UiA University of Agder

Master

An Analysis of Phishing Susceptibility Through the Lens of Protection Motivation Theory

REMI RUDI

SUPERVISOR

Wael Soliman

University of Agder, 2023
Faculty of Social Sciences
Department of Information Systems

Table of Contents

1 PREFACE 7
2 ABSTRACT 8
3 INTRODUCTION 10
4 BACKGROUND 14
4.1 Systematic Literature Review Methodology and Characteristics 14
4.1.1 Article Databases Used in This Thesis 15
4.1.2 Exclusion- and Inclusion Criteria 16
4.1.3 Literature Review Technique 18
4.2 Phishing Literature – what is phishing? 18
4.2.1 Types of Phishing 19
4.2.2 Common Theories in Phishing Literature 21
4.2.3 Data Gathering Methodologies in Phishing Literature 22
4.2.4 Demographics in the Phishing Literature 23
4.3 Protection Motivation Theory 24
4.3.1 The Creation of PMT and Common Occurrences 25
4.3.2 PMT in Information Security 26
4.3.3 PMT in Phishing 27
4.3.4 Versions and Extensions of PMT 27
4.3.5 How PMT Research is Lacking 28
4.3.6 Future Use of PMT to Explain Phishing Susceptibility 29
5 METHODOLOGY 30
5.1 Data Collection 32
5.2 Data Analysis 33
6 FINDINGS 35
6.1 Findings Supported by PMT 35
6.1.1 Intrinsic Rewards have Positive Effects on Protection Motivation 35
6.1.2 High Efficacy Decrease Uncertainty and Phishing Susceptibility 36
6.1.3 Low Response Cost Allows Employees to do Proper Security Checks 37
6.2 Findings Not Supported by PMT 38
6.2.1 Higher Perception of Vulnerability and Perception of Severity Does not Automatically Decrease Phishing Susceptibility 38
6.2.2 Lack of Fear Appeal Does Not Mean That Employees are Less Secure 39
6.3 Protection Motivation vs Protective Mindset 40

7 DISCUSSION 41
7.1 Theoretical Implications 41
7.2 Practical Implications 43
7.3 Limitations and Future Research 43
8 CONCLUSION 45
9 REFERENCES 46
10 APPENDIX 56
10.1 Appendix A – interview guide 56
10.2 Appendix B – Thematic analysis of interviews 58
10.3 Appendix C – literature review table 63
10.4 Appendix D 64

List of figures

Figure 1 Protection Motivation Theory as designed by Rogers (1983) – Appendix D……24

List of tables

Table 1 – information about the participants……33

1 PREFACE

These last written words of this thesis represent my battle that has been writing this master's thesis to complete my master's degree in cybersecurity at the University of Agder in Kristiansand, Agder. I have been writing this thesis since January until June of 2023. I have faced challenges during this time, and due to some unfortunate circumstances, they have not all been resolved. This thesis is my proof that I have been able to work whilst struggling, and that I have the capacity to work through hardship, and the capability to do that work well. Although this thesis could not have been completed without the support of the people around me.

For this, I would like to thank my supervisor Mr. Wael Soliman for believing when I did not and helping me continue a project, I have little love for. I would also like to thank him for the long conversations we had which created further understanding and conversations that created and kept a spur of motivation going until the very end. I would also like to give my friends a large thank you for believing in me and not allowing myself to completely sink. I would also like to share my feeling of accomplishment as we all have struggled with our own issues this past semester. Standing together, we are strong, and we are successful. Furthermore, I would like to extend my gratitude for my contact at the financial company which allowed me to gather data and has given me all the information I should ever need. Lastly, my family. This thesis would not exist without them. Thank you.

To the reader. I wish you the best as you are reading this.

Remi Rudi,
Kristiansand, Agder, Norway. 01.06.23 16:20

2 ABSTRACT

Users of communication tools are vulnerable to a cyberattack called phishing which aims to trick a recipient into giving away information or access that the attacker should not have. There is a great need to protect the recipient from becoming a victim of phishing. Protection can be done a multitude of ways; however, the human will be last barrier of entry when all digital protection fails. This is why anti-phishing training is used to enable email users to see the difference between real email and phishing attacks.

This research explores the use of Protection Motivation Theory (PMT) to analyse phishing susceptibility by interviewing ten employees in a large financial company. The analysis spanned all aspects of the original Protection Motivation Theory and sought to answer the research question: *"How do employees in a company protect themselves against phishing attacks?"*. Furthermore, the study investigated the relationship between the experiences of the participants and what the theory suggested would increase protection motivation.

The analysis resulted in findings that were consistent with PMT on the positive effects of rewards for employees to increase protection motivation. Furthermore, a low response cost led to a positive effect where employees had the freedom to properly examine the emails they received and handle them accordingly. Last finding that was consistent with PMT was the positive effect of high efficacy which led to the enabling of employees to make their own decisions based on their experience and knowledge. Surprisingly, findings also contradicted some core aspects of PMT. These include the perception of vulnerability and severity in combination with fear appeal. Although the perception of vulnerability and severity was high, the fear appeal was very low. This is inconsistent with PMT as high perception of vulnerability and severity should lead to high fear appeal. Most importantly, these findings suggest that fear appeal is not as necessary as research has proposed and that protective behaviour in the absence of fear appeal can be replaced by a protective mindset.

These findings point to important implications both in theory and in practice. The theoretical implications include the support of rewards and response cost positively affecting protection motivation if rewards are high and response cost is low. Another implication is that fear appeal contrary to peer-reviewed research might not be as important if the company itself focus on security and promote a healthy method of dealing with phishing attacks. The final theoretical implication is the protection behaviour that is a protective mindset. The concept correlates with

multiple different behaviours that promote secure behaviour; however, it does so by analysing the need of fear appeal and promote research which investigates protective behaviours without the need for PMT's version of fear appeal.

The practical implication of this study includes the promotion of a healthy protective mindset which can be achieved by anti-phishing training, phishing simulations, and voluntary high awareness when looking at emails. Furthermore, findings show that the financial company studied in this thesis provide a great understanding of secure behaviour and the requirements to achieve it. However, this is done by forcing training whilst experiencing organisational support and incentives to do well. Although it could seem harsh, this has worked well, and should continue to work well.

3 INTRODUCTION

As internet became more available, long distance communication became easy and accessible as soon as computers, emails, and messaging services were invented and made available to the public. Just as easily did scammers transform this available technology into a weapon that could ruin lives by mass sending requests to tens, hundreds, or thousands of people to transfer their life savings for the potential to receive even larger sums of money in return (Hong, 2012). The first phishing emails were invented.

To assume that phishing emails would stop as people caught on to them would probably be a naïve way of thinking. Phishing only grew as a concept and as a method of scamming people for money as smart schemes continued to flourish on the internet (Hong, 2012; Alkhalil et al., 2021; Abroshan et al., 2021). An increasing number of phishing emails were sent, and so did the number of phishing victims. Unfortunately, as phishing emails became more effective, so did the motivation to have more potential recipients. This made email lists a sought-after resource and even more attacks were made to different services that had a large user database with emails stored on them (Polakis et al., 2010). This further increased the range of phishing emails dramatically as it became hundreds of thousands or a million email addresses instead of thousands. This meant that if even one per cent of recipients gave a small monetary amount of $5USD, the scammer would receive $50.000USD. In other words, phishing stopped being effective at scamming people out of their life savings but remained lucrative as a mass-scam with small amounts of money as the goal.

Even though phishing emails have been used to gain money by tricking unsuspecting individuals, phishing has evolved to also trick individuals to gain access to a service used by them. This has been done by acting as a third party and asking the victim to provide their email and password because something was wrong (Rajivan & Gonzalez, 2018; Carroll et al., 2022). As people were warned about those attack methods, spoofing websites became a viable option as the attackers could visually copy a service website and collect data that was provided (Aleroud & Zhou, 2017). Unfortunately, spoofing websites never went away as they are still effective if used in combination with incredibly legitimate-looking emails (Aleroud & Zhou, 2017; Gupta et al., 2018). The goal of these scams is to access the service with the stolen credentials and use whatever the service provided.

As phishing attacks became more sophisticated, they also became more targeted. Phishing attacks evolved into what is called spear-phishing attacks which

aim to trick a specific user by using enough personalised information to make them believe that the email is real, and the contents can be trusted (Benenson et al., 2017; Burns et al., 2019). These emails often target high ranking employees or users with specific security clearances (Xu et al., 2023). This is to gain access to the back end of services or gain access to internally stored information. This can be devastating for any company that either stores personal data or use a system to contain and execute services and functions specific to that company. Another danger of phishing is not necessarily that the data is stolen, but rather that the data is locked down or inaccessible by the owners. The software installed to encrypt data and lock down systems is called ransomware and was very prevalent in the mid to late-2010s (Tandon & Nayyar, 2018; Bekkers et al., 2023). This software is often able to work due to the initial contact point to the back end being through phishing. Therefore, phishing is a major issue that should be addressed and avoided as much as possible. However, it is easier said than done to not be a target if you are part of an important infrastructure or a large company.

Due to the potential damage of a phishing attack, anti-phishing training and technical protective solutions such as email filters and machine learning are being utilized to avoid phishing emails and the risk of someone becoming a victim of phishing (Bhardwaj et al., 2021). However, this is not failproof and does demand attention and updates to work optimally. If put in a private context, most people will have less than optimal email security which leads to them receiving large amounts of phishing emails if their email has been in a compromised database as mentioned above (Harrison et al., 2016). This means that people using normal email services will need to be extra diligent when browsing their inbox. However, what could happen if phishing emails managed to bypass technical solutions and land in the inbox of a large and important company? There is a chance that a virus is spread around the company's private network and collect information or classified projects or gather and extract information. To avoid this, what must a company and their employees do to avoid such attacks? That is the research question this thesis will attempt to answer*: "How do employees in a company protect themselves against phishing attacks?"*.

Statements collected through interviews in the financial company will be used to answer the research question. It should focus on the employees and their experience and knowledge to accurately interpret the thoughts and actions behind their protective actions. Furthermore, the findings should highlight what the thoughts and actions are and why employees choose to protect or not protect themselves in a certain way. Finding parts of a solution could lead to a new understanding of how employees think when there is high risk of damage if someone falls victim to phishing.

The highlighted findings were both consistent and inconsistent with PMT. The first finding consistent with PMT is that rewards, both intrinsic and extrinsic, have

positive effects on protection motivation. This is based on the employees' opinions and feelings that an intrinsic reward in more motivating than an extrinsic reward. The intrinsic rewards are obtained through passing phishing simulations and completing anti-phishing training. The rewards themselves are receiving a digital trophy along with a "security champion of the month" title and confirmations through email when the participants correctly identified phishing email and either reported or deleted it. This was the opposite of the assumption made beforehand and was an interesting finding.

The second finding was that high efficacy decrease uncertainty and lower phishing susceptibility by improving the confidence employees have when deciding to click on an email, report, or delete it. The high efficacy stems from the training and experience the employees receive. However, it also comes from the freedom employees have available to report everything they find suspicious. This is an efficient way of processing emails without risking being phished. If the reported emails are legitimate, they are returned to inbox. No damage has occurred, and the employee did not waste time checking the validity of the email for longer than necessary.

The third finding that was consistent with PMT was that low response costs allows employees to do proper security checks. In this company, there are no response costs when checking emails as there are no resource limits put in place. Instead, the resource limits are restricted by the employees themselves and administered by themselves. However, an interesting result is that most employees spend at most 20 seconds when checking the validity of an email. If the contents are relevant, but the email does not seem credible, they will report the email and receive a confirmation from the security team letting them know the status of the email instead of risking being a victim of phishing.

A finding that was not consistent with PMT is perception of vulnerability and severity. The two aspects are normally able to decrease phishing susceptibility by increasing the fear appeal. However, participants had different views on the perceived vulnerability and severity in addition to being and not being a phishing victim. Put simply, there were participants who thought of phishing as a very dangerous threat that could trick them who had been phished, and participants that had not been phished. The same happened to the participants that thought phishing was an annoyance and believed that they would not get phished. Multiple participants have gotten phished before, and multiple participants have not. This leads to an inconsistency that PMT does not consider.

The last finding was that a lack of fear appeal does not mean that protection motivation decrease. This is a contradiction to PMT and is not supported. This was the most surprising finding due to the expectancy of fear appeal being necessary to create protection motivation. This also caused a discussion about the need of fear appeals and if employees can protect themselves without being afraid whilst

looking at email. The practical implication of this is that protection motivation without fear appeal is a protective mindset which is more of a passive state of being constantly aware of dangers rather than relying on fear to notice the threat of an email.

The contents after this introduction delve into the background of phishing and protection motivation theory to explain what the research have previously found and be the basis for knowledge and expectations for this thesis. Furthermore, the method of how the data will be collected, and who data will be collected from is the next point of interest before the data itself is analysed and presented as findings. After the findings are presented, they will be discussed and compared to phishing and PMT literature. At this stage, theoretical and practical implications will be presented before the limitations and possible future research. At last, the conclusion will be presented to end the thesis.

4 BACKGROUND

The background section will consist of the most common research methods and theories in the general phishing literature. Furthermore, it will contain a breakdown of Protection Motivation Theory as used in this study. The list of articles used for this literature review can be found as appendix C.

4.1 Systematic Literature Review Methodology and Characteristics

The purpose of this literature review is to achieve a general overview of the literature presented by other researchers on the topic of phishing. The process of finding articles required the use of multiple article databases and their search engines. Furthermore, specific search terms were used to narrow down searches to exclude articles that did not exclusively focus on phishing, but for example general cybersecurity instead. Furthermore, relevance was focused on by limiting the use of articles that was released more than 10 years ago. Phishing literature, attack techniques, and the understanding of human behaviour has been improved greatly just the last decade, therefore, looking at literature prior to 2013 may result in finding opposing conclusions to similar issues that has been proven to be inaccurate in newer literature. Finally, different filtering methods were used to decrease the number of irrelevant articles.

The characteristics of the literature review based on Cooper's Taxonomy of Literature Reviews model (Cooper, 1988) includes focus, goal, perspective, coverage, organization, and audience. These characteristics was explored further by Randolph (2009) and explain in stages how a literature review can be done in practise. The characteristics of this literature review can be explained by the same parameters as mentioned by Randolph (2009). The focus of this literature review is to find the main theories used in the general phishing research literature. In addition, and as a biproduct, the focus will also be on the research methods used, the researched participants, and what kind of phishing that is most prevalent in research (e.g., email phishing, spear-phishing, SMiShing (SMS phishing), social engineering by phone, spoofing websites etc.). The main goal is to generalize the research and identify the central issues presented in the research. There will also be a small critique of the main theory studied throughout this thesis. My own perspective will be attempted to stay neutral throughout the thesis as the results will be based on what worked and what failed in the theory. Any critique of any theory will be in

the perspective of "how could the situation have ended differently whilst using this theory" instead of "this theory created the potential for failure and is therefore not valid or usable". Therefore, there are no known personal biases towards any phishing theory.

The method of coverage is a representative sample of phishing literature. Randolph (2009) explains this technique as "far from fool proof", and I must agree. However, under no circumstances will an exhaustive coverage nor a central coverage truly be the best option for this thesis. An exhaustive coverage would require multiple researchers and months of time to complete, and a central coverage would not cast a wide enough net to properly find the exhaustive and slightly unique theories that are used in phishing literature. Therefore, a representative sampling cast the widest net with the least chance of being biased in the representation of phishing literature. On the topic of representing the literature is also how the literature is organized in the paper itself. There are three ways of organizing information, by presenting information in a chronological format, conceptual format, or methodologically meaning splitting the information into chapters. It is further specified that organization of information does not need to be exclusively one method. Therefore, this literature review will use a methodological organization of information, splitting the chapters into concepts, and presenting the contents of each concept in chronological order. In other words, using all three methods. The last concept of a good literature review is who the target audience is. Randolph (2009) explicitly recommends that a dissertation such as a master's thesis is written with the supervisor and reviewers in mind, scholars second, and not focus on the general non-academic audience. Therefore, the literature review will explain all concepts that are specific to phishing and the main theory but avoid explaining concepts that are generally understood to be standard practise or common knowledge within the research community. The purpose of this literature review is after all to be informative for those who are already familiar with concepts associated with information security.

4.1.1 Article Databases Used in This Thesis

There are many article databases out there which works as a search engine. An example of this is "google scholar" that in most cases search the whole web for article databases and return all relevant articles defined on the search. In the case of phishing, google scholar returns 124 000 results with the search term "phishing". This is decreased to 37 700 articles when limited to 2013-2023. By searching ""Phishing"" (phishing in single quotes), the results are still 36 500 relevant articles. By limiting the search to force the use of "phishing" in the title results in 5320 articles. The number of articles available are still too many to effectively be used

as a methodology for a master's thesis literature review. Instead, article databases with more filtering are the solution.

Article databases with many options for filtering are plentiful, but some have more reading restrictions than others, even with university access. Therefore, the choice of which databases to use was quite simple. There were six main databases; ScienceDirect, SpringerLink, Wiley Online Library, IEEE Xplore, Informs PubsOnLine, and AIS eLibrary. These databases all platform different publishers and would therefore cover the most relevant InfoSec publishers. Another main feature of all databases mentioned is the filtering system. These filters help the reader find articles that will be relevant. Some simplifying filters are publishing year, discipline, subdiscipline, publisher, and article type. In combination with keywords and search terms, every search could be narrowed down to create specific niche results. ScienceDirect is the database which returned the largest number of articles on first search. By searching "phishing" and filtering for subscribed journals, the number of articles were 2965. By searching "phishing" as a keyword, limiting the publishing date to 2013-2023, subscribed journals, research articles, and no subject limitations, only 228 articles were shown. However, 228 articles are still many, therefore, exclusion criteria were introduced.

4.1.2 Exclusion- and Inclusion Criteria

Exclusion criteria is used to validate the quality of an article. The criteria are in this case based on the information needed for the thesis, and phishing is the most important aspect of this literature review. One quick-check criterion was that the article in question must have mentioned the word "phishing" at least 20 times. This is to exclude the articles that only use phishing as examples of cybercrime or social engineering. However, this literature review calls for phishing specific literature as validation for mapping out phishing in research literature. One finding was that most phishing focused studies included the word "phishing" 80+ times, even in a short article. However, articles that contained "phishing" as an example used the word less than 25 times. Therefore, the exclusion criteria of minimum 20 instances of "phishing" in an article was quickly changed after reading less than 10 articles and increased to produce more relevant articles. Doing the same thing for all the other databases resulted in effective and high-quality results.

Another exclusion criterion is time of publishing. Because the task was to find what the current literature says about phishing, there would be no point going back to before phishing was considered to be a severe threat to security. Due to the explosive development, methods used for phishing in 2023 are more advanced than ever as most people become more aware of poorly written emails, fraudulent SMSs, and spoofing websites. Therefore, attackers also evolve and focus on the

personal parts of emails to create more legitimacy and have a larger chance of tricking the victim. Looking at Dodge et al. (2007), the phishing example use an unnatural spoofed university email, ask the student to fix an issue with an assignment submission using a link, and refer to an address that does not exist. Due to information availability, an address would be very easy to confirm, an email could be spoofed much easier using publicly available university emails, and links could be hidden in an attachment where "a professor" has sent them the assignment in question. Of course, there will always be victims that get phished using 10+ year old methods with the same grammatical and contextual errors included. However, phishing today may very well be hidden in the spoofing website that a link refers to, not the email itself. Kelley et al. (2023) tested a spoofed version of amazon.com, and only those with strong analytical reasoning or great memory recall of how the webpage is supposed to look at succeeded most of the time. However, this is only possible when the participants have real prior knowledge about phishing. As this would not be the case for most people in 2013, the criterion persists.

The last exclusion criterium was to avoid the technical articles that exclude the human in phishing susceptibility. These articles mainly focused on the algorithms that detect and handle phishing emails before they arrive at the computer user. This is mainly to increase the focus on the human phishing detection and theories that explore the human behaviour. Although anti-phishing tools mostly run in the background unseen by anyone other than engineers, there are anti-phishing tools that actively and visibly help users detect phishing and improve their ability to do so. However, such articles often discuss whether a user fully gain an advantage in detecting phishing emails or if such tools could be a hinderance. An example of this is Schuetz et al. (2022) who found that users will not fully trust anti-phishing tools, and if the user experience inaccurate information provided by the tool, the level of trust plummet. There are also cases where the users do not trust the tool because of the lack of transparency which in turn led to an underutilization and misguided use of the tools and their features (Schuetz et al., 2022). Because some tools are visible to the users and directly affect how they act when receiving an email, those studies are applicable to the thesis, however, invisible anti-phishing tools which do not affect human behaviour are irrelevant and excluded from the thesis and literature review.

On the other hand, an inclusion criterion is that the paper must be written in English or Norwegian as that is the only two languages I understand. The paper must also have at least one clear methodology which could be an experiment, qualitative research, quantitative research, or theoretical study where the result is based on data from other research articles. The articles must also include which group the participants can be categorized in and how many participated. Grouping participants in this context means either their place of work, personal characteristic, or another commonality between the participants. The article must be published,

and peer reviewed by a known and credible journal such as journals from the Senior Scholar's Basket of Eight to provide legitimacy to the article. Lastly, the more citations an article has, the larger chance it must be included. This is not an inclusion or exclusion criterion; however, the number of citations does provide a general guide to whether the article has been contested or iterated upon. Although citation can be a guide, it does not provide enough information alone to the relevance and quality of the information it contains. An article from 2023 has not been published for long enough for others to both have taken notice AND published an article of their own with it as a reference. Therefore, articles with a lower number of citations shall not be discriminated against on that basis alone. Based on the exclusion and inclusion criteria, articles should be sortable by another person and generate the same secondary list from the initial first search spanning 163 articles.

4.1.3 Literature Review Technique

The result of the literature review and search ended up being 65 articles with direct relevance to phishing. This was accomplished by searching the mentioned databases, applying filters, applying exclusion criteria, and removing duplicates. Some articles were also found by snowballing from article to article and was therefore not found by using a database. Snowballing is a technique used to search the references in an article to find similar and relevant information (Wohlin, 2014; Jalali & Wohlin, 2012). However, articles can only reference older information, therefore, snowballing forwards by looking at citations, or secondary use of an article has also been a useful technique to find newer information on the same topic. Most databases have a feature that allow the reader to see the articles citing a primary source, therefore, allowing the reader to follow a paper trail to newer information. This is a proven method of finding relevant and related research and has worked well whilst finding research for this thesis. However, as researched by Jalali & Wohlin (2012), database searches did find many research articles that snowballing did not catch. As a result of this, both database searches and snowballing were used to find the 65 articles that ended up being a portrayal of modern phishing literature.

4.2 Phishing Literature – what is phishing?

Phishing is an invasive and malicious technique to trick victims into giving something to the attacker through digital means, not knowing that the result is a loss of control or assets (Luga et al., 2016; Butavicius et al., 2015; Rajivan & Gonzalez, 2018). Many researchers and governments have tried to find a way to make

phishing an inefficient tactic to swindling people, but no one has found an absolute method of hindering phishing attacks. However, there are many methods used to limit the effectiveness of phishing and create awareness amongst people to avoid phishing attacks (Zhao et al., 2017). These are methods such as anti-phishing training, phishing susceptibility theory, and reward/punishment methods (Zhao et al., 2017; Musuva et al., 2019; Jaeger & Eckhardt, 2020; Junger et al., 2017). To unveil the usefulness of these theories, this literature review will contain a synthesis of how the theories are used in practise.

Phishing is a plague to everyone on the internet trying to do legal and legitimate business. Everyone must receive a vaccine to limit the efficiency of this plague and in the future, eradicate it. However, as of now, the vaccine takes form in two different shapes: anti-phishing training (APT) and technical defences (TD) (Bhardwaj et al., 2021; Gupta et al., 2017). The focus will be on APT; however, TDs are the first lines of defence that should filter out most unwanted e-mail, but already in 2012 there were many ways of bypassing TDs and receive phishing emails (Parmar, 2012). However, TDs may introduce positive reactions to the use of email filters (Martin et al., 2021), but can also create distrust in email filtering systems (Butavicius et al., 2020). The significant factor to trust in email spam- or phishing filters is accuracy (Martin et al., 2021; Butavicius et al., 2020; Schuetz et al., 2022). When accuracy in spam filtering is low, the trust in the filter itself is decreased. Although, even if the accuracy of tools is 100%, not all users would trust them (Schuetz et al., 2022). Then, what is the solution? Either create perfect email filters or create perfect APT that makes all humans able to detect phishing scams 100% of the time. Unfortunately, neither has been done yet, so maybe the answer is a combination of the two.

Does the perfect APT exist, and are humans capable of using a method perfectly 100% of the time? The perfect APT could be the inclusion of every theory in existence alongside days and weeks of practise, or it could be to always have emails manually checked by professional anti phishing email checkers. The idea of a perfect defence is a utopian fantasy if there are malicious actors in the world. Therefore, the solution beyond TDs could be to prepare for a breach and follow general policy advice from researchers and security companies that provide data to back up their advice. Most defences will depend on the type of phishing, therefore, the is not a single solution that can be perfectly used to avoid all phishing attempts.

4.2.1 Types of Phishing

There are many types of phishing using social engineering methods (Krombholz et al., 2015; Bhardwaj et al., 2021; Aleroud & Zhou, 2017; Gupta et al., 2018). As mentioned earlier, this thesis will cover the social phishing technique: email

phishing. However, other social phishing types are website spoofing, vishing, SMiShing, and spear-phishing (Bhardwaj et al., 2021, Gupta et al., 2018). Although many of these phishing techniques exists, not all are researched to the same degree. Of the 65 articles found during the literature review, 31 articles focused specifically on phishing and spear-phishing, 5 focused on spoofing websites, 7 focused on the general concept of social engineering, and 22 focused on phishing as a general concept. Based on these findings, most articles focus on email phishing or the general concept of phishing. Email phishing is also the greatest threat of all social engineering methods due to the ease of sending emails loaded with malicious content. After all, phishing can target anyone with false links to spoofing websites, links that contain a fraudulent payment request, attachments that infect the device, or attachments that tries to copy a part of the device such as browser access tokens that allow the malicious actor to visit a website logged in as the victim without needing authorisation information (Singh & Chaudhary, 2022; MITRE ATT&CK, 2023).

A second version of email phishing is spear-phishing by email. Spear-phishing works on the same principle; however, the goal is to create an email with enough personal information to trick an advanced recipient or trick the recipient to do an advanced action (Parmar, 2012; Gupta et al., 2017; Butavicius et al., 2015; Xu et al., 2023). According to Xu et al. (2023), 97% of those specifically targeted by spear-phishing fall victim to the attack. A spear-phishing email would normally use information not specifically available by the easiest search request in a search engine. Although, emails with simple information may trick many, an email with a personal tone, use of specific names or titles, has genuine and correct language, has correct greeting and ending to the email, somewhat correct or spoofed email address, and on-topic or relevant content is needed to trick those who are in higher positions of power or of important status to an organization for example army personnel (Xu et al., 2023; Burns et al., 2019; Krombholz et al., 2015). The spear/phishing attacks that specifically target high value or high-status victims is also called whaling and is used to gain access to accounts or information from high/ranking individuals (Gupta et al., 2018; Krombholz et al., 2015). Spear-phishing is a high threat high reward method of attacking someone, however, it does take a lot of resources and time to create an effective spear-phishing campaign and is therefore less used. On the other hand, spear-phishing is more effective than normal phishing, therefore, being a large threat to victims of large responsibilities.

Another social engineering technique is spoofing websites that does not require the specific use of phishing emails. A specific example is to create a website with an easy-to-make writing mistake URL that looks very similar to the real website. Luga et al. (2016) refer to a specific case where a webpage named “faceboook.com” was created to scam legitimate “facebook.com”-users to give away their email and password (Aleroud & Zhou, 2017; Bhardwaj et al., 2021). There

are many ways that the technique would not be effective due to two-factor authentication such as email or SMS verification, or an app authenticator. However, because many reuse their passwords, malicious actors may try the same email and password on other sites that may end up working. Emails may also be collected and added to a spam list used to send out more phishing emails to trick the same victims again. This is also one of the reasons for why large corporations often own similar website URLs to their original such as “gooogle.com” or “gogle.com” which will redirect to “google.com”. Therefore, website spoofing is an effective way of scamming victims and should be researched further.

4.2.2 Common Theories in Phishing Literature

Amongst the 65 articles, not every article used a specific theory to show their research, nor did many articles use the exact same version of theories. Amongst the most important theories and themes are:

Theory of planned behaviour (4)
Protection motivation theory (4)
Cognitive processing theory (5)

Other patterns also emerged and resulted in 49 articles that studied human behaviour. Within the theories that studied behaviour were many similar theories to the three highlighted ones, although enhanced, built on, or changed. Many articles as mentioned also took a holistic approach to a theme and studied susceptibilities, social engineering, or training. There were also multiple articles that studied and explained the phishing taxonomy of which there was a pattern of an increasing number of methods that are viable attack-methods as time has passed (Gupta et al., 2018; Bhardwaj et al., 2021). Overall, the most common and prevalent theories in phishing research ended up being theory of planned behaviour, protection motivation theory, and cognitive processing theory where all have a common focus of processing own behaviour and acting upon the analysed result (Grassegger & Nedbal, 2021; Vrhovek et al., 2023; Chen et al., 2021; Jaeger & Eckhardt, 2020; Singh et al., 2023; Harrison et al., 2016). Although these are the major theories, there are still a distinct lack of research done specifically within phishing. Searching SpringerLink and using the keywords “protection motivation theory” and “phishing”, 23 results appeared. However, almost all results used phishing as examples and was not the focus of the research. The same result unfolded as another 21 articles appeared when using “theory of planned behaviour”, and 41 results for “cognitive processing”. However, these results are a testament to the frequency of use of each theory within the phishing research/phishing cybersecurity subject. Furthermore, the three theories are well established in multiple genres of research where

behaviour is an important factor. These genres vary from covid-19 vaccine psychology (Griffin et al., 2022; Wen & Liu-Lastres, 2022) to self-protection from torrential rain and floods (Banerski & Abramczuk, 2023; Kakimoto & Yoshida, 2022). Due to the way these theories explain human behaviour, one resulted in being an appropriate fit for the research method to be used in this thesis. That theory was protection motivation theory.

4.2.3 Data Gathering Methodologies in Phishing Literature

Four research methodologies were used to collect and process data in most articles found during the literature review. These were quantitative (19), qualitative (5), experiments (36), and theoretical studies (7). Quantitative is meant as a survey-type information collection methodology without study control (Cobo-Sánchez & Blanco-Mavillard, 2020). This could either have been done using a descriptive or analytical method of approach which targets one of many types of studies (Cobo-Sánchez & Blanco-Mavillard, 2020). The other type of quantitative study is experiments which includes and focus on a study control (Cobo-Sánchez & Blanco-Mavillard, 2020). These two quantitative studies are a large majority of research methods used in phishing research.

Theoretical studies in this context are meant as studies that does not use primary data, but instead use data from multiple different studies done by others. These studies are mostly used as an argument to why a relation or conclusion exist based on the referred sources. These are often found in literature reviews, but also in the case of Abbasi et al. (2021) where they used multiple results from studies to create a theoretical model, in this case “the phishing funnel model”. The model is untested in the specific paper, therefore, being a theoretical study with a theoretical model using real collected data to create it. A theoretical study can also be a paper where something is proposed but unvalidated. This is not by any means a negative opinion on theoretical studies, but rather an observation to classify studies that are otherwise very different to quantitative and qualitative research studies.

Qualitative research that focuses on the individual and their beliefs and experiences (Bleiker et al., 2019), however, are not widely researched. This can be construed as a lack of qualitative research in phishing, or just that contacting phishing victims is too difficult and a huge liability challenge in accordance with GDPR and personal data. Another ethical dilemma connected to interviewing victims is exactly that. Victimization. A study found that police officers were prone to PTSD, secondary trauma, and burnout when they saw reports of a traumatic experience in the news (Perez et al., 2010). Therefore, it can be argued that there is a chance of secondary trauma when interviewing phishing victims to specifically recall how they became victims and the causes of the successful phishing attack. however, if

done in accordance with ethical principles, any issues relating to trauma should be solvable by having participants willingly join the study. Therefore, any established researchers should be able to find participants to further studies and research questions that require interviews or other personalised information gathering processes. However, because of the lack of qualitative research on this topic, this thesis would have explored protection motivation theory in relation to phishing victims using a qualitative research approach. However, due to the same issue as other researchers who cannot get in contact with enough phishing victims, this thesis will focus on phishing susceptibility through the lens of protection motivation theory.

4.2.4 Demographics in the Phishing Literature

The participants in phishing literature are often not varied. This is based on an unfortunate reality where the easiest source of information for researchers in most cases will be students either on their own university or other universities. Students and faculty staff are the main participants in 27 studies. An upside to using students and faculty staff is that the potential number of participants is very high, but the variety is very low. An excellent example where using students resulted in many participants is Sutter et al. (2022). They managed to have 31940 participants responding to 288000 phishing emails. These statistics would be exceptionally difficult to achieve by polling, surveying, or experimenting with in large corporations or organizations. Therefore, students and faculty staff does provide an exceptional opportunity for researchers to gain accurate information that could reflect the general population as well.

Another group of participants are based on work sector. This could be healthcare, mechanical engineering, economics, or IT. These are studies that specifically relate to the sector in questions and finds related conclusions to help the specific sector solve an issue. An example is Gordon et al. (2019) who sent 2.9 million emails during an experiment on US healthcare employees. They found that 1 in 7 healthcare employees clicked on phishing links which is a large risk for hospitals all over the US. This study helped the healthcare sector specifically realise that something had to be done with their employees' phishing training to decrease the risk of a successful phishing attack.

A third generalisation of participants are online survey sites such as Amazon's mechanical turk which is a crowdsourcing marketplace (Singh et al., 2023), SurveyCircle (Grassegger & Nedbal, 2021), and Qualtrics (Butavicius et al., 2020). These participants are often randomized users on the different survey sites and marketplaces that answers surveys for fun or for a small reward. Therefore, the background of each participant is difficult to determine, however, a method like this does form a group of participants that could represent the general population.

The participants are quite varied in the literature if not a bit too skewed towards university students and faculty staff as participants.

4.3 Protection Motivation Theory

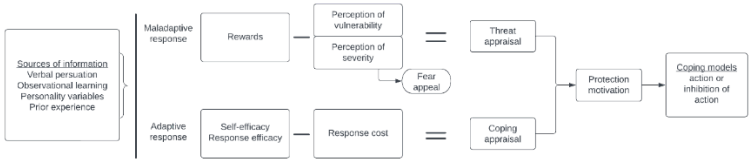

Figure 1 Protection Motivation Theory as designed by Rogers (1983) - appendix D

A major theory used to avoid phishing attacks by promoting protection motivation is protection motivation theory (PMT) first created by Rogers (1975) but revised and used in practice by Rogers (1983) later. The theory has an expectancy of people to protect themselves from threats and change their behaviour to do so (Rogers, 1983; Chenoweth et al., 2009; Herath & Rao, 2009; Vance et al., 2012; Haag et al., 2021). Further research on PMT uncovered two possible outcomes from fear and threats of danger. Haag et al. (2021) refer to their model which introduce coping modes as adaptive coping and maladaptive coping whilst Bax et al. (2021) refer to the two results as protection behaviour and maladaptive behaviour. Adaptive coping and protection behaviour refer to the same protective result, whilst the remaining two results refer to maladaptation where the person experience fear do not cope or change their behaviour to protect themselves (Haag et al., 2021; Bax et al., 2021). The reaction fear is also referred to as “behavioural intention” (Ajzen, 1991; Chenoweth et al., 2009; Herath & Rao, 2009; Johnston & Warkentin, 2010; Anderson & Agarwal, 2010; Vance et al., 2012; Herath et al., 2014; Tsai et al., 2016). In a phishing context, Bax et al. (2021) confirmed that a higher individual perception of threat will cause a bigger emotional response and thus create a higher motivation for self-protection and adaptive behaviour. Dang-Pham and Pittayachawan (2015) also confirmed that high self-efficacy served as motivation for students to protect themselves from malware. However, more students trusted their network at home and would be less attentive to avoid malware on home-networks (Dang-Pham & Pittayachawan, 2015, p. 293). In an extended model including the theory of habit, Vance et al. (2012) found that habit has a significant effect on compliance with information security policies (ISPs) which could include policies regarding phishing response and susceptibility. Another main finding was that unless ISPs was ingrained well as a habit, thus proving high response efficacy, a slight inconvenience in productivity or quality of work would

revert self-efficacy and decrease the motivation to protect themselves (Vance et al., 2012, p.194).

The revised version of Rogers' (1983) version of the protection motivation theory model contains eight factors. A change from Rogers (1975) is the introduction of self-efficacy as noted by the authors themselves which affect the response probability of protection motivation (Rogers et al., 1983). The adaptive response states that response efficacy and self-efficacy increase the probability of protection motivation, whilst response cost does not. Whether the self-efficacy is high enough to overcome the response cost is decided in a coping appraisal *which evaluate the ability of the person to cope with and avert the danger* (Rogers et al., 1983). The maladaptive response is affected by rewards and the perceived severity and vulnerability which also create fear arousal. Whether or not to participate in protection motivation is decided in the threat appraisal stage where the decision of the severity of the threat is large enough to motivate self-protection. Reasons for why protection motivation is relevant is due to the sources of information which leads to the responses, appraisals, and coping methods associated with PMT. The sources of information may stem from either environmental or intrapersonal background where verbal persuasion and observational learning are environmental sources of information, whilst personality variables and prior experience is interpersonal sources of information (Rogers et al., 1983). The last aspect of the PMT model is the coping modes which would be the result of previous information and the appraisals that is done throughout the interaction or situation. The coping modes can vary from one act to multiple or repeated multiple acts depending on the protection motivation. The protection motivation could lead to either action or inaction to self-preserve and self-protect and marks the end of the protection motivation theory schema.

4.3.1 The Creation of PMT and Common Occurrences

PMT was revised by Rogers (1983) to be used in psychology and has been used in psychology since the 1990s (Heise et al., 1997; Thompson, 1997; Burgess & Wurtele, 1998). Since 2000, PMT has been used in a multitude of subject areas. Using ScienceDirect and searching "protection motivation theory" as a keyword, social sciences (140), environmental science (76), business, management, and accounting (65), computer science (61), and psychology (55) are the five subject areas where PMT is most prominent. The theory has been used to explain certain motivations for solving for example a health issue such as smoking (Yan et al., 2014), educating youths about distracted driving (Carter & McBride, 2015), or protection from or protecting the environment (Dang et al., 2014; Tapsuwan & Rongrongmuang, 2015; Keshavarz & Karami, 2016). However, the theory has

been used much more since the Covid-19 pandemic broke out in 2019/2020 and has been a commonly used theory to explain protection behaviour in multiple different subject areas. Before 2019, PMT used to be the main theory used in about 15 articles each year according to the ScienceDirect database. However, in 2019, the number rose to 28, in 2020 the theory was used 27 times, and the year after in 2021 it resulted in 46 articles. In 2022, PMT was used in a record amount of 62 articles in one year and has been the topic in 31 articles as of May of 2023. This shows that although PMT started as a theory in the subject area of psychology, it has been shown to work in many other areas of interest where the goal is protection motivation.

Every article database has its own focus and its own publications. Therefore, using another database can result in widely different results in terms of common occurrences of PMT. SpringerLink, another well-known article database gives a result of 385 articles containing the exact phrase “protection motivation theory” within the “medicine and public health” subject area. The subdisciplines further proves that PMT is used in various health related research varying from medicine (220), public health (217), and psychology (147) to epidemiology (114) and environmental health (102). Furthermore, other subject areas using PMT in articles published by SpringerLink are business & management (64), earth sciences (51), specialised psychology (49), and environment (43). Therefore, it can be argued that PMT is a theory that can analyse the ingrained actions humans take to self-protect and is proven to be a reliable method to anticipate the resulting actions someone might make in accordance with affecting factors. However, the theory can also explain the behaviour related to protecting other things such as the environment (Chen, 2020; Badsar et al., 2022) and explain behaviour affecting businesses (Cismaru & Lavack, 2006; Nelson et al., 2011; Preßler et al., 2022).

4.3.2 PMT in Information Security

PMT has been actively used to improve security behaviour in various contexts and situations. The main goal has been to promote the understanding of security intention, secure and compliant behaviour, cyber security awareness training, and improving cross-cultural security behaviours (Verkijka, 2018; Ogbanufe et al., 2023; Khan et al., 2023; Thompson et al., 2017; Menard et al., 2018; Abraham & Chengalur-Smith, 2019). This is done by different means often related to fear appeal (Vrhovec & Mihelič, 2021; van Bavel et al., 2019) or self-efficacy (Verkijika, 2018; Boss et al., 2015). Bax et al. (2021) mention the roles of rewards and response costs to self-protect and have protection motivation. PMT has been used by multiple authors in information security to fully apply protection motivation to information security and is, based on peer-reviewed studies, an effective method

of improving all PMT-relevant aspects of cyber security (Shillair et al., 2015; Jansen & Schaik, 2018).

4.3.3 PMT in Phishing

Although PMT has been used in major parts of information security and is a well-established model used in healthcare and multiple other subject areas, the model as described by Rogers (1983) has faced many alterations, versions, and extensions to be used in phishing. There are multiple literature reviews focusing on either phishing or PMT without any significant crossover. An example of this is Haag et al. (2021) which focus on PMT in information systems security research where "phishing" is only mentioned as contextual examples. In addition, as previously stated in the theory part of the literature review, there are not many articles that compile and compare theories used to analyse phishing behaviour at all. However, individual articles mostly discuss how PMT can be used to improve online security behaviour (Bavel et al., 2019; Shillair et al., 2015; Bavel), apply information security training (Meso et al., 2014; Ogbanufe et al., 2023), and fear moderation (Vrhovec & Mihelič, 2021; Boss et al., 2015) to mention some themes. This does not mean that PMT is not used in phishing literature, however, it does mean that it is not very prevalent or that PMT require modification to be applicable in phishing research.

4.3.4 Versions and Extensions of PMT

Although PMT does not occur frequently in research the exact way Rogers (1983) designed and revised the model, enhanced, and extended versions are used to better explain the concepts of phishing attacks that the original model was unable to do. These include looking at maladaptive behaviours first researched by Witte (1992,1994) who looked at the failing fear appeal in earlier research and continued development on the Extended Parallel Process Model (EPPM) which focus on the success and failure of fear appeal regarding threats. This has been further developed and used in the context of phishing by Wang et al. (2017). They extended EPPM to include a large focus on successful coping, adaptive and maladaptive coping responses, and the role of negative emotional arousal. Another research group who used the EPPM is Bax et al. (2021) who found that rewards and response costs greatly affect the maladaptive and security behaviour in response to phishing emails. A different case is Bekkers et al. (2023) who studied the effect of the EPPM in the "*motivations of entrepreneurs to take future protective measures against cybercrimes"*, more specifically ransomware which often require some

sort of phishing attack to be successful. These examples use Rogers (1975, 1983) model as a base for Witte's (1992, 1994) EPPM to explain the success and failure of all behaviour related to phishing attacks.

4.3.5 How PMT Research is Lacking

There are very few if any theories that are correct in every situation. Models often cater to a specific situation or behaviour and must be altered to function as well when used in non-intended ways. PMT is a theory used in major parts of research and has been altered and adapted to fit in many completely different situations where protection motivation is a factor (Bethany et al., 2022; Badsar et al., 2022; Banerski & Abramczuk, 2023). In information security, PMT has been successfully used to explain and improve security behaviour, protective technologies, and security training for many years (Chenoweth et al., 2009; Herath & Rao, 2009; Fischer-Preßler et al., 2022; Haag et al., 2021; Khan et al., 2023). However, Vance et al. (2012) found that vulnerability does not increase the intention to comply with ISPs which directly oppose the PMT model. Furthermore, an inconsistency in security behaviour is explained by Dang-Pham and Pittayachawan (2015, p. 293) where students had the ability and knowledge needed to successfully protect themselves against malware at university where their self-efficacy is high and trust in the university network is low, however, at home in the same situation, they would not perceive risk the same which would lead to lower intention to avoid malware and increase risk of malware attacks.

A gap in information for PMT studies is the data used in all mentioned studies for PMT. Almost all has used a quantitative research methodology which gives an accurate representation of what the researchers allow the participants to answer, but not exactly how the participants would formulate the answer themselves. Put simply, there are not enough qualitative research articles on PMT to truly find an undeniable connection between threat and protection motivation without finding and filtering out other variables that could mean the same thing to a participant. In addition, Haag et al. (2021) in their review of PMT research found that 76.1 percent of studies included a one-time point survey. An issue is also that most research focus on protection motivation and how to increase self-efficacy and adaptive coping, however, only six percent of pre-2021 studies investigated maladaptive coping and how to directly decrease it (Haag et al., 2021). This shows that there is a need for qualitative research to continuously research how and why people do not adapt their behaviour or coping responses, but instead choose or unconsciously practise maladaptive behaviour.

Furthermore, there has been few major attempts to use a plain version of Rogers' (1983) PMT model to explain phishing attacks and protection motivation from

phishing emails. Unfortunately, research have not solved the topic of phishing through the lens of PMT as there are challenges associated with the breakdown of how phishing attacks are successful using PMT and a qualitative method. However, there is also no research done to disprove the possible function of PMT to explain a lack of protection motivation when the victims do not know that they are being attacked. These are all important and interesting topics that should be studied further to find if PMT could influence the perception of threats that users know are lurking but not obvious and ever-present.

4.3.6 Future Use of PMT to Explain Phishing Susceptibility

PMT is very versatile theory used evaluate protection motivation in many different subject areas. However, it has not been used to study phishing susceptibility to the degree that PMT has been used to study general security behaviours, security training, and ISP compliance. Therefore, a gap has been identified where PMT should be used in more qualitative research to find more nuanced differences in answers to understand what a user really feels about the subject. Furthermore, PMT should be researched in the context of phishing susceptibility and phishing training simulations. And lastly, PMT should be researched in the context of actual phishing victims to better understand the process of being phished. This could also be of assistance to Chen et al. (2021) to confirm their very interesting phishing stage model. However, this thesis will focus on how employees protect themselves from phishing by using core aspects of PMT.

5 METHODOLOGY

To understand how to conduct interviews and ask the correct questions when inquiring about phishing based on PMT, a method of breaking down the model and understanding each part is crucial. This will ensure understanding of the model and allow for more specific questions to be created and used. Part of understanding is to create a definition. However, this model has already been defined by the authors and many others who have given critique, therefore, the definition of each aspect of the PMT model in this thesis will be a compiled view of many authors with a critical view of each aspect. However, most aspects will be explained the same way as Rogers et al. (1983) intended.

Sources of information is a crucial aid in the investigation of thought process and understanding of any situation. Anyone would be better equipped to deal with a situation if the individual would have prior experience or opportunities to learn about the issue at hand (Sheng et al., 2010). Therefore, with a focus on the sources of information, the questions asked to begin the interview should be pointed towards the environment the person find themselves in and intrapersonal qualities. The environmental questions should regard how others affect their own decisions in reference to verbal persuasion and what they have learned from systems and people around them (Rogers et al., 1983). The intrapersonal skills, referring to the communication that take place in one's own mind, will regard how the person approaches unknown situations and the methods used to cope with said situation (Rogers et al., 1983). These coping methods might stem from previous coping processes in prior experience which is a crucial factor in how the cognitive mediating process conclude. Combining questions regarding environmental and intrapersonal sources of information should in combination lead to an understanding of how the participant would react to a phishing attack or explain in retrospect why they became a victim of a phishing attack.

The cognitive mediating process contains many aspects as previously mentioned and does create a challenge in the line of questioning when attempting to cover all bases and understand how the participant acted during the process before coming to the a conclusion where they were phished or not. The first response factor is intrinsic and extrinsic rewards where the goal is to increase self-satisfaction or social approval (Rogers et al., 1983). According to the model, both types of rewards decrease the probability of maladaptive behaviour (Rogers et al., 1983; Bax et al., 2021). The questioning regarding these rewards should be built around the mastery participants achieve and feedback that participants receive from their

place of work or colleagues as intrinsic rewards would cover the self-motivated work that accomplish personal mastery and purpose. Extrinsic rewards would cover the vast number of ways that a person could receive social approval with a superior, bonuses, or even punishments. However, both types of rewards could be negated if met with the wrong understanding of the severity and vulnerability of phishing email. The wrong understanding in a phishing context would be to not take a threat seriously enough as many emails may look like a real email. Therefore, threat arousal should be a part of phishing training and must be a contributing factor to why a person might be wary when receiving any email. The line of questioning regarding threat appraisal could be in the direction of how phishing emails are though of by the superiors and in the security culture. the desired answers would be to receive answers where fear of phishing emails is prevalent, but not the fear of punishment as it has been proven that fear of punishment does not constitute good security behaviour (Boss et al., 2015).

The last set of questions has to do with the adaptive response where efficacy is put against response cost. Efficacy includes both response efficacy and self-efficacy where the common definition would describe them as the belief in the ability one might have to perform a certain behaviour (Rogers et al., 1983). The difference between the two mentioned efficacies is that response efficacy is the belief that the response is correct to whatever the action might be (Rogers et al., 1983). Self-efficacy on the other hand is the pure belief in one's own ability to do the correct thing according to their knowledge (Rogers et al., 1983). As the counter, response cost is how much resources it takes to keep the efficacy high and whether the effort is worth it. The weight of each factor is weighed against each other in the coping appraisal and if the response cost outweighs the efficacy, the person will end up using less resources than needed on a task and might miss a step or piece of information that could sway a decision. This could also be a resulting factor to a person being phished.

Using the described methodology, answers to the questions should be able to answer the research question and the process of how a person becomes phished by not focusing on protection motivation. The answers should also be informative to a degree where security holes, missing guidelines, and poor cyber hygiene or security culture can be identified (Tejay & Mohammed, 2023). Questions will be asked in a semi-structured interview format to include the possibility of follow-up questions to further understand both context and further details in their situation. The goal is to allow for the participant to tell their story with slight nudges to further the story's start and end, and to have a more detailed middle section where any mistakes or inconsistencies may show up. The answers will be analysed to fit within the confines of the PMT model to confirm or plausibly deny reasons to why a person has not used protection motivation to avoid being phished. A more detailed version of the interviews can be found as "Interview guide" in appendix A.

5.1 Data Collection

This study interviewed ten participants from a large well-known international financial company. The participants were interviewed after a conversation with a contact within the company where employees could volunteer for an interview on phishing. This started as a phishing victim study, however, due to the low number of volunteers from multiple companies, there was a change of direction to focus on general phishing within one company. This led to three total interviews. Two interviews were conducted with one participant each, and the last interview had eight participants. There were clear challenges when designing an interview guide for one participant to suddenly interview eight. However, the solution was to truncate and specify the important questions and remove some pleasantries in the start of the interview. All three interviews spanned a timeframe from 35 to 50 minutes. To remain completely transparent, participant number three to ten is in the same interview. However, each participant gave answers that were either unique, built on what another participant had said, or gave a different answer altogether. Therefore, they have been sorted as different participants even though eight participants were intensely interviewed in 50 minutes. A table of participants can be seen below as table 1.

The reason for choosing these participants was due to their inherent knowledge about security policies and how training, rewards, and punishment was within the company. However, it very quickly became apparent that all employees know these things due to the importance of information security and the focus on phishing. Therefore, it was mostly due to availability that eight of ten participants were top level management, one participant was the manager of regional security, and one participant who volunteered early with the position as lawyer at the company. Another reason for choosing the different participants is the experience they have with email and with the company itself. Not a single participant has less than 20 years of experience with email and all participants have worked at the company for more than a year. Firstly, the experience with emails allows the participants to speak with knowledge of how email used to be and how it has changed. This alongside the experience they have with detecting spam, ads, and phishing emails will provide a valuable point of view. Secondly, due to everyone having more than one year of experience with the company means that all participants have been part of a phishing campaign for a minimum of one year with extensive training. This proves useful to tell the story of how well the anti-phishing training and phishing campaign works. In addition, experience within the company also allows for the participants to explain their emotions connected to fear appeals much easier than a newly hired employee.

Participant #	Experience in the company	Experience with email	Gender	Age	Work Position
1	14 years	>25 years	Male	59	Director
2	14 months	>20 years	Female	51	Lawyer
3	23 years	>30 years	Male	50	Vice president
4	15 years	>30 years	Female	55	Senior vice president
5	11 years	>25 years	Male	46	Director
6	6 years	>20 years	Male	34	Director
7	20 years	>25 years	Male	47	Director
8	6 years	>25 years	Female		Director
9	Almost 2 years	>30 years	Male		Manager Regional Security
10	2 years	>20 years	Male	37	Vice president

Table 1 - information about the participants

The answers that were collected using two individual interviews and one group interview with eight participants have been analysed using a thematic analysis with deductive and inductive codes. The deductive codes were formed using the different aspects of PMT and the inductive codes were formed using phishing and security policies as basis for new points of view.

5.2 Data Analysis

Thematic analysis methodology is a data coding framework that aims to sort data into themes (Braun & Clarke, 2006; Attride-Stirling, 2001). The specific methodology used in this thesis is described by Braun and Clarke (2006) as a deductive method where data is sorted into an already existing coding framework. The coding framework is the model of protection motivation theory which include multiple aspects. Each aspect of PMT acts like a code to the answers that were given during the data gathering. According to Braun and Clarke (2006), the phases are to be familiarized with the data, generating codes, searching for themes, reviewing those themes, defining and naming themes, and producing the report. However, for this thesis, thematic analysis methodology will only be used in addition to the interview methodology to sort and identify themes. Therefore, the process has been altered and will follow a different structure that looks like this; identifying themes, gathering data based on themes, get familiarized with data, generating codes, reviewing themes, and finally producing the report.

The methodology has been developed since the initialisation of the data gathering stage. As described previously, the interviews were conducted to specifically gather information about the different aspects of PMT in relation to phishing, in addition to whatever the participants found interesting themselves or what I as the interviewer would have liked more answers to. The aspects of phishing were translated into more words and into contexts that the participants could recognise from their own experience without knowing the PMT model. As the interviews was transcribed, the information could easily be allocated to the different themes, most of the time. Some data gathered spanned multiple themes and was at that point

included into both, but clearly stated. Furthermore, the themes were reviewed to be increasingly pointed to the specific data. This follows the idea of both Braun and Clarke (2006) and Attride-Stirling (2001) where the themes must be reviewed and possibly changed as the analysis takes place. Finally, a document with all themes, codes, statements, and separate information was developed and finalised to finish the modified thematic analysis.

As mentioned, all aspects of PMT were transformed into codes and developed further to be the themes used in the modified thematic analysis. The easiest solution that was also used was to pick apart the model as described in the PMT chapter of the background. First the participants were asked about their experience with email and what they thought of the use of email, how it has developed, and what it is used for now. This in addition to when the participants started using email was the grounds for prior experience and knowledge on the topic of email phishing. Following the experience were questions that directly related to the PMT model and its aspects. The first questions were related to the response from the organisation on phishing attacks in general and then pointing the question more towards rewards and punishments as the questioning went on. Then the topic of severity and vulnerability was discussed both on an organisational and personal level. Afterwards was the topic of emotional responses to emails and phishing emails. These were aimed at fear appeal and the possible transition to efficacy which was the next theme. These included both self-efficacy and response efficacy where the participants were asked if they felt confident in their abilities to both discriminate against phishing emails and be confident when discriminating. Connected to efficacy is the response cost where the participants were asked to describe their process when discriminating against phishing emails and to what degree they were consistent when evaluating personal vs work related email and internal vs external emails. Lastly, the participants were asked as a follow-up question where they would specify, if applicable if they had any coping methods when dealing with email phishing. There were a few answers to this question, but mostly answers to the ongoing phishing campaign that the company was doing. The analysis can be seen as a text in appendix B.

6 FINDINGS

The goal of this master's thesis was to answer the following research question: *"How do employees in a company protect themselves against phishing attacks?"*. This was done by interviewing 10 employees in the large financial company using PMT as a basis to create interview questions related to how they perceived the aspects that Rogers (1983) meant would affect protection motivation. The main findings will be explored in the coming sections of 6.1 which explain the findings supporting PMT, 6.2 which explain how two aspects of PMT are not supported by the findings, and section 6.3 which explore the possibility that the crucial part of PMT may not be so crucial in all circumstances after all.

6.1 Findings Supported by PMT

Findings supported by PMT entails the findings that were found to match the designed purpose of PMT. This includes section 6.1.1 which present the positive effects of intrinsic rewards, 6.1.2 which focus on the positive effects of efficacy, and finally 6.1.3 which introduce the benefits of lowering response costs. The different findings will be explained further in the coming sections.

6.1.1 Intrinsic Rewards have Positive Effects on Protection Motivation

Protection Motivation Theory has been used to evaluate aspects of anti-phishing security in a large financial company and has provided insight into how aspects of anti-phishing measures have been effective in accordance with PMT. Therefore, the first finding is that PMT correctly anticipated is rewards. As previously mentioned, rewards can be either intrinsic, extrinsic, or both. The anticipated result was that extrinsic rewards would be the dominating form of rewards to motivate the employees to protect themselves. This was on the basis that the company used for analysis was a large organization with thousands of employees who was assumed to be motivated by extrinsic factors first and intrinsic factors second. The rewards could have been monetary, travel related, services such as a spa weekend, or something similar. This would be based on that the employees would do their work based on expecting those rewards. Instead, the participants made no remarks about the importance of the monetary value nor acknowledgement from others by

receiving a physical reward. This sentiment is echoed by participants stating that they receive a great reward by reporting the correct emails: *"I also feel as though I have succeeded when I receive feedback after 5 minutes after I have successfully reported an email sent via the phishing campaign.*" [Interviewee #4], being the security champion of the month: *"The biggest reward would probably be to receive the email saying that you are the security champion of the month."*[Interviewee #10], and receiving a digital trophy: *"The greatest reward was getting the digital trophy at the end of this period"*, or just trying to compete with themselves on doing the best they can: *"I feel as though the phishing campaign is a competition with myself to do the best I can."* [Interviewee #8].

The statements clearly propose that extrinsic rewards are not as important as just doing a good job and feeling like they have done a good job. This goes against the initial expectation that extrinsic rewards would be an important factor in motivating security, however; it is in accordance with PMT where either intrinsic or extrinsic rewards would improve and promote protection motivation, therefore, PMT successfully anticipates the rewards as a motivation for protection in this organisation. Not only are the employees intrinsically rewarded as they successfully identify and report phishing emails, but they are also able to have fun with the experience as two participants mentioned: *"However, I do like to lead a phishing- or spam email on if I clearly see that there is no danger and say that I am not interested in the end to waste their time"* [Interviewee #8], and *"In addition, there is a humour reward associated to poorly constructed phishing emails that makes you think: "what were they thinking?" when designing the bad phishing email."* [Interviewee #3]. This could be an additional reward of identifying the phishing emails and having fun with how easily they managed to discriminate the phishing email from other emails. Based on this information, PMT correctly anticipated the aspect of rewards.

6.1.2 High Efficacy Decrease Uncertainty and Phishing Susceptibility

The second finding that matched the expectation was the level of efficacy. However, there was an unexpected result when the efficacy decreased for whatever reason. First, the efficacy refers to the self-confidence participants have as they evaluate a phishing email and the self-confidence they have as they respond to the email. The response is not necessarily to answer the email itself, instead, a response could be to ignore, delete, or report the suspicious email. Based on this the participant's efficacy was high. No participant explicitly uttered that they were directly uncomfortable with an assumed phishing email ever. This supports the PMT model's view on efficacy. However, as soon as the response-efficacy lowers the self-efficacy remains high and results in an immediate report or deletion of the

email. There are no punishments for doing this and improves the perceived trust in the employees. It can be argued that the high efficacy increases the chance of a good coping response due to the result it would have on emails that does not prove secure. This is reflected by participants stating: *"I have a high degree of response-efficacy and is very quick when I go through my emails. Out of 50 emails, 49 will probably be deleted or reported by looking at the email header."* [Interviewee #1]. Another participant states: "*I always have my checks that I do before clicking on anything, especially on external emails. I always look at the true sender's email address and google the domain if I am uncertain that it is legitimate."* [Interviewee #5]. Most other participants echoed the same statements stating that this is improved by the training they have received previously. *"I do believe I have high self-efficacy and believe that it is justifiable with all the training and passed simulations I have."* [Interviewee #1]. In total, it can be argued that every participant has high total efficacy.

6.1.3 Low Response Cost Allows Employees to do Proper Security Checks

The third unexpected, but positive finding is phishing being a low response cost for most participants. There are no expectations from the organisation to spend the least possible time checking emails and creating an unnecessary risk for a mistake to be made. Due to this, participants state that they spend the time they need to make sure any email they would want to interact with is real. However, due to the risk and training they have received, most participants prefer to not spend more than 20 seconds to check if an email is legitimate. This is the unexpected finding due to the expectation that most emails would be relevant due to the email-addresses not being public. However, it was found that a better solution would be to send the suspected email to the security division and receive the email in return if it was legitimate. The exception was one participant whose work is mainly reading documents. Therefore, reading emails and spending time in meetings will only divert them from doing actual work causing them to artificially creating a time limit and risking not spending enough time checking all their received emails for signs that points towards phishing. The participant specified:

> *"My job is not to read emails; however, it does take much of my time. Therefore, if I spend much time evaluating every email that comes through, I would not be able to do my actual job. Between the meetings I have and reading emails, I have many other documents I must read though to do my job. Therefore, I tend to spend too much time reading emails and that affects my workflow and amount of work I can do elsewhere." [Interviewee #2]*

Overall, the PMT model assumed the correct result even though it was more due to the participants' own ability to limit the personal response cost for themselves instead of being set hard limits by the organisation they work for.

6.2 Findings Not Supported by PMT

Findings not supported by PMT refer to aspects that does not correlate with the findings of this study. This includes section 6.2.1 which found that the perception of vulnerability and severity does not improve protection motivation just because they are high. Furthermore, section 6.2.2 includes the main finding which specify that fear appeal is not necessarily needed for protection motivation to be present. These findings are explored further in the coming sections.

6.2.1 Higher Perception of Vulnerability and Perception of Severity Does not Automatically Decrease Phishing Susceptibility

The fourth finding is that PMT anticipated the perception of vulnerability and severity to be high. These aspects entail the understanding to which degree that the organisation would be compromised if successfully attacked and how severe the consequences could be. The employees were found to be well-aware of the vulnerable state of their organization if they would become a phishing victim *"the danger is that very important or classified information could be collected if a machine is successfully infected. This could be months of work to fix due to an issue that is big business but cheap crime."* [Interviewee #1]. However, the perception of vulnerability of themselves was very split. Participants were either very confident or they had very high self-awareness. The participants who were very confident had an almost negligent way of thinking of phishing. They meant that they could not be phished or that they were above average aware of phishing and had a higher ability of discovering phishing attacks amongst real emails. On the other hand, participants with a high level of self-awareness showed confidence but also an understanding that they are not perfect. Therefore, there could always be a chance that they made a mistake and would become a victim of phishing.

The reason that this finding is not supported by PMT is that there were participants with high confidence that had gotten phished, and those who had not. The same is the case for those who have high self-awareness. The ones who had high confidence boasted about the status of phishing in their life and describing phishing as noise, an annoyance, and irritation.

> *"Phishing emails are just an annoyance and noise in the day-to-day operation of the organisation as well as privately. However, as much as they (phishing emails) are an annoyance, I do believe I am above average capable of seeing the difference between real and fake emails". [Interviewee #6]*

The participants also thought about the punishments if they were tricked too many times saying that the punishments could be a little harsh: *"The punishment for failing a few times is a bit too high considering you can get fired easily within 2 years if you are not careful"* [Interviewee #10]. This severity of punishment seems to also be known to all participants and has been understood by all employees. Other participants think of the severity of phishing as a legitimate issue and thinks that one can never be too prepared. The same participants enjoy learning and receive great intrinsic reward for doing the e-training courses. There were in total less participants who had gotten phished who were very self-aware than those who had very high confidence. The PMT model does not explain that connection and the result of the perception of vulnerability and severity in comparison to fear appeal will be discussed in the next section.

6.2.2 Lack of Fear Appeal Does Not Mean That Employees are Less Secure

The fifth finding is that PMT does not support the level of fear appeal caused by the perception of severity and vulnerability. High fear appeal should be a result of a high perception of vulnerability and high perception of severity. In addition, fear appeal should provoke a fearful response to whatever threat presents itself and therefore promote protection motivation. Based on the analysis of what participants said and how they conveyed their answers when asked about the connection between fear and phishing, the most common answer was: there is none.

> *"I do not fear phishing. (…) I am not worried about my economy or having my information stolen, but it is trouble, right? It is trouble and an annoyance to have to change all my information in the banks and insurance companies and so on." [Interviewee #1]*

This statement quite easily sums up how all participants thought of the connection between the emotion of fear and phishing. This is very unexpected and wrong according to PMT. Due to high perception of vulnerability and severity; fear appeal should have been high, and phishing should be a lead cause to thinking there is a threat. However, there could be multiple alternatives to fear such as software solutions to warn the employees:

> *"I do not fear emails or phishing very much. We have systems that does a great job at sorting out phishing emails, and every email from*

> *external addresses are marked with a yellow banner waning that the email is not sent from internal addresses. This makes me more aware of potential phishing but does not instil fear in me." [Interviewee #2]*

and a large degree of awareness:

> *"I do not fear phishing, but I am very aware of them. At some point you must find and use a balance of function and paranoia. (…) If something continues to be suspicious, I will just report it." [Interviewee # 3]*

The freedom provided by the company to take no risks and report everything suspicious, the high efficacy, the intrinsic rewards, the low response cost, and the lack of fear appeal might not point to a successful threat and coping appraisal, however, it does stop the employees from being phished by legitimate phishing attacks. Therefore, this might not be a success on the part of PMT, rather a successful and healthy protection mindset by the employees. This does not mean that PMT is wrong in its entirety, but rather inconclusive as used in this thesis.

6.3 Protection Motivation vs Protective Mindset

Protection motivation theory has been used for many years to look at information security and social engineering, however, it has not been used as much in its most basic form as designed by Rogers (1983) in phishing. The last finding is that the reason why PMT provided a limited explanation for this interview study is that phishing is unannounced, unknown, and unpredictable. There are no situations where being constantly paranoid of a threat would be healthy in the long term. Therefore, based on the interviews and statements from the participants, a state of being constantly aware of a threat but not actively searching for it and still successfully protecting oneself, could instead be described as a protective mindset. Due to the entire PMT model relying on the fear appeal, it cannot explain a situation in which there is no fear but still successfully create protection motivation. This is why PMT has been picked apart by multiple researchers and concluded to be unconvincing as it has never been found to be adequate in its most basic form due to the paralysis it faces when fear is absent. Simply put, both protection motivation and a protective mindset achieve the same protective result, but a protective mindset does not require fear to be effective.

7 DISCUSSION

This study discusses the use of Protection Motivation Theory in relation to phishing susceptibility by interviewing employees with phishing training and phishing simulations as a core part of their information security. The goal was to find if PMT could be applied in its entirety without modification to understand why the employees of a financial company avoids phishing attacks. The interview study found that the building blocks of fear appeal; perception of vulnerability and perception of severity, was not effective at increasing fear appeal. This is due to each employee understanding the implications that a successful phishing attack could have on the company. Due to the motivation to protect themselves without fear appeal, a suggestion is that protection motivation without fear appeal would be a protective mindset where everyone wants to remain secure and do their best to accomplish this goal. The implications of this will be explained in the next sections.

7.1 Theoretical Implications

There were five findings in the relationship between the participants who are employees in a large financial infrastructure company, phishing, and protection motivation theory. The aspects where PMT predicted correctly include high rewards, high efficacy, and low response cost. There were also suggestions that was not supported by PMT. There was the finding of both perception of vulnerability and severity leading to two noticeable attitudes towards phishing. This includes the self-awareness attitude and the high confidence attitude. Both attitudes had phishing victims and participants that had never been phished. Thus, leading to a finding that was not supported by PMT. The fifth finding was where PMT was completely unsupportive which include the most important principle of PMT: fear appeal. This was a surprising finding which sparked the idea of the last finding. There might not be protection motivation that keep the employees from being phished, rather it is a protective mindset instead. Although these findings are interesting, how do they compare to literature?

According to Bax et al. (2021), the roles of rewards affect maladaptive behaviour more than protective behaviour. According to their research, there is a chance that rewards bypass protection motivation and affect maladaptive behaviour directly. This can be very positive as with high rewards, maladaptive behaviour has

the chance of being decreased. This directly correlates with the findings in this thesis by increasing the intrinsic rewards and offering extrinsic rewards there appears to be a disconnect between protection motivation and rewards. Therefore, this idea could be a sign of a protective mindset instead of protection motivation.

Although protection motivation is seen to be increased due to a correct application of fear appeal (Jaeger & Eckhardt, 2020; Boss et al., 2015), participants acknowledged that they did not feel fear for phishing attacks at all. This is very inconsistent compared to the research even though the participants were very aware of both vulnerability and severity of phishing. This has an implication that fear does not need to be present to do protective behaviour. Any idea that PMT must be used as designed has been proven wrong by well-documented research and is often criticized for overstating the importance of perception of vulnerability and response costs (Bax et al., 2021; Mou et al., 2022). In addition, Boss et al. (2015) and Dupuis & Renaud (2021) provide context that purposefully creating fear appeal must have a very good reason and should probably be avoided if possible as there are ethical issues with creating psychological stress related to fear. This also related to security related stress and the negative effects that can be a result of constantly worrying about security (Yazdanmehr et al., 2023).

However, Johnston et al. (2015) suggested that researchers have misspecified the theory within the context of information security and suggest that research in infosec does not make a good enough distinction between *"threats to one's self and threats to one's data property".* Therefore, Johnston et al. (2015) found that *"sanctioning rhetoric is able to enhance the effectiveness of a fear appeal, thus leading to stronger intentions to comply with information security policy.".* The idea is also noted by Jansen & Schaik (2019) who state that *"fear appeals have great potential to promote security behaviour by making end users aware of threats and simultaneously providing behavioural advice on how to mitigate these threats.".* This goes against finding five as there was no fear appeal exclaimed by the participants in this study. Therefore, the finding suggests that the opposite is also possible where a protective mindset could negate the need of fear appeal as described by Johnston et al. (2015).

The idea of a protective mindset is not a new development in research as security behaviour has been a well-documented topic across multiple subjects in information security (Chen et al., 2022; Ogbanufe et al., 2021; Tam et al., 2022). However, it is often defined as coping behaviours and not as a protective mindset. The difference would be that a mindset is purposely focused on protection and wants to succeed, however, coping behaviour is a product of a mediating process such as the cognitive mediating process (Rogers et al., 1983). Therefore, it could be argued that a different security behaviour is used by participants of this study to create a protective mindset instead of protection motivation.

7.2 Practical Implications

As phishing as a technique of attack is continually developing, so are the people who discover and avoid these attacks. However, results show that fearing phishing as a threat does not equate to better defence, nor does deescalating phishing from a threat to an annoyance. According to the results, a healthy dose of awareness and understanding of the threat is needed alongside a motivation to not become a victim of phishing. This requires a protective mindset. However, a protective mindset also requires training, simulations, and a real-life practical application of the theory that is taught. As shown, complying with phishing policies and avoiding phishing attacks does not require the user to be an expert, however, it requires high-awareness and some suspicion when dealing with email. Deleting or reporting 49 of 50 emails might not be efficient, however, it is secure.

Furthermore, results show that this financial company could be a great template and show other companies that fear is not needed. In fact, if other companies have issues with phishing even when using fear, this proves Chen et al. (2022) that fear appeal has the potential to backfire. Therefore, an implication would be to attempt a forceful use of training and simulations and explain the reasoning why it is forced. Although Ogbanufe et al. (2021) studied stewardship theory, this also proves that organisational support increases voluntary security behaviour such as this study. The last practical implication is to try a transition into a less or no fear based phishing training model and give incentives to do well (Bax et al., 2021).

7.3 Limitations and Future Research

There are limitations to this study that calls for future research. As mentioned in section 4.3.6, the thesis was supposed to be about phishing victims in isolation studied through the lens of PMT. However, due to the lack of voluntary phishing victims to interview, the plan fell through. This would have been the most interesting method of researching this topic as much as finding that fear is not needed for someone to successfully protect themselves against phishing is interesting, to find the lead cause to why people become victim to phishing would have been even better.

The second limitation is the participants in the study. Eight of ten participants were on a director level or higher in their current organisation. This means that the results are skewed towards the upper management and does not take into consideration how the remaining employees working on the different teams' experience phishing. This leaves much room for further research on the same topic to the extent that lower management employees might have different security policies than the participants. Furthermore, these findings should not be taken as undeniable and

irrefutable fact that could be generalized as ten participants is a small sample size and a very specific group of participants. If there was more time, I would have liked to interview more employees from either the same company or a different company. This would have given more depth in the data instead of the specific information that I collected this time.

The third limitation is my skill as an interviewer and an analyst. There are better ways of conducting interviews to gain more information in the timeframe for each interview. There are also better ways to ask questions to increase the quality of the answers received. Furthermore, analysing the interviews may have been done more effectively if the analysis methodology was not an afterthought to the interviews. Therefore, this limitation is on my skillset as a student and not a peer-reviewed author with much previous experience.

8 CONCLUSION

As phishing remains a strong threat to all technology users, it is important to detect and improve methods of protection. Protection motivation has been found to be useful in situations where the user knows about the imminent threat, however, how can users protect themselves against a threat they do not know is present. Using PMT to do an interview study of a large financial company, it was found that the participants do not fear phishing. However, all other aspects of PMT could be successfully identified in their behaviour and thought process. Therefore, a suggestion is that when all prerequisites for successful protection motivation according to PMT is present except for fear appeal, the resulting behaviour could be a protective mindset which would require determination more than fear. This is the result of participants finding intrinsic rewards present and fulfilling, high self- and response-efficacy, low response cost, and high perception, and understanding of vulnerability and severity. I conclude that fear appeal in the context of phishing susceptibility is not necessarily the best way to motivate protection motivation as the participants in this study has done well without it.

9 REFERENCES

Abbasi, A., Dobolyi, D., Vance, A., & Zahedi, F. M. (2021). The Phishing Funnel Model: A Design Artifact to Predict User Susceptibility to Phishing Websites. *Information Systems Research*, *32*(2), 410-436. https://doi.org/10.1287/isre.2020.0973

Abraham, S., & Chengalur-Smith, I. (2019). Evaluating the effectiveness of learner controlled information security training. *Computers & Security*, *87*, 101586. https://doi.org/https://doi.org/10.1016/j.cose.2019.101586

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process. *IEEE Access*, *9*, 44928-44949. https://doi.org/10.1109/ACCESS.2021.3066383

Afroz, S., & Greenstadt, R. (2011, 18-21 Sept. 2011). PhishZoo: Detecting Phishing Websites by Looking at Them. 2011 IEEE Fifth International Conference on Semantic Computing,

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211. https://doi.org/https://doi.org/10.1016/0749-5978(91)90020-T

Aleroud, A., Abu-Shanab, E., Al-Aiad, A., & Alshboul, Y. (2020). An examination of susceptibility to spear phishing cyber attacks in non-English speaking communities. *Journal of Information Security and Applications*, *55*, 102614. https://doi.org/https://doi.org/10.1016/j.jisa.2020.102614

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, *68*, 160-196. https://doi.org/https://doi.org/10.1016/j.cose.2017.04.006

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy [Review]. *Frontiers in Computer Science*, *3*. https://doi.org/10.3389/fcomp.2021.563060

Al-Qahtani, A. F., & Cresci, S. (2022). The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19 [https://doi.org/10.1049/ise2.12073]. *IET Information Security*, *16*(5), 324-345. https://doi.org/https://doi.org/10.1049/ise2.12073

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, *34*(3), 613-643. https://doi.org/10.2307/25750694

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312. https://doi.org/https://doi.org/10.1016/j.chb.2014.05.046

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, *60*, 185-197. https://doi.org/https://doi.org/10.1016/j.chb.2016.02.065

Attride-Stirling, J. (2001). Thematic networks: an analytic tool for qualitative research. Qualitative Research, 1(3), 385-405. https://doi.org/10.1177/146879410100100307

Badsar, M., Moghim, M., & Ghasemi, M. (2022). Analysis of factors influencing farmers' sustainable environmental behavior in agriculture activities: integration of the planned behavior and the protection motivation theories. *Environment, Development and Sustainability*. https://doi.org/10.1007/s10668-022-02468-3

Banerski, G., & Abramczuk, K. (2023). Persuasion illustrated: Motivating people to undertake self-protective measures in case of floods using 3D animation focused on components of protection motivation theory. *International Journal of Disaster Risk Reduction*, *89*, 103575. https://doi.org/https://doi.org/10.1016/j.ijdrr.2023.103575

Bax, S., McGill, T., & Hobbs, V. (2021). Maladaptive behaviour in response to email phishing threats: The roles of rewards and response costs. *Computers & Security*, *106*, 102278. https://doi.org/https://doi.org/10.1016/j.cose.2021.102278

Bekkers, L., van 't Hoff-de Goede, S., Misana-ter Huurne, E., van Houten, Y., Spithoven, R., & Leukfeldt, E. R. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. *Computers & Security*, *127*, 103099. https://doi.org/https://doi.org/10.1016/j.cose.2023.103099

Benenson, Z., Gassmann, F., & Landwirth, R. (2017, 2017//). Unpacking Spear Phishing Susceptibility. [https://link.springer.com/chapter/10.1007/978-3-319-70278-0_39]. Financial Cryptography and Data Security, Cham.

Bethany, G., Mark, C., & Paul, N. (2022). Applying an extended protection motivation theory to predict Covid-19 vaccination intentions and uptake in 50–64 year olds in the UK. *Social Science & Medicine*, *298*, 114819. https://doi.org/https://doi.org/10.1016/j.socscimed.2022.114819

Bhardwaj, A., Al-Turjman, F., Sapra, V., Kumar, M., & Stephan, T. (2021). Privacy-aware detection framework to mitigate new-age phishing attacks. *Computers & Electrical Engineering*, *96*, 107546. https://doi.org/https://doi.org/10.1016/j.compeleceng.2021.107546

Bleiker, J., Morgan-Trimmer, S., Knapp, K., & Hopkins, S. (2019). Navigating the maze: Qualitative research methodologies and their philosophical foundations. *Radiography*, *25*, S4-S8. https://doi.org/https://doi.org/10.1016/j.radi.2019.06.008

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors [Article]. *MIS Quarterly: Management Information Systems*, *39*(4), 837-864. https://doi.org/10.25300/MISQ/2015/39.4.5

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3, 77-101. https://doi.org/10.1191/1478088706qp063oa

Buckley, J., Lottridge, D., Murphy, J. G., & Corballis, P. M. (2023). Indicators of employee phishing email behaviours: Intuition, elaboration, attention, and email typology. *International Journal of Human-Computer Studies*, *172*, 102996. https://doi.org/https://doi.org/10.1016/j.ijhcs.2023.102996

Burgess, E. S., & Wurtele, S. K. (1998). Enhancing parent-child communication about sexual abuse: a pilot study. Child Abuse & Neglect, 22(11), 1167-1175. https://doi.org/https://doi.org/10.1016/S0145-2134(98)00094-5

Burns, A. J., Johnson, M. E., & Caputo, D. D. (2019). Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce*, *29*(1), 24-39. https://doi.org/10.1080/10919392.2019.1552745

Butavicius, M., Parsons, K., Lillie, M., McCormac, A., Pattinson, M., & Calic, D. (2020). When believing in technology leads to poor cyber security: Development of a trust in technical controls scale. *Computers & Security*, *98*, 102020. https://doi.org/https://doi.org/10.1016/j.cose.2020.102020

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016). Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails.

Butavicius, M., Taib, R., & Han, S. J. (2022). Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. *Computers & Security*, *123*, 102937. https://doi.org/https://doi.org/10.1016/j.cose.2022.102937

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going Spear Phishing: Exploring Embedded Training and Awareness. *IEEE Security & Privacy*, *12*(1), 28-38. https://doi.org/10.1109/MSP.2013.106

Carroll, F., Adejobi, J. A., & Montasari, R. (2022). How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society. *SN Computer Science*, *3*(2), 170. https://doi.org/10.1007/s42979-022-01069-1

Carter, L., & McBride, M. (2015). Distracted Driving among Teens: How can We Educate and Protect Our Youth? *Procedia Engineering*, *107*, 485-487. https://doi.org/https://doi.org/10.1016/j.proeng.2015.06.107

Chen, M.-F. (2020). Moral extension of the protection motivation theory model to predict climate change mitigation behavioral intentions in Taiwan. *Environmental Science and Pollution Research*, *27*(12), 13714-13725. https://doi.org/10.1007/s11356-020-07963-6

Chen, R., Gaia, J., & Rao, H. R. (2020). An examination of the effect of recent phishing encounters on phishing susceptibility. *Decision Support Systems*, *133*, 113287. https://doi.org/https://doi.org/10.1016/j.dss.2020.113287

Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X., Moody, G. D., & Willison, R. (2021). Understanding Inconsistent Employee Compliance with Information Security Policies Through the Lens of the Extended Parallel Process Model. *Information Systems Research*, *32*(3), 1043-1065. https://doi.org/10.1287/isre.2021.1014

Chen, Y., Luo, X., & Li, H. (2022). Beyond adaptive security coping behaviors: Theory and empirical evidence. *Information & Management*, *59*(2), 103575. https://doi.org/https://doi.org/10.1016/j.im.2021.103575

Chenoweth, T., Minch, R., & Gattiker, T. (2009). *Application of Protection Motivation Theory to Adoption of Protective Technologies*. https://doi.org/10.1109/HICSS.2009.74

Cismaru, M., & Lavack, A. M. (2006). Marketing communications and protection motivation theory: Examining consumer decision-making. *International Review on Public and Nonprofit Marketing*, *3*(2), 9-24. https://doi.org/10.1007/BF02893617

Clarke, N., Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information management & computer security.*, *20*(1), 18-28. https://doi.org/10.1108/09685221211219173

Cobo-Sánchez, J. L., & Blanco-Mavillard, I. (2020). Nuclear elements for drafting a research project with quantitative methodology. *Enfermería Intensiva (English ed.)*, *31*(1), 35-40. https://doi.org/https://doi.org/10.1016/j.enfie.2019.12.001

da Silva, C. M. R., Fernandes, B. J. T., Feitosa, E. L., & Garcia, V. C. (2022). Piracema.io: A rules-based tree model for phishing prediction. *Expert Systems*

with Applications, *191*, 116239. https://doi.org/https://doi.org/10.1016/j.eswa.2021.116239

Dang, H. L., Li, E., Nuberg, I., & Bruwer, J. (2014). Understanding farmers' adaptation intention to climate change: A structural equation modelling study in the Mekong Delta, Vietnam. *Environmental Science & Policy*, *41*, 11-22. https://doi.org/https://doi.org/10.1016/j.envsci.2014.04.002

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university. *Comput. Secur.*, *48*(C), 281–297. https://doi.org/10.1016/j.cose.2014.11.002

Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. Computers & Security, 26(1), 73-80. https://doi.org/https://doi.org/10.1016/j.cose.2006.10.009

Dupuis, M., & Renaud, K. (2021). Scoping the ethical principles of cybersecurity fear appeals. *Ethics and Information Technology*, *23*(3), 265-284. https://doi.org/10.1007/s10676-020-09560-0

Ferreira, A., & Teles, S. (2019). Persuasion: How phishing emails can influence users and bypass security measures. *International Journal of Human-Computer Studies*, *125*, 19-31. https://doi.org/https://doi.org/10.1016/j.ijhcs.2018.12.004

Fischer-Preßler, D., Bonaretti, D., & Fischbach, K. (2022). A Protection-Motivation Perspective to Explain Intention to Use and Continue to Use Mobile Warning Systems. *Business & Information Systems Engineering*, *64*(2), 167-182. https://doi.org/10.1007/s12599-021-00704-0

Frank, M., Jaeger, L., & Ranft, L. M. (2022). Contextual drivers of employees' phishing susceptibility: Insights from a field study. *Decision Support Systems*, *160*, 113818. https://doi.org/https://doi.org/10.1016/j.dss.2022.113818

Ge, Y., Lu, L., Cui, X., Chen, Z., & Qu, W. (2021). How personal characteristics impact phishing susceptibility: The mediating role of mail processing. *Applied Ergonomics*, *97*, 103526. https://doi.org/https://doi.org/10.1016/j.apergo.2021.103526

Goel, S., Williams, K. J., Huang, J., & Warkentin, M. (2021). Can financial incentives help with the struggle for security policy compliance? *Information & Management*, *58*(4), 103447. https://doi.org/https://doi.org/10.1016/j.im.2021.103447

Gordon, W. J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., Parkulo, M., Sanford, B., Scheib, P., & Landman, A. B. (2019). Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. *JAMA Network Open*, *2*(3), e190393-e190393. https://doi.org/10.1001/jamanetworkopen.2019.0393

Gordon, W. J., Wright, A., Glynn, R. J., Kadakia, J., Mazzone, C., Leinbach, E., & Landman, A. (2019). Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. *Journal of the American Medical Informatics Association*, *26*(6), 547-552. https://doi.org/10.1093/jamia/ocz005

Grassegger, T., & Nedbal, D. (2021). The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. *Procedia Computer Science*, *181*, 59-66. https://doi.org/https://doi.org/10.1016/j.procs.2021.01.103

Guedes, I., Martins, M., & Cardoso, C. S. (2022). Exploring the determinants of victimization and fear of online identity theft: an empirical study. *Security Journal*. https://doi.org/10.1057/s41284-022-00350-5

Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*(2), 247-267. https://doi.org/10.1007/s11235-017-0334-z

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails. *Online Information Review*, *40*(2), 265-281. https://doi.org/10.1108/OIR-04-2015-0106

Heise, E., Gerjets, P., & Westermann, R. (1997). The influence of a waiting intention on action performance: Efficiency impairment and volitional protection in tasks of varying difficulty. *Acta Psychologica*, *97*(2), 167-182. https://doi.org/https://doi.org/10.1016/S0001-6918(97)00027-9

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service [https://doi.org/10.1111/j.1365-2575.2012.00420.x]. *Information Systems Journal*, *24*(1), 61-84. https://doi.org/https://doi.org/10.1111/j.1365-2575.2012.00420.x

Herath, T., & Rao, R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *EJIS*, *18*, 106-125. https://doi.org/10.1057/ejis.2009.6

Hong, J. (2012). The state of phishing attacks. *Commun. ACM*, *55*(1), 74–81. https://doi.org/10.1145/2063176.2063197

Haag, S., Siponen, M., & Liu, F. (2021). Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future. *SIGMIS Database*, *52*(2), 25–67. https://doi.org/10.1145/3462766.3462770

Ikhsan, M. G., & Ramli, K. (2019, 23-26 June 2019). Measuring the Information Security Awareness Level of Government Employees Through Phishing Assessment. 2019 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC),

Iuga, C., Nurse, J. R. C., & Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences*, *6*(1), 8. https://doi.org/10.1186/s13673-016-0065-2

Jaeger, L., & Eckhardt, A. (2021). Eyes wide open: The role of situational information security awareness for security-related behaviour. *Information Systems Journal*, *31*(3), 429-472. https://doi.org/https://doi.org/10.1111/isj.12317

Jalali, S., & Wohlin, C. (2012). *Systematic Literature Studies: Database Searches vs. Backward Snowballing* Proceedings of the ACM-IEEE International Symposium on Empirical Software Engineering and Measurement, https://doi.org/10.1145/2372251.2372257

Jansen, J., & van Schaik, P. (2018). Testing a model of precautionary online behaviour: The case of online banking. *Computers in Human Behavior*, *87*, 371-383. https://doi.org/https://doi.org/10.1016/j.chb.2018.05.010

Jansen, J., & van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*, *123*, 40-55. https://doi.org/https://doi.org/10.1016/j.ijhcs.2018.10.004

Jingguo Wang, Y. L., H. Raghav Rao. (2016). Overconfidence in Phishing Email Detection. *Journal of the Association for Information Systems*, *17*. https://doi.org/DOI: 10.17705/1jais.00442

Johnston, A., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, *34*, 549-566. https://doi.org/10.2307/25750691

Johnston, A., Warkentin, M., & Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric. MIS Quarterly, 39, 113-134. https://doi.org/10.25300/MISQ/2015/39.1.06

Junger, M., Montoya, L., & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, *66*, 75-87. https://doi.org/https://doi.org/10.1016/j.chb.2016.09.012

Kakimoto, R., & Yoshida, M. (2022). Evacuation action during torrential rain considering situation awareness error using protection motivation theory. International Journal of Disaster Risk Reduction, 82, 103343. https://doi.org/https://doi.org/10.1016/j.ijdrr.2022.103343

Kelley, N. J., Hurley-Wallace, A. L., Warner, K. L., & Hanoch, Y. (2023). Analytical reasoning reduces internet fraud susceptibility. *Computers in Human Behavior*, *142*, 107648. https://doi.org/https://doi.org/10.1016/j.chb.2022.107648

Keshavarz, M., & Karami, E. (2016). Farmers' pro-environmental behavior under drought: Application of protection motivation theory. *Journal of Arid Environments*, *127*, 128-136. https://doi.org/https://doi.org/10.1016/j.jaridenv.2015.11.010

Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. *Computers & Security*, *125*, 103049. https://doi.org/https://doi.org/10.1016/j.cose.2022.103049

Kwak, Y., Lee, S., Damiano, A., & Vishwanath, A. (2020). Why do users not report spear phishing emails? *Telematics and Informatics*, *48*, 101343. https://doi.org/https://doi.org/10.1016/j.tele.2020.101343

Lawson, P., Pearson, C. J., Crowson, A., & Mayhorn, C. B. (2020). Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy. *Applied Ergonomics*, *86*, 103084. https://doi.org/https://doi.org/10.1016/j.apergo.2020.103084

Li, W., Lee, J., Purl, J., Greitzer, F., Yousefi, B., & Laskey, K. (2020). Experimental Investigation of Demographic Factors Related to Phishing Susceptibility. https://doi.org/10.24251/HICSS.2020.274

Luo, X., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. *Computers & Security*, *38*, 28-38. https://doi.org/https://doi.org/10.1016/j.cose.2012.12.003

Martin, S. R., Lee, J. J., & Parmar, B. L. (2021). Social distance, trust and getting "hooked": A phishing expedition. *Organizational Behavior and Human Decision Processes*, *166*, 39-48. https://doi.org/https://doi.org/10.1016/j.obhdp.2019.08.001

Menard, P., Warkentin, M., & Lowry, P. B. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers & Security*, *75*, 147-166. https://doi.org/https://doi.org/10.1016/j.cose.2018.01.020

MITRE. (2023). *Access Token Manipulation*. MITRE ATT&CK. Retrieved 25.04.2023 from https://attack.mitre.org/techniques/T1134/

Mou, J., Cohen, J., Bhattacherjee, A., & Kim, J. (2022). A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach in Search Advertising. *Journal of the Association for Information Systems*, *23*, 196-236. https://doi.org/10.17705/1jais.00723

Musuva, P. M. W., Getao, K. W., & Chepken, C. K. (2019). A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility. *Computers in Human Behavior*, *94*, 154-175. https://doi.org/https://doi.org/10.1016/j.chb.2018.12.036

Nelson, K., Cismaru, M., Cismaru, R., & Ono, T. (2011). Water management information campaigns and protection motivation theory. *International Review on Public and Nonprofit Marketing*, *8*(2), 163-193. https://doi.org/10.1007/s12208-011-0075-8

Ogbanufe, O., Crossler, R. E., & Biros, D. (2021). Exploring stewardship: A precursor to voluntary security behaviors. *Computers & Security*, *109*, 102397. https://doi.org/https://doi.org/10.1016/j.cose.2021.102397

Ogbanufe, O., Crossler, R. E., & Biros, D. (2023). The valued coexistence of protection motivation and stewardship in information security behaviors. *Computers & Security*, *124*, 102960. https://doi.org/https://doi.org/10.1016/j.cose.2022.102960

Paek, S. Y., & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and Justice*, *43*(4), 626-642. https://doi.org/https://doi.org/10.1016/j.ijlcj.2015.02.003

Perez, L. M., Jones, J., Englert, D. R., & Sachau, D. (2010). Secondary Traumatic Stress and Burnout among Law Enforcement Investigators Exposed to Disturbing Media Images. *Journal of Police and Criminal Psychology*, *25*(2), 113-124. https://doi.org/10.1007/s11896-010-9066-7

Petrič, G., & Roer, K. (2022). The impact of formal and informal organizational norms on susceptibility to phishing: Combining survey and field experiment data. *Telematics and Informatics*, *67*, 101766. https://doi.org/https://doi.org/10.1016/j.tele.2021.101766

Pfeffel, K., Ulsamer, P., & Müller, N. H. (2019, 2019//). Where the User Does Look When Reading Phishing Mails – An Eye-Tracking Study. Learning and Collaboration Technologies. Designing Learning Experiences, Cham.

Polakis, I., Kontaxis, G., Antonatos, S., Gessiou, E., Petsas, T., & Markatos, E. P. (2010). *Using social networks to harvest email addresses* Proceedings of the 9th annual ACM workshop on Privacy in the electronic society, Chicago, Illinois, USA. https://doi.org/10.1145/1866919.1866922

Rajivan, P., & Gonzalez, C. (2018). Creative Persuasion: A Study on Adversarial Behaviors and Strategies in Phishing Attacks [Original Research]. *Frontiers in Psychology*, *9*. https://doi.org/10.3389/fpsyg.2018.00135

Rameem Zahra, S., Ahsan Chishti, M., Iqbal Baba, A., & Wu, F. (2022). Detecting Covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system. *Egyptian Informatics Journal*, *23*(2), 197-214. https://doi.org/https://doi.org/10.1016/j.eij.2021.12.003

Randolph, J. (2009). A Guide to Writing the Dissertation Literature Review. *Research, and Evaluation*, *14*. https://doi.org/https://doi.org/10.7275/b0az-8t74

Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, *59*, 26-44. https://doi.org/https://doi.org/10.1016/j.cose.2016.01.004

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *J Psychol*, *91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. *J Exp Soc Psychol*, *19*, 469-479.

Salloum, S., Gaber, T., Vadera, S., & Shaalan, K. (2021). Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey. *Procedia*

Computer Science, *189*, 19-28. https://doi.org/https://doi.org/10.1016/j.procs.2021.05.077

Schuetz, S. W., Steelman, Z. R., & Syler, R. A. (2022). It's not just about accuracy: An investigation of the human factors in users' reliance on anti-phishing tools. *Decision Support Systems*, *163*, 113846. https://doi.org/https://doi.org/10.1016/j.dss.2022.113846

Shamya Karumbaiah, R. T. W., Alexandra Durcikova, Matthew L. Jensen. (2016). Phishing Training: A Preliminary Look at the Effects of Different Types of Training. WISP 2016 Proceedings. 11 [https://aisel.aisnet.org/wisp2016/11].

Sheng, S., Lanyon, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010, 04). *Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions* Conference on Human Factors in Computing Systems - Proceedings,

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*, 199-207. https://doi.org/https://doi.org/10.1016/j.chb.2015.01.046

Simon, V., Igor, B., & Blaž, M. (2023). Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign. *Computers & Security*, *125*, 103038. https://doi.org/https://doi.org/10.1016/j.cose.2022.103038

Singh, K., Aggarwal, P., Rajivan, P., & Gonzalez, C. (2023). Cognitive elements of learning and discriminability in anti-phishing training. *Computers & Security*, *127*, 103105. https://doi.org/https://doi.org/10.1016/j.cose.2023.103105

Steinmetz, K. F., Pimentel, A., & Goe, W. R. (2021). Performing social engineering: A qualitative study of information security deceptions. *Computers in Human Behavior*, *124*, 106930. https://doi.org/https://doi.org/10.1016/j.chb.2021.106930

Stembert, N., Padmos, A., Bargh, M. S., Choenni, S., & Jansen, F. (2015, 7-9 Sept. 2015). A Study of Preventing Email (Spear) Phishing by Enabling Human Intelligence. 2015 European Intelligence and Security Informatics Conference,

Steves, M., Greene, K. and Theofanos, M. (2019). A Phish Scale: Rating Human Phishing Message Detection Difficulty, Workshop on Usable Security and Privacy (USEC) 2019, San Diego, CA, US, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927333 (Accessed April 27, 2023).

Sturman, D., Valenzuela, C., Plate, O., Tanvir, T., Auton, J. C., Bayl-Smith, P., & Wiggins, M. W. (2023). The role of cue utilization in the detection of phishing emails. *Applied Ergonomics*, *106*, 103887. https://doi.org/https://doi.org/10.1016/j.apergo.2022.103887

Sutter, T., Bozkir, A. S., Gehring, B., & Berlich, P. (2022). Avoiding the Hook: Influential Factors of Phishing Awareness Training on Click-Rates and a Data-Driven Approach to Predict Email Difficulty Perception. *IEEE Access*, *10*, 100540-100565. https://doi.org/10.1109/ACCESS.2022.3207272

Taib, R., Yu, K., Berkovsky, S., Wiggins, M., & Bayl-Smith, P. (2019, 2019//). Social Engineering and Organisational Dependencies in Phishing Attacks. Human-Computer Interaction – INTERACT 2019, Cham.

Tam, C., Conceição, C. d. M., & Oliveira, T. (2022). What influences employees to follow security policies? *Safety Science*, *147*, 105595. https://doi.org/https://doi.org/10.1016/j.ssci.2021.105595

Tandon, A., & Nayyar, A. (2019, 2019//). A Comprehensive Survey on Ransomware Attack: A Growing Havoc Cyberthreat. Data Management, Analytics and Innovation, Singapore.

Tapsuwan, S., & Rongrongmuang, W. (2015). Climate change perception of the dive tourism industry in Koh Tao island, Thailand. *Journal of Outdoor Recreation and Tourism*, *11*, 58-63. https://doi.org/https://doi.org/10.1016/j.jort.2015.06.005

Tejay, G. P. S., & Mohammed, Z. A. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. Information & Management, 60(3), 103751. https://doi.org/https://doi.org/10.1016/j.im.2022.103751

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, *70*, 376-391. https://doi.org/https://doi.org/10.1016/j.cose.2017.07.003

Thompson, T. (1997). Do we need to train teachers how to administer praise? self-worth theory says we do. *Learning and Instruction*, *7*(1), 49-63. https://doi.org/https://doi.org/10.1016/S0959-4752(96)80730-4

Tsai, H.-y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138-150. https://doi.org/https://doi.org/10.1016/j.cose.2016.02.009

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, *123*, 29-39. https://doi.org/https://doi.org/10.1016/j.ijhcs.2018.11.003

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, *49*(3), 190-198. https://doi.org/https://doi.org/10.1016/j.im.2012.04.002

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security*, *77*, 860-870. https://doi.org/https://doi.org/10.1016/j.cose.2018.03.008

Vrhovec, S., Bernik, I., & Markelj, B. (2023). Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign. Computers & Security, 125, 103038. https://doi.org/https://doi.org/10.1016/j.cose.2022.103038

Vrhovec, S., & Mihelič, A. (2021). Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. *Computers & Security*, *106*, 102309. https://doi.org/https://doi.org/10.1016/j.cose.2021.102309

Washo, A. H. (2021). An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports*, *4*, 100126. https://doi.org/https://doi.org/10.1016/j.chbr.2021.100126

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, *120*, 1-13. https://doi.org/https://doi.org/10.1016/j.ijhcs.2018.06.004

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs*, *59*(4), 329-349. https://doi.org/10.1080/03637759209376276

Witte, K. (1994). Fear control and danger control: A test of the extended parallel process model (EPPM). *Communication Monographs*, *61*(2), 113-134. https://doi.org/10.1080/03637759409376328

Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/2601248.2601268

Xu, T., Singh, K., & Rajivan, P. (2023). Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks. *Applied Ergonomics*, *108*, 103908. https://doi.org/https://doi.org/10.1016/j.apergo.2022.103908

Yan, Y., Jacques-Tiura, A. J., Chen, X., Xie, N., Chen, J., Yang, N., Gong, J., & MacDonell, K. K. (2014). Application of the Protection Motivation Theory in predicting cigarette smoking among adolescents in China. *Addictive Behaviors*, *39*(1), 181-188. https://doi.org/https://doi.org/10.1016/j.addbeh.2013.09.027

Yazdanmehr, A., Li, Y., & Wang, J. (2023). Employee responses to information security related stress: Coping and violation intention [https://doi.org/10.1111/isj.12417]. *Information Systems Journal*, *33*(3), 598-639. https://doi.org/https://doi.org/10.1111/isj.12417

Zhao, R., John, S., Karas, S., Bussell, C., Roberts, J., Six, D., Gavett, B., & Yue, C. (2017). Design and evaluation of the highly insidious extreme phishing attacks. *Computers & Security*, *70*, 634-647. https://doi.org/https://doi.org/10.1016/j.cose.2017.08.008

Zhuo, S., Biddle, R., Koh, Y. S., Lottridge, D., & Russello, G. (2023). SoK: Human-Centered Phishing Susceptibility. *ACM Trans. Priv. Secur.*, *26*(3). https://doi.org/10.1145/3575797

10 APPENDIX

10.1 Appendix A – interview guide

Interview guide

- Greetings and formalities

SOURCES OF INFORMATION

- What do you work with?
    - Has that always been your job, or do you have other experience?
    - How long have you been working here?
        - How long did you work at the other workplace?
- How do you feel about receiving emails?
- How long have you been receiving emails for?
- Have they become more complicated since you started using emails?
    - How so?
- Have you seen phishing emails before?
    - How often do you see phishing emails?
    - How long have you been receiving phishing emails?
    - Have you ever been a phishing victim before?
        - How was that experience compared to this one?
- How is phishing handled within the company?
    - How often do you talk with your coworkers about phishing?
    - How is the focus on encouraging each other to avoid phishing emails?
    - Do you ever learn anything phishing related from coworkers?
        - If not, where do you learn phishing related information?

COGNITIVE MEDIATING PROCESS – MALADAPTIVE RESPONSE

- How is the response to avoiding phishing attacks from peers and superiors?
    - If no response, do you get any other rewards for avoiding phishing emails?
        - If no rewards, how would rewards affect your process when receiving emails?
        - What should the rewards be? Clap on the shoulder, kind word, or something monetary?
- How is phishing described amongst your peers?
    - Which connotation does phishing have when discussed?
    - How is phishing referred to in terms of severity?
    - What is your emotional response when you hear about phishing?
        - If not really a response, what was your emotional response when you got phished?

    - How would you describe the relationship between fear and phishing emails?
        - If little or no relationship, what can the relationship be described as?

COGNITIVE MEDIATING PROCESS – ADAPTIVE RESPONSE

- How do you feel about your own ability to discern a phishing email from a real email?
    - What do you believe first when you process an email? That the email is a scam or a real email?
        - What would be the factors that decide whether it is a scam or real email?
    - Do you have high self-confidence when you decide that something is fake?
        - If not, how could that self-confidence be improved?
- How does the difficulty of differentiating between real or fake emails affect your motivation to spend time and resources to check for legitimacy?
    - How much resources are accepted to spend in your workplace to check if emails are legitimate?
        - If not sure, would 1 minute per email be an unjust amount of time to spend on just the legitimacy of the email?
    - How is time spent on security discussed in the workplace, or at all?

THEIR PHISHING EXPERIENCE

- What was the process of you becoming phished?
    - Did you notice immediately?
    - Do you remember what the email was about?
    - How was it convincing?
    - What did the email want you to do?
    - Which security checks did you do before doing what the email wanted you to do?

10.2 Appendix B – Thematic analysis of interviews

Code one was assigned to rewards which include intrinsic rewards and extrinsic rewards. There were varied answers to how rewards affected the participants, however, most agreed that the major reward was the intrinsic reward they would feel after doing well in the phishing campaign. This could be from having an empty inbox as mentioned by participant 4 mentioning that they feel great when receiving feedback. "*I receive a great feeling from having an empty inbox and knowing that I have done my work well. I also feel as though I have succeeded when I receive feedback after 5 minutes after I have successfully reported an email sent via the phishing campaign. This brings me great joy.*" *Participant 2 has the same opinion stating: the biggest reward would probably be to receive the email saying that you are the security champion of the month. That is great motivation. Participant 10 thought of the rewards differently: I think a previous system where I worked before was better. That involved points-based tasks and training with direct competition between the employees. This caused a friendly rivalry at work where you competed to gain the most points by doing the best work and learning the most. The greatest reward was getting the digital trophy at the end of this period. The current system does not motivate me as well as the one from the previous job. Participant 8 had a different approach to the reward system: "I feel as though the phishing campaign is a competition with myself to do the best I can. However, I do like to lead a phishing- or spam email on if I clearly see that there is no danger and say that I am not interested in the end to waste their time." Participant 3 follows participant 8 in trying to see the humour: "I think phishing emails can be quite annoying both real and from the phishing campaign, but I do acknowledge the reward I feel when I do well. In addition, there is a humour reward associated to poorly constructed phishing emails that makes you think: "what were they thinking?" when designing the bad phishing email. You must see the fun in some phishing emails on occasion between all the serious or difficult emails that is sent". The three remaining participants specify that phishing emails are nothing but small obstacles and annoyances on a daily basis and does not feel any reward when succeeding on a phishing test because it is a part of the job and a matter of course to succeed on the phishing test. There are also extrinsic rewards for the employee that does best on the phishing campaign over a three-month period. However, the $500USD does not create any emotional investment nor interest over the digital trophy that clearly state that they had successfully caught and reported phishing emails with great accuracy. Therefore, the extrinsic reward that exist is not interesting compared to the intrinsic rewards that most participants mentioned.*

The second code is perception of vulnerability where most participants are aware and agree on the fact that the organisation and themselves are always vulnerable to phishing emails. However, very few makes the distinction between being vulnerable to phishing and acknowledging that they are always in great risk of being phished. This is due to the laid-back attitude where they always resort to the policies in place and rely on the training they have received and their personal experiences. Participants 6 and 9 demonstrate that they believe that they are above average capable of avoiding phishing attacks. One participant has never been phished due to their background in security, however ironic, participant 6 has been tricked by the phishing campaign before as they note: "phishing emails are just an annoyance and noise in the day-to-day operation of the organisation as well as privately. However, as much as they (phishing emails) are

an annoyance, I do believe I am above average capable of seeing the difference between real and fake emails, even though I have been a victim before as ironic as it is". Participant 9 states the same, although they have a very strict method of reporting an email where no more than 10 seconds are used to validate the email. If they are not able to validate the email it is sent via a report to the security team. Others note that phishing has become very prevalent and is in an ever-changing state to where constant re-training is needed. Multiple participants collectively add onto the discussion where the baseline is that emails are in constant change. One participant adds: "emails has become a tool for tricking, marketing, and advertising. There is a possibility that I will be a phishing victim multiple times". Participant 7 add in opposition: "I think phishing is focused on too much. I do not mean that we should stop focusing on phishing, however, I do think we neglect many other ways that someone can get tricked and give up information." The participant then gave some examples that resembles vishing and SMiShing. Participant 1 gave their understanding of vulnerability to also include the assets that are vulnerable if a phishing attempt was successful as they note: "the danger is that very important or classified information could be collected if a machine is successfully infected. This could be months of work to fix due to an issue that is big business but cheap crime." As a collective, all participants in this organization are acutely aware of the vulnerabilities connected to phishing is very dangerous and is a high-risk issue.

Perception of severity is the third code indicating how dangerous the consequences are if they get phished. Severity in this case focuses on the consequences that participants would face if they got phished. Overall, all employees seemed to know what the consequences were and how they could be affected if they made mistakes multiple times. Participant 1 was very aware of the consequence where they could be fired according to policy if they failed the phishing tests 9 times in 24 months as they stated: "they have this e-learning program that sends out phishing tests that monitor the employee and whether they get tricked or not. It is actually so strict that if you get tricked 3 times you get an oral warning, and if you get tricked 6 times you get a written warning and so on until you get fired." The participant further explain that this is well known by all employees. This is confirmed by participant 2 who mention that: "you can actually get fired after 18 failures as you need three written warnings as required by the labour laws. However, I find the strictness to be a relief as everyone takes security just as serious. Because of the monitoring done locally on the computer, you can also be punished for leaving your computer without locking it because it is an inherent security risk. This is all understandable and everyone is informed when they start in the company and are reminded of the consequences if they fail a phishing test. It can be frightening at first, but you understand very quickly that it is for your own good." Other participants note the same ideas and agree with some caveats. Participant 10 noted: "the punishment for failing a few times is a bit too high considering you can get fired easily within 2 years if you are not careful". Participant 2 has a background that equate to them knowing the law well, therefore, some employees might think that the punishment is harsher than it really is. Due to none of the participants being tricked more than twice in much more than two years does could mean that a few employees overestimate the punishment, or the mistakes needed to be fired. The other seven participants shared the same perception of severity but did not seem worried.

Code four is the fear appeal that should be based on code two and three. This means that perception of vulnerability and severity should be the decisive factors to the degree of fear appeal. However, participant 1 described the relationship between phishing and fear like this: "I do not fear phishing. (...) I am not worried about my economy or having my information stolen, but it is trouble, right? It is trouble and an annoyance to have to change all my information in the banks and insurance companies and so on. Participant 2 thinks of the relationship between fear and phishing like this: "I do not fear emails or phishing very much. We have systems that does a great job at sorting out phishing emails, and every email from external addresses are marked with a yellow banner waning that the email is not sent from internal addresses. This makes me more aware of potential phishing but does not instil fear in me." When asked if they check for suspicious emails that are sent from internal email addresses: "I do not do the checks on internal emails, no. That is maybe something I need to start doing." Participant 3 mentions: "I do not fear phishing, but I am very aware of them. At some point you must find and use a balance of function and paranoia. (...) If something continues to be suspicious, I will just report it." Multiple participants then go on to share the same notion that phishing does not induce fear; however, it is something that needs to be controlled using phishing training and simulations.

Code 5 and code 6 goes on to measure efficacy in forms of self-efficacy and response-efficacy. This means the confidence that a participant has in that their answer and solution to an issue is correct. Participant 1 says this about their self-efficacy: "I have a high degree of response-efficacy and is very quick when I go through my emails. Out of 50 emails, 49 will probably be deleted or reported by looking at the email header." The participant does not mention that there has ever been an issue with this method. However, they do mention on the topic of self-efficacy: "I have a good understanding of phishing and how to discover phishing emails. I do believe that the chance of me being phished is very low. However, I believe that the way I would get phished is by having or spending too little time evaluating an email and not doing all my checks. That is what will get me one day." This shows that the participant is familiar with the risks associated with having too high self-efficacy. Participant 2 notes the difference between work and private email and states this: "I think that since I was started in this company, I have gotten a lot better at checking for phishing. However, I do not check my private email as well as my work email. This is due to the number of spam and phishing emails that I receive every single day. Therefore, I will only check my private email when I expect an email. Otherwise, I go through the same checks to not get phished." They go on to make the same point as participant 1: "I do believe I have high self-efficacy and believe that it is justifiable with all the training and passed simulations I have. However, having too high self-efficacy does make for a dangerous situation if you choose to not spend enough time looking at the email and going through the checks you are supposed to do. Then there is a risk I will be phished." Multiple other participants also share a similar opinion: "I think that having high response-efficacy is good and that my awareness is high. However, I think this is due to the continuous training we have where we learn about new techniques that are used. There is always a chance of failing a phishing test when a new type of phishing appears, and due to this we must always work on our skills." The sentiment is shared by multiple other participants as one adds: "I always have my checks that I do before clicking on anything, especially on external emails. I always look at the true sender's email address and google the domain if I am

uncertain that it is legitimate." A couple of participants echo their previous statements about them having a higher degree of awareness and understanding than the average and would not be phishing victims. However, they also echo the same ideas that training is important, but the frequency of phishing simulations is too high at times.

Code 7 regards response cost and if the organisation set any limit to the amount of time they can spend on checking for legitimacy. There are 9 similar answers that points out that there is no limit and that they can spend as much time as they want checking for legitimacy. An opinion is echoed by the 9 participants who answer the same: if they are unsure of the legitimacy of an email after 20 seconds, they will delete or report it based on relevance. The one differing opinion relates to multiple factors: "My job is not to read emails; however, it does take much of my time. Therefore, if I spend much time evaluating every email that comes through, I would not be able to do my actual job. Between the meetings I have and reading emails, I have many other documents I must read though to do my job. Therefore, I tend to spend too much time reading emails and that affects my workflow and amount of work I can do elsewhere." This opinion is a very important perspective that oppose the other 9 participants and should not be ignored due to it being the opinion of one participant.

Code 8 regards threat appraisal and is an evaluation of code 1-4. Based on the answers given, a finding was that not a single participant felt fear, and the intrinsic reward should not be able to encourage protection motivation alone. However, all participants felt a protection motivation even when they did not know if there was a danger present or not. There is a major personal focus on the intrinsic rewards, and an organisational focus on the severity and vulnerability due to phishing. However, the participants did not seem to actively show their worries as they seemed in control of every aspect of the phishing threat. This does not mean that the perceived severity and perceived vulnerability does not have an effect; however, it is a puzzling choice of communication when talking about a threat that could be devastating to their organisation.

Code 9 refer to the coping appraisal which include the aspects from code 5-7. Is involves the efficacies and response costs related to validating the validity of emails. The gist of the coping appraisal is nearly identical to code 7 where 9 participants ended up having high self- and response-efficacy in addition to next to zero response cost except the one participant who must set artificial time limits for themselves. Other than this, there should be no reason for why the protection motivation should not always be present and the participants be unlikely to get phished.

Code 10 is the last code in the thematic analysis, and it does not pertain to the main aspects of the PMT model. Rather, it is connected to the maladaptive coping methods that was used when someone got phished. One participant got phished on their private email but using the company laptop. They explain the situation like this: "I had just come off a call with my telecom supplier and received an email from what appeared to be the same company. They used my full name and explained that there was a change in my invoice which was exactly what I had just been in a phone with them about. I ended up clicking on the attachment with the new invoice and nothing happened. I understood at that point that something was wrong. My laptop was remotely locked and quarantined after 15 minutes and I had to get a new operating system image loaded onto my laptop." In essence, the participant got phished due to the extreme timing and context of the

phishing email. Another participant explained two work related phishing incidents related to stressful situations: "In both situations I was off work when I got an email from my boss informing me that I had to transfer money to another account as I worked in accounting at the time. The text was in big bold letters, and I opened the email on my phone. I clicked the link and loaded a webpage that I could not access without my laptop. I got an email not too long after saying it was a phishing attack and no transfers was to be made. The other occasion was also on my time off when I received an email from my director saying I needed to forward the email to a certain group of people. I did that on my phone and received a warning letter afterwards that I had been phished through the internal phishing campaign and an email was sent to my supervisor. It was really frightening at that time, but I understood why it was so serious. Now I exclusively check work emails on my laptop and go through the checks I have set for myself." Another participant had the same experience where they forwarded a link to multiple coworkers and received an email stating that they had gotten phished.

10.3 Appendix C – literature review table

ors	Phishing susceptibility	Predictive analysis	Digital phishing detection	Threat avoidance theory	Gamification theory	Protection motivation theory	Signal detection theory	Contextual theory	Prospect theory	Theory of planned behaviour	Cognitive processing theories	Dual process theory	Routine activities theory	Practise theory	Cue utilization
Abbasi et al., 2021	x	x													
Afroz & Greenstadt, 2011	x		x												
Al-Qahtani & Cresci, 2022	x														
Aleroud et al., 2020	x									x					
Aleroud & Zhou, 2017	x		x												
Arachchilage & Love, 2014	x			x											
Arachchilage et al., 2016	x			x	x										
Bax et al., 2021	x					x									
Benenson et al., 2017	x														
Bhardwaj et al., 2021	x		x												
Buckley et al., 2023	x														
Burns et al., 2019	x														
Butavicius et al., 2020	x														
Butavicius et al., 2016	x														
Butavicius et al., 2022	x						x								x
Caputo et al., 2014	x														
Carroll et al., 2022	x														
Chen et al., 2020	x														
Chen et al., 2021	x					x									
Clarke et al., 2012	x														
da Silva et al., 2022	x	x													
Ferreira & Teles, 2019	x														
Frank et al., 2022	x							x							
Ge et al., 2021	x						x								
Goel et al., 2021	x								x						
Gordon, Wright, Aiyagari, et al., 2019	x														
Gordon, Wright, Glynn, et al., 2019	x														
Grassegger & Nedbal, 2021	x									x					
Guedes et al., 2022	x														
Gupta et al., 2018	x														
Harrison et al., 2016	x										x				
Ikhsan & Ramli, 2019	x														
Iuga et al., 2016	x														
Jaeger & Eckhardt, 2021	x					x									
Jingguo Wang, 2016	x		x								x				x
Junger et al., 2017	x														
Kelley et al., 2023	x											x			
Kwak et al., 2020	x										x				
Lawson et al., 2020	x						x								
Li et al., 2020	x														
Luo et al., 2013	x														
Martin et al., 2021	x														
Musuva et al., 2019	x										x				
Paek & Nalla, 2015	x												x		
Petrič & Roer, 2022	x														
Pfeffel et al., 2019	x														
Rajivan & Gonzalez, 2018	x														
Rameem Zahra et al., 2022	x		x												
Rocha Flores & Ekstedt, 2016	x									x					
Salloum et al., 2021	x		x												
Schuetz et al., 2022	x		x												
Shamya Karumbaiah, 2016	x				x										
Singh et al., 2023	x										x				
Steinmetz et al., 2021	x													x	
Stembert et al., 2015	x														
Steves, 2019	x														
Sturman et al., 2023	x														x
Sutter et al., 2022	x														
Taib et al., 2019	x														
Vrhovec et al., 2023	x					x				x					
Washo, 2021	x														
Williams et al., 2018	x														
Xu et al., 2023	x														
Zhao et al., 2017	x		x												
Zhuo et al., 2023	x														

10.4 Appendix D