situations they may face (Aldawoord and Skinner, 2019) as an interactive learning tool.

Organizations must ensure that employees act in compliance with the organizational cyber security policies. These guidelines often highlight the consequences of breaches against those who do not comply. Expert NA said that in some cases leaders put pressure on employees by sanctioning those who do not comply. Using fear to encourage employees to behave in compliance with the security policies is understandable when cyber security incidents can have devastating consequences. A recent survey of organizations found that 42% punish employees for cyber security breaches and that 15% name and shame employees (Renaud, 2021). Interviewee NA pointed out that he has seen situations where organizations punish or shame employees which has the reverse effect of causing employees not to report incidents of cyber breaches. NA emphasized that timing is critical when a mistake has occurred so avoiding reporting it may escalate damage. Hence, NA underlined the importance of managing and responding to threats and recovery from attacks as key elements for a robust cyber security policy. Thus, using punishment and shame may make an organization more fragile and vulnerable.

In the extant literature we find that human error is reported to be one of the major causes of security breaches and that humans are referred to as the weakest link in cyber security (Clark et al., 2011; Ovelgönne et al., 2017; Li et al., 2019; Parsons et al., 2015). In the interviews, some argued that human error is a significant cause of cyber breaches, while other interviewees suggested that it might be incorrect to blame human error for cyber breaches. Next, we will explore the key arguments of both perspective in this debate.

Human errors can manifest in multiple ways. One common way is people giving sensitive information out pursuant to phishing attacks. Although cyber security training on password hygiene and phishing email attacks can reduce the risk of human error significantly, there will still be the possibility of someone making a mistake. Interviewees sharing this perspective reported that mistakes occur because employees are lazy or distracted and may act without being focused. This refers to what is sometimes called system 1 thinking; the human habit of affective decision making, where decisions are based on unconscious, automatic and effortless thinking (Khaneman, 2011). This behavior was corroborated in several of the interviews as one of the major causes why trained employees become victims of email phishing attacks.

Vasileios Mavroeidis, a cyber security researcher at University of Oslo, said: “No matter how much training or education you give your employees, there will always be someone, who at one time, eventually will make a mistake. What should I do in that case? Implement more training? No, I believe the way to go is to implement more technical solutions”. According to other interviewees, implementing more training and education will at a certain point lead to diminishing returns. This perspective suggests that the way to solve humans being the weakest link in cyber security is through technological solutions.

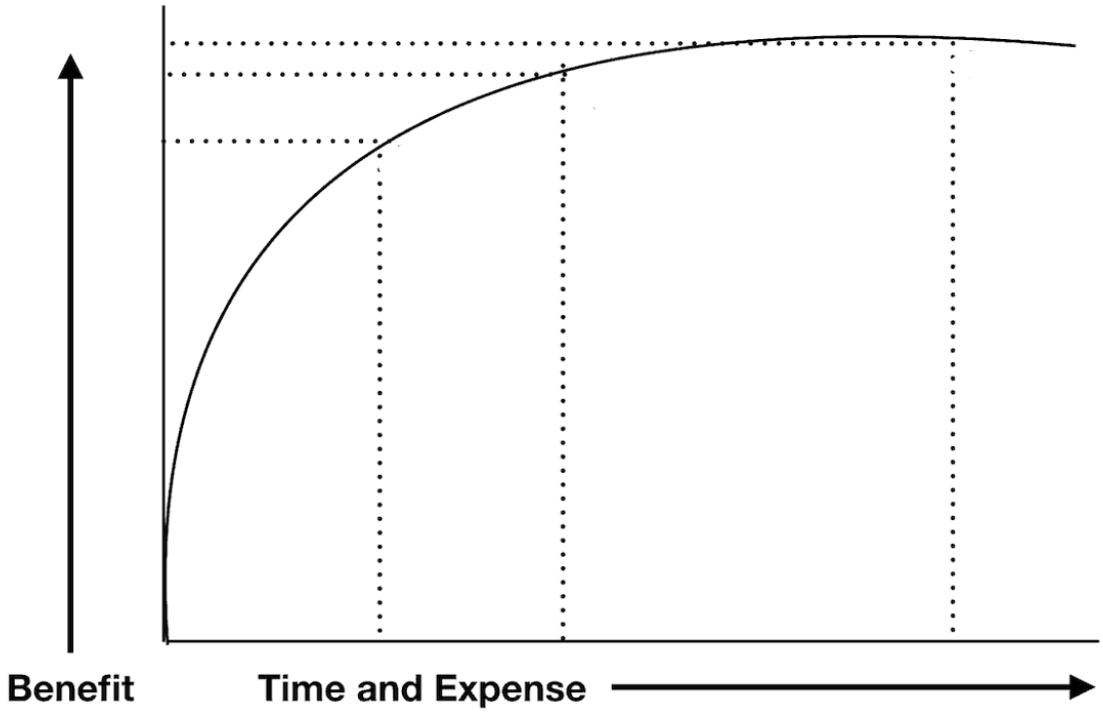


Figure 4: Illustration of diminishing returns on cyber security training

However, to conclude that human error is a significant cause of cyber breaches only leads us to a blind spot. Timothy Rohrbaugh argued that blaming human error is just a shortcut: “I disagree that we are the weakest link in cyber security, it is counterproductive to say that humans are the weakest link, and it is also counterproductive to say that human errors are the cause of most cyber breaches… We can relate everything on the defenders’ side to being a human error. But that is not really the case, it is borne along the way that they did not anticipate every action or the one action that allowed them to be compromised.” This statement suggests that we should rather shift the focus from pointing towards human error and instead assume a more holistic perspective of looking at how organization should have made it harder for the attacker to exploit

a vulnerability. There are often several phases an attacker needs to go through to execute a targeted phishing attack.

This statement contradicts much of the literature as well as other experts who attributed human error as the major locus of cyber security vulnerability. According to another interviewee, a social engineer can compromise your friends account and send you an email from that account with a link that you assume is safe. Because you trust your friend you will most likely click on the document that is attached in the email and download it. In this case it is hard to tell whether this is a human error or not. Social engineers use these kinds of sophisticated attacks and then experts blame the cyber breach on human error. To execute a targeted phishing attack, the social engineer needs to go through several stages before the actual attack can be executed. Since the nature of targeted phishing attacks implies multiple stages, it is reasonable to think that organizations should try to identify potential vulnerabilities along the way and try to block the attack before it happens. Identifying potential threats is called threat intelligence. Threat intelligence, monitoring of networks and vulnerabilities, as well as testing potential vulnerabilities are activities that have to fail before a human error can arise. The expert maintained that instead of saying that humans are the cause of cyber breaches, organizations should focus on having a security program that anticipates what is most likely to happen, and from there create a strategy on how to identify and respond to threats.

Although it may be a “shortcut” or overstatement to assign the real cause of security breaches to human error for, working professionals with cyber security training are still becoming victims of phishing emails. The experts pointed to three main reasons why this occurs:
1) Attacks are too good.
2) Humans can be lazy, distracted and not concentrated when acting.
3) Current cyber security training and education is in some cases not adapted to individual idiosyncrasies (variabilities in interest, motivation and learning abilities), resulting in some personnel not getting the minimum required knowledge.

Questionnaire 4.2

Having established that email phishing attacks pose significant threats to the societies and organizations, it is useful to determine the composition of the most vulnerable groups based on demographics. Understanding this may be critical for development of training or education

program that is adapted to individuals representing different demographic characteristics. This questionnaire simulates real life phishing attacks, where the respondent is supposed to identify which emails are legitimate, and which ones that are email phishing attacks.

The experts reported that an issue with cyber security training is often that it is too standardized and does not take into consideration that some people are more tech savvy than others. In this study we analyzed: age, profession (tech or non-tech worker), geographical location and sex related to the performance of the respondents doing the questionnaire. Comparing demographics and performance was done to identify whether some personal characteristics are significant relative to individual cyber security performance. These variables were selected because they may be generally regarded as meaningful indicators.

There were 134 respondents from 13 nationalities in this study. The most represented countries were Norway, Germany and Portugal which constituted 34%, 19% and 13% of respondents in the questionnaire. There were 42,54% females and 57,46% males. The largest age group was young adults from 16-29. 37,31% of the respondents worked in tech or cyber security, and 62,69% were in other domains.

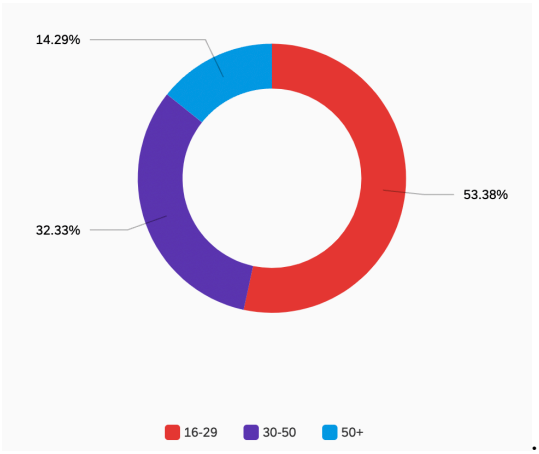


Figure 5: Age distribution of participants.

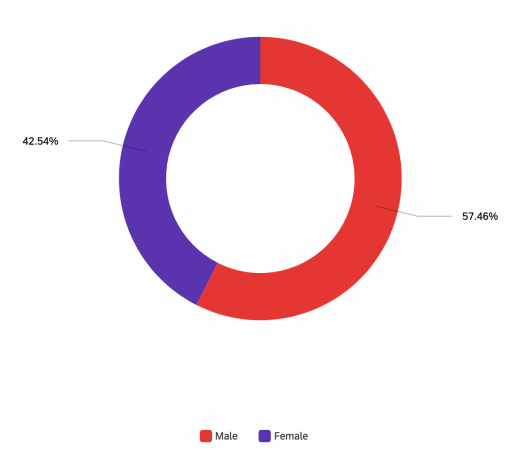


Figure 6: Gender distribution of participants

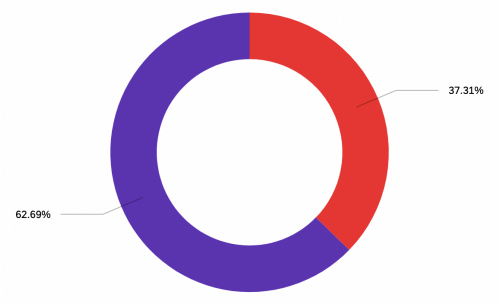
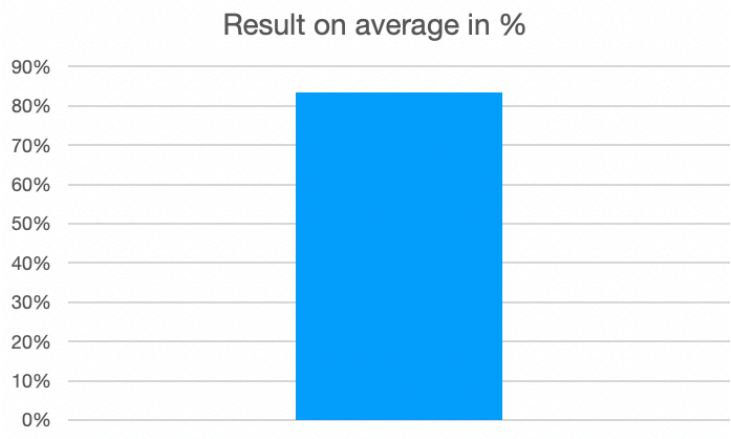


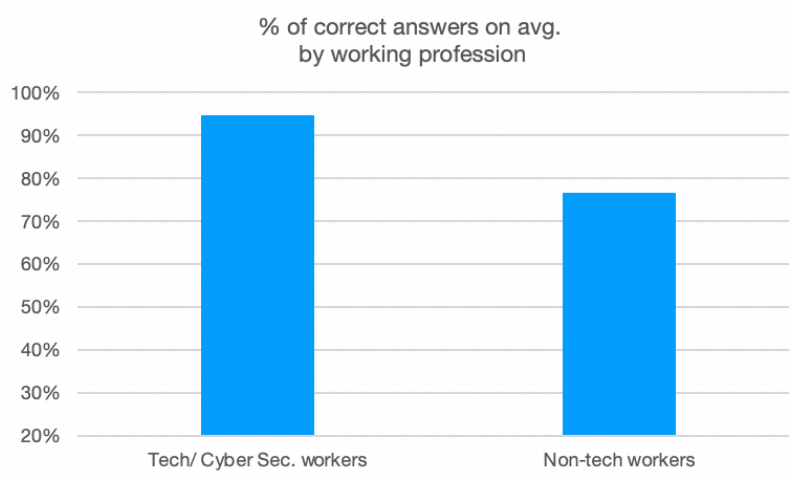
Figure 7: Distribution working profession



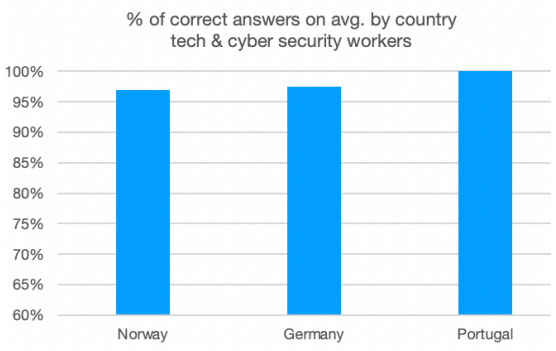
The average score on the simulated phishing test was 83,3% by the 134 participants. The lowest score was 50% and the highest was all correct. It is complex to interpret the significance of the average score since there are numerous factors that may have influenced the average performance on this test. Normally, workers are expected to identify all phishing mails that they receive, hence they get 100% right according to the experts we interviewed. However, the context of this study may have created a bias towards lower performance. Among other things, we may assume that respondents had a lower risk perception compared to a real-life scenario. In a real-life context people may spend more time analyzing an email or even asking someone for advice before choosing whether an email is a phishing scam or not. Since there were no consequences for bad performance in this test, respondents may have been less alert compared to a real-life scenario. Another factor may be how the test was presented. Usually, users are able to interact with the email to double check irregularities before coming to a conclusion. Moreover, if one hovers over the URL link (which is one of the common safety procedures) it's easier to detect whether the link is forwarding you to a legit webpage or not.

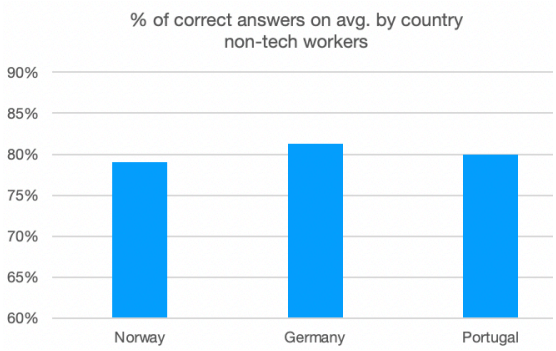
In this questionnaire the respondents would not have been able to perform the interactive tests with the email to get feedback in real-time. Therefore, the test we performed might have a bias towards lower performance, since in a real-world scenario the user would have had more options to check whether the email was a phishing scam or not. Another crucial factor one usually takes into consideration is the relevance of the email one receives. In this case the respondents had no relationship to the context or the content of the email, which is normally something that you would have in mind before judging the email to be a phishing scam or not.

The most significant variable that determined how well the respondent did on the simulated phishing test was whether that person had a profession in tech or cyber security, or not. Non-tech workers got on average 76,6% of the questions correct while tech or cyber security workers got on average 94,75% correct. This is a significant difference in performance, which may indicate that working in tech or cyber security is correlated with being on average better at determining which emails are secure which are phishing scams. This is also consistent with our qualitative findings.

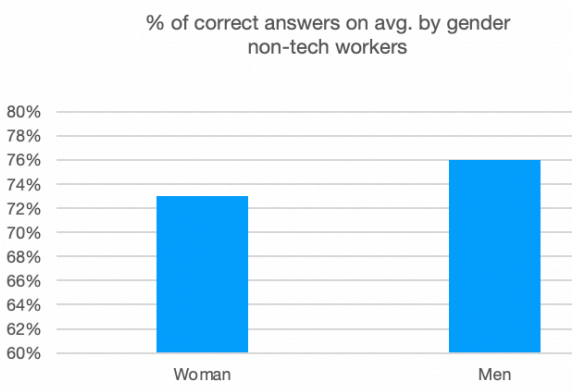


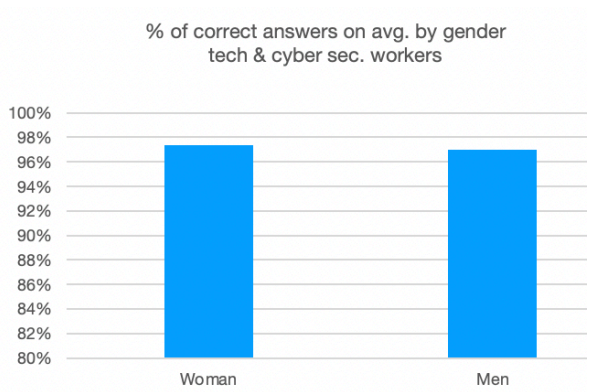
To explore whether country of origin had any significance on performance of participants we had to separate the tech and cyber security workers from those who did not have tech-related jobs. Since the number of tech and non-tech workers participating in this study was not equally divided by each country, we had to split them into two groups. (Working profession is divided into two groups for the next analysis as well for the same reason). There were 18 cyber security and tech workers from Norway, 10 in Germany and 3 in Portugal. The average scores from the three countries were: 97%, 97,5% and 100%. For non-tech workers there were 28 participants from Norway, 14 from Germany and 13 from Portugal. The average scores from the three countries were: 79%, 81,25% and 80%. The low variation in average scores may indicate that the origin of country has no significant bearing on the performance of the participants in the study.



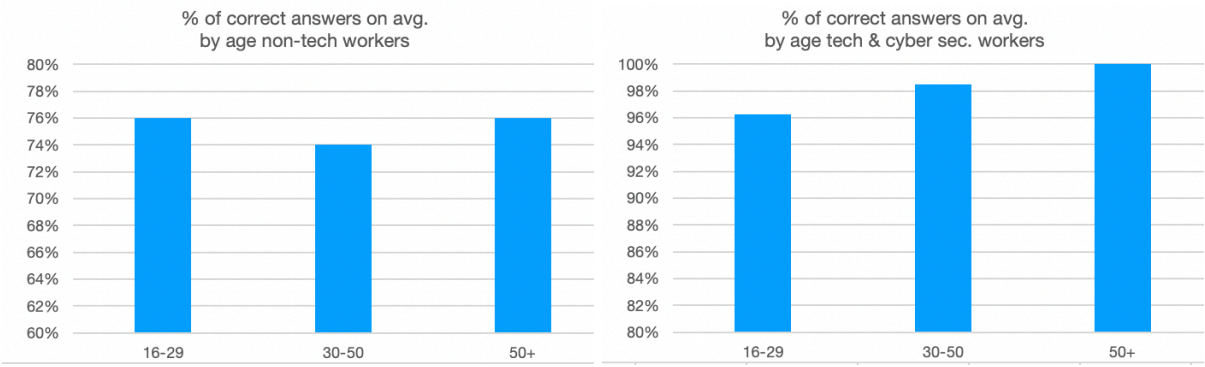


There were 55 women (19 in tech and cyber security) and 79 men (29 in tech and cyber security) participating in the study. For non tech workers men scored on average 76%, while woman 73%. For tech and cyber security workers woman scored on average slightly better than men, with 97,4% correct answers on average while med scored 97%. Moreover, gender seems to be irrelevant on how well someone performs at detecting phishing attacks based on these studies.





Here also we find that age does not have a significant influence on average scores. The highest average score for non-tech workers was 76% for both the age group 16-29 and 50+, while the lowest average score was in the age group 30-50 which had 74% of correct answers on average. The variation in average score between the age groups was higher for tech workers, however, it is still not a significant difference. Also, the low representation of tech and cyber security workers in the 50+ group (only 3 individuals) may have created a less accurate representation of the expected average score. With the low variation in average score in both groups we may conclude that age is not a significant variable to predict performance for on phishing test.



Our questionnaire key insights can be summarized as follow:

- Phishing attacks may be hard to detect
- Working professions in tech and cyber security are on average better able to predict the authenticity of an email compared to individuals working in non-tech related jobs
- Age, country origin and gender do not have a significant impact on an individual's ability to detect phishing emails

Final discussion 5.0

Findings from the literature and from the qualitative interviews suggest that phishing emails remain a significant threat to governments, organizations and individuals. The results from our questionnaire point in the same direction – that individuals struggle to identify which emails that are legitimate, and which are not. According to the interviewees we spoke with there are three main reasons why email phishing attacks remain a significant threat for trained working professionals. These attacks can be highly sophisticated with content and context that presents users with seemingly no indication of fraud. Since business and human relations often are based on trust, people may become victims of attacks that are simply too well executed. Another reason why phishing attacks remain a threat to organizations is that employees can make mistakes. Our biological makeup is not primed to be worried about threats when working or browsing on the computer. Moreover, if an employee is lazy, distracted, not concentrating or in another state where the person is not fully vigilant towards identifying threats of a phishing email, mistakes may occur. The third factor presented by some of the experts was that in some cyber security training, individual variability pertaining to interest, motivation and learning abilities is not taken into consideration. This may result in some employees not being at the required level of security knowledge, since many training programs assume that everyone is similar, which is not always the case.

Implementing cyber security training is indeed correlated with having a more robust cyber hygiene. However, we believe that it is important to reevaluate how training is being done, since organizations that have implemented cyber security training still have employees who become victims of phishing attacks. Evidence from the experts suggests that training needs to be more customized and effective. In contemporary life, a diversified workforce has been recognized to be beneficial. But lack of homogeneity means that there needs to be a likewise heterogenous approach to cyber security training. In highly diversified organizations, it is reasonable that there are differences that need to be accounted for across levels of the organization rather than having a "one size" fits all solution. Experts further suggested that organizations need to keep up with the increasingly sophisticated social engineering nature of cyber threats. Using alternative tools like games and simulations may be beneficial for training purposes.

Experts and the literature confirm that human error is one of the major causes to cyber breaches. While we think it is reasonable to say that some of the attacks arise due to human error, we believe it is important to have a holistic perspective on the causes of failure. Humans are indeed the last line of cyber defense and security but if a social engineer has managed to pass several cyber defenses and phases and acquired information necessary to execute an attack, it may be incorrect to state that the failure was ultimately a human's fault.

This holistic approach entails continuously monitoring networks for vulnerabilities, having white hat hackers who try to expose network vulnerabilities (including performing phishing attacks on employees) and employing a threat intelligence team that searches for potential threat actors. These are key elements of what can be defined as a robust cyber security. Organizations need to do what they can to be prepared and should to try stay one step ahead of a possible attack. Cyber security is complex and requires a multi-pronged solution which is the nature of effective future cyber security strategies.

Conclusion 6.0

This thesis has explored and attempted to answer the following research question "why trained working professionals in organizations fail to protect themselves and their organization from email phishing attacks." Through analyzing the results from our findings we have identified factors that may contribute to answering the research question.

A robust cyber security will remain fragile to phishing emails and methods used by today's cyber criminals may be too complicated for humans to be shielded from these complex attacks. The nature of the game is simply that it is unrealistic to prevent these attacks from occurring. Organizations must continuously use strategies to reduce the probability of a loss event and reduce the time it takes to discover the attacks. This study highlights that cyber security training and education often fail to adapt to individual variabilities. This implies the need for more adapted training initiatives to increase the effectiveness of measures and hence reduce the probability of loss events. The other factor that leads to organizations and their employees failing to protect themselves from phishing attacks may be the human proclivity towards making unintentional mistakes.

However, according to Timothy Rohrbaugh, we need to be careful simply to blame human error as the root cause for phishing attacks becoming a bigger threat and costing more. He argued instead that companies need to have a holistic approach, anticipating the weak links through threat intelligence, monitoring of networks and penetration testing. It will be crucial to have an accurate perspective towards the situation as the threat landscape is becoming increasingly complex.

This study is significant since it goes into an emerging and complex domain of cyber security that has become critical in the modern business world. Findings from our research will hopefully bring attention to areas of cyber security that can improve, an essential factor for keeping us protected from cyber criminals.

Future research 6.1

In this study we established that current measures used to educate employees on cyber security and phishing emails may lack efficacy. There is a need to explore how we may design new methods of training suited for organizations with a diversified workforce. It would be interesting to look at which training and education protocols that may best be adapted for the different personnel types. Previous research (Aldawood and Skinner, 2019) suggests that games and simulation in cyber security training are effective. Exploring the use of games and simulations as well as other interactive training modules and analyzing their effectiveness would be interesting.

The literature also pointed to humans being the weakest link in cyber security. As organizations have adapted awareness training as part of their cyber security, there is disagreement on whether human error is the cause of failure. It would be interesting to explore if humans are still the weakest link in cyber security after implementation of more effective training and education. Or if there are other domains in cyber systems that are key vulnerabilities. Knowledge of organizational weaknesses across the board is beneficial for minimizing attacks.

Future research could also engage in more quantitative drill down regarding weighting human error vulnerability criteria insofar as this is possible. For instance, when humans are in system 1 mode, are they more likely to be exploited by social engineering based upon liking versus social proof or another phenomenon mentioned by Cialdini. It may actually be impossible to become this granular which would reveal how human error and social engineering remain an intractable problem and something likely to become graver as AI's are deployed to capitalize on human fragility.

It would also be useful to undertake case studies of hundreds of organizations that have been victims of a phishing attack to ascertain if there are common patterns that can be revealed in the way attacks occurred. Although this will be significant research, it may be difficult to perform as information within organizations often remains highly confidential about the nature of particular attacks and the extent of the damage caused. Future research within the field of cyber security would benefit from more openness and transparency from organizations that have become victims of phishing and other cyberattacks as it will provide more experiences to analyze and learn from to create solutions for this problem.

Limitations 6.2

Looking back on the research that was performed and the execution and deliberate choices made, it is clear that some choices made influenced the findings and conclusions drawn. Performing semi-structured interviews may present several limitations as people have varying perceptions and the setting itself may create biased responses. The participants had varying degrees of experience as well as different roles in the field, which led to different answers on certain topics. Since qualitative research is interpretative, our personal biases may have influenced the findings. The experts were also a small sample of the industry and the

representativeness of the points of view presents limits with regard to generalizability. However, the data collected from the interviews is considered reliable, as there is no sign of information being incomplete or inaccurate.

The quantitative data collection from the questionnaire poses several limitations. There are limitations with regard to the format (as discussed in the findings) and also there were limited participants in certain groups that were studied. A larger cohort would have helped present a more accurate representation of the groups.

Another limitation in this study is the lack of transparency pertaining to the subject of being researched. Cyber security is a highly confidential field of work, which poses restrictions on the knowledge that is shared in the field. Organizations that have become victims of a ransomware attack will often be very careful about saying how the attacker managed to compromise them, whether it was through a remote access control or an email phishing attack. This poses limitation related to timing and access to insights from organizations with trained professionals that had been victim of a phishing attack. We would recommend that future researchers examine the research question in collaboration with several organizations that have become victims of email phishing attacks.

Bibliography:

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237-248. https://doi.org/10.1080/0144929X.2012.708787

Aldawood, Hussain, and Geoffrey Skinner. "An Advanced Taxonomy for Social Engineering Attacks." *International Journal of Computer Applications* 177, no. 30 (2020): 1-11.

Anand Jeyaraj, Amir Zadeh & Vikram Sethi (2021) Cybersecurity Threats and Organisational Response: Textual Analysis and Panel Regression, Journal of Business Analytics, 4:1, 26-39, https://doi.org/10.1080/2573234X.2020.1863750

Bloomberg, 2021. "White House Faces Rising Pressure as Gasoline Shortages Grow" https://www.bloomberg.com/news/articles/2021-05-11/biden-waives-some-gasoline-mandates-to-address-fuel-shortages

Cialdini, Robert B. 2009. Influence: The Psychology of Persuasion. Rev. ed. New York, NY: Collins.

Cocola-Gant, Agustín. "Holiday Rentals: The New Gentrification Battlefront." *Sociological Research Online* 21, no. 3 (2016): 112–20. https://doi.org/10.5153/sro.4071

Conteh, Nabie Y., and Paul J. Schmick. "Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks." *International Journal of Advanced Computer Research* 6, no. 23 (2016): 31. http://dx.doi.org/ 10.19101/IJACR.2016.623006

Cyber Security and Infrastructure Security Agency, 2021. "Best Practices for Preventing Business Disruption from Ransomware Attacks" https://www.cisa.gov/uscert/ncas/alerts/aa21-131a

Ergen, A., Ünal, A. N., & Saygili, M. S. (2021). Is It Possible to Change the Cyber Security Behaviours of Employees? Barriers and Promoters. *Academic Journal of Interdisciplinary Studies*, *10*(4), 210-210. https://doi.org/10.36941/ajis-2021-0111

Federal Bureau of Investigation, Internet Crime Report, 2020. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Ferreira, A., Coventry, L., & Lenzini, G. (2015, August). Principles of persuasion in social engineering and their use in phishing. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 36-47). Springer, Cham.

Furnell and Clark. "Power to the people? The evolving recognition of human aspects of security." Computers and Security, issue 8 (2012): 983-988. https://doi.org/10.1016/j.cose.2012.08.004

Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. In *Insider threats in cyber security* (pp. 85-113). Springer, Boston, MA. https://link.springer.com/chapter/10.1007/978-1-4419-7133-3_5

Hadnagy, Christopher. 2011. Social Engineering: The Art of Human Hacking. Indianapolis, Indiania: Wiley.

ISO/IEC 27032 Cybersecurity Guideline. n.d. Accessed September 24, 2020. https://iso27001security.com/html/27032.html

Jack, E. P., & Raturi, A. S. (2006). Lessons learned from methodological triangulation in management research. *Management research news*. https://doi.org/10.1108/01409170610683833

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973-993.

Johannessen, A., Christoffersen, L. & Tufte, P. (2016). Introduksjon til samfunnsvitenskapelig metode (5. utg.). Abstrakt

Johnson-Laird, P. N. (1983). *Mental models: Towards a cognitive science of language, inference, and consciousness* (No. 6). Harvard University Press.

Kahneman, Daniel. 2011. Thinking, Fast and Slow. London: Penguin Books

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, *47*(2), 263–291. https://doi.org/10.2307/1914185

KPMG International, 2021. «From enforcer to influencer» https://assets.kpmg/content/dam/kpmg/xx/pdf/2021/08/from-enforcer-to-influencer.pdf

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong, J., & Nunge, E. (2007a). Protecting people from phishing: The design and evaluation of an embedded training email system. In *Conference on human factors in computing systems – proceedings* ACM New York, NY, USA (pp. 905–914). https://doi.org/10.1145/1240624.1240760

Li, Tong, Kaiyuan Wang, and Jennifer Horkoff. 2019. “Towards Effective Assessment for Social Engineering Attacks.” In 2019 IEEE 27th International Requirements Engineering Conference (RE), 6. Jeju Island, Korea (South): IEEE. https://doi.org/10.1109/RE.2019.00051

Lohani, Shivam. "Social engineering: Hacking into humans." *International Journal of Advanced Studies of Scientific Research* 4, no. 1 (2019).

Luo, Xin, Richard Brody, Alessandro Seazzu, and Stephen Burd. 2011. “Social Engineering: The Neglected Human Factor for Information Security Management.” Information Resources Management Journal 24 (3): 1–8. https://doi.org/10.4018/irmj.2011070101

Mitnick, K., & Simon, W. (2003). *The art of deception: Controlling the human element of security*. New York: Wiley

O'Hara, Margaret, Richard Watson, and C. Kavan. 1999. "*Managing the Three Levels of Change*." IS Management 16 (June): 63–70. https://doi.org/10.1201/1078/43197.16.3.19990601/31317.9

OEST, Adam, et al. Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale. In: *29th {USENIX} Security Symposium ({USENIX} Security 20)*. 2020. p. 361-377. https://www.usenix.org/system/files/sec20-oest-sunrise.pdf

Ovelgönne, Michael, Tudor Dumitraş, B. Aditya Prakash, V. S. Subrahmanian, and Benjamin Wang. 2017. "Understanding the Relationship between Human Behavior and Susceptibility to Cyber Attacks: A Data-Driven Approach." ACM Transactions on Intelligent Systems and Technology 8 (4): 1–25. https://doi.org/10.1145/2890509

Parsons, Kathryn Marie, Elise Young, Marcus Antanas Butavicius, Agata McCormac, Malcolm Robert Pattinson, and Cate Jerram. 2015. "The Influence of Organizational Information Security Culture on Information Security Decision Making." Journal of Cognitive Engineering and Decision Making 9 (2): 117–29. https://doi.org/10.1177/1555343415575152

Renaud, K., Searle, R., & Dupuis, M. (2021, October). Shame in cyber security: effective behavior modification tool or counterproductive foil?. In *New Security Paradigms Workshop* (pp. 70-87). https://doi.org/10.1145/3498891.3498896

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3).

Saunders, M., Lewis, P. & Thornhill, A. (2016). Research methods for business students (7. utg.). Pearson Education.

Shashidhar, N., & Chen, L. (2015). An Indistinguishability Model for Evaluating Diverse Classes of Phishing Attacks and Quantifying Attack Efficacy. *International Journal of Security*, *9*(2), 15.

Simon, H. A. (1952). Comments on the Theory of Organizations. *American Political Science Review*, *46*(4), 1130-1139.

Solms, Rossouw von, and Johan van Niekerk. 2013. "From Information Security to Cyber Security." Computers & Security 38 (October): 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Soll, J, Milkman, K, Payne, J (2015). *Outsmart your own bias: How to broaden your thinking and make better decisions*. Harvard Business Review. https://hbr.org/2015/05/outsmart-your-own-biases

Statista, 2021. « Size of the cybersecurity market worldwide from 2021 to 2026» https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/

The Wall Street Journal, 2021. "JBS Paid $11 Million to Resolve Ransomware Attack". https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781

University of Newcastle (2020). *Research methods: What are research methods.* https://libguides.newcastle.edu.au/researchmethods

Vayansky, I., & Kumar, S. (2018). Phishing–challenges and solutions. *Computer Fraud & Security*, *2018*(1), 15-20. https://doi.org/10.1016/S1361-3723(18)30007-1

Venky Anant, Jeffrey Caso, and Andreas Schwarz. McKinsey and Company, "COVID-19 crisis shifts cybersecurity priorities and budgets." 2020. https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets

Warren Buffet, Berkshire Hathaway annual shareholder meeting 2017. https://buffett.cnbc.com/video/2017/05/06/afternoon-session---2017-berkshire-hathaway-annual-meeting.html

Wasington Post, 2021. "FBI email system compromised by hackers who sent fake cyberattack alert". https://www.washingtonpost.com/nation/2021/11/14/fbi-hack-email-cyberattack/

Webster, Jane, and Richard T Watson. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review." MIS Quarterly 26 (2): 13–23.

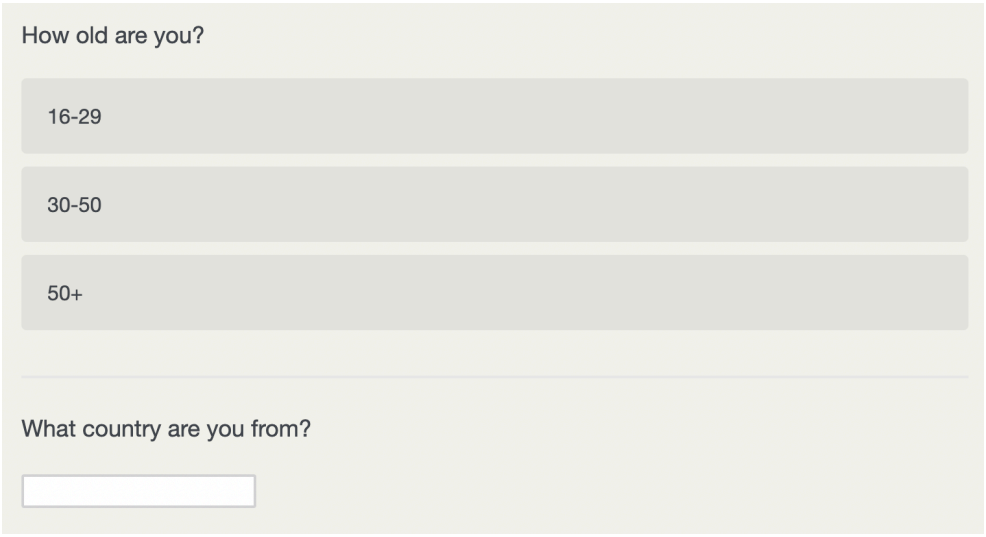
World Economic Forum, 2021. The global risk report (16th edition) https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research note—influence techniques in phishing attacks: an examination of vulnerability and resistance. *Information systems research*, *25*(2), 385-400. https://doi.org/10.1287/isre.2014.0522

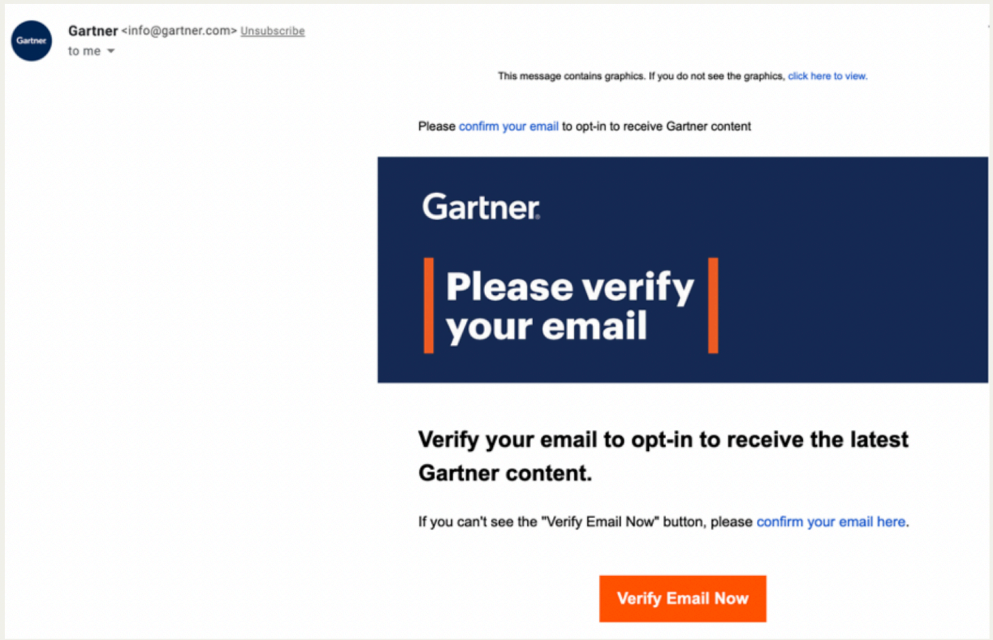
Yan, Robertson, Yan, Yong Park, Bordoff, Chen, Sprissler, "Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?" Computers in Human Behavior, 2018: 375-382. https://doi.org/10.1016/j.chb.2018.02.019

Appendix:

Phishing test questionnaire:

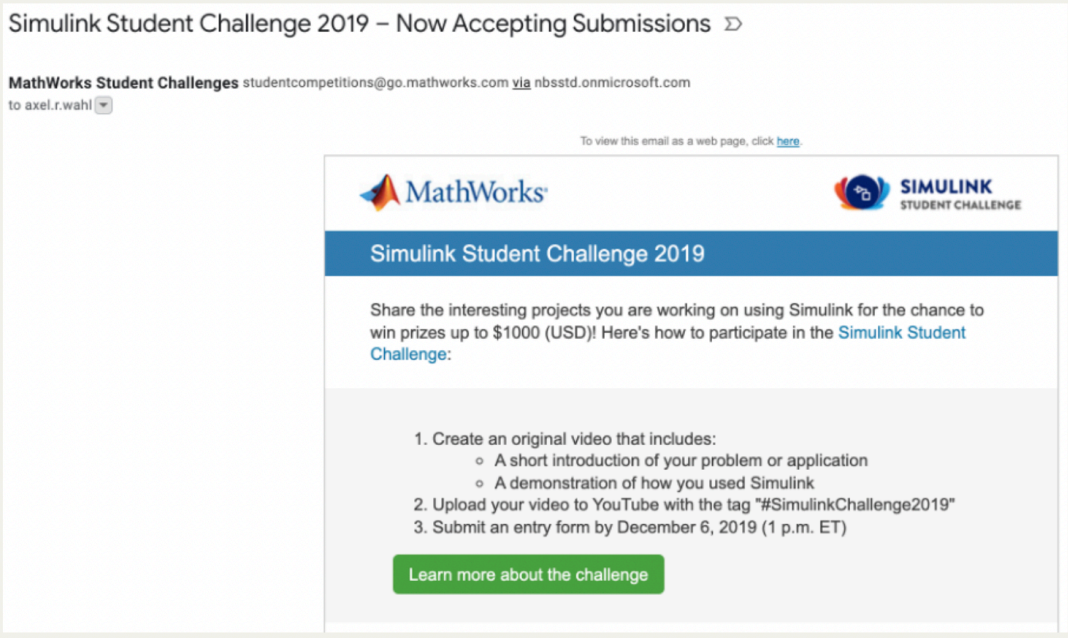


In this simulated phishing test you will be presented with 8 emails that someone has received. 5 of them are recognized as phishing scams and 3 others of them are recognized as secure emails. Your job is to recognize the ones that are secure to interact with and the ones that are a phishing scam. Good luck!



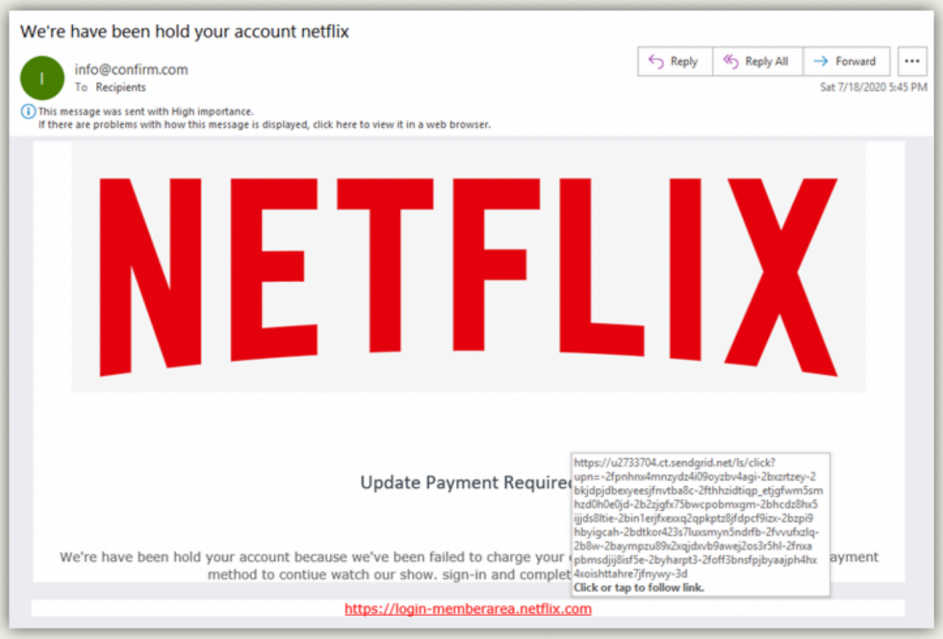
Secure

Phishing scam



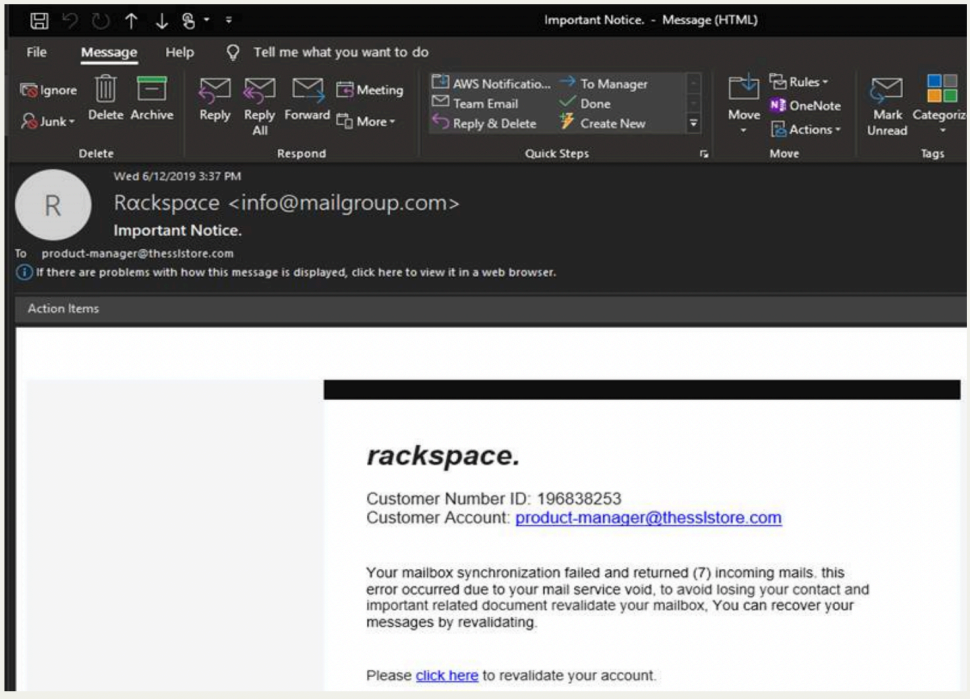
Secure

Phishing scam



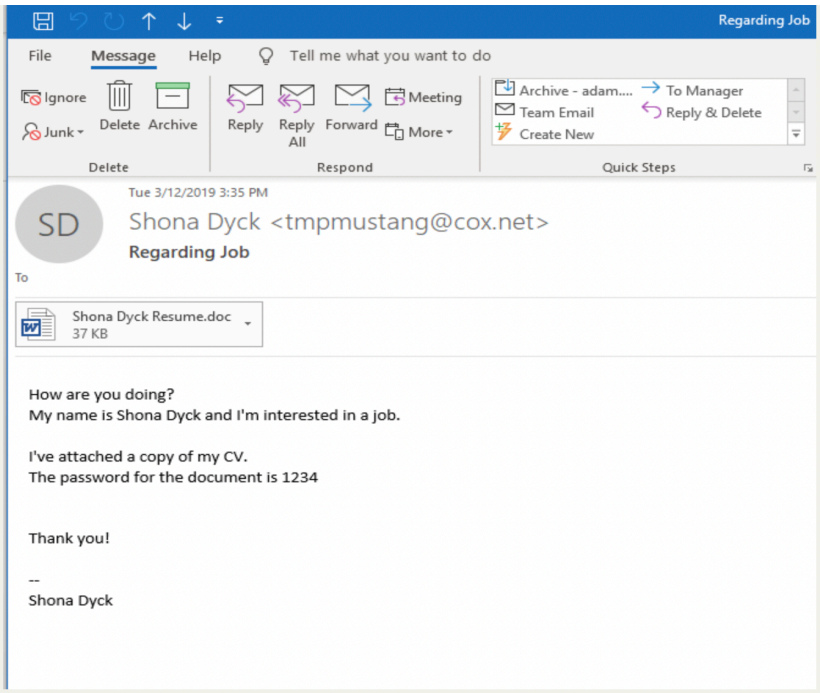
Secure

Phishing scam



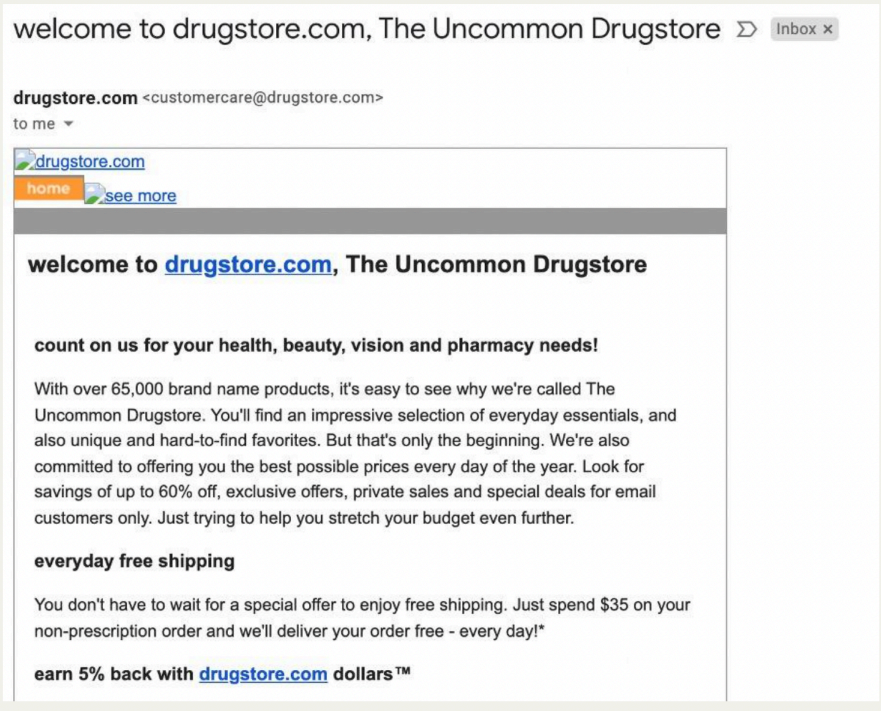
Secure

Phishing scam



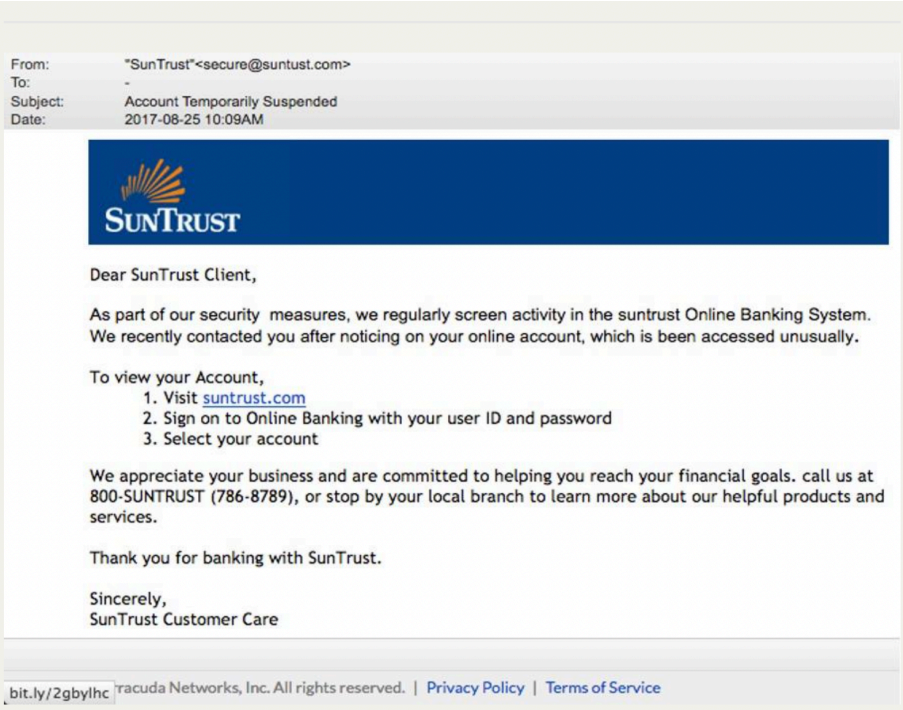
Secure

Phishing scam



Secure

Phishing scam



From: "SunTrust"<secure@suntust.com>
To: -
Subject: Account Temporarily Suspended
Date: 2017-08-25 10:09AM

SUNTRUST

Dear SunTrust Client,

As part of our security measures, we regularly screen activity in the suntrust Online Banking System. We recently contacted you after noticing on your online account, which is been accessed unusually.

To view your Account,

1. Visit suntrust.com
2. Sign on to Online Banking with your user ID and password
3. Select your account

We appreciate your business and are committed to helping you reach your financial goals. call us at 800-SUNTRUST (786-8789), or stop by your local branch to learn more about our helpful products and services.

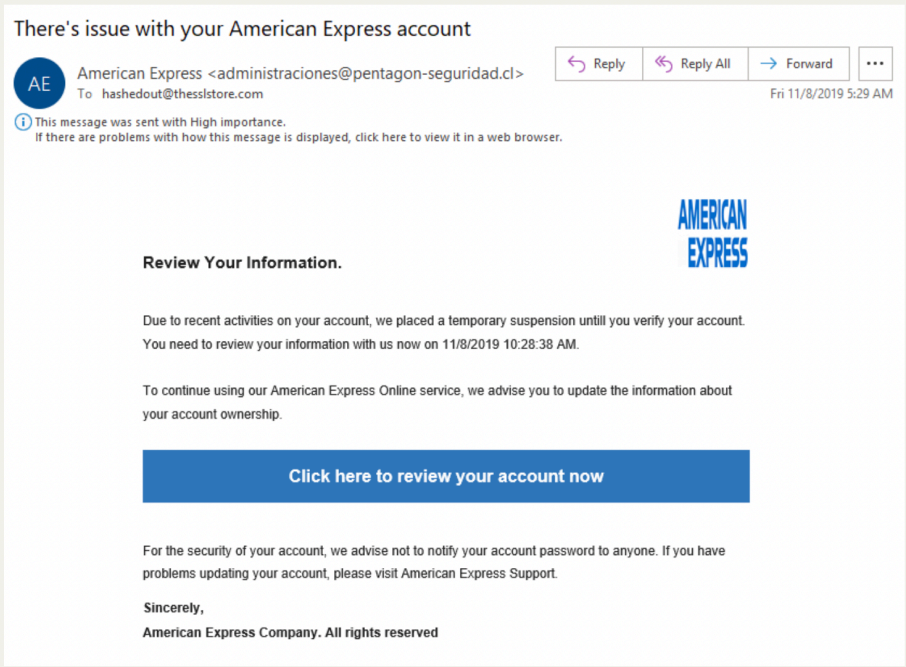
Thank you for banking with SunTrust.

Sincerely,
SunTrust Customer Care

bit.ly/2gbylhc racuda Networks, Inc. All rights reserved. | Privacy Policy | Terms of Service

Secure

Phishing scam



There's issue with your American Express account

AE American Express <administraciones@pentagon-seguridad.cl>
To hashedout@thesslstore.com

Reply | Reply All | Forward | ...
Fri 11/8/2019 5:29 AM

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.

AMERICAN EXPRESS

Review Your Information.

Due to recent activities on your account, we placed a temporary suspension untill you verify your account. You need to review your information with us now on 11/8/2019 10:28:38 AM.

To continue using our American Express Online service, we advise you to update the information about your account ownership.

Click here to review your account now

For the security of your account, we advise not to notify your account password to anyone. If you have problems updating your account, please visit American Express Support.

Sincerely,
American Express Company. All rights reserved

Secure

Phishing scam