Hook, Line and Sinker: A Case Study of An Older Persons' Experience of Responding to a Phishing Email

A Thesis submitted by

Kara Joyce Montefiore

For the award of

Masters of Science (Research) (Psychology Specialisation)

2022

Abstract

Phishing emails are a form of cybercrime that has, for the past 20 years, affected thousands of older persons in Australia. Each year approximately 200 million dollars have been scammed from this vulnerable population, and these emails remain a significant concern. Readily available education and information do not appear to have significantly affected older persons recognising one of these emails. Demographic information shows that older persons are more likely to engage with these emails than any other cohort. This study examined an older person's experience with a phishing mail through a single case analysis to better understand how older persons interact with phishing emails. Examination of the email communication between the phisher and the older person and a series of interviews with the older person provided the data to apply the Theory of Deception and Social Judgment Theory to understand better why the older person engaged with the phishing email. The analysis of the email communication and interviews proved the complex nature of why older persons are more susceptible to phishing emails. The theories can contribute to a transtheoretical model or framework to understand the experience of phishing among older adults. This study emphasises that education and information for older persons regarding phishing emails must be person-centred.

CERTIFICATION OF THESIS

This Thesis is entirely the work of Kara Joyce Montefiore except where otherwise acknowledged. The work is original and has not previously been submitted for any other award, except where acknowledged.

Principal Supervisor: Tanya Machine

Associate Supervisor: Sonya Winterbotham

Student and supervisor's signatures of endorsement are held at the University.

ACKNOWLEDGEMENT STATEMENT

This research has been supported by an Australian Government Research Training Program Scholarship. The completion of this study could not have been possible without my supervisors' support and consistent encouragement, Dr Jan du Preez and Dr Tanya Machin. This journey started with a meeting with Dr Machin about what to do after completing my undergraduate degree. The time Dr Machin spent with me discussing various ideas led to an appointment with Dr. du Preez, and before I knew it, Dr. du Preez and Dr Machin had agreed to be my supervisors, and the journey began. Dr du Preez and Dr Machin have shown endless patience, always listening, challenging, and guiding me. I will always be grateful and humbled; you never let me give up, and you stayed with me till the end; thank you. I wish to thank Sonya Winterbotham for coming on board and supporting me in completing my thesis. I am grateful for the time you have taken to provide additional support to myself and Dr Machin. I want to express deep and sincere gratitude to my parents for their love and support. Their patience has meant so much throughout this journey, and I would not have completed my studies without you. I want to pay special attention to my Nanna, who sparked my interest in learning more about the aged community and planted the seed of curiosity. I wish to thank my brother, sister-in-law, my beautiful nieces, "the aunties," and my uncles and cousins for their encouragement throughout this journey; it has meant so much.

Finally, I would like to thank my dear friend Clare who volunteered time; she did not have to study with me, encouraged and was always willing to be a sounding board. Your friendship has been invaluable, and I am thankful to have you as a friend.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

%: Percentage.....2, 14, 17

ABS: Australian Bureau of Statistics..... 16-17

ACCC: Australian Competition and Consumer Commission 1-2, 5, 7, 10, 17, 19, 22, 45-47

AOL: American Online.....3, 4

ATO: Australian Taxation Office 9, 10, 33

e.g., for example,.....1, 2, 27, 57

ELM: Elaboration Likelihood Theory……12, 27

et al.: and other..... 1-47

HSM: Heuristic-Systematic Model……....12, 27

i.e: id est, that is 1, 2, 3, 17, 23, 49

ICT: Information Communication Technology 17, 72

ISP: Internet Service Provider 4

n.d.: no date.....2, 70

org 2, 4, 68, 70

pp: pages 21

SJT: Social Judgement Theory…….15, 27, 28, 56-59

SMS: Short Message Service.....5

TA: Thematic Analysis..... 34-36, 38,

TD: Theory of Deception…….11, 12, 14, 27, 56

URL: Uniform Resource Locator 5, 14

WHO: World Health Organisation 17,

1: Research Rational

Introduction

The 21st century faces two global phenomena: an aging population and the continued rapid inclusion of technology in everyday life (Russell, 2005; Umanailo et al., 2019). Rapid technological advancements profoundly impact how older people engage with their environment, such as accessing everyday services. These impacts include contact with financial institutions and access to personal banking and health information, transportation ordering (i.e., taxi-type services such as Uber), and communication with family and friends (Russell, 2005; Umanailo et al., 2019). While technological and communication advancements provide benefits, they also generally present problems and challenges for society (Szabo et al., 2019; Williams & Polage, 2019). For example, benefits include the ability for people to connect more easily through emails and share information and communicate with others through sites such as Facebook or Twitter. The challenges of these advancements are they are evolving exponentially and continue to be a source of concern for individuals' privacy and security. For example, personal data is more frequently shared, and people must have an email address to use and interact with many online services and resources (Janez-Martion et al., 2021; Vayansky & Kumar, 2018).

Focused criminal behaviour using technology has also rapidly increased, with older persons more likely to be affected and become victims of this behaviour (Australian Competition and Consumer Commission Scamwatch (ACCC, 2021, 2020, 2019). More specifically, these criminal behaviours focus on scamming individuals – most often through emails – for their personal information and/or to obtain money through fraudulent means. An older person's financial and psychological impact from engaging with these fraudulent emails can be devasting and include long-term psychological, emotional, and economic effects (Carlson, 2006; Williams et al., 2017). The ACCC (2021, 2020, 2019) has shown that older

persons are the most affected demographic of these fraudulent emails, despite multiple resources to provide information and education. Therefore, the importance of better understanding why an older person may engage with a phishing email is essential.

Cybercrime rates are increasing, with tech-savvy criminals manipulating and exploiting the everyday use of online services that have become commonplace in contemporary society (Vayansky & Kumar, 2018). One form of cybercrime that continues to be particularly concerning is Phishing, a socially engineered technique to acquire private and sensitive information such as usernames, passwords, and financial and identification details (Alsayed & Bilgrami, 2017; Vayansky & Kumar, 2018). In 2019, over 25,000 phishing scams were reported to the ACCC Scamwatch, with 32.8% of these phishing scams delivered via email.

The financial loss of $1,517,864 in 2019 shows a considerable increase from $363,270 in 2015 (ACCC, 2019). The ACCC (2020) reports that as of April 2020, there have been 10,689 different types of phishing scams, resulting in a total loss of $309,108. The developmental stage most affected by phishing scams is that of older persons (those over 65 years -old), with approximately 30% of this group having previously engaged in a scam. Phishing scams can be delivered in various ways, including phone calls, text messages, social media sites (e.g., Facebook or Google searching), and emails (ACCC, 2020). Emails have continued to be a profitable delivery method for cybercriminals since email first became commonplace in the late 1990s (ACCC, 2021; McCombie, 2008; Phishing Org, n.d.).

When focusing just on emails, phishers (i.e., people who engineer and carry out phishing scams) typically send bulk emails to unsuspecting individuals. They scrape email information through different sources, including websites containing email addresses, or they use artificial intelligence to target individuals. These emails contain information indicating there is something wrong with an individual's account (e.g., often a bank account or web-

based subscription services such as iTunes) and that the person should respond to this information by clicking on a link contained within the email to verify their ID or confirm their password (Alsayed & Bilgrami, 2017; Carlson, 2006). The individual is then redirected to a fake website and asked to enter personal details, thus enabling phishers to access the victim's accounts, or upload malicious malware to the individual's computer, often for tracking or monitoring purposes (Alsayed & Bilgrami, 2017; Carlson, 2006). These phishing emails' primary purpose is to deceive people into thinking the email is from an established and trusted organisation or institution for dishonest gain (Bose, Chen, Leung, & Guo, 2011; Williams, Beardmore, & Joinson, 2017). In constructing phishing emails, phishers use familiar logos, colours, and legitimate-looking website links (Vayansky & Kumar, 2018; Williams et al., 2017). For example, if the phishing email were from a particular financial institution (i.e., Westpac), it would contain the bank's logos and symbols, text and/or language the bank would typically use. The email signatures from a fictitious bank staff member with an authentic branch or divisional details. The underlying expectation for a successful phishing attempt is that the targeted individual will not notice the subtle differences between a legitimate email from the organisation and the constructed phishing email and additionally will not check web addresses to confirm the details before clicking on any redirection links (Vayansky & Kumar, 2018; Williams et al., 2017).

Aims and research question

Given that older people are more likely to engage with phishing emails and that the impacts of phishing can be significant, it is essential to gather in-depth knowledge about why a person would engage with a phishing email. Therefore, the aim of this research is to better understand why an older person engages with a phishing email by focusing on a single case study of one older person’s experience. The research question is why did an older person engage with, and continue to engage with a phishing email?. Current literature and research

focus predominately on using quantitative data in controlled environments or qualitative data gathered through surveys. Qualitative data in surveys is also quite limited and will not have the depth and breadth that a case study will provide. A single case study design allows for data from different sources and methods. It provides rich data within a real-world context that other qualitative methods do not provide. Data sources can then focus on the email correspondence between an older person and a phisher and provide additional depth to the research by using interview responses from the older person. While the case study design is not a research method, email correspondence significantly adds to that real-world context, and interviews will assist in better understanding the complexity of one older person's decision-making and the impacts of a phishing email.

History of Phishing

While there is no universally accepted definition of Phishing, the term first appeared in an American newspaper in 1997, which reported on the latest online scam to get people to hand over their account details with the intent to defraud the consumer (Monhammad, Thabtah, & McCluskey, 2015; Phishing.org, 2018; Radar & Rahman, 2013; Rekouche, 2011). The earliest phishing scams focused on stealing an individual's identification and logging in to an Internet Service Provider (ISP) without paying for internet use (Radar & Rahman, 2013; Rekouche, 2011). The individuals responsible for these scams were initially referred to as *Haxor*, later called phishers, in the late 1990a after a program designed to steal people's details by flooding email accounts with fraudulent emails and links to fake websites (Banu & Banu, 2013; Radar & Rahman, 2013; Rekouche, 2011).

More recently, Aleroud and Zhou (2017) identified four dimensions of Phishing: Communication Media, Target Environments, Attack Techniques and Countermeasures. Communication Media requires the human element and people to interact with the phishers' applications (Aleroud & Zhou, 2017). The basic premise of a fraudulent phishing email is to

obtain confidential information from the victim, such as bank account details, which are then used to steal money or launch other attacks on the victim (Banu & Banu, 2013; Bisson, 2019; Mohammad et al., 2015). This form of Phishing also mimics official correspondence from perceived legitimate organisations such as banks or government departments (Bisson, 2019; Banu & Banu, 2013). These emails will typically ask the phishing victim to confirm, update, or validate their organisational credentials, often instructing them to click on a URL link included in the email (Bisson, 2019; Mohammad et al., 2015). Over time, phishing or attaches have used other forms of day-to-day electronic communication such as SMS messages, links embedded in Facebook pages and other online social media platforms. Email continues to be the most prevalent form of phishing attack; people have access to emails more readily through apps on their smartphones and tablets. Understanding why a person would engage with a phishing email requires a combination of frameworks, theories and models to explain the complexity of the why.

Social Engineering Framework

Since the mid-1980s, phishing emails have been studied to improve computer security and educate the public and organisations, yet individuals continue to engage with these emails (Ferreira & Teles, 2019; Parsons et al., 2019; Williams & Polage, 2018). Research into why people engage with phishing emails has often focused on the role social engineering plays, the commonly used term to describe how current social behaviours, influences, and changes play a role in the future development of societies (Ferreira & Teles, 2019; Tetri & Vuorinen, 2013). Social engineering within the context of Phishing is the psychological manipulation of people into performing actions or disclosing confidential information (Cialdini, 2009; Ferreira & Teles, 2019; Parsons et al., 2019; Williams et al., 2017). Tetri and Vuorinen (2013) argue individuals who create these fraudulent emails are manipulating what could be considered the weak human element to bypass technical protection (Mann, 2008).

Phishing emails deceive the victim into believing the email is trustworthy, using personal and contextual information and thus providing validation for the victim to engage with it (Cialdini, 2009; Ferreira & Teles, 2019; Parsons et al., 2019). Many factors influence a person engaging with a phishing email: their understanding of technology at the time, how the person processes information, and the external influences of their day-to-day experience (Tetri & Vuorinen, 2013; Ferreira & Teles, 2019).

Many models have been developed within the Social Engineering framework to understand social engineering attacks' uses. One of the challenges with using only one model or framework is a model is a presentation in schematic form (Mitnick & Simon, 2003; Mouton et el., 2015; Zheng et al., 2019). In contrast, a framework is a structure or system (Mitnick & Simon, 2003; Mouton et el., 2015; Zheng et al., 2019). One model or framework does not fully include all aspects of social engineering. For example, there are two models within the Social Engineering framework; phased-based and conceptual (Zheng et al., 2019). The phased-based model focuses on the attack process, a form of the social engineering attack cycle where if the phisher does not achieve their goal, they will repeat previous steps in the cycle to achieve their desired outcome (Mitnick & Simon, 2003; Zheng et al., 2019). Within the phase-based model, there are four-phase; researching target/targets, rapport building, exploiting the trust and utilizing information gained (Mitnick & Simon, 2003; Zheng et al., 2019). The conceptual model focuses on every attack step, elaborating on Mitnick's four phase-based models, from determining the attack's goal to the successful conclusion (Mouton et el., 2015). What these two models assist in explaining is the steps a phisher will take, but it does not elaborate on how they achieve each step. As noted previously, social engineering within the context of Phishing is psychological manipulation, so what social psychological tools does the phisher use? (Cialdini, 2009; Ferreira & Teles, 2019; Parsons et al., 2019; Williams et al., 2017). To better understand the techniques of

social engineering – that is, to get an individual to engage with a phishing email - phishers will manipulate social influences in sophisticated ways (Parsons et al., 2019; Williams et al., 2017).

The Social Engineering Personality Framework consists of six main ideas, developed from social influences that impact everyday life: authority, consistency, liking, reciprocity, scarcity, and social proof (Cialdini, 2009; Ferreira & Teles, 2019; Parsons et al., 2019; Uebelacker & Quiel, 2014; Williams et al., 2017). These ideas provide a structure or system for the phisher to achieve their goal. Authority refers to a person or entity that is perceived to be in a position of power. The victim would be more likely to comply with an organisation such as a government agency or bank because people engage with them daily; there are potential consequences when you do not reply to them (Cialdini, 2009; Ferreira & Teles, 2019). Consistency involves repetitive behaviour; for example, phishers will rely on an individual opening email out of habit as this is something that they do regularly. Liking comes from being drawn to the email; something familiar is for their attention. Reciprocity involves the victim wanting to give back; for example, in social situations, the simple act of gift-giving can require the recipient to give back, according to social etiquette rules (Parsons et al., 2019; Williams et al., 2017). Phishers will use scarcity to manipulate the victim to "act now or miss out," as if the perceived prize, for example, was a one-time claim. Social proof, also known as informational social influence, explains how people copy others' actions to undertake behaviour in any given situation (Parsons et al., 2019; Williams et al., 2017). An individual will engage with phishing emails where they think they should, such as responding to a request to sponsor a child in need overseas. Phishing emails often use a combination of these influences that lure the individual to engage with them. An example of how phishers can combine these aspects of social influence into a phishing email was in March 2019. An email believed to be from the Australian Taxation Office (ATO) was sent to over 300,000

Australians (refer to Figure 2) (ATO, 2020).

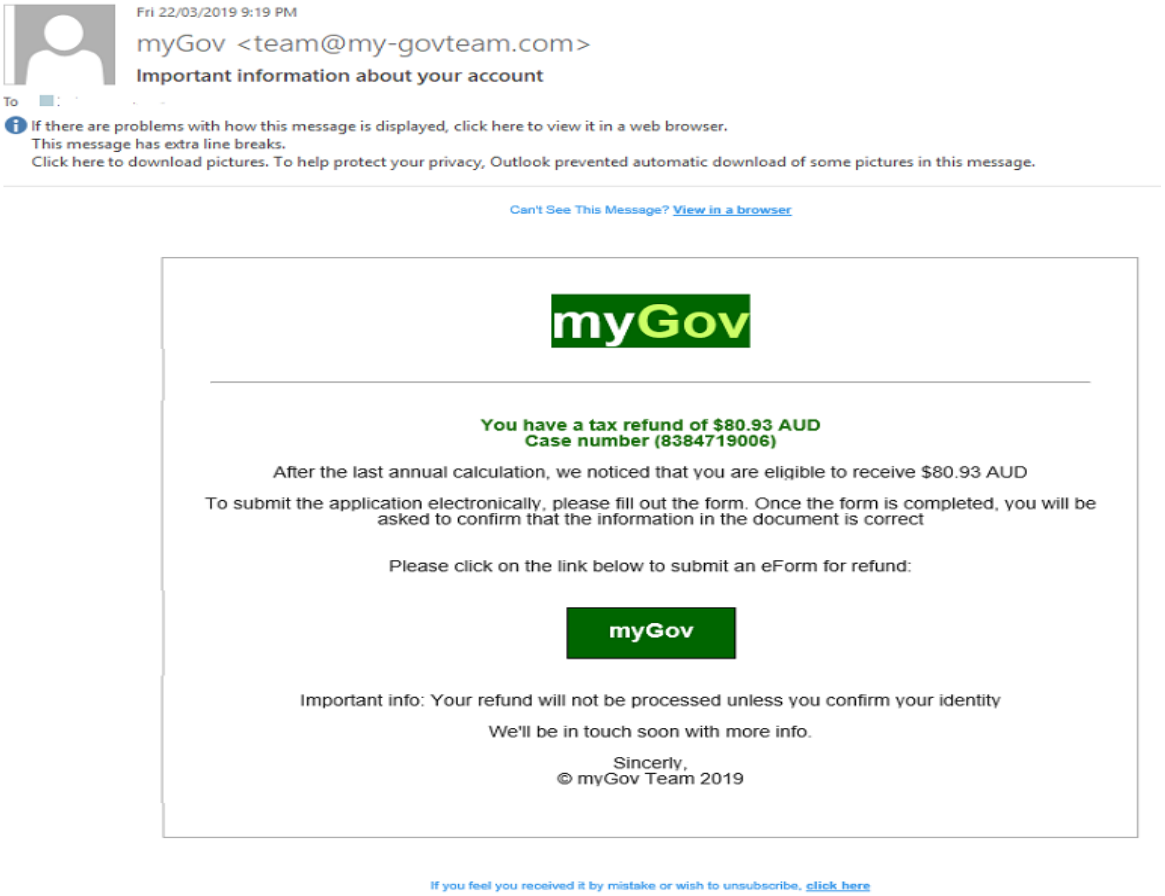

Figure 2. An example of the email sent out to Australians by a phisher impersonating the Australian Taxation Office (ATO, 2020).

This email is an example of using the social engineering Personality Framework and the phase-based model. The phishers targeted people after the end of the financial year who may have already received a tax return, the first phase, establishing the target. The phisher used authority and the influence of reciprocity to lure the targeted audience to engage with the email. The authority is the Australian Taxation Office (ATO), a department of the Australian Federal Government (Parsons et al., 2019; ATO, 2020). Using the ATO, the phisher established rapport with their victims using familiar language and images. The phisher used the influence of reciprocity to exploit the victim's trust in the ATO by being instructed to click on the link in the email, confirm their identity, and receive an unexpected

tax refund. The last phase of this model is the phisher utilising the information the victims provided. The Social Engineering framework can provide the structure to understand better why a person will engage with a phishing email. The limitation of this framework is that it appears to explain why the approach will or should work but does not answer why is it then that some people are more vulnerable than others.

Cognitive, Behavioural and Emotional Factors

Individual human judgement and behaviours, such as those reinforced by habit, responses to authority and external influence such as tactics of persuasion and deception, have informed the understanding of people's responses to phishing emails. Antivirus companies use phishing detection software as a first line of defence in protecting consumers from phishing emails. Identifying and analysing the features of phishing emails has informed phishing detection software, and this focus continues to be relevant (Ferreira & Teles, 2019; Parson et al., 2019). Focusing on the physical features of a phishing email allows for a better understanding of the information the victim is accessing before deciding to open or not open an email message. This software cannot determine the complex human element required to understand the influence or what persuaded the victim; does the subject line have an influence, or is the victim noticing a particular time or date stamp on the email? (Ferreira & Teles, 2019).

Persuasion is one technique phishers will use and which impacts our daily lives and society in powerful ways (Asfer & Bairmani, 2021; Bayl-Smith et al., 2021; Naksawat, Akkakoson & Loi, 2016). Persuasion has been defined in many ways and used by politicians, advertisers, and journalists, to name a few, to affect and influence people daily. Communication that relies on persuasive language and messages can now travel more quickly and further via the introduction of television, smartphones, and the internet. Over time, persuasion has become more subtle, devious, complex and impersonal. For example,

advertisers often use deceptive messaging to influence and persuade a targeted audience instead of sending a general message about products or information they want to share. Nasksawat et al. (2016) report, “with the assistance of present-day technologies, the content of persuasive messages can be changed, giving new meaning that was not originally embedded and that was not intended by the original sender” (pp. 4). Persuasion can achieve positive outcomes, such as implementing change, persuading people to recycle used rubbish or changing people’s proven unhealthy habits such as smoking (Asfer & Bairmani, 2021; Bayl-Smith et al., 2021; Naksawat et al., 2016). There are adverse outcomes, such as salespeople taking advantage of people or spreading misinformation. The negative side of using persuasive communication or persuasion, in general, has been and continues to be used by phishers who apply these strategies to convince readers to agree with what they have deceitfully plotted (Asfer & Bairmani, 2021; Bayl-Smith et al., 2021; Naksawat et al., 2016).

Phishers have become experts in constructing emails and combining the elements of the real-world feel, ease of use, expertise, trustworthiness, and tailoring. A complex interaction of cognitive, behavioural, and emotional factors contributes to an individual identifying a phishing email, being susceptible to those emails, and subsequently engaging with these emails (Purkait et al., 2014). The interactions of these three factors are not linear - they can take different forms and directions. For example, behavioural habits of regular daily email use can influence the cognitive effort used in attending to emails and diminish the cognitive load required to recognise a phishing email (Gavett et al., 2017; Purkait et al., 2014). People’s perceptions can also elicit an emotional response, including a physical reaction to urgent messages requiring a response (Gavett et al., 2017; Purkait et al., 2014). Habits, emotions and physical responses thus influence the cognitive processes needed to recognise these emails (Gavett et al., 2017; Purkait et al., 2014). These will be explored within the Theory of Deception and Social Judgement Theory.

The Theory of Deception

The Theory of Deception (TD) theorises deception requires the cognitive interaction between two parties where there is a conflict of interest. One party manipulates the environment in the case of a phishing attack (Grazioli & Wang, 2001; Johnson et al., 2001). In turn, shaping the environment of the other party, the potential victim, thus promoting a false representation of the situation and bringing about the desired action (Grazioli & Wang, 2001; Johnson et al., 2001). Purkait et al. (2014) found cognitive factors such as attention vigilance and short-term memory positively correlated with detecting phishing emails and websites. The first stage of TD requires the individual to identify the inconsistent cues within a phishing email, concluding there is no deception and nothing wrong with what they see (Grazioli & Wang, 2001; Johnson et al., 2001). At this stage of the deception, the individual needs a cue, as such, to either engage or not. Vishwanath et al. (2018) note that suspicion is a unidimensional construct for detecting deception and a better predictor of deception-detection accuracy. Regarding the first stage of TD, if the individual has not identified anything suspicious, then according to Vishwamath et al. (2018), it is predicted they will more likely engage with the email.

The second stage refers to the hypothesis generated by the individual to explain the difference between their expectations and the cues they have observed (Grazioli & Wang, 2001; Johnson et al., 2001). During the third phase, the victim will evaluate the hypothesis generated to either engage with a phishing email or not (Grazioli & Wang, 2001; Johnson et al., 2001). This decision is made by comparing and drawing on experiences and feedback developed over time (Grazioli & Wang, 2001; Johnson et al., 2001). The final stage of deception requires the individual to conclude the accepted hypothesis they have developed, which can come from one or several weaker ones (Grazioli & Wang, 2001; Johnson et al., 2001).

Highlighting the complexity of engaging with a phishing email, the individual at each stage of TD must cognitively process the information they are viewing. Two models of cognitive processing or cognitive-information handling can describe the factors that influence the outcome of TD: the Heuristic-Systematic Model (HSM) and the Elaboration Likelihood Model (ELM). HSM refers to the two modes of information processing: systematic and heuristic (Chen & Chaiken, 1999). Systematic processing requires effort and information-processing resources as the individual carefully examines an argument's quality within the persuasive context to make judgments and decisions (Chen & Chaiken, 1999; Vishwanath et al., 2018). Heuristic processing requires less effort and is more efficient and economical. It uses more straightforward decision rules or cognitive heuristics triggered by adjunct cues in the context to make decisions (Vishwanath et al., 2018). Current research has highlighted individuals who use heuristic processing have an increased likelihood of being deceived by social media, whereas systematic processing results in more reasoned decisions and less risk of being deceived (Vishwanath et al., 2018). Vishwanath et al. (2018) theorised that an individual who uses heuristic processing at a high level decreases their suspicion about the integrity of a phishing email. In contrast, systematic processing at a higher level will increase the individual's suspicion.

ELM, like HSM, can also describe why individuals engage with phishing emails. ELM is a model that uses a dual process to describe the change of attitudes developed by Petty and Cacioppo (1986). They suppose ELM provides a framework for the fundamental processes underlying the effectiveness of persuasive communications through organising, categorising and understanding information received (Petty & Cacioppo, 1981). ELM, like HSM, uses two routes of persuasion; individuals will use the centre route when they have considered the strength of the information through careful and thoughtful consideration (Petty & Cacioppo, 1981; Petty and Cacioppo, 1986). The second route, referred to as the peripheral

route, the individual will consider nonverbal cues of the information, some simple cues in the context of a persuasive message (Petty & Cacioppo, 1981; Petty and Cacioppo, 1986). Ferreira and Teles (2019) theorised that the overall cognitive effort expended in email processing decreases with attention to visual and phishing deception triggers. Thus, these models cannot be used to predict or examine which factors influence the outcome, they provide a description only.

How information is processed is dependent on the individual's actions, which require some degree of cognitive mediation (Vishwanath et al., 2018). Email use presents a strong case for habituation, and people regularly engage with emails throughout the day, thus, repeating the behaviour numerous times (Vishwanath et al., 2018). When web surfing, individuals will routinely check their emails in the morning and evening as part of their daily routine, which can also be why they repeatedly go online (Vishwanath et al., 2018). Many email exchanges can be relatively benign; thus, cognitive involvement can relax, and formulaic patterns of use can form (Vishwanath et al., 2018). Behaviour is a critical factor that can contribute to whether a person will respond to a phishing email or not. One practice often associated with phishing emails and response rates is a habit. Vishwanath (2015) noted that checking emails is routine, making it easier for people to click on hyperlinks automatically. Wood and Runger (2016) suggest that they reduce their ability to narrow their focus and limit their consideration, even when transparent decision-making is required, something necessary for recognising a phishing email. Education programs that focus on habitual behaviours can support the creation of effective habits, but these have limited success (Vishwanath, 2015). Habitual practice of accessing potentially fraudulent email is reinforced as people now have easy access to emails on their phones, thus allowing them to frequently check emails more efficiently regardless of time or location (Vishwanath, 2015).

While cognition and behavioural factors are essential, emotion's role in detection and susceptibility must also be addressed.

Individuals will differ in their susceptibility to phishing emails. Iuga et al. (2016) sought to understand better the role of susceptibility and why some individuals engage with phishing emails, despite the warnings readily reported in the media. Iuga et al. (2016) asked 382 participants to differentiate between a legitimate and a Phishing Facebook page using a fake Facebook login page with subtle differences such as an incorrect URL or spelling. Only six participants achieved a 100% detection score, accounting for only 1% of the sample. Even in controlled environments where individuals are aware that they will be viewing fraudulent information, they will still find it challenging to identify and detect. At some point in Iuga et al. (2016) study, the participants who could not detect the fraudulent emails had accepted the hypothesis they had generated as noted within the phases of TD. The participants used either; heuristic processing at a high level which decreased their suspicions about the information they were seeing or used the peripheral route focusing on a nonverbal cue of information. Iuga et al. (2016) study had similar results to a study conducted by Dhamija et al. (1996), which was replicated by Alsharnouby et al. (2015) nearly 20 years later.

Alsharnouby et al. (2015) noted when individuals are more focused and concentrate on why they are online; they are less likely to be focused on security indicators such as misspellings or, in general, receiving suspicious emails in the first place. Dhamija et al. (1996) and Alsharnouby et al. (2015) studies were interested in improving detection strategies to identify fraudulent emails. Interestingly, although these studies were completed nearly 20 years apart and technological advancements have increased significantly, their results were surprisingly similar. Only approximately 50% of participants in both studies correctly identified either a phishing email or a fraudulent website (Alsharnouby et al., 2015; Dhamija et al.,1996). The participant's perception of the situation they found themselves in

and the cues from the emails informed their judgment about whether they were looking at a real or fake website. The findings of Dhamija et al. (1996) and Alsharnouby et al. (2015) studies are very similar to the findings of Iuga et al. (2019) study (completed several years after Alsharnouby et al. (2015) study). In all three studies, even when individuals are in controlled environments where they know they will be engaging with phishing emails and fraudulent information, they will still be deceived.

Social Judgement Theory

Social Judgement Theory (SJT) is a perspective for understanding human judgement in social situations (Brehmer, 1988; Cooksey, 1996; Doherty & Kurz, 1996). SJT, as a metatheory, provides direction for the research of human judgement, and embedded in this theory is the theory of perception (Brehmer, 1988; Cooksey, 1996). Preception theory assumes an individual will not have access to explicit information about objects in the environment. Perception is a complicated process facilitated by proximal cues (Brehmer, 1988; Cooksey, 1996; Doherty & Kurz, 1996). Thus, making a judgment involves the combination of information from a set of cues into a decision about some general situation and circumstances connected to the individual (Brehmer, 1988; Cooksey, 1996; Doherty & Kurz, 1996).

Perceptions, beliefs, emotional responses and self-awareness influence engagement with phishing emails and emphasise the role of emotional factors in decision making and reacting. Cyber-risk beliefs are the individual's perceptions about the risks associated with online behaviours, bridging the subjective knowledge of online dangers and experiences and the efficacies of dealing with threats (Vishwanath et al., 2018). The scam speculates individuals will systematically process emails if they perceive their cyber actions as risky and need to be more confident in their decision due to the risk (Vishwanath et al., 2018). Individuals will use heuristic processing when they believe their actions are less risky, thus

requiring lower confidence in their decisions due to the perceived minimal risk factors to the conclusion they make (Vishwanath et al., 2018). Vishwanath et al. (2018) hypothesised that cyber-risk beliefs would be negatively related to heuristic processing and positively related to systematic processing.

Emotional triggers such as empathy, excitement, panic, and curiosity influence people's decision-making and judgment (Cross, 2015; Williams et al., 2017). When emotional responses are elicited by a phishing email, people are at risk of harm (Williams et al., 2017). Individuals high in self-awareness tend to be less susceptible to the persuasive text of a phishing email (Williams et al., 2017). Williams et al. (2017) noted that being vulnerable in general was due partly to a focus on heuristic processing; thus, self-control requires an expanded cognitive effort and uses resources to regulate behaviour. They believed that a lapse in self-control was because of individual motivations such as desire, money, and other forms of satisfaction. External stimuli provided the situational opportunity to engage with the phishing email (Williams et al., 2017). For example, people who feel lonely and disconnected from family and friends will be attracted to fraudulent emails requesting aid or promising a new and exciting romantic relationship (Cross, 2015; Cross et al., 2014).

Some researchers have also proposed that trust is essential in determining whether people will engage with a phishing email. People will exhibit more confidence if future communications align with previous interactions with legitimate emails (Williams et al., 2017). Williams et al. (2017) inferred that people would use truth bias to deal efficiently with the vast amounts of sensory information they receive daily. They theorised "if the legitimacy of every piece of incoming information required systematic evaluation, people's limited cognitive resources would quickly be overloaded" (Williams et al., 2017, pp. 414).

Older Persons

The Australian Bureau of Statistics (ABS, 2020) and the World Health Organisation (WHO, 2018) refer to older people as 65 years or older. Many developed countries have accepted 65 years old to be when a person has reached older adulthood; for Australians, 67 years old is considered retirement age (ABS, 2016; ABS, 2020; WHO, 2018). The ABS (2020) estimated that from 1999 to 2019, Australians aged 65 years and older have grown from 12.3% to 15.9% of the overall population. By the end of the 30th of June 2019, the number of individuals aged 65 and older increased by 125 400, or 3.2% (ABS, 2020). Additionally, Australians 85 years and older had increased their numbers by 117.1% compared to the total population growth of 34.8% over the same period (ABS, 2020). By June 2019, this older cohort had increased by 12 600 people, or 2.5%, to approximately 515 700 people (ABS, 2020).

For older persons to engage and take advantage of the online services that have become commonplace in modern society, they must firstly engage with information and communication technology (ICT) (Vacek & Rybenska, 2015). Over 13.7 million Australians subscribe to broadband service, and for older Australians, 50% (i.e., those over 65 years old) use the internet for banking and 43% for social networking (ABS, 2019). This age group is the most affected cohort by phishing scams, making up 28% of the overall population and in 2019 had the highest financial loss of over $431,000 due to these scams (ACCC, 2020). As of April 2020, older persons had lost over $98 000 due to phishing scams in Australia, according to the Australian Competition and Consumer Commission (ACC, 2020). These statistics highlight the importance of continuous research on why older persons engage more with these emails than any other age group. Vacek and Rybenska (2015) noted that technology advances at such a rate that even younger generations struggle to keep up. Even though there has been a significant increase in mobile device and computer ownership, the

use and reliance on the internet in the overall population finds older adults still lagging in these areas (Lee et al., 2018). Technology and the dependence on technology and communication in daily life are only increasing (Lee et al., 2018).

Peine and Neven (2018) proposed the direction of research on aging and technology needs to address the digitization of societies and the effect this has on people's experience in later life. They suggest that interventionist logic constrains current research on aging and technology (Peine & Neven, 2018). Since the 1980s, a convergence of technology and demographic changes in society ignited the studies of gerontologists and human-factor engineering (Peine & Neven, 2018). Earlier research focused on the practical application of technology and how to assist older persons (Peine & Neven, 2018). During the 1990s, Gerontechnology became an official field of research, consolidating aging and technology (Peine & Neven, 2018). Though studies differ slightly in their range and labels of interventions and life domains, the logic underlying this analysis is the effects of technology on numerous insights of health, mobility, and social connectedness (Giaccardi, Kuijer, & Neven 2016; Peine & Neven, 2018).

Giaccardi et al. (2016) and Loe (2010) note older persons have been consistently using technologies and forming their own skill sets and technology literacy since the invention of technological advancements such as washing machines, television and phones (Peine and Neven, 2018). Peine and Neven (2018) believed focusing on the possible impact of new technologies on aging and studying existing technologies used by older people is empirically and theoretically illuminating. It offers opportunities for attuning the design of innovations with existing technologies, skill sets, and technological literacy. During their research, Lee et al. (2018) reported that age, education, and computer experience influenced people to adopt and generally have a positive attitude towards technology use, including owning and using computers. One of the challenges for older persons to have a positive

attitude is the confidence that at their age, they can learn how to use computers and new technologies (Lee et al., 2018). Suppose an older person is confident in learning how to use new technology. In that case, the question could be asked, if an older person has the confidence to learn to use emails and accept this form of communication in their everyday life, will they be less likely to engage with a phishing email?

The themes and ideas that form our current understanding of why older persons are more susceptible to engaging with phishing emails than other age groups have been extensively explored (ACCC, 2017; Gavett et al., 2017; Purkait et al., 2014; Vacek & Rybenska, 2015). However, there does appear to be a discrepancy between the findings of government agencies and research in this area. For example, the ACCC Scamwatch has reported that since 2015, persons 65 years and older are more likely to respond to phishing than any other age group (ACCC, 2021). Current research, such as Gavett et al. (2017), hypothesised that older persons were more susceptible to phishing than younger persons and found no significant difference between the age cohorts participating in their research. Purkait et al. (2014) theorised older persons would be more susceptible, and their results showed the older participants in their study were more susceptible.

Gavett et al. (2017) asked participants to complete a battery of tests assessing executive functioning, decision-making abilities and web browser activities. The focus of the study was on the instrumental activities of daily living (such as financial management), driving and medication adherence, enhanced activity of everyday life (such as online banking), and the role of executive functioning on both younger and older persons (Gavett et al., 2017). Their results suggested that while executive functioning and processing played a role in the susceptibility of younger (M = 22 years) and older persons, older persons took more time to process information, increasing sensitivity to being susceptible (Gavett et al., 2017). It is important to note that the younger cohorts were university students, and Gavett et

al. (2017) theorised this could have affected their study's ecological validity. Cognitive and learning factors were also hypothesised to protect a person from being susceptible to phishing emails, and level of education was associated with not being susceptible (Gavett et al., 2017). These findings contradicted the results of Purkait et al. (2014), who found the level of education was associated with being susceptible. In the Purkait et al. (2014) study, learning and cognitive factors appeared not to provide protection, as in Gavett et al. (2017). There could have been a mismatch between theory and reported experiences, or other unknown factors were not being addressed in either study. Another aspect of cognition is the natural cognitive decline that some older persons experience and how this can play a role in older's engaging with a phishing email (Gavett et al., 2017; Purkait et al., 2014; Vacek & Rybenska, 2015; Vacek & Rybenska, 2016).

Aging is often associated with impairments in memory and working memory can decline as a person ages (Solesio-Jofre et al., 2011). As working memory is a capacity-limited system, storage and processing are affected, resulting in impaired attention capacity and limited maintenance (Solesio-Jofre et al., 2011). Solesio-Jofre et al. (2011) presented older participants with new information while learning and memorising specific material and associations of different items or things. Age-related deficits affected their ability to suppress irrelevant information (the latest data) and correctly recognise previously known associations (Solesio-Jofre et al., 2011). These findings could potentially explain discrepancies in Gavett et al. (2017) and Purkait et al. (2014) findings regarding education protecting from being susceptible. Suppose an older person was educated and informed about phishing emails and how to spot them. According to Solesio-Jofre et al. (2011), the older person will not be able to draw on this already learned information with the presentation of new information. The new information has attracted their attention and provided the conditions for irrelevant information to affect their ability to process phishing emails with suspicion, which according

to Purkait et al. (2014), has made them susceptible. As an older person's working memory may play a role in their capacity to recognise a phishing email, there could also be a physiological explanation, as many older persons can experience cognitive decline.

Spreng et al. (2017) hypothesised that brain differences in regions involved in social-emotional functioning (general feelings of anguish, wellbeing, and quality of peer relationships) are associated with financial exploitation in older adulthood. One physiological finding was cortical thickness for older persons who had been financially exploited had significantly reduced cortical thickness in the right anterior insula cortex and right posterior superior temporal cortices (Spreng et al., 2017). These regions are involved in effective decision-making, social cognition, and reward anticipation. The differences in the insula cortex may affect an older person's ability to detect a threat "or disrupt the integration of threat-related information into decision-making processes during social interactions" (Spreng et al., 2017, pp. 13-67). Suppose the older person has a reduced ability to see a threat. In that case, this will leave them at a higher risk of exploitation, particularly in complex, even emotionally volatile contexts (something phishers will try and induce) (Spreng et al., 2017).

The default networks comprised the posterior cingulate cortex, which was the inferior parietal lobule, lateral, and medial temporal lobes (Spreng et al., 2017), comparing these networks, older persons exploited and those who had not found the aged persons influenced had reduced salient network integrity. The functional connectivity between the left anterior insula and other regions was significantly lower (Spreng et al., 2017). The default network is associated with social reasoning, which is "necessary for fluid social interactions where complex, multimodal social cues must be integrated to accurately infer the intentions of others" (Spreng et al., 2017, pp. 13-67). This is significant because phishers manipulate social norms and cues to coerce individuals to engage with their emails. Spreng et al. (2017) theorize that age-related changes in default network brain regions may disrupt the processing

of social cues, leading to impairments in social reasoning, making them more susceptible to exploitation.

Ebner et al. (2018) noted that older persons appeared to be particularly vulnerable to cybercrimes attacks. As reported previously, this cohort is often associated with a decline in cognitive decline and increasing negative change in socioemotional functions, how one relates to their emotions and relationship to their society after decision-making (Ebner et al., 2018; Spreng et al., 2017). Focusing on behavioural susceptibility to deception, specifically in online environments, Ebner et al. (2018) reported having an awareness of online deception risk was associated with cognitive and socioemotional capacities. They sought to understand if variations within ages for any of these associations contributed (Ebner et al., 2018). Ebner et al. (2018) study indicated that older persons are more vulnerable to phishing emails, especially with cognitive and socioemotional impairments (Ebner et al., 2018). As other studies (ACCC, 2017; Gavett et al., 2017; Purkait et al., 2014; Vacek & Rybenska, 2015) focused on an older person, Ebner et al. (2018) theorised there are varying levels of cognitive functioning and being susceptible with the older person cohort itself. Older persons aged 65 years to 74 years may have more computer experience and showed no associations between functional levels and being susceptible (Ebner et al., 2018). Thus, they inadvertently created a form of cognitive protection.

In contrast, older persons over 74 years old had less experience and had already entered a stage of natural cognitive decline that affected their ability to detect such frauds (Ebner et al., 2018). Ebner et al. (2018) study only adds to the complexity of being able to generalise a theory or perspective to understand why an older person engages with a phishing email. They have identified that there may be differences within the age cohort itself with varying degrees of cognitive functioning and being susceptible, which other studies have not

identified or sort to better understand (Ebner et al., 2018; Gavett et al., 2017; Purkait et al., 2014; Vacek & Rybenska, 2015).

Current Research Phishing and Older Persons

For older persons who have experienced phishing, there can be severe financial, emotional, psychological, and physical consequences (Croft et al., 2019; Cross, Richards, & Smith, 2016). Cross et al. (2016) conducted 80 in-depth interviews of Australian individuals (aged 30 – 77) who had lost $10,000 or more in online fraud scams. Results showed financial loss could vary depending on the individual's perception of the event, from minimal economic damage interpreted as insignificant (i.e., the amount lost has not disrupted their quality of life or current living standards) to severe financial loss. For example, the person must return to paid employment to support themselves because they have lost their savings (Cross et al., 2016). A person's independence can also be affected by the need to depend on others for financial support (Cross et al., 2016). Silva and Boemer (2009) state that older people value being financially secure because it gives them a sense of independence and autonomy, aiding them in maintaining emotional and psychological wellbeing. So, losing this security can have devastating effects. For example, the psychological impacts of phishing can result in a person experiencing depression, which can lead to suicidal ideation (Cross et al., 2016). The most-reported emotional responses are distress, anger, shame, embarrassment, shock, worry, and loneliness to being Phishing victims (Cross et al., 2016). While most victims of phishing emails will experience at least one of the emotions, these experiences will vary in severity. Less painful emotional experiences can result in the individual using, for example, humour as a coping mechanism or rationalising their knowledge in a matter-of-fact way (Cross, 2015; Cross et al., 2016). More painful emotional experiences, such as shame and embarrassment, can develop into distressing psychological issues such as depression (Cross et al., 2016).

The ACCC (2017) has proposed that the number of victims over 65 who experience phishing may be underreported. Cross et al. (2016) suggests that individuals who do not report being a victim can be because of the lingering emotional impact experienced, such as embarrassment and shame. Another reason is the phenomenon of victim-blaming. Cross' (2015) study demonstrated the surprising prevalence of victim-blaming and how this can affect an older person from coming forward to report being phished. Older persons reported not wanting to look "stupid." They believed admitting they had been a victim meant others may view them as unable to look after themselves; thus, the older person may lose their independence (Cross, 2015; Cross et al., 2016). Cross (2015) found greed was another reason people reported engaging with phishing emails. These people later blamed themselves for being manipulated and were less likely to admit being phished, thinking that 'they should have known better' (Cross, 2015). People attribute greed/gullibility to responding to scam emails and victim-blaming instead of ascribing blame to cybercrime perpetrators (Cross, 2015).

Another flow-on effect of phishing is the physical well-being of the older person. Shame and worry can result in weight loss due to a lack of appetite because of the stress these emotions can evoke (Cross et al., 2016). Insomnia and nausea can also be a side effect of the worry and anger felt by the individual (Cross et al., 2016). Not being able to sleep over an extended period is a distressing experience. Thus, a vicious cycle of negative emotional, physical, and cognitive effects could occur if the person phished has insomnia (Cochen et al., 2009). For example, attention is impaired due to tiredness; thus, an older person may be more susceptible to accidents. Cognitive abilities such as decision-making diminish because the individual does not have the cognitive capacity to think things through clearly (Cochen et al., 2009).

Oliveira et al. (2017) sought to understand decision-making concerning cybersecurity by focusing on behavioural measurements and the effects of trust and deception on aging, with trust theorised as fundamental for satisfying social relationships. Some research evidence has shown that a person's perceived confidence increases with aging, but sensitivity to untrustworthy information declines with aging (Oliveira et al., 2017). Between August 2015 and November 2016, Oliveira et al. (2017) analysed the internet use of younger and older adults (N=100 younger, N=58 older). Theorising older internet users would be more susceptible to the embedded influences in the life domain, such as safety and security, in the context of a specially created phishing email. This study also theorised that older adults were unaware that they were more susceptible.

Using Cialdini's (2009) Principle of Influence previously explored and the context of a particular life domain as the framework for this study, Oliveira et al. (2017) studied participants in their own homes engaging in daily study-related internet browsing for an hour a day. Participants were required to commit for approximately 15 minutes to each of the following specific activities:

1. Reading an information source
2. Reading entertainment/social network sources
3. Engaging in unstructured browsing time
4. Checking/handling emails from the email account the user had registered for the study (Oliveira et al., 2017)

These activities were designed to ensure the participants engaged in diverse activities and regularly checked their emails, and a base rate of the targeted behaviour can be established (Oliveira et al., 2017). Throughout the 21 days, the participants received phishing emails formatted with similar word lengths and structure, covering various life domains

based on the literature and included information about events and contexts related to the area where the participants lived (city or country) to increase believability (Oliveira et al., 2017). Oliveira et al. (2017) showed that older persons were more susceptible to phishing email attacks, and scarcity and authority, as noted within the Social Engineering Personality Framework, were the most effective weapons. These results were identified by the number of times the participants clicked on the various links on the phishing email (Oliveira et al., 2017). Further investigation of the data breakdown showed that the younger participants were more susceptible to the emails that used scarcity, and the older participants were more sensitive to the emails that used reciprocation (Oliveira et al., 2017).

This paper highlights the theory that people engage with a phishing email is contextual, a complex interaction of internet users' age, gender, the weapon of influence, and life domains of these emails in this instance, referred to (Oliveira et al., 2017). Iuga et al. (2016) theorised training and warning solutions should be age-related to specific vulnerabilities of an individual's demographics. One of the limitations of this study was the number of older persons who participated. Previously older persons were less likely to report they have been a cybercrime victim or do not believe they have the necessary technological skills to participate. Another limitation of the study was that even though there was deception, the participants were aware they were participating in a research project, making them more aware and primed to be suspicious. It is important to note that these findings are inconsistent with the studies looked at in this paper (Cross, 2015; Cross et al., 2016; Ebner et al., 2018; Gavett et al., 2017; Purkait et al., 2014; Vacek & Rybenska, 2015), further adding to the complex nature of why older persons engage in phishing emails.

To summarise, research has already shown that being phished can impact an older person. Qualitative research has focused on the person's experience *after* being phished. In contrast, the quantitative analysis focused on variables such as susceptibility and cognitive

processes. The proposed research aims to explore the experience of a specific older person phished to understand better the process a person goes through when engaging with fraudulent emails and have a clear idea of potential themes in future research.

Research Rational

Due to the continuing prevalence of phishing attacks via an email delivery system and the continued statistical findings of older persons being one of the most affected cohorts in the population, a detailed examination of one older person's experience of engaging with one of these emails is worth investigating. The literature discussed have all used a quantitative approach with varying results to understand this phenomenon (e.g., Cross, 2015; Cross et al., 2016; Gavett et al., 2017; Purkait et al., 2014; Vacek & Rybenska, 2015; Vacek & Rybenska, 2016). Theories, such as HSM, ELM, TD and SJT have been discussed and demonstrate the complexity of the process someone can go through when engaging with a phishing email. This study aims to better understand the experience of one older person who engaged with a phishing email. By using a descriptive case study approach, the researcher can then utilise emails and interviews to better understand the process and experience of an individual who has engaged in a series of phishing emails. This type of research design then allows for an in-depth exploration of the complexity of why an older person would engage and provides an additional layer of understanding beyond a simple survey research design. An older person who was a victim of a phishing email took part in three interviews and provided the email correspondence between themselves and the phisher, thus allowing for a more in-depth explanation about the emails and their thoughts and actions at the time they were received. The third interview was not used in the analysis as the participant did not speak further to their experience of engaging with a phishing email and spoke only of current world events not related to the study. The older person is then able to share why they use emails, the

benefits and challenges of using technology in everyday life, their life experience and how these things may or may not have influenced their decision to engage.

2: Method

Methodology

A qualitative research approach has been selected to investigate the experience of one older person who engaged with a phishing email. Research has shown why an older person commits to phishing are complicated, and many theories and models are used to understand this phenomenon. Focusing on the experience of one older person and analysing their written interactions with a phisher, provides more in-depth information about the experience and could lead to further research in the development of future education and awareness programs. Qualitative research provides the framework for an in-depth analysis, such as older persons and Phishing, and explores individuals' experiences through their own words and other documentation (Smith, Flowers & Larkin, 2009). Unlike Quantitative research, which is bound by the strict codification of methods, statistics, and scientific writing, a Qualitative approach to research allows for the use of creativity and innovation (Marecek, 2003). Qualitative researchers observe the changing salience of identities and actions, a feature of social life that experiments and self-report scales cannot readily see (Marecek, 2003). Data on structural conditions, deviances in behaviours, norms, systems, patterns, processes, or consequences can be explored best with qualitative methods highlighting critical elements of sociological theories, SJT and TD, that may explain why older persons respond to phishing emails (Glaser & Strauss, 2017). Marecek (2003) notes three aspects of qualitative research; firstly, qualitative research seeks to understand psychology within the contexts of history, culture, and society. Secondly, the qualitative study aims to understand the individual in their world, that is, the social locations they occupy (Marecek, 2003). Thirdly, Qualitative research regards the individual as a meaning-making, reflexive, intentional person who seeks to understand others' human experiences and actions through a qualitative psychology lens (Marecek, 2003).

Qualitative research examines human actions and social ideals through individual experience (Marecek, 2003). Relying on the standardised measures, which rest on the beliefs regarding aspects of mental life they seek to learn more about, are created in the same way across different settings, at different times, and in different social groups (Marecek, 2003). The multiple facets of the specific phenomenon are revealed and understood through various data sources (Baxter & Jack, 2008). The data recorded through this research approach can be sensitive and everyday facts about social systems and structure can be grasped (Glaser & Strauss, 2017). Maintaining a clear relationship between the questions asked, and the research question drives the project (Braun & Clarke, 2006). Questions focus on how collective dynamics, institutional arrangements, and shared language practices set in motion, sustain and interrupt ways of being in the world (Marecek, 2003). Marecek (2003) states, "When qualitative inquiry yields a different picture than quantitative data, the question confronting researchers is not simply, 'Which is truer?' But a more difficult one, 'What kind of truth am I interested in hearing?' (p.54). Qualitative research can draw results from these various sources using diverse techniques and strategies, such as interviews, participant observations, physical descriptions, and surveys (Gallagher, 2019; Yin, 2014). These converge triangularly, and results can also benefit from the prior development of theoretical propositions to guide data collection and analysis (Gallagher, 2019; Yin, 2014).

An in-depth and detailed examination of one older person's experience uses a Case study approach. Case study research can address a phenomenon on a wide variety of levels, such as phenomena in whole societies, business corporations, social movements, or communities or institutions (such as prisons), to more focused scenes of interaction or aspects of an individual's life (Elger, 2010). Case studies also provide an in-depth investigation of a specific phenomenon within a real-life context. Thus, a case study is appropriate if the context is relevant to the phenomenon. Case study design then relies on multiple data sources

for evidence (Yin, 2018). This qualitative approach can also highlight relationships to understand the phenomena holistically (Gallagher, 2019; Yin, 2014). A case is an individual, an event, an entity, or a unit of analysis. It examines the phenomenon in question in the context of its real-life setting through various lenses (Noor, 2008; Yin, 2014). In this research, the case was specifically bound by participant age, with research reflecting the increased risk for those over 65. The units of analysis include the phishing email, participant email responses, and first-person account via in-depth interview. The interviews were used to better understand why an older person engaged with a series of phishing emails. By interviewing the person first, reviewing the emails, and then interviewing the participant again for further clarification, this then allows for a deeper understanding of their thoughts and actions during the phishing experience. The emails were reviewed in detail after the first interview, the email correspondence documents were provided during the first interview. The emails, physical artefacts, are then able to be used as a prompt for further explanation. More specifically, using email documentation allows for the participant to provide their thoughts and feelings about the interactions with the phisher, and the interviews all for the participant to explain why and how they engaged with the phishing email.

Case study research allows for the consideration of many details, permitting possible relationships between decision/s or patterns of events (Schramm, 1971). Case studies can answer how and why, considering how the phenomenon has been influenced by the context of the situation, collecting a variety of data sources that will allow the data to illuminate the case (Baxter & Jake, 2008; Yin, 2014). Baxter and Jake (2008) observed that Case studies are potentially more than just being able to deal with complex situations through a clear lens. This study will use a single-case to focus the research within the confines of time and space on one older person's experience with engaging with a phishing email and to analyse the

phishing email correspondence between the other person and the phisher and to discuss with the participant their experience at each stage of the engagement.

Recruitment and Participant Details

Before starting the research, ethical approval was obtained from the University of Southern Queensland Human Ethics Committee (approval number H18REA216). As the aim of the study was to explore the experience of an older persons with a phishing email, a purposive sample was required (Etikan, Musa, & Alkassim, 2016; Luborsky & Rubinstein, 1995). Specifically, a participant aged 65 years old or older and had engaged with a phishing email. The principal researcher created an advertisement posted on the University of Southern Queensland on-campus community notice and research boards for an extended period. An ad was further displayed on the principal researcher's Facebook page to encourage snowballing. Individuals who expressed an interest in the study contacted the principal researcher via email and phone. Individuals who expressed an interest in the project were sent an information sheet explaining the project's purpose, participation, potential benefit and risks, consent to participate, and confidentiality. Incentives to participate in the study were not offered to potential participants. Whilst several participants contacted the principal researcher, only one participant was willing to commit to an interview.

The participant Jenny (a pseudonym) is a 72-year-old widowed female who experienced phishing via an email and lives in Regional Queensland. Jenny self-describes herself as "ok" with technology, "I know what I know," and she mainly uses her desktop computer to engage with emails. She uses her android phone for messenger and texting. The phishing emails started when she received an email believed to have been from a relative and described her reasons for engaging with the emails as she thought she was helping her relative. Jenny knew of fake emails before engaging with one and had ignored emails from

people or organisations she did not recognize. Since her experience, Jenny has used a paid email account service and reported she no longer receives "strange" emails.

Design and Procedure

Design. A multiple-case study was initially planned for the research and could have been utilised as the research methodology if more people were willing to participate, thus allowing for distinct cases for comparison. However, with only one participant, a decision was made to conduct multiple interviews and to utilise the email communication between the phisher and the participant to allow more in-depth examination of the phishing experience. Thus a descriptive case study was used as the methodology. A descriptive case study allows for the phenomenon of engaging with a phishing email and the real-life context in which it occurred (Yin, 1994). Descriptive studies seek to identify patterns and connections by using a single case sample that is detailed and in-depth. Having only one participant, the principal researcher decided to use a descriptive case study to answer the research question. A descriptive case study allows the phenomenon of engaging with a phishing email and the real-life context in which it occurred (Yin, 1994). This type of case study was determined to be the most appropriate as the participant had a copy of the email interaction with the phisher and was able to speak to and describe each individual interaction they had.

Data collection and handling. As the research aims were experiential, data was collected via two semi-structured interviews (please refer to Appendix A) and the email documentation of the phisher and participant email correspondence. During the first interview, Jenny handed the principal researcher a copy of the email correspondence between herself and the phisher. Jenny referred to some lines within the email correspondence during the first interview but did not go into detail about their experience in relation to the email correspondence. The email correspondence was copied to allow the principal researcher to focus the second interview on clarifying and gathering further information about Jenny’s

experience. The principal researcher focused the interviews on what Jenny thought about each interaction with the phisher, how she processed this information and when she realised the emails were not from her relative. Jenny responded to the phisher 21 times over the course of several weeks. Two interviews took place face-to-face at the mutually agreed upon time at the participant's home. The principal researcher conducted a third interview via phone because of COVID-19 social distancing and self-isolating recommendations of the Federal and State Health Departments in 2020. While the third interview did take place, no new information related to the research was discussed, and as such no information was included in the analysis.

At the beginning of each interview, the principal researcher explained the meetings would be recorded, and the consent form was discussed to ensure Jenny understood the aim of the research. The first interview began with general conversation to build rapport with the participant, and Jenny chose a pseudonym she would like to use. During this interview, Jenny alsp provided to the principal researcher a copy of the email correspondence she had had with the phisher. The principal researcher made one set of copies of the documentation and returned the originals to Jenny. A transcript of the email documentation was written up and all identifying information was removed before the analysis was started. The principal researcher used the same analysis to analyse the first two interview transcripts and email documentation.

The first interview was approximately 30mins in length. Whilst six main questions with prompting were asked in relation to Jenny's experience, Jenny did not discuss her experience in detail rather, her tone was more matter-of-fact. At the conclusion of the first interview, the principal researcher requested a follow-up interview to clarify any points from the first interview and after reviewing the email documentation. The time between the first and second interviews was approximately three months as this was the earliest both principal

researcher and participant could find a time to meet. The second interview went for approximately an hour, and Jenny was more willing to describe her experience in detail and was able to reflect more on her experience. Both interviews followed a semi-structured design, please refer to Appendix A, to allow Jenny time to reflect on the first interview and expand on her thoughts and feelings about technology and general email use after the phishing scam. The third and final interview was conducted six months after the second interview, following the same design as the first two. However, no new information relevant to the research was provided by the participant.

Data analysis. Thematic analysis (TA) was used to focus on identifiable themes and patterns in the interview transcript and the correspondence between Jenny and the phisher (Aronson, 1994; Javadi & Zarea, 2016). TA focuses on identifiable themes and patterns of living and behaviour and is an increasingly popular method for systematically identifying, organizing and offering insight into patterns of meaning (themes) across the data set (Braun & Clarke, 2012; Fereday & Muir-Cochrane, 2006; Javadi & Zarea, 2016). Making sense of collective or shared meanings and experiences, TA can be used to make sense of commonalities (Braun & Clarke, 2006; 2012).

One of the advantages of TA is the ability to focus the data in many ways, analysing meaning across the entire data set, or an aspect of a phenomenon in-depth, reporting distinct or semantic meanings or interrogating the latent meanings, assumptions and ideas that lie behind what is stated (Braun & Clarke, 2006; 2012; Tuckett, 2005). The principal researcher analysed documentation and interview data together to better understand Jenny's thinking process and allow for generalisations from specific data observations. Inductive reasoning is a primary continuum of a qualitative approach to research (Javadi & Zarea, 2016). The principal researcher actively made a series of choices as to what form of TA theory they were using and to understand and explain why they used this form (Braun & Clarke, 2006; 2012).

An inductive approach is a bottom-up approach driven by what is in the data – codes and themes derived from the data's content, mapped by analysis closely matching the content of the data (Braun & Clarke, 2006; 2012; Tuckett, 2005). The principal researcher highlighted words, phrases and sentences in the documentation that matched Jenny's responses to the email documentation. For example, the word urgent became a code and any phrase or sentence that used this word or similarly, the principal researcher highlighted it. It is essential to note that the analysis does not automatically link to the semantic data content when a combination of approaches for coding and analysis is used (Braun & Clarke, 2006; 2012).

TA is a repetitive process, not linear, and follows six analysis phases (Braun & Clarke, 2006; 2012; Javadi & Zarea, 2016). In the first phase of the analysis, the principal researcher transcribed the recorded conversations with Jenny by repeatedly listening to the recorded interviews. The principal researcher used an inductive approach to the analysis to ensure the codes and themes developed by the content (Braun & Clarke, 2006; 2012). Re-reading the transcripts, the principal researcher became familiar with the data, highlighting relevant parts of the interview that the principal researcher felt helped answer the aim of this research, to understand better why an older person would engage with a phishing email. Using systematic analysis, the principal researcher used Jenny's responses and thoughts on specific sentences, words and phrases she pointed to in the email documentation to generate initial codes. Systematic analysis aided in providing the building blocks for further analysis, the second phase of TA (Braun & Clarke, 2006; 2012; Tuckett, 2005).

The highlighted sections the principal researcher identified contributed to addressing the research aim became the codes used. The most detailed information that is meaningful to understand was the phenomenon of engaging with a phishing email (Boyatzis, 1998; Braun & Clarke, 2006; 2012). The codes do not provide fully worked-up explanations but a mix of descriptive and interpretive relevant to answering the research aim (Braun & Clarke, 2006;

2012; Tuckett, 2005). The principal researcher completed several sweeps of the transcripts to develop and assign codes (Braun & Clarke, 2006). Codes used included: urgent, “Jim's phrasing”, help, remote, engaged, keeping connected, connection and family. Once coded, capturing the diversity and patterns in the data, the codes appeared across more than one data point. The principal researcher carried the analysis to phase three of the TA (Braun & Clarke, 2006; 2012).

Phase three of the analysis is where the codes were further reduced to themes; as Braun and Clarke (2006) state, themes "capture something important about the data concerning the research question and represent some level of *patterned* response or meaning within the data” (p. 82). Themes were identified using an active approach to search for themes, reviewing the coded data to identify overlap and similarities between the codes (Braun & Clarke, 2012). It was during this phase; the principal researcher noticed the similarity between the act of fishing and the codes that had been identified.

As the phisher had hacked into Jenny’s cousin’s email account and sent an email using their email address, the code “Jim’s phrasing” links into the bait being cast. This also linked into the code urgent as this word was used to catch the attention of someone. The codes remote and help, links into the theme of Playing the Line as the request to get help urgently. The phisher states that they are somewhere that they themselves are unable to access the resources they need, so need the help of someone. Throughout the email correspondence, Jenny remained connected to the phisher and responding to their request thinking it was a family member who needed help. This links to the codes of family and connection as this is something important to Jenny in her life. The final theme of the sinker is linked to all the codes as in combination, they all contributed to the outcome and Jenny sending the money to the phisher. Through this dynamic process, relationships between the codes, the principal researcher began to consider how the themes would come together to tell

the overall story of the participant engaging with a phishing email (Braun & Clarke, 2021). The principal researcher drew the potential during phase four to ensure the themes represent the data and the story.

During the fourth phase, the principal researcher further refined the themes, ensuring they had enough data to support them and work concerning the data (Braun & Clarke, 2006, 2012). The principal researcher used two levels of analysis, reviewing the data at the level of the coded extracts and reviewing the entire data set (Braun & Clarke, 2006; 2012). During the first level, the principal researcher was guided by the following questions suggested by Braun and Clarke (2006), when checking the potential themes against the collated extracts of data and ensuring they meaningfully capture the relevant data; a) is this a theme or a code, b) does the theme say something about the research question and data set, c) what does the theme include and exclude, d) does the data sufficiently support the theme, e) are the themes coherent? In the second level of analysis, the principal researcher reviewed the themes concerning the entire data set, re-reading the data set one more time to ensure the themes developed were meaningful (Braun & Clarke, 2006; 2012). When the principal researcher was confident the themes fit together and reflected the story they would tell about the data, the analysis moved into phase five, naming and defining the themes (Braun & Clarke, 2006; 2012).

During phase five, the principal researcher identified what each theme was about and what aspect of the data they captured (Braun & Clarke, 2006; 2012). Sub-themes were identified for each of the four identified themes, giving structure to the broad, complex themes (Braun & Clarke, 2006; 2012). The principal researcher selected quotes for analysis that will inform the reader of the data narrative and how it connects to the research aim, an older person's experience of engaging with a phishing email (Braun & Clarke, 2006; 2012). At the end of this phase, the principal researcher named each theme, reflecting the research

aim and naming the appropriate sub-themes ensuring the reader has a clear idea of what each theme is about in the overall story of the report and the sixth and final phase of the analysis began (Braun & Clarke, 2006; 2012). The final stage of TA for the principal researcher was producing the report, telling the complicated story of an older person's experience of engaging with a phishing email (Braun & Clarke, 2006; 2012). Unlike quantitative research, which requires a researcher to analyse data then write a report on their findings, qualitative research involves writing and analysis interwoven during these stages (Braun & Clarke, 2006; 2012).

Researcher Reflexivity

It is essential for any researcher who wishes to generate knowledge through qualitative research, to engage in Reflexivity (Berger, 2015). The following is a statement of the measures I took to understand and limit bias and preconceived ideas through the research process. Before starting this study, I was already interested in understanding people's lives during the later years of their experience. This interest was fostered during my undergraduate degree and later led me to work in the community aged services. Daily I was engaged with older persons (65 years and older) to support them in staying in their own homes and liaising with service providers that provide in-home support. I experienced firsthand the challenges older persons can face navigating technology to get their needed help. Many government and service providers use technology to streamline services and make these programs so important to the aged community and cost-effective. One aspect of technology needed was email, even when the person did not communicate with family or friends via this medium. For older persons to access government funding, they require an email address. Many older persons do not have one and rely on relatives' email addresses, making them feel they are losing their independence and thus control of making decisions for themselves.

Working in remote Southern Queensland, I supported an older person who had engaged in a phone scam. As a result of this phone scam, the older person sent money to the scammer via an online bank transfer. The older person experienced significant distress and embarrassment from what she had done and never fully acknowledged the scam, only saying she “was harassed to continue giving money to someone”. The older person did not report what happened to her family or any governing authority. Supporting this older person through this process furthered my interest in wanting to understand why older persons appeared to be more susceptible.

Through my experience with looking after an older relative, I have often wondered how it must feel to have lived a long life and been fascinated by things such as emails, Skype, and other forms of communication that were not around 40 years ago. Email communication has always explicitly been of interest to me. When I started this study, there was a lot of news coverage about email hacking and people receiving fraudulent emails from the taxation office or Netflix, for example. I often thought that an older person would respond to such an email, would they know if it was not real, or would they engage and what would be their reasoning for doing so.

One of this study's challenges was identifying my own biases when interviewing the participant. Through the extensive reading and my experience with a former client, I felt I already had a narrative of why my participant engaged with the phishing email. It was challenging to see beyond "it's simply complicated and what is needed is more support and person-centred education" and provide academic proof. Besides this straightforward narrative, I had regular check-ins with my supervisors throughout this study. During these meetings, both supervisors challenged me to reflect and focus on why this study was essential and what contribution it might make to academia. My supervisors supported e in unpacking the data and incorporating the theme of phishing and fishing practice to provide the linkage I

needed to understand the research aim better and explain my findings uniquely. These meetings supported me in focusing on jenny's experience, not to generalise her actions but to remember these were her actions, which is one individual experience.

3: Results and Discussion

Across the two types of data (Interviews and Email Documentation), four main themes emerged that capture one older person's experience of engaging with a phishing email. These four themes were: *(1) Casting the bait, (2) Playing the line, (3) Bringing the catch in* and *(4) The sinker*. Table 1 summarises the identified themes, each of the themes are discussed in detail using the participant's quotes and quotes from the Phisher's email correspondence that best represent the themes.

Table 1

Themes Identified During Thematic Analysis of Interviews with Jenny and Email Documentation Between Jenny and the Phisher

Theme	Theme Description	Illustrative quotes
Theme 1: Casting the bait	The techniques and tricks the Phisher uses to create the fraudulent email and the reaction of the victim to engage	"I have an urgent outstanding bill which I need to sort immediately. … It's urgent, please" (Phisher)
Theme 2: Playing the line	The way the phisher maintains the illusion/deception to keep the victim engaged and the victim's continued engagement	"Thanks a lot. I will get to you as soon as I leave western union. I truly appreciate this. Cheers Jim" (Phisher)
Theme 3: Bringing the catch in	The victim following through with the phisher's request, and the interplay after that as the phisher continues to make further requests	"I really hate to stress you …" (Phisher) "The money goes in to your Australian account. BSB needed etc." (Jenny)
Theme 4: The sinker	The moment the victim becomes aware of the deception, stops engaging.	"I just cannot believe your request. It is just out of the question, apart from the fact that you have not been at all forthcoming with what this is all about." (Jenny)

Theme 1: Casting the Bait

Phishing emails like the sport/hobby/occupation of fishing are remarkably similar in their intent. A fisherman casts a lure with an attractive object on the end of the hook; this object has been considered as ensuring it gets as much attention as possible. For fishermen, it attracts fish, for a phisher, it attracts a victim. The phisher who constructed the email that

lured Jenny to engage with followed this same ritual; they created an object, in this case, a message requesting financial assistance, attached it to a hook, an email, and caste it, sending the email out.

The phisher in this study had taken an extra step; they hacked into Jenny's cousin Jim’s (pseudonym) email account and distributed their fraudulent email from his email account. As Bisson (2019) and Banu and Banu (2013) stated earlier, spear phishing focuses on either an individual or a particular group of people; the email contacts were found in Jim's email account in this instance. While this phishing email has a lot of similarities to a deceptive phishing email, mimicking correspondence from a well-known person, it was more personalised, for example, than the Taxation email sent in 2019. This email was only sent to those in Jim's email contacts and not thousands of other people (ATO, 2020).

The bait construction highlights what Cialdini (2009) and Parsons et al. (2019) noted as necessary to the phisher, the victim of their email, believing the email to be valid by trustworthy, personal, and contextual information. The phisher in this study did just that; by hacking into Jenny's cousin's email account, they created a fraudulent email that increased their chances of someone engaging with them. Anyone who had been in regular email correspondence with Jim would think they were opening an email from a trusted person or an email address they recognised, thus increasing the phisher's chances of engaging.
The phisher's use of reciprocity, scarcity and social proof is evident in the bait/message they constructed and how they use it to activate stage one of the Deception Theory.

> Hi
>
> Sorry to bother you.
>
> I just arrived in Cyprus and I can’t access my account from here till I get back.
>
> I have an urgent outstanding bill which I need to sort immediately. Can I get a

loan of 2850 pound or whatever amount is available. You will have it as soon as I get back. It’s urgent please. I’ll advise on how to send it.

I will be very busy but will frequently check my email for your response.

Hope you New Year is smoother than the last few.

cheers jim. (Phisher)

Need an answer ASAP. Pls

cheers jim (Phisher)

Reciprocity and social proof, in this instance, involve the phisher anticipating Jenny wanted to help Jim. Williams et al. (2017) viewed reciprocity and social proofing as exchanging Jenny's support for Jim, with Jim willing to return the money asap, and he will no longer be in a difficult situation. Jim will reciprocate her kindness of helping him out by giving back the money as soon as he can, engaging in a socially appropriate way, helping a friend or, in Jenny's case, her cousin. By thinking this, Jenny diminished any suspicious thoughts and skepticism about the email from Jim. Through the lens of SJT, she has judged the email and given her connection to Jim, helping him become socially appropriate. As Jenny noted, "… I just thought he was just so much a good friend as a cousin that you know …." When applying the TD to understand her response, Jenny did not question the email, nor did she identify inconsistent such as the email not directly addressing her. Jenny did not perceive anything wrong with the email and thus engaged (Grazioli & Wang, 2001; Johnson et al., 2001). The phisher used deceptive language to create a lexicon cue by creating phrases that sounded like Jim to Jenny, such as "urgent" and "immediately." "in Cyprus, and I can't access my account from here … I have an urgent outstanding bill which I need to sort immediately". Previously stating she "just want to help", Jenny was susceptible to this language. During the interview, Jenny pointed to the email correspondence several times, noting the words "urgent" and "immediately, "I just thought it was all valid and quiet... "

The combination of reciprocity, social proof, and scarcity all played their part in Jenny wanting to help her cousin and believing that Jim needed assistance right away. Jenny's belief in the email's validity reflects the transition from stage one of the TD to the second stage. As previously stated, Jenny did not notice any inconsistencies in the email. Thus, Grazioli and Wang (2001) and Johnson et al. (2001) noted that deception will be successful without being aware of seeing these things. As Jenny transitioned to stage two, she reflected: "yeah and because the language that they were using in his email ... made you think." During this stage of deception, Grazioli and Wang (2001) refer to the hypothesis a person will formulate when rationalising. Jenny demonstrates this when she says: "… he must have some family problems that have made it difficult for him to ask family for some financial help".

This statement by Jenny illustrates stage two of the phisher's deception; Jenny rationalises why Jim would be emailing her for assistance when this is something he had not done. When discussing what Jenny thought when she opened and read the email from Jim, she rationalised why he would be emailing her and asking for help. This form of rationalized decision-making requires the individual, such as Jenny, to systematically choose among possible choices that build on what is the most concrete reason (Doherty & Kurz, 1996). Jenny reflected, "because he is quite well off in his own, I would have thought and arghhh … so there's … I just wanted to help him immediate."

This comment further highlights Jenny was entering the third stage of the deception, continuing to evaluate her reasoning or, in the case of TD, her hypothesis and, based on this information, decided to help Jim. Grazioli and Wang (2001) and Johnson et al. (2001) state that during this third phase, the individual relies on previous experiences and responses, which have happened over an extended period, to decide to engage. When interviewing Jenny, she reflected on her relationship with Jim, "I I just thought he was just so such a good friend as a cousin that you know … that it was must be fairly dire … and I had no second

thoughts about helping him." Jim had never previously asked Jenny for financial assistance before; she reflected during the interviews the language the phisher used was remarkably similar to the language Jim would have used, "you see they could use his phraseology they … having access to his emails … they they've been able to use his his phraseology … like 'cheers Jim' that's how he talks."

Jenny accepted that Jim needed her help and engaged. It is interesting to note that Ferreira and Teles (2019) believed the cognitive effect it takes for someone to recognise a fraudulent email diminishes when their attention is on visual triggers. The phishers also use lexicon cues in their emails, using the same signature of 'cheers Jim', a common phrase he used, as Jenny noted. While the lexicon cue influenced Jenny to interact with the email, it was the visual triggers that Jenny focused on. Reading the words, and visual cues, urgent and immediate, ultimately triggered Jenny's response to help Jim as they triggered her naturally caring nature to act. The lexicon cues Jenny focused on were the language used, and Jenny herself stated several times during interviews that she did not hesitate to help Jim because of the style used. Jenny's desire to assist him diminished the cognitive effort it would have taken for her to recognise the fraudulent email. This cognitive consistency will be explored further in other themes. When Jenny decided to engage, casting the bait by the phisher was a success. Jenny was now on the hook, and it was up to the phisher to ensure he could bring his catch in.

Theme 2: Playing the Line

One of the tips for any fisherman to ensure your fish stays on the line is to reel it in slowly. Releasing the tension of the line, allowing the line to slack, then reeling it in a bit more, then repeating these actions, the fish will struggle less, and you will successfully catch your fish. The interplay between Jenny and the phisher was remarkably similar, using consistent language, repeated instructions, expressing gratitude, and always responding promptly. The phisher used this "play the line" technique to keep Jenny engaged.

As stated before, Jenny's reasons for engaging with the phishing email are complicated, with many variables influencing and informing her discussions throughout the interplay. In terms of SJT and the TD, Jenny consistently rationalised her engagement with the phisher, unconscious at times, or by her reflections when discussing it. For Jenny, she did not identify any inconsistent cues in the phisher's email, the first stage of the TD. Even though she was aware of "fake emails", she judged to engage because she wanted to assist her cousin. Throughout Jenny's interview, she regularly noted that she "just wanted to help".

To better understand why Jenny took the next step in her "engage with the phisher," SJT can assist in providing the framework for this next part of Jenny's experience. Because SJT seeks to explain how an individual will process the message or messages given, it shows how Jenny treated the information given to her in the email (Asemah & Nwammuo, 2017). Jenny's relationship with her cousin Jim provided the anchor or stance needed for her to evaluate the message's contents and accept that what she was reading was real (Asemah & Nwammuo, 2017).

During interviews, it was noticeably clear that Jenny has relationships with her family and friends close to her. When discussing her children, her late son and her two daughters, for example, she reflected the following, "because I remember my young son who has since died a lovely boy (Jenny, referring to her late son) and I look after my grandchildren a lot to help my girls." When asked what she thought when she opened the email, given her strong familiar feeling and emotions toward her family, it is not surprising that she responded, "well, I would have just opened it and seen it and … been concerned … and think … ow Jim ..aw this person … my cousin … well this must be serious if he's requesting me to help him." Having such secure connections to her family, it is, upon reflection, not surprising Jenny had no hesitation in wanting to help Jim. Oliveira et al. (2017) noted as a person ages their perceived trust in others they are close to increases, and they can become less sensitive to

misleading information. These secure emotional connections for Jenny are factors that play a significant role in someone being more susceptible to phishing emails (Purkait et al., 2014). The validity of the SJT provides a theoretical framework for understanding this stage of Jenny's interaction with the phisher.

Jenny was and continues to be actively volunteering at a not-for-profit hospice, assisting families who have recently relocated to Australia. Jenny reflected that she has always been involved in community work and has a lifelong interest in politics, “I work for the hospice as a volunteer,” and she also noted she was active in local politics. From these statements, is it clear that Jenny has a strong social identity? When she spoke of her family, work, and involvement and interest in local politics with a lot of pride, the core idea of Social Identity Theory (Stets & Burke, 2000). Having a strong social identity may have influenced her because helping Jim can be perceived as psychologically significant and simply part of Jenny's nature to want to help (Asemah & Nwammuo, 2017; Stets & Burke, 2000). It is essential to acknowledge the complexity of someone deciding to engage with a phishing email. Regarding Jenny, several theories can assist in explaining why she participated or, more importantly, why she did not question the email and was so quick to rationalise why Jim would be asking for help.

For older people such as Jenny, who have entered a retirement stage, there can be a sense of lost purpose or even becoming lonely and disconnected from families and friends. Other people can struggle with this stage of life as they lack a sense of purpose for a job. Some can become reliant on others’ for financial and practical support, diminishing their independence. Jenny is a person who is now at a stage in her life where she is retired and spends her time caring for others, her family, the responsibility of her volunteer work and her continued involvement in community interests. These activities provide her life with purpose

and continued independence. Throughout the interview, Jenny often spoke of helping others and reacting when others ask for help.

With Jenny committing to help Jim and engage with the phishing email, the phisher could "play the line" and keep Jenny engaged for as long as they did. Throughout the email correspondence, the phisher keeps Jenny involved by letting her know how easy it is for her to help him. Even during the early stages of the communication, Jenny inquired about sending the money through a bank transfer. This form would have been a more common form of internal money transfer. An example of how much Jenny had become invested in helping Jim while raising this with the phisher at such an early stage of their interaction, she did not question it any further. The phisher insisted Jenny use Western Union and assisted her in doing so, with the persuasive tone evident in the following exchange:

> Jenny: What do you think about sending it online. How does the money get from me to the western union online?
>
> Phisher: You can got it on line, with your credit card. Just click on the western union link below and send through)
>
> Jenny: It needs to be send to a bank account or mobile phone
>
> Phisher: The best option is by sending it at western union agent location. All they require is the receivers name and address.

The exchange between Jenny and the phisher shows Jenny evaluating the information at this point as if she is again at stage one of the TD. She has verbally acknowledged there are inconsistent cues in the directions the phisher has given her, wanting to send the money to a bank account to complete the transfer and the phisher saying no; it just needs to be sent via money order. Then throughout this exchange, Jenny goes through the stages of Deception Theory again as she revaluates continually rationalising her decisions. Jenny's perception of the situation that it is all valid has been made easier in a way because of the connection to

Jim, which is consistent with SJT and the Purkait et al. (2014) study (Brendt, 1988; Cooksey, 1996; Doherty & Kurz, 1996). Another element the phisher uses while "playing the line" is consistency; his answers to questions Jenny asks are consistent, and his message never changes. He consistently thanks Jenny and acknowledges the trouble she has gone through to help him out. For example, he says: “Thanks a lot … I really appreciate this …thanks a lot for all your effort on me’, and later “ It’s important … I truly appreciate this … Hope it won’t be too much troubles for you” (phisher). The phisher’s instructions on how to use Western Union and create the money order never waver, using the same language to reassure Jenny it is not difficult to send the money this way instead of directly via a bank transfer. The phisher would always reply the same way, “Just click on the western union link below and send through … pls check the link below” and “click on the western union link below and then click on the link below and fill the form.”

Scarcity is also used by the phisher consistently throughout his email responses, repeating the following statement, “I will frequently check my email for your response.” The phisher limits his responses and does not further explain other than requiring the money, the frequency of checking their emails and how grateful they are that Jenny is helping them. With the use of scarcity combined with the other social influences, Jenny's willingness to assist "Jim" can be seen to have the desired effect, as shown by the timestamps on the email exchanges. Jenny received the first email from the phisher at 11:12 am, and she responded at 5:34 pm that afternoon. During this time, Jenny questioned sending the money via Western Union instead of completing an online bank transfer (i.e., bank to bank transfer). Between 5:34 pm and 10:17 pm on that Thursday, Jenny and the phisher exchanged eight emails. During these responses to the phisher, the only thing Jenny questioned was how the money is transferred, during the interview, Jenny reflected:

> so I just ran around and … as I said I am pretty matter of fact person and found out about Western Union and went down to Clifford Gardens and … and did all the things I had to do to send him the money

As previously stated, Jenny's main concern was that her cousin, whom she felt close to, needed her assistance. Jenny was so convinced she was helping her cousin, that she let "Jim" know she had to go to her bank and when she would be sending the money, including what she was doing that day:

> I will have to arrange with the bank in the morning, Friday, to withdraw the $ as they only allow $1000 without notice. I will have to arrange with the bank in the morning … I work at the (name withheld) office … tomorrow morning, 9:30am. I have to be there at that time … so I will try and get it done around 9 am ish tomorrow morning

The phisher does not push Jenny and consistently thanks her for her help, simply repeats the instructions on how to use Western Union:

> Hope it won't be too much troubles for you. Just send it to this Name (withheld) and Address: Engomi Nicosia Cyprus (Cyprus Euro). Please get back to me with the Money Transfer Control Number (MTCN) on the receipt including your full details you use in sending, it's important.
>
> Cheers jim

The exchanges between Jenny and the phisher also demonstrate "playing the line", Jenny is metaphorically pulling on the line by questioning how to transfer the money, showing some resistance, and the phisher lets the line relax enough to provide reassurance as if it were only to commence reeling the line back in again. These interactions were so successful for the phisher that they could maintain communication with Jenny for seven days.

Theme 3: Bringing the Catch In

Many fishermen bringing in the catch can be a euphoric experience; they have spent a lot of time making sure they have used the right lure, patiently played the line, and now they have their net ready to bring in their catch. If a phisher experiences the same thing as a fisherman, it can only be speculated that once the phisher has received their financial gain, they will experience some reward. This is usually the last stage of their interaction with the phisher and the phishing email for people who engage with a phishing email. The bait has been taken; they have interacted with the phisher, and will now have either given over their details or sent money to the phisher, believing they are assisting the individual.

For Jenny, this stage of her interaction with the phisher is interesting because not only did Jenny send money to the phisher, she did it twice. During the interviews, Jenny reflected that her late son assisted her in initially setting up her email account and provided general IT support when she started using emails and computers. "I remember my young son he's say 'mum you have to pay for proper email … you know what … providers, so I have always paid you know for Telstra whatever it is whoever I am with". The Purkait et al. (2014) study on the interactions of cognitive, behavioural, and emotional factors in detecting phishing emails found attention, vigilance and short-term memory were necessary. Jenny is an older person aware of phishing emails and how they can easily fool people. Jenny believed (and still feels) that she would not receive email scams by paying for an email service provider. When she received the email from Jim, she did not think she had to pay too much attention to it nor be vigilant to the possibility that the email was not from her cousin:

:

> Jenny: so I have always paid you know for Telstra whatever it is whoever I am with … whereas if you go gmail and all these other cheap yahoo and things

> that are free, they get a lot of scam … any when you got good umm security cover you know

This belief was and is a significant factor in why Jenny did not initially realise the email was fake. Vishwanath et al. (2018) stated that an individual's cyber-risk beliefs and modes of cognitive processing can lead to suspicion. Jenny's opinion that she was safe from scam emails inhibited her ability to detect the phishing email. Taking Purkait et al's. (2014) study Jenny's emotional response to wanting to help her cousin and her belief about being protected from scam emails. It is not surprising that she did what the phisher asked of her.

TD and SJT has shown why Jenny continued to engage with the phisher. Jenny engaged in rationalisation at each stage of her interaction with the phisher. Previously stated, she questioned why she could not do a bank-to-bank transfer, and she accepted the reason the phisher gave her

> Jenny: What do you think about sending it online. How does the money get from me to the western union online?
>
> Phisher: You can got it online with your credit card. Just click on the western link below and send through

Twenty-four hours after reading the phishing email, Jenny sent via Western Union the amount of money the phisher had requested. Several hours after the phisher had received Jenny's email confirming the money was received, the phisher made another request. "I am sorry to bother once again, I will need extra 2200 (euros) more, something came up, and I have to sort it out before I leave". Jenny's response demonstrates hesitation, "I do not have access to any more cash. I suppose I could put it on to my credit card … how long are you away?"

The phisher's response remained the same, and he lets her know how he wants her to send the money and is always asking how much interest she is being charged and promising to pay it back with the rest of the money

> Phisher: I do not know what your strategy is for placing it, could you pls send it through western union on your credit card and let me know how much interest it will incur. I really need you to send the 2200 (euros) the same way. I will pay back your money with all interest.

During these email communications, the phisher started to acknowledge he was asking a lot of Jenny, "Thanks so much for the mail response, and you have been so wonderful to me … thanks so much for your effort for me, kindly forgive me for stressing you."

Throughout the second request for money, Jenny's reactions reflect the first stage of deception; she has perceived something is not normal yet cannot connect to the deception. She stated in the interviews, "I started to get concerned after a while." The process of rationalising again may have been cognitively taxing on Jenny because she goes as far as to make the following comment to the phisher, "On reflection (in the shower!) I am beginning to find this story quite bizarre. I am happy to help you, but am puzzled that such a savvy, well-travelled person as yourself is unable to access his bank account."

She has questioned the situation and asked why someone like her cousin would require such financial assistance. According to the TD, Jenny uses the same hypothesis she developed earlier and sends money to the phisher for the second time. Jenny used systematic processing to make her second decision to help her cousin. Vishwanath et al. (2018) state that an individual such as Jenny will examine the quality of the argument within the persuasive context to make judgments and decisions.

For Jenny, was the persuasive context her desire to help her cousin, which made the quality of the argument to help so strong, even when she started to question it? This theory

further highlights the complexity of an older person engaging with a phishing email, the rationalisations or thought processes required are not linear.

Theme 4: The Sinker

The sinker refers to when Jenny realises she's been involved in a scam. The events and experiences that happened to her after. Jenny reflected that she started to become suspicious after she had sent the second lot of money and even went to great length in one of the email exchanges about her day to sort of test the phisher. The phisher asks, "How was your day? Just want to say thanks once again for the help you rendered. What's your program for tomorrow?"

During this exchange, Jenny went into detail about going to a farewell party at her local church and how she would support another parishioner. She ended this email by saying, "I am sure you did not expect to receive such a detailed explanation of my day!" The response from the phisher was the moment she realised she'd been scammed. The phisher started his response by saying how much he appreciated her help, "I knew it from time that you are good-hearted and so wonderful … it is good to help people of God and I believe your kind and loving heart will continue to reward you."

The email communication between Jenny and the phisher shows that they had become confident that Jenny would continue to assist them as their third request for money was significantly larger than the first two requests. The phisher even gave a reason for asking for more money.

> Phisher: I was able to fix a bit here but I'm still having issues with some documents from the mortgage company I need to get before I leave here. I need to come up with 7, 800 euro ASAP. Please I want you to do your best for me as soon as you can.

The last request from the phisher was enough for Jenny to realise this was a scam,

> Jenny: I just cannot believe your request. It is just out of the question, apart from the fact that you have not been forth at all forthcoming with what this is all about. I have not queried you, as I am not that sort of person, but really …

When Jenny declined to send another payment, the phisher stopped sending emails immediately. The phisher no longer emailing Jenny is not uncommon; once a phisher has been unmasked, so to speak, they move on to another victim (Bisson, 2019; Banu & Banu, 2013). Unlike many people who have been scammed by phishers, Jenny reported her experience to the authorities.

Jenny experienced embarrassment and shock, reflecting:

> I lead a pretty busy life I mean I think people are silly all these people you hear get ties up with these … arghh for goodness sake … you know … can't you see who silly that was and here I am … really taken for a ride well and truly.

The interesting thing to note is the impact on Jenny's life was less than what other victims of scams have experienced. Cross et al. (2016) acknowledged that an older person's reactions and how an experience like this can impact a person are very varied. Jenny, during this time, was a very financially independent person (and still is today), dealing with this experience in a very matter-of-fact way and, when discussing it, does so in that manner. During the first interview, Jenny stated, "I'm not an alarmist sort of person you know you just get on with life and things happen … you've just got to try to prevent it through not connecting with something like that".

Throughout the interviews, Jenny often referred to her upbringing and several experiences in her life she feels made her able to cope with challenging moments:

> You just get on with life … well my mother was a wonderful person both my parents were returned servicemen and dad died in 1959 and he was only 37 and there were 6 of us so dad died and three months later the 4th little boy was knocked off his bike and killed going off with some friends he's only 8 and ahh but mum wasn't a victim sort of person we were from the bush originally and she grieved but she just wasn't a victim and ‘why's this happen to me' or fall in a heap you know I just suppose you learn from those experiences.

Jenny's life narrative has informed how she deals with the personal tragedies she has experienced and her ability to move past the initial embarrassment and shame she felt after the phishing email. Browne-Yung, Walker, and Luszcz (2015) examined resilience and coping in older persons using the Life Narrative method and identified aspects of self-identity being positively correlated with coping strategies when faced with the challenges of aging. Aging is a lifelong process that encompasses growing up and growing old. Many people view aging as a time of physical and cognitive decline where people retire over 67. Older people must navigate a world through the lens of ever-evolving technology and the technological advancements of the modern age.

SJT and TD provide a framework for understanding why Jenn engages with the phishing email and the decisions and influencing factors. At each stage of the interaction, lexicon cues influenced Jenny, her perceptions and understanding of her world and what role she plays in it. Jenny was a victim of a phishing email, as many other older persons have been and continue to be. Her experience highlights the complexity of how a older person makes decisions when confronted with an fraudulent email and the numerous variables that interact with one another to inform and shape these decisions.

4: Conclusion

This research aimed to examine the experience of an older person engaging with a phishing email. The principal researcher used the TD and SJT as a foundation to understand why Jenny, the participant, was deceived into engaging with the fraudulent email. Through analysis of the email correspondence between Jenny and the phisher and interviews, these theories provided a framework to understand Jenny's experience. While there is previous literature which has investigated phishing, this study specifically focused on an older person's experience with engaging with a phishing email through an in-depth descriptive case study. This study analysed the email correspondence between a phisher and their victim using thematic analysis. The email correspondence provided insight into the phisher's language and how it was used to influence Jenny into engaging and ultimately sending money to the phisher. Previous studies (e.g., Oliveira et al, 2017; Ebner et al, 2018) refer to the type of language a phisher will use and do not detail the sentences and other grammatical aspects of the email or use actual email correspondence in their research. Having the opportunity to read and have a victim of fraud explain in their own words their thinking and interpretation of the phishing was invaluable and addressed a gap in the literature.

To understand why Jenny engaged and continued to engage with the phisher is complicated, , it is difficult for one theory to fully explain why Jenny continued to engage with the phisher despite having previous information to be able to identify them and the risk associated. The stages of the TD explained how the phisher used language to keep Jenny engaged. The framework of SJT explained how Jenny's nature and desire to help someone she was close to and in need influenced her judgement of the fraudulent email. Together these theories provide an understanding of Jenny's choices to engage with the email requests. For Jenny, the TD can only provide the framework to understand her acceptance of the hypothesis that the email was authentic and from her cousin. In the first stage of the TD, the

phisher hacked into Jenny's cousin's email and used language that would be familiar to those who know him to deceive a contact into engaging with them. The phisher's use of reciprocity, social proof and scarcity in the language they used in the email provided the necessary environment for Jenny to want to engage. Keeping the message short and using words to create a sense of a need to respond immediately is how many phishers are successful in their deceptions.

This study highlights the strength of lexicon cues. The language used in the phisher's email to Jim's contacts are strong influence and can distract and diminish a person's ability to recognise a fraudulent email. In the second stage of deception, victims like Jenny will rationalise why they are engaging, even when the email is suspicious. Throughout the interview, Jenny referred to the language in the email, noting that her cousin was financially secure. Yet, the words in the email contradicted the information Jenny already had. Older people who support those in their lives and put others before themselves go through the third stage of deception, still rationalising. Still, the desire to help continues to influence them, and they will engage.

SJT delivers Jenny's interpretation and response framework, anchored in her natural desire to support those around her and those she feels close to. These beliefs were further reflected in the work Jenny did in her life. Jenny had a strong social conscience and engaged in community volunteer work and local political activism. SJT stated people would not have access to explicit information such as being aware or vigilant to suspicious emails and relying on judgements based on their worldview. Jenny's judgement anchor, social consciousness, perceived the email to be correct and aligned with her anchor influencing her to engage. Jenny's perception of the situation was complicated by the proximity of cues within the email. SJT reports the proximity of environmental cues complicates perceptions of the

situation. For Jenny, her nature to help others in need informed her decision to accept the email as accurate.

Limitations and Future Directions

The limitations of this study are the complexity of an older person engaging with a phishing email is challenging to represent. When writing results and discussions, a linear approach is often taken with a beginning, middle, and end; this study is not linear (Hodkinson & Hodkinson, 2001). The themes show a lot of overlap and repetition of theories and stages of theories. The amount of data, when revisited, would possibly reveal other issues not addressed in this study. Understanding the participant's emotional reactions within the context of their social solid identity, resilient nature, and matter-of-fact attitude was challenging to unpack within the theoretical frameworks used for this study.

Case study research is not to generalise, the TD and SJT was able in part to help understand Jenny's experience, but they will not be able to explain the 10 689 incidents of phishing scams older persons engaged with as of April 2020 (ACCC, 2020; Hodkinson & Hodkinson, 2001). Hodkinson and Hodkinson (2001) and Yin (2014) note case studies cannot make typical claims. There is no empirical evidence to know if what Jenny went through is representative of the larger population because there is no way of establishing probability (Baxter & Jake, 2008).

Further research should address the impact of an older person's upbringing and life experience. The participant in this study reflected on their childhood and life experiences, which significantly influenced how they cope with challenges in their lives. Close ties to family and community played a vital role in the participant’s decision to engage with the phishing email. A larger participant pool to explore these themes in more detail will provide further insight into decision-making. Using other theoretical frameworks in conjunction with the ones used in this study and comparing results may enable the research to explore

education and learning tools to support older persons to be more informed and vigilant regarding recognising phishing emails.

Strengths and Possible Implications

Being able to answer why an older person would engage with a phishing email and continue to engage is difficult. Each older person who has engaged with a phishing email has their own lived experience, worldview judgement and level of confidence in using emails for communication and as an everyday necessity. What will influence one older person will be different for another. The strength of this study is having access to the email correspondence between the participant and the phisher. Providing a unique insight into not only what the phisher said but also how the participant responded. The participant's lived experience also provides an opportunity to understand how they dealt with being a victim of a phishing email and what they have learned from the experience. This data source could be invaluable for educational programs specifically designed for older persons. The participant’s experience shows the complexity of an older person's decision-making process and illustrates the many variables that can influence these decisions. The complex nature of what influences an older person to engage in a phishing attack remains a barrier to effective older persons' education.

This research aimed to understand better the experience of one older person who engaged with a phishing email. Sharing this real-world example could contribute to more holistic educational tools for older people to learn from and to build their resilience to the influences of phishing emails. This approach would be very practical, especially if, like the participant in this research, the older person finds fulfillment in helping others or wishes to feel useful in their older years. The participant was motivated to engage due to their nature; they make themselves available to support their family, and their desire to help influences their decision-making daily. The continued pursuit of understanding the complexities of older people's engagement with phishing attacks and providing targeted person-centred education

to protect this susceptible population is essential. This cohort is growing in numbers and is increasingly required to access email as a primary point of contact, thus providing phishers with more opportunities. Phishers are constantly changing how they construct their emails, and the sophistication of AI and bots is not only being incorporated into emails, but technology is becoming more sophisticated.

Why would an older person engage and continue to engage with a phishing email? To fully answer this question, it is essential to understand how the phisher uses emails to attract an older person and what 'tools of the trade they use'. It is also essential to understand how an older person makes judgements and what motivates them daily; do they feel disconnected from their loved ones? Are they a "helper"? Older people vary in their life experience and capacity to navigate technology in the modern era. Universal email fraud educational tools will not be effective for all older persons. A holistic approach provides education on detecting or recognising a phishing email and how a phisher uses emails, for example, using lexicon cues. Part of the holistic approach would also be to ask the older persons to reflect on their own life experiences and to recognise how they make decisions and what influences them. The complexity of an older person engaging with a phisher is a complicated interaction where variables such as technology, lexicon cues, perceptions, habits, vulnerabilities, greed, day-to-day life and worldview judgements interact to detect the fraud or to fall victim to it.

Appendix A

Interview Guide for Interview One and Two

(Note: example of questions and prompts used)

1) Could you give me a brief history of your use of technology?

   prompts: reasons for using eg computers, electronic communication

2) How do you feel about technology?

   prompts: emails, using, communicating with others

3) Can you describe what your day-to-day is like?

   prompts: routine, checking emails, socialise

4) Could you describe what you were doing before opening your email that day?

   prompts: anything different, working, different routine?

5) Can you describe what you were thinking when opened the email?

   prompts: something you often think?, how did that make you feel?, concern, what did you think of…?

6) How do you feel about your experience of engaging with the phishing email?

   prompts: why do you feel like that?, Do things differently?, Has relationships changed with cousin?

References

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

Alhojailan, M. I. (2012). Thematic analysis: A critical review of its process and evaluation. *West East Journal of Social Sciences, 1*(1), 39-47. Retrieved from http://westeastinstitute.com/journals/wp-content/uploads/2013/02/4-Mohammed-Ibrahim-Alhojailan-Full-Paper-Thematic-Analysis-A-Critical-Review-Of-Its-Process-And-Evaluation.pdf

Alsayed, A. O., & Bilgrami, A. L. (2017) E-Banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities. *International Journal of Emerging Technology and Advanced Engineering, 7*(1), 109-115. Retrieved from https://www.researchgate.net/profile/Anwar-Bilgrami/publication/315399380_E-Banking_Security_Internet_Hacking_Phishing_Attacks_Analysis_and_Prevention_of_Fraudulent_Activities/links/59f19d7c0f7e9beabfca5f17/E-Banking-Security-Internet-Hacking-Phishing-Attacks-Analysis-and-Prevention-of-Fraudulent-Activities.pdf

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies, 82*, 69-82. doi: 10.1016/j.ijhcs.2015.05.005

Aronson, J. (1995). A pragmatic view of thematic analysis. *The qualitative report, 2*(1), 1-3. doi: 10.46743/2160-3715/1995.2069

Asfer, A., Sabri, N. S., & Bairmani, H. K. (2021). Persuasion in Cyber Blackmail's Emails: A pragma-dialectical Study. *Review of International Geographical Education Online, 11*(5). doi: 10.48047/rigeo.11.05.118

Asemah, E. S., & Nwammuo, A. N. (2017). Implications of social judgement theory for persuasive advertising campaigns. *Journal of Research in National Development, 15*(1). Retrieved from https://www.ajol.info/index.php/jorind/article/view/158507

Australian Bureau of Statistic. (2017). *Internet activity, Australian, June 2017* (Catalogue No. 813.0) [Fact sheet]. Retrieved from http://www.abs.gov.au/ausstats/abs@.nsf /0/00FD2E732C939 C06CA257E19000FB410?Opendocument

Australian Competition and Consumer Commission Scamwatch (2017). *Phishing statistics.* [Fact sheet]. Retrieved from https://www.scamwatch.gov.au/about-scamwatch/scam-statistics?scamid=31&date=2017

Australian Competition and Consumer Commission Scamwatch (2018). *Phishing statistics*. [Fact sheet]. Retrieved from https://www.scamwatch.gov.au/about-scamwatch/scam-statistics?scamid=31&date=2018

Australian Competition and Consumer Commission Scamwatch (2020). *Scam statistics.* [Fact sheet]. Retrieved from https://www.scamwatch.gov.au/about-scamwatch/scam-statistics?scamid=31&date=2019

Australian Competition and Consumer Commission Scamwatch (2020). *Phishing statistics*. [Fact sheet]. Retrieved from https://www.scamwatch.gov.au/about-scamwatch/scam-statistics?scamid=31&date=2020

Australian Competition and Consumer Commission Scamwatch (2020). *Phishing statistics*. [Fact sheet]. Retrieved from https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/phishing

Australian Competition and Consumer Commission Scamwatch (2020). *Phishing statistics*. [Fact sheet]. Retrieved from https://www.scamwatch.gov.au/scam-statistics/targeting-scams

Banu, M. N., & Banu, S. M. (2013). A comprehensive study of phishing attacks. *International Journal of Computer Science and Information Technologies*, *4*(6), 783-786. doi: 10.1.1.643.766

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The qualitative report*, *13*(4), 544-559. Retrieved from http://111.nova.edu/ssss/QR/QR13-4/baxter.pdf

Bayl-Smith, P., Taib, R., Yu, K., & Wiggins, M. (2021). Response to a phishing attack: persuasion and protection motivation in an organizational context. *Information & Computer Security*. doi: 10.1108/ICS-02-2021-0021

Berger, R. (2015). Now I see it, now I don't: Researcher's position and reflexivity in qualitative research. *Qualitative research*, *15*(2), 219-234. doi: 10.1177/1468794112468475

Bisson, D. (2019). *6 common phishing attacks and how to protect against them.* Retrieved from https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), 77-101. doi: 10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2012). Thematic analysis. *American Psychological Association* (Vol. 2, pp. 1-15).doi:10.1037/13620-004

Brehmer, B. (1988). The development of social judgment theory. In *Advances in Psychology* (Vol. 54, pp. 13-40). doi: 10.1016/S0166-4115(08)62169-X

Browne-Yung, K., Walker, R. B., & Luszcz, M. A. (2017). An examination of resilience and coping in the oldest old using life narrative method. *The Gerontologist*, *57*(2), 282-291. doi: 10.1093/geront/gnv137

Carlson, E. L. (2006). Phishing for elderly victims: as the elderly migrate to the internet fraudulent schemes targeting them follow. *Elder LJ*, *14*, 423-452. Retrieved from https://theelderlawjournal.com/wp-content/uploads/2019/01/carlson.pdf

Chen, S., & Chaiken, S. (1999). The heuristic-systematic model in its broader context. In S. Chaiken & Y. Trope (Eds.), *Dual-process theories in social psychology* (pp. 73-96). New York: Guilford Press.

Chen, X., Bose, I., Leung, A. C. M., & Guo, C. (2011). Assessing the severity of phishing attacks: A hybrid data mining approach. *Decision Support Systems*, *50*(4), 662-672. doi:10.1016/j.dss.2010.08.020

Cialdini, R. B. (2009). *Influence: Science and Practice* (Vol. 4). Boston, MA: Pearson education.

Cochen, V., Arbus, C., Soto, M. E., Villars, H., Tiberge, M., Montemayor, T., ... & Verny, M. (2009). Sleep disorders and their impacts on healthy, dependent, and frail older adults. *The Journal of Nutrition, Health and Aging*, *13*(4), 322-329. doi:10.1007/s12603-009-0030-0

Cooksey, R. W. (1996). The methodology of social judgement theory. *Thinking & Reasoning*, *2*(2-3), 141-174. doi: 10.1080/135467896394483

Croff, R. L., Witter IV, P., Walker, M. L., Francois, E., Quinn, C., Riley, T. C., ... & Kaye, J. A. (2019). Things are changing so fast: Integrative technology for preserving cognitive health and community history. *The Gerontologist*, *59*(1), 147-157. doi: 10.1093/geront/gny069

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, *21*(2), 187-204. doi:10.1177/0269758015571471

Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice*, *518*, 1-14. doi: 10.3316/informit.30056690391621

Dhamija, R., Tygar, J. D., & Hearst, M. (2006, April). Why phishing works. *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581-590). doi: 10.1145/1124772.1124861

Doherty, M. E., & Kurz, E. M. (1996). Social judgement theory. *Thinking & Reasoning*, *2*(2-3), 109-140. doi: 10.1080/135467896394474

Ebner, N. C., Ellis, D. M., Lin, T., Rocha, H. A., Yang, H., Dommaraju, S., Donovan & Oliveira, D. S. (2018). Uncovering susceptibility risk to online deception in aging. *The Journals of Gerontology: Series B*, *00*(0), Volume 75, Issue 3, Pages 522–533,1-12. doi: 10.1093/geronb/gby036

Elger, T. (2010). Bounding the case. *Encyclopedia of Case Study Research*, *1*, 55-59.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1-4. doi: 10.11648/j.ajtas.20160501.11

Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, *5*(1), 80-92. doi:10.1177/160940690600500107

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. doi: 10.1016/j.ijhcs.2018.12.004

Gallagher, J. R. (2019). A Framework for Internet Case Study Methodology in Writing Studies. *Computers and Composition*, *54*, 102509. doi:10.1016/j.compcom.2019.102509

Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *Plus One*, *12*(2), e0171620. doi:10.1371/journal.pone.0171620

Giaccardi, E., Kuijer, L., & Neven, L. (2016). Design for resourceful ageing : intervening in the ethics of gerontechnology. In P. Lloyd, & E. Bohemia (Eds.), *Proceedings of DRS 2016, Design + Research + Society Future-Future-Focused Thinking: 50th Anniversary International Conference, Brighton, UK, 27-30 June 2016* (Vol. 1)

Glaser, B. G., & Strauss, A. L. (2017). *Discovery of Grounded Theory: Strategies for Qualitative Research*. London, England; New York, New York : Routledge

Grazioli, S., & Wang, A. (2001). Looking without seeing: understanding unsophisticated consumers' success and failure to detect Internet deception. *ICIS 2001 proceedings*, 23. Retrieved from https://aisel.aisnet.org/icis2001/23

Hodkinson, P., & Hodkinson, H. (2001). The strengths and limitations of case study research. *In learning and skills development agency conference at Cambridge*, *1*(1), 5-7. Retrieved from https://www.academia.edu/31677978/The Strengths and_Limitations_of_Case_Study_Research

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

Javadi, M., & Zarea, K. (2016). Understanding thematic analysis and its pitfall. *Journal of Client Care*, *1*(1), 33-39. doi: 10.15412/j.jcc.02010107

Lee, C. C., Czaja, S. J., Moxley, J. H., Sharit, J., Boot, W. R., Charness, N., & Rogers, W. A. (2019). Attitudes toward computers across adulthood from 1994 to 2013. *The Gerontologist*, *59*(1), 22-33. doi: 10.1093/geront/gny081

Loe, M. (2010). Doing it my way: Old women, technology and wellbeing. *Sociology of health & illness*, *32*(2), 319-334. doi: 10.1111/j.1467-9566.2009.01220.x

Luborsky, M. R., & Rubinstein, R. L. (1995). Sampling in qualitative research: Rationale, issues, and methods. *Research on aging*, *17*(1), 89-113. doi:10.1177/016402 7595171005

Marecek, J. (2003). Dancing through minefields: Toward a qualitative stance in psychology. In P. M. Camic, J. E. Rhodes, & L. Yardley (Eds.), *Qualitative research in psychology: Expanding perspectives in methodology and design* (pp. 49-69). Washington, DC, American Psychological Association. doi: 10.1037/10595-004

McCombie, S. (2008). Trouble in Florida: The Genesis of Phishing attacks on Australian Banks. doi: 10.4225/75/57b2712140cbd

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Mohammad, R. M., Thabtah, F., & McCluskey, L. (2015). Tutorial and critical analysis of phishing websites methods. *Computer Science Review*, *17*, 1-24. doi: 10.1016/j.cosrev.2015.04.001

Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014, August). Social engineering attack framework. In *2014 Information Security for South Africa* (pp. 1-9). doi: 10.1109/ISSA.2014.6950510

Naksawat, C., Akkakoson, S., & Loi, C. K. (2016). Persuasion strategies: use of negative forces in scam e-mails. *GEMA Online® Journal of Language Studies*, *16*(1), 4-17.

Retrieved from https://eprints.ums.edu.my/id/eprint/13928/7/ Persuasion%20Strategies%20Use%20of%20Negative%20Forces%20in%20Scam%20E-mails.pdf

Nam, S., Han, S. H., & Gilligan, M. (2019). Internet use and preventive health behaviors among couples in later life: Evidence from the health and retirement study. *The Gerontologist*, *59*(1), 69-77. doi: 10.1093/geront/gny044

Noor, K. B. M. (2008). Case study: A strategic research methodology. *American Journal of Applied Sciences*, *5*(11), 1602-1604. doi: 10.3844/ajassp.2008.1602.1604

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., ... & Ebner, N. (2017, May). Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 6412-6424). doi: 10.1145/10.1145/3025453.3025831

Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2019). Predicting susceptibility to social influence in phishing emails. *International Journal of Human-Computer Studies*, *128*, 17-26. doi: 10.1016/j.ijhcs.2019.02.007

Peine, A., & Neven, L. (2019). From intervention to co-constitution: new directions in theorizing about aging and technology. *The Gerontologist*, *59*(1), 15-21. doi: 10.1093/geront/gny050

Petty, R. E., & Cacioppo, J. T. (1981). Attitudes and persuasion: classic and contemporary approaches, Wm. C. *Brown, Dubuque, IA*. doi: 10.4324/9780429502156

Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. In *Communication and persuasion* (pp. 1-24). New York, NY: Springer doi: 10.1016/S0065-2601(08)60214-2

Phishing. Org (n.d.). Retrieved February 28, 2018, from http://www.phishing.org/history-of-phishing

Purkait, S., Kumar De, S., & Suar, D. (2014). An empirical investigation of the factors that influence internet user's ability to correctly identify a phishing website. *Information Management & Computer Security*, *22*(3), 194-234. doi:10.1108/IMCS-05-2013-0032

Rader, M., & Rahman, S. (2015). Exploring historical and emerging phishing techniques and mitigating the associated security risks. *arXiv preprint arXiv:1512.00082*.

Rekouche, K. (2011). Early phishing. *arXiv preprint arXiv:1106.4692*.

Ross, M., Grossmann, I., & Schryer, E. (2014). Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. *Perspectives on Psychological Science*, *9*(4), 427-442. doi:10.1177/1745691614535935

Russell E. Morgan, (2005) Technology greets the age wave, *The Gerontologist*, *45*(5), 704–710. doi: 10.1093/geront/45.5.704

Silva, M. D. G. D., & Boemer, M. R. (2009). The experience of aging: a phenomenological perspective. *Revista Latino-Americana de Enfermagem*, *17*(3), 380-386. doi: 10.1590/s0104-11692009000300016

Smith, J. A. (2004). Reflecting on the development of interpretative phenomenological analysis and its contribution to qualitative research in psychology. *Qualitative research in psychology*, *1*(1), 39-54. doi:10.1191/147808870qp004oa

Solesio-Jofre, E., Lorenzo-López, L., Gutiérrez, R., López-Frutos, J. M., Ruiz-Vargas, J. M., & Maestú, F. (2011). Age-related effects in working memory recognition modulated by retroactive interference. *Journals of Gerontology Series A: Biomedical Sciences and Medical Sciences*, *67*(6), 565-572. doi: 10.1093/gerona/gir199

Spreng, R. N., Cassidy, B. N., Darboh, B. S., DuPre, E., Lockrow, A. W., Setton, R., & Turner, G. R. (2017). Financial exploitation is associated with structural and functional brain differences in healthy older adults. *Journals of Gerontology Series A:*

Biomedical Sciences and Medical Sciences, *72*(10), 1365-1368. doi: 10.1093/gerona/glx051

Stets, J. E., & Burke, P. J. (2000). Identity theory and social identity theory. *Social psychology quarterly*, *63*(2), 224-237. doi: 10.2307/2695870

Szabo, A., Allen, J., Stephens, C., & Alpass, F. (2019). Longitudinal analysis of the relationship between purposes of internet use and well-being among older adults. *The Gerontologist*, *59*(1), 58-68. doi: 10.1093/geront/gny036

Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. *Behaviour & Information Technology*, *32*(10), 1014-1023. doi: 10.1080/0144929X.2013.763860

Tuckett, A. G. (2005). Applying thematic analysis theory to practice: a researcher's experience. *Contemporary Nurse*, *19*(1-2), 75-87. doi:10.5172/conu.19.1-2.75

Uebelacker, S., & Quiel, S. (2014, July). The social engineering personality framework. In *2014 Workshop on Socio-Technical Aspects in Security and Trust* (pp. 24-30). IEEE. doi: 10.1109/STAST.2014.12

Umanailo, M. C. B., Fachruddin, I., Mayasari, D., Kurniawan, R., Agustin, D. N., Ganefwati, R., ... & Sutomo, S. (2019). Cybercrime Case as Impact Development of Communication Technology That Troubling Society. *Int. J. Sci. Technol. Res*, *8*(9), 1224-1228. Retrieved from https://www.academia.edu/40485359/Cybercrime Case As_Impact_Development_Of_Communication_Technology_That_Troubling_Society ?auto=citations&from=cover_page

Vacek, P., & Rybenska, K. (2015). Research of interest in ICT education among seniors. *Procedia-Social and Behavioral Sciences*, *171*, 1038-1045. doi: 10.1016/j.sbspro.2015.01.276

Vacek, P., & Rybenská, K. (2016). The most frequent difficulties encountered by senior citizens while using information and communication technology. *Procedia-Social and Behavioral Sciences*, *217*, 452-458. doi:10.1016/j.sbspro.2016.02.013

Vayansky, I., & Kumar, S. (2018). Phishing–challenges and solutions. *Computer Fraud & Security*, *2018*(1), 15-20. Retrieved from http://www.researchgate.net/profile/Sathish-Kumar-26/publication/322823383_Phishing_-_callenges_and_solutions/links/5acde9fa4585154f3f420911/Phishing-challenges-and-solutions.pdf

Virginia, B., & Victoria, C. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*, 77–101. doi:10.1191/1478088706qp063oa

Vishwanath, A. (2015). Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack. *Journal of Computer-Mediated Communication*, *20*(5), 570-584. doi:10.1111/jcc4.12126

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, *45*(8), 1146-1166. doi: 10.1177/0093650215627483

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, *72*, 412-421. doi:10.1016/j.chb.2017.03.002

Williams, E. J., & Polage, D. (2019). How persuasive is phishing email? The role of authentic design, influence and current events in email judgements. *Behaviour & Information Technology*, *38*(2), 184-197. doi: 10.1080/0144929X.2018.1519599

Wood, W., & Rünger, D. (2016). Psychology of habit. *Annual Review of Psychology*, *67*. 289-314. doi:10.1146/annurev-psych-122414-033417

World Health Organisation, (2018). *Health statistics and information systems.* Retrieved from http://www.who.int/healthinfo/survey/ageingdefnolder/en/

Wright, R., Chakraborty, S., Basoglu, A., & Marett, K. (2010). Where did they go right? Understanding the deception in phishing communications. *Group Decision and Negotiation, 19*(4), 391-416. doi: 10.1007/s10726-009-9167-9

Yardley, L. (2000). Dilemmas in qualitative health research. *Psychology and Health*, *15*(2), 215-228. doi: 10.1080/08870440008400302

Yin Robert, K. (1994). *Case study research: Design and methods* (2nd ed.). Thousand Oaks, CA: Sage Publications.