The Relationship Between Social Persuasion Strategies, Phishing Features and Email Exposure Time on Phishing Susceptibility

Tazin Tanvir

This thesis is submitted in partial fulfilment of the Honours degree of Bachelor of Psychological Science (Honours)

School of Psychology

University of Adelaide

September 2020

Word Count: 9,445

Table of Contents

List of Figures..........4

Abstract..........5

Declaration..........6

Contribution Statement..........7

Acknowledgements 8

The relationship between social persuasion strategies, phishing cues, and email exposure time on phishing susceptibility 9

Phishing Emails *9*

Phishing Email Characteristics and Susceptibility..........*11*

Social persuasion in phishing emails. 11

Persuasion strategy prevalence. 13

Exposure time. 15

Exposure time and social persuasion strategies. 15

The number of phishing features in phishing emails. 17

The Current Study *19*

Method 19

Participants..........*19*

Design *20*

Measures..........*20*

Demographic questionnaire. 21

Email exposure time. 21

Email stimuli. 21

Email sorting task. 22

Procedure *24*

Pilot study. 24

Results 25

Overview of Analyses *25*

Data reduction. 27

Analysis of persuasion strategies, exposure time, and phishing susceptibility (H1, H2). 27

Analysis of the interaction between persuasion strategies, and exposure time (H3). 29

Social persuasion strategies and phishing susceptibility. 31

Exposure time and phishing susceptibility. 32

Exposure time and the effectiveness of persuasion strategies 32

The number of phishing features and phishing susceptibility. 33

Strengths of the current study. 35

Limitations and future directions. 36

Conclusion 37

References 39

Appendix A: Examples of Email Stimuli. 45

Appendix B: Pilot Study Results. 50

List of Figures

FIGURE 1. EXAMPLES OF EMAILS USED. 26

FIGURE 2. SECOND PART OF THE PILOT STUDY. 28

FIGURE 3. THE EFFECTS OF PERSUASION STRATEGY AND PHISHING DETECTION RATE (H1), EXPOSURE TIME AND PHISHING DETECTION RATE (H2) AND INTERACTION BETWEEN EXPOSURE TIME AND PERSUASION STRATEGIES (H3). 30

Abstract

A ‘phishing email’ aims to persuade an unsuspecting individual to reveal personal credentials and sensitive information. Currently, the global costs to businesses and individuals associated with phishing related attacks are reported in the hundreds of millions of dollars. While technological interventions capture a proportion of these phishing emails, ultimately, the human user is the last line of defence in determining the legitimacy of the email. ‘Phishers’ aim to exploit human weaknesses through the use of various persuasion strategies that create a sense of urgency and time pressure to respond to emails. Typically, individuals must also rely on subtle phishing features in an email to determine if the email is genuine or an attempted phish. Furthermore, phishers take advantage of the assumption that users determine the legitimacy of emails in a short amount of time. The present study aims to examine the impact of these email characteristics of persuasion strategies, the number of phishing features, and exposure time on phishing detection and susceptibility. Using an online survey platform, participants (N= 136) completed an email sorting task where they were required to review and sort 60 incoming emails from the inbox of ‘Professor Alex Jones’. Several significant results were obtained supporting the hypotheses. It demonstrated that individuals are better able to detect a phishing email when it utilises common persuasion strategies (authority and scarcity), and contain a greater number of phishing features. It also revealed that with increased email exposure time, individuals had a better phishing detection rate. However, the effect of identifying phishing emails with common persuasion strategies was not greater during shorter exposure time, providing a non-significant result. A greater understanding of these email factors associated with phishing susceptibility could lead to more tailored awareness campaigns and/or training programs to increase phishing detection and reduce susceptibility.

Keywords. Phishing, Persuasion Strategies, Features, Email Exposure Time

Declaration

“This thesis contains no material which has been accepted for the award of any other degree of diploma in any University, and, to the best of my knowledge, this thesis contains no material previously published except where due reference is made. I give permission for the digital version of this thesis to be made available on the web, via the University of Adelaide's digital thesis repository, the Library Search, and through web search engines, unless permission has been granted by the School to restrict access for a period of time.”

September 2020

Contribution Statement

I would like to acknowledge that this Honours research project was a collaborative process between myself, another student researcher, and my two supervisors. In writing this thesis, my supervisors and I collaborated to generate research questions of interest and design the appropriate methodology. I conducted the literature search with the guidance of my supervisors. I would like to highlight that myself and my research partner, both equally worked together to collate, create, and validate the stimuli utilised in the "Email Sorting Task". Out of 60 emails that were utilised in this study, I created thirty of the emails. On Qualtrics, I created the second part of the pilot study questionnaire regarding the ranking of persuasion strategies. My research partner and I were responsible for all participant recruitment and testing, and my supervisors provided all participation incentives. I also assisted in creating the data spreadsheets for the main and pilot study from which my supervisors conducted the data analyses in the “Results” section using SPSS. I collaborated with them to generate the graphs using Excel for the “Results” section and with guidance, interpreted the output of the results. I wrote up all aspects of the thesis which was reviewed by my primary supervisor.

Acknowledgements

I would like to thank both of my supervisors, Dr. Jaime Auton and Dr. Daniel Sturman, whose guidance has allowed me to complete this thesis to the best of my ability. Thank you to both of you for being patient with me and constantly explaining things in different ways when I was struggling to understand a potentially simple concept. Thank you, Daniel, for assisting me with my thesis presentation, hypothesis development, analysis of results, and teaching me how to write and phrase things more concisely and succinctly. Thank you, Jaime, for providing me with comfort when I was stressed, keeping me focused in the present, teaching me how to put attention to detail in my work and for always asking numerous "out of the box" questions which broadened my knowledge. I also had the pleasure of having you guys as my Organisational Psychology lecturers which I thoroughly enjoyed. Thank you both for your time and dedication and for allowing me to learn and gain so much knowledge and skills from you.

I would like to thank my research partner and friend, Oliver Plate, with whom I worked to develop the stimuli of this study. Our dedication and teamwork have finally paid off as we ran a successful study and are now graduating Honours with our amazing theses. Thanks for teaching me how to keep calm and cool under stress. Could not have asked for a better research partner!

Thank you to my family and friends who always made sure I was physically and mentally well by making plans so that I could take a break when I was too indulged in my studies. To my parents for always supporting and believing in me. I know you guys are always proud of me.

The relationship between social persuasion strategies, phishing cues, and email exposure time on phishing susceptibility

Phishing Emails

Commonly administered through emails, phishing is a form of deception, persuading unsuspecting individuals to perform certain actions in an attempt to obtain personal credentials and sensitive information (Chen, Mishler, Hu, Li, & Proctor, 2018; Lawson, Pearson, Crowson, & Mayhorn, 2020; Parsons, Butavicius, Delfabbro, & Lillie, 2019; Pattinson, Butavicius, Parsons, & Mccormac, 2016). This is often achieved through requesting online users to reply to the sender, click on embedded links or download malicious attachments to divulge usernames and passwords or inadvertently install malware (Chen et al., 2018). Phishing emails are becoming more prevalent, targeting and compromising an organisation's information security, posing as a huge real-world problem. According to a report by Verizon (2019), 32% of data breaches in 2019 in Australia were through phishing. It was targeted at sectors such as education, health, and financial organisations (Verizon, 2019). Currently, the global costs to organisations and individuals associated with phishing-related attacks have been reported in the hundreds of millions of dollars (ACCC, 2019; Bissell, LaSalle, & Dal Cin, 2019).

Although numerous technological advancements exist such as email filtering systems or authentication devices, phishing emails are becoming more sophisticated and harder to detect (Chen et al., 2018; Lawson et al., 2020; Parsons et al., 2019; Pattinson et al., 2016). While these technologies are broadly effective in reducing the number of phishing emails being shown to users, the human user is the last line of defence when determining the legitimacy of the email. However, existing literature repeatedly identifies individuals' poor capacities for detecting online phishing with more than 90% of individuals falling victim to some form of phishing (Hong, Kelley, Tembe, Murphy-Hill, & Mayhorn, 2013). Even when primed to detect phishing, participants fail to detect 47% of phishing stimuli (Alsharnouby, Alaca, & Chiasson, 2015). The 2019 Cost Breach Data report by Ponemon Institute, based on interviews with companies who experienced a data breach between July 2018 and April 2019, found that the average cost due to human error in recognising phishing emails was about $3.5 million.

An example of the poor capacity of individuals in detecting phishing was in 2019 when the Australian Catholic University (ACU) staff could not recognise a phishing attempt and were successfully phished. The staff received a phishing email that pretended to be from the Vice-Chancellor of the ACU and requested the users to click on a link and enter credentials into a fake ACU login page. As a result, several of the staff members lost their bank account details as well as their money (Fellner, 2019). Even more recently, there has been a gradual increase in COVID-related phishing attacks since January 2020 in Australia (Muncaster, 2020). COVID-19-themed phishing attacks were in the form of scams, brand impersonation, blackmail, and business emails. It was targeted at Australian organisations across a range of sectors including the government, the retail industry, the education, and the health sector (Chen et al., 2018).

Besides the financial impacts, there are also psychological impacts associated with phishing attacks. Phishing victims generally experience feelings of embarrassment and distress which stem from monetary loss. Victims also showcase distrust towards internet-based communication that consequently minimises their internet usage (Chen et al., 2018; Lawson et al., 2020; Parsons et al., 2019; Pattinson et al., 2016). Further damages from phishing attacks also include reputational harm, theft of corporate secrets, and the exposure of classified information (Jensen, Dinger, Wright, & Thatcher, 2017).

In light of the significant impacts of phishing attacks at an individual and an organisational level, and the errors that individuals can make when appraising the legitimacy of emails, there is an urgent need for phishing-related research. Research in this area will provide an understanding of how phishing emails can be recognised and who might be most vulnerable to these attacks. This research could help to inform training and policy which might lower the occurrence of phishing attacks as well as increase phishing recognition and reduce victim susceptibility.

Phishing Email Characteristics and Susceptibility

Social persuasion in phishing emails. Successful email-related phishing attacks commonly utilise social persuasion to gain compliance from their recipients. Social Persuasion is the process involved in modifying someone's beliefs, values, attitudes, and behaviour (Simons, 1976). Individuals are exposed to persuasive communication across many different contexts: for example, volunteering agencies may persuade one to volunteer for a good cause, retail companies may persuade one to purchase a particular product, and political parties may persuade one to vote for a specific candidate (Chen et al., 2018; Lawson et al., 2020; Parsons et al., 2019; Pattinson et al., 2016). Within psychology, the most widely accepted classification of social persuasion is Robert Cialdini's six principles of influence: authority, reciprocity, commitment and consistency, social proof, liking and similarity, and scarcity (Cialdini, 2007). These principles have been utilised to influence human decision-making in various contexts such as fund-raising, advertisements, and health information systems (Cialdini, 1993, 2001; Cialdini & Goldstein, 2002; Kaptein, Markopoulos, de Ruyter, & Aarts, 2009).

Likewise, several studies have showcased that successful email-based phishing attacks also utilise persuasive strategies to exploit human psychology in persuading individuals to provide personal and sensitive information (Chen et al., 2018). Specifically, Akbar (2014), Atkins and Huang (2013) and Zielinska et al. (2016) demonstrated that the strategies of authority and scarcity were the most frequently employed strategies in phishing attacks. Whilst, the principles of reciprocity and social proof were the least commonly employed strategies.

It is critical to consider how influential the two most frequent strategies are because phishers are increasingly implementing these strategies in their phishing emails. Yet, individuals' detection rate for phishing emails utilising these common persuasion strategies is still not perfect as they often fail to detect it 30% of the time. It is critical to examine the two less frequent strategies because phishers may begin embedding these uncommon persuasion strategies more frequently, in an effort to increase susceptibility. Hence, examining these common versus uncommon strategies will aid in developing more tailored phishing training programs and campaigns. Accordingly, this will provide better knowledge and understanding regarding these persuasion strategies and how to tackle and mitigate its phishing susceptibility. It is also important to note that there is dearth research examining this relationship and, as such, this is the first study that aims to examine this relationship and provide a basis for future research.

The authority persuasion strategy instils fear, influencing individuals to comply with a request of someone in a position of power such as law enforcement personnel, or government officials (Chen et al., 2018; Lawson et al., 2020; Parsons et al., 2019; Pattinson et al., 2016). This is because social learning encourages people not to question authority. Thus, individuals are somewhat conditioned or may feel obligated to respond in order to avoid negative consequences such as punishment, or losing privileges (Chen et al., 2018). This is evident in the most famous scientific experiments about obedience like the Milgram-Experiments and the Stanford Prison Experiments. These studies illustrated the power of authority and how it may even let us act against our beliefs and ethics. Authority can be readily attained in emails through features like titles, signatures, and logos, presenting an email as more credible, authentic, and trustworthy. In the domain of phishing emails, phishers may impersonate an authoritative entity such as the Australian Federal police requesting to pay a fine to avoid losing the license (Chen et al., 2018; Lawson et al., 2020; Parsons et al., 2019; Pattinson et al., 2016).

The scarcity persuasion strategy is based on reactance, that is, individuals respond to a valued object, experience, or opportunity when its availability is limited (Frauenstein & Flowerday, 2020). This amplifies an individual’s desire for that object or opportunity because they do not want to miss out on it. Phishers introduce a feeling of pressure through making calls for urgent action. In the phishing domain, a phisher may craft an email where they provide a limited amount of time such as "24 hours to respond before your account will be blocked" emphasising an urgency. This in turn, makes the recipient respond quickly to the request in a worry of the suspension of their account.

The reciprocity persuasion strategy is based on the idea that individuals feel obliged to repay an act of kindness or favour (Chen et al., 2018). This is an effective persuasion strategy because it fosters trust between relationships providing a way to exchange services. The pressure of obligation is at times so great that, to get rid of it, an individual will give back a greater favour than he or she received before. In phishing, a phisher may send an email of a Woolworths voucher, and ask an individual to come and shop at Woolworths (Jones, Towse, Race, & Harrison, 2019).

The social proof persuasion strategy involves social validation and consensus that, people are more likely to respond to a request if they observe that others have also complied with the request (Chen et al., 2018). This can be leveraged through claiming endorsements from groups such as peer groups. The behaviours of others assist an individual in determining the risk of performing a behaviour under uncertainty. The effect of conformity is indicated in the Solomon Ache (1950), "Elevator Experiment" and the "Line Test". It demonstrated that individuals blindly followed the majority of the group (such as to face the wrong way in an elevator) even when the response was incorrect. In a phishing context, an individual may respond to a survey if notified that others have already undertaken this action (Jones et al., 2019).

Persuasion strategy prevalence. Numerous studies have directly manipulated how individuals' susceptibility is affected by the social persuasion strategies in phishing emails. A novel, online study by Parsons et al. (2019), found that different persuasion strategies had different effects on the likelihood of the participants clicking on either a genuine or a phishing email. Participants were more likely to identify phishing emails that used the scarcity and authority strategies compared to other strategies. This finding is supported by findings by Butavicius et al. (2015), where emails that incorporated scarcity and authority persuasion strategies were far less likely to be considered safe compared to no-principle strategies. Parsons et al. (2019) also indicated that participants were least likely to identify a phishing email when it contained the reciprocity strategy (Parsons et al., 2019). In contrast, another study by Wright et al. (2014), found that participants were most susceptible to the social proof strategy.

These differences in susceptibility can be explained through the inoculation theory (McGuire, 1961). William J. McGuire's theory of inoculation is a theory of resistance against persuasive influence, based on a biological metaphor. McGuire (1961) argues that attitudes of individuals become inoculated against persuasive attacks (McGuire, 1961). This can be achieved through repeated exposure by learning from a threat, or trial and error, in much the same way that one's immune system can be inoculated against viral attacks (Compton, Jackson, & Dimmock, 2016). This theory has been applied in numerous fields such as marketing and advertising, alcohol, and smoking prevention as well as public relations. In the context of phishing, the use of the persuasion strategies of scarcity and authority has increased over time, becoming more common (Zielinska et al., 2016). This means that people have likely been exposed to phishing emails with appeals to urgent and authoritative actions. This could have occurred through experience by likely being a victim, maybe from education approaches, or even through simulation, and phishing related gaming with damaging effects. Henceforth, they may have little difficulty recognising and resisting these persuasion strategies (Parsons et al., 2019; Taib et al., 2019). On the other hand, participants in the studies of Parson et al. (2019) and Wright et al. (2014) may have detected the reciprocity and social proof strategies less likely because these principles are less common in phishing emails. Therefore, people may not have been exposed to phishing emails containing these persuasion strategies enough to develop immunity.

Hypothesis 1**:** Participants will be more likely to detect phishing emails that utilise the more commonly used persuasion strategies (authority, scarcity), compared to emails that utilise the less commonly used persuasion strategies (social proof, reciprocity).

Exposure time. According to the Radicati Marketing Research report between 2015-2019, based on the worldwide IT use databases, surveys, and the vendor information of sales, individuals receive an average of 121 emails per day (Radicati Group, 2015). Due to the lack of time in everyday life, individuals do not always have the time to properly appraise each email. As such, the improper appraisal of emails can potentially result in missing out on detecting phishing features, such as questionable URL links, sender addresses, and spelling and grammatical errors. Studies have depicted that participants under time pressure (versus without such time pressure) made fewer correct decisions regarding phishing emails as they missed detecting phishing features (Chen et al., 2018). Hence, exploring the effects of exposure time given to participants to read and respond to emails and its effect on phishing detection is an important question to address experimentally. This can lead to the creation of more tailored videos, readings, and seminars to educate individuals concerning the dangers associated with impulsively responding to phishing emails. For example, a platform called PishGuru incorporates interactive anti-phishing training materials in the form of comic strips which provides questions along the way for the participants to answer (Kumaraguru, Sheng, Acquisti, & Cranor, 2008).

Hypothesis 2: Participants will be more likely to detect a phishing email when given a longer time to examine an email, compared to a shorter time to examine an email.

Exposure time and social persuasion strategies. Phishing emails introduces a component of time pressure in their requests by providing limited time to respond. Under such time constraints, recognising persuasion strategies is likely to be important in assisting to detect an attempted phish (Wright et al. 2010). Additionally, under time pressure it is likely to be easier to detect the common persuasion strategies compared to the uncommon strategies due to inoculation theory (McGuire, 1961). According to the inoculation theory, due to the increased use of common persuasion strategies in phishing emails and through repeated exposure, individuals may have developed resistance against these strategies relative to the uncommon persuasion strategies.

This notion can be further explained through the use of Dual-Process Theory (Chowdhury, Adam, & Skinner, 2019; Harrison, Svetieva, & Vishwanath, 2016a, 2016b; Klein, 2016; Xu & Zhang, 2012; Zhang, Burd, Luo, & Seazzu, 2012). This approach posits that there are two systems of processing information: system 1 and system 2. System 1 processing is often described as intuitive, fast, effortless, or pattern recognition, triggering an automated mode of thinking. It channels the available information based on prior-similar situations (Jones et al., 2019). In routine and familiar situations, individuals may effectively utilise system 1 processing to decrease the gathering of too much information, reducing their cognitive load whilst still sustaining optimal decision outcomes (Chen et al., 2018). For example, while driving, an individual may automatically begin to slow down to a stationary position when they see the traffic lights turning yellow. In the context of phishing, it can be implied that due to the increased utilisation and repeated exposure to authoritative and urgent phishing emails, individuals may have become familiar with these common persuasion strategies. This alternatively allows for the quick and fast recognition of phishing emails containing these principles under a tight time constraint.

In contrast to system 1, system 2 processing is characterised as a more analytical, deliberate logical, and rational side to the thinking process (Jones et al., 2019). It is dependent on careful and deliberate processing through a conscious application of rules, making it a much slower and cognitively demanding process (Chen et al., 2018). The analytical system is engaged usually when there are uncertainty and complexity, needing time to avoid errors (Jones et al., 2019). Thus, it can be deduced that as individuals have not been exposed to, and rather, lack the knowledge regarding the uncommon strategies (complex and uncertain task). Subsequently, they would need to utilise a more system 2 type processing to slowly deliberate and analyse the phishing emails to identify it as an attempted phish. Even more, with a slower System 2 processing approach, participants may not be able to accurately classify emails when under the tight time constraints. Therefore, it can be deduced that performance is likely to be particularly poor for uncommon strategies when individuals have more or less time to appraise an email.

Hypothesis 3: In both longer and shorter exposure-time conditions, participants will be better able to identify phishing emails with common persuasion strategies, compared to phishing emails with uncommon persuasion strategies. However, this effect will be greater in the shorter exposure condition compared to longer exposure conditions.

The number of phishing features in phishing emails. The importance of cues in decision making has been well established in other domains including fire-fighting (Klein, 1998), in-flight weather-related decision making (Stokes, Kemper, & Marsh, 1992), and chess (DeGroot, 1966). A feature is derived from the availability of a repertoire of cues in the long-term memory that can be triggered in response to a specific stimulus. A cue is a learned, feature-event association that has been established through repeated association in the past, guiding individuals in employing the most appropriate response (Gaba, Howard, & Small, 1995). For example, for an individual who is not tech-savvy and does not frequently utilise emails to communicate, a phishing feature (such as an illegitimate URL) will not be meaningful. This is because it will not trigger any feature-event suspicions regarding the phishing email, leading to not being able to identify it as an attempted phish. Comparatively, a tech-savvy individual may have frequently come across several phishing emails with specific phishing features. In this instance, they likely to have learned a feature-event association (cues). This will allow them to cognitively process and attain the phishing features from long-term memory. It will then trigger an association (suspicions) regarding the phishing email, leading to employing the appropriate response of identifying an email as a potential phish. The capacity for features (an aspect of cues) guiding the decision-making process is particularly evident among experienced decision-makers such as expert fingerprint examiners, and chess players (Robson, Searston, & Edmond, 2020).

Features in the context of phishing emails are any suspicious or distinctive characteristics of an email that gives away the fact that it is a phish (after the development of a feature-event association). For example, an authority email containing several spelling errors will create a higher level of suspicion that the email is a potential phish because it reduces authenticity (Muniandy & Muniandy, 2013). Researchers have identified common features inherent in phishing emails that recipients associate with for phishing emails (Parsons et al., 2015; Zielinska, Welk, Mayhorn & Murphy-Hil, 2016). These include spelling and grammatical errors, a sender’s address that does not match the expected domain name, and questionable URL links. These features arouse suspicions \ because it goes against traditional norms and ruins the credibility of the source (Chen et al., 2018). For example, Vishwanath et al. (2011) portray that the URL conveys more information regarding the page to which a link points to, which engenders trust. For instance, if the link does not contain some element regarding the intended page and has unusual texts and numbers embedded, the trust based on that URL would be unfounded. In like manner, unusual sender addresses and spelling mistakes lose professional tone because the reader cannot relate to the message (Blythe, Petrie, & Clarke 2011; Kim & Kim, 2013). With all that, it can be implied that a greater number of phishing features should provide more evidence and aid in the identification that an email is a phish and increase the likelihood of detection.

Currently, there is a lack of research in phishing that has examined the variable of the number of features on phishing susceptibility. However, one study that does exist, illustrates support to this contention that more phishing features equal better detection. Zielinska et al. (2014) recruited ninety-six participants from Amazon Mechanical Turk (MTurk) to partake in an email management task that assessed participants' phishing susceptibility. Participants were presented with numerous emails containing one or more phishing features. After viewing, the participants had to determine if the email was a legitimate or a phishing email. Results reflected the notion that when emails contained three phishing features (fake URL, bad grammar, and a warning), 83% of the participants correctly identified emails as a phish. Conversely, when there was one phishing feature (fake URL), only 30% of individuals detected it as a phish (Jones et al., 2019). Exploring and attaining a greater understanding of features could be used to aid in the development of cue-based training. Cue-based training programs would be a highly cost-effective means of improving human performance in the organisational settings, specifically for phishing to reduce phishing susceptibility.

Hypothesis 4: Participants will be more likely to identify phishing emails when they contain a greater number of phishing features compared to a lesser number of phishing features.

The Current Study

The current study aims to examine the influence of persuasion strategies, the number of phishing features, and exposure time on the detection of phishing emails. In line with the method used in Parsons et al. (2019), the detection of phishing emails was measured based on the performance in an email sorting task. This task required participants to appraise and sort a series of incoming emails from the inbox of a fictitious University of Adelaide Professor named “Alex Jones”. Each email was designed using the direct manipulation of one of Cialdini's (2007) four social persuasion strategies these were social proof, scarcity, authority, and reciprocity. At the same time, few emails were also designed to contain no persuasion strategies. Emails were systematically manipulated to contain either one phishing feature (illegitimate URL) or three phishing features (spelling errors, illegitimate URL, and illegitimate sender's email address). Half of the participants were given seven seconds to appraise each email while the other half were given fifteen seconds to appraise each email.

Method

Participants

One hundred and thirty-six participants completed this study. The majority of the participants were female (73.6%), and they ranged in age between 17 and 54 years old (*M* = 22.78, *SD* = 7.97). Thirty-four participants were recruited from the general public using snowball and convenience sampling via advertising on social media. As well, one hundred and two first-year psychology students from the University of Adelaide were recruited using the SONA System, the University's online participant pool. In exchange for their participation, participants from the general public could elect to go into a prize-draw to win one of five of the $20 Coles/Myer gift cards, whereas the first-year psychology students received course credit. Participants were required to be fluent in English to participate. The data from 58 participants were excluded due to incomplete responses. Participants reported spending a minimum of zero mins to 360 mins (six hours) every day on the computer, with an average of five hours 45 mins (*SD* = 2.75). The sample of participants also reported that they received a minimum of three emails to a maximum of 150 emails per day, with an average of 16 emails per day (*SD* = 21.56).

Design

The study comprised a 2 (Email Type: Phishing, Genuine) x 5 (Persuasion Strategy: Authority, Scarcity, Reciprocity, Social Proof, No Technique) x 3 (Phishing Features: Zero, One, Three) x 2 (Email Exposure Time: Shorter, Longer) unbalanced factorial mixed design. Here, the email type, the persuasion strategies, and the phishing features were within-group factors, whilst the email exposure time was the between-groups factor. The dependent variable was the phishing detection rate.

Participants in each email exposure time condition were shown 60 emails (40 genuine emails, and 20 phishing emails) in the same order. The emails were manipulated by being classed as either phishing or genuine emails by embedding a varying number (zero, one, three) of phishing features (URL, Spelling and grammatical errors, and sender's address). The genuine and phishing emails were also manipulated to contain one of the five persuasion strategies, authority, scarcity, reciprocity, social proof, and no strategy. The email exposure variable is referred to the length of time participants had to view each email before categorising the email.

Measures

Demographic questionnaire. Participants completed a series of demographic questions regarding their age, gender, time spent using a computer per day, confidence with computer use, and the number of emails received per day.

Email exposure time. The participants were randomly allocated into the shorter email exposure time (seven seconds) or the longer email exposure time (15 seconds) condition. The exposure time is referred to the length of time an individual viewed an email before categorising the email. There is scarce research regarding the amount of time individuals take to view an email. One analysis was found by Litmus Email Analytics, which indicated that the average time spent reading an email has increased over the years by nearly 7% to 11.1 seconds between 2011 and 2016 (White, 2017). This report provided information about the potential time frames to use (7s and 15s) and hence, a pilot study (described below) was conducted to validate the exposure-times of this study.

Email stimuli. There were 60 emails used in this task. To create the email stimuli, the researchers sourced genuine emails that they had received in their email inboxes. Emails were also selected on the basis in which they were thought to reflect each of the five persuasion strategies (social proof, authority, reciprocity, scarcity and no strategy). The emails were also required to contain 100 words or less, as this ensured that participants had the same amount of time to read and appraise each email. For example, emails from government agencies, such as the Australian Federal Police or the Australian Taxation Office, were selected by the researchers as containing the authority strategy. Similarly, emails from organisations such as Footlocker and, Woolworths asking readers to redeem a voucher were thought to contain the reciprocity strategy. A pilot study was undertaken to confirm that the persuasion strategies thought to be embedded in each email, were perceived as such by a larger sample (see the pilot study for more details). A total of 60 emails were created, with 20 phishing and 40 genuine emails. A greater number of genuine email stimuli compared to phishing email stimuli were used in an effort to reflect real-world email correspondence (Parsons et al., 2019).

Out of the 60 emails, 20 were turned into phishing emails by embedding the three most typically found phishing features in phishing emails: spelling and grammatical errors, sender address, and URL. The number of features was manipulated as follows; all the URL links were actual URLs obtained from previous verified phishing emails. During the email sorting task, participants could hover over the button to see the URL. The sender addresses were also attainted from previous verified phishing emails. The spelling and grammatical errors were manipulated such that there was one homonym-spelling error such as “we advice you” instead of “we advise you” and one grammatical error such as double full stops. This ensured that the obviousness of the mistakes was balanced in each phishing email (Chen et al., 2018). These two spelling errors were always in the first two lines of the emails after the greeting, so that the participants in the shorter exposure time had time to read and evaluate the mistakes in each email. Out of the 20 emails, fifteen phishing emails contained one of these phishing features (e.g. spelling errors), while five of the emails contained three of these phishing features (Spelling and grammatical errors, URL, and sender address). Conversely, 40 of the genuine emails contained no phishing cues and were left unchanged. Besides these manipulations, both phishing and genuine emails were standardized, with recipient details, greeting, and the subject font being kept constant to avoid the effects of extraneous variables. Even more so, all the personal details within each email were modified to “Alex Jones”. Participants were instructed that all emails were taken from the inbox of ‘Alex Jones’ and to assume that they were deliberately sent and of relevance to them. Refer to Figure 1 below to see two examples of the email stimuli utilised in the study incorporating social persuasion strategies, varying number of features and being viewed for shorter and longer email exposure time.

Email sorting task. The online survey platform, Qualtrics[1] was used to deliver this email sorting task. During the task, the participants were randomly allocated by the Qualtrics platform, into

[1] This study was originally planned to be conducted in a lab-based setting. However, due to COVID-19, it was adapted to be an online survey-study. One of the benefits of an online survey-study is that it is convenient for the participants to complete at their own pace, time, and preferences, which can increase response rates. It also allows researchers to reach a wider audience by sharing it on the social media platform, and it reduces administration costs and effort (Evans & Mathur, 2005). Most

either the short 7s email exposure time-condition or the long 15s exposure time-condition. Then they were told to imagine that they were the assistant to Professor "Alex Jones". As part of their role, participants were asked to evaluate and sort a series of 60 pre-designed emails (plus one practice email) into classifications. They were asked to assume that they were deliberately sent and of relevance to Alex Jones, as all the personal details within each email were modified to "Alex Jones". Depending on the email exposure time-condition, some participants were presented with each email for seven seconds or 15 seconds. The countdown timer was available on top of the email, so they knew how much time they had left to appraise the email. After the time elapsed, they were presented with a new page and asked to sort the emails into the following list of categories: “Urgent (emails, personal or work-related, that Alex needs to respond to within the next 24-48 hours)”, “Teaching (emails from colleagues regarding the coordination of university courses)”, “Research (emails regarding Alex’s research and research opportunities)”, “Banking (Alex’s personal banking)”, “Online purchases (receipts from purchases Alex has made)”, “Social Media accounts (notifications from Alex’s social media accounts)”, “Official (personal emails from official agencies e.g. Medicare, ATO, AFP)”, “Spam (advertisement emails of no consequence)”, “Phishing (emails that seem fraudulent or malicious)”, “Miscellaneous (emails that don’t fit into any other category)”. There were several categories to disguise the fact that this was a phishing study (see below for more information). The categories were presented in each email-question; hence participants were not required to memorise it.

In this study, the participants were not informed that they were electing to participate in a phishing study. It was conducted in this manner to minimise the effect of subject expectancy. Previous research has showcased that an awareness of partaking in a phishing study leads to more suspicions and bias towards making phishing-based decisions. As such, it results in better performance in identifying phishing emails (Chen, Mishler, Hu, Li, & Proctor, 2018; Downs et al.,

importantly, an online-based study reduces the effect of researcher bias and allows respondents to answer more comfortably, honestly, and objectively (Evans & Mathur, 2005).

2007; Parsons, Butavicius, Delfabbro, & Lillie, 2019; Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2015; Pattinson, Butavicius, Parsons, & Mccormac, 2016). The University of Adelaide's Human Research Ethics Board granted ethical approval for such a lack of disclosure (ref no: 20/39).

Procedure

All participants were provided with a participation information sheet and were required to complete a checkbox to provide voluntary consent and access the survey. Participants responded to a series of demographic questions and were then randomly allocated into either the 'shorter email exposure time' condition or 'longer email exposure time' condition. The participants completed the email sorting task as described above. Participants took on average 30 minutes to complete the study in the shorter email exposure condition and 45 minutes in the longer email exposure time condition.

Pilot study. The pilot study was conducted in two-parts aiming to validate the email exposure times (part 1) and whether the persuasion strategies embedded in the 60 emails were perceived as such by participants in the email sorting task (part 2). There were nineteen, first-year psychology participants from the University of Adelaide (4 males, 14 females, 1 other), aged between 16 and 28 years old (*M* = 19.05, *SD* = 2.50). They were recruited using the SONA Systems and were granted course credit for their time. First-year psychology students who partook in the pilot study were not allowed to participate in the main study. One participant was excluded because of incomplete responses.

In the first part of the study, participants completed a series of demographic questions including age, gender, hours of computer use. They then viewed the same 60 emails utilised in the main study and sorted them into categories. The email stimuli were divided into 20 sets (three emails in each set) and differed in the amount of time participants had to read each email; the times were 3 seconds, 7 seconds, 9 seconds 15 seconds. This took about 40 minutes to complete. As with the main study, the participants in the pilot study were not informed not explicitly told they would be responding to phishing emails.

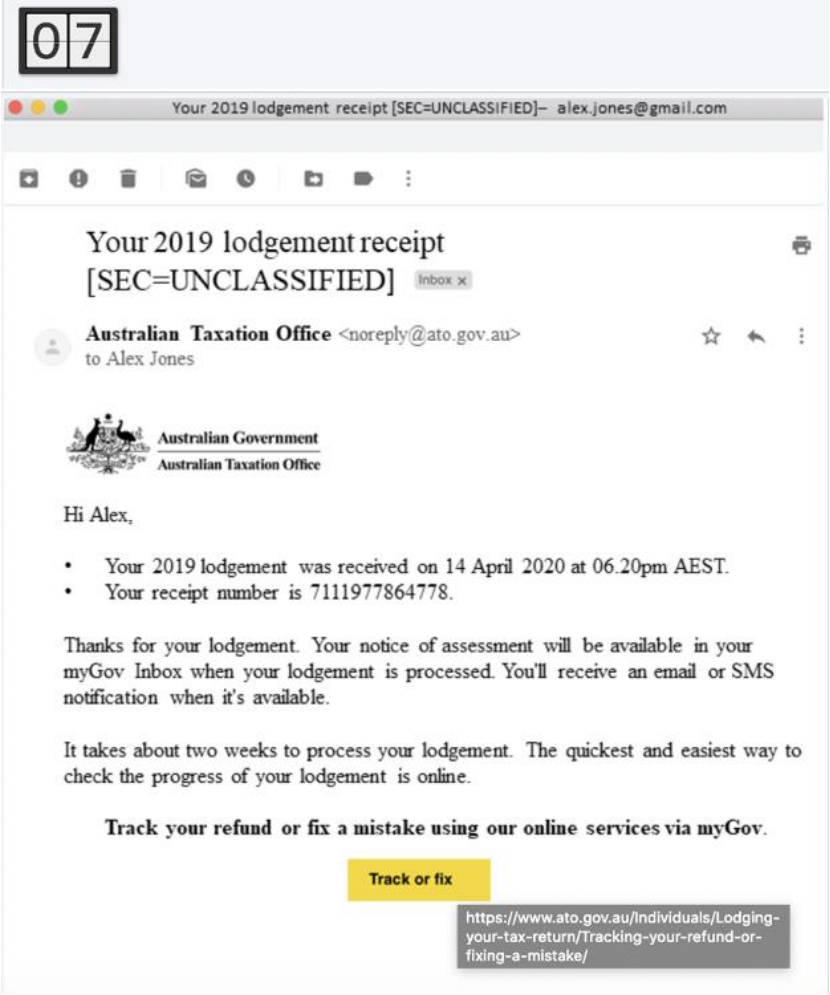
In the second part of the study, participants were shown the same email stimuli without any time constraints and were given the definitions for each of the four social persuasion strategies. They were also given a “no-principle” option, which is an email that does not utilise any of Cialdini’s strategies. The participants were informed that they were not required to memorise the definitions. This is because the definitions were presented at the bottom of each email for their convenience. They were instructed to read the descriptions, and when they felt confident in their understanding, viewed the 60 emails in random order. Then, they had to rank up to three strategies that they thought were *most* present in each email (refer to Figure 2).

The results of the pilot study indicated that seven seconds was best for the shorter email exposure time and 15 seconds was best for the longer exposure time. It also revealed that for 19 of the 20 phishing emails the principle that was *most* frequently selected to be *most* present matched the intended principle across three ranked choices. For example, for the four phishing emails that were manipulated to contain the ‘reciprocity' strategy, 'reciprocity' was ranked as the most present strategy by 89% of participants across three ranked choices: see the full table of results in Appendix B. It was noted that for the ‘no strategy’ phishing emails, the cumulative totals of the intended ‘no principle’ strategy, obtained lower rankings across the three choices (only 64% of the participants) in comparison to the other strategies. This was not of concern as it was assumed that for the ‘no strategy” technique, participants were primed to look for persuasion strategies. These results provided sufficient evidence to validate 7 seconds and 15 seconds for the exposure time conditions. It also provided sufficient evidence suggesting that the emails that were manipulated to emulate a specific social persuasion strategy were in fact perceived in line with their intended strategies.

Results

Overview of Analyses

To analyse H1, H2, and H3, a series of Analysis of Variance (ANOVA) tests were run. For



Your 2019 lodgement receipt [SEC=UNCLASSIFIED]– alex.jones@gmail.com

Your 2019 lodgement receipt [SEC=UNCLASSIFIED] Inbox ×

Australian Taxation Office <noreply@ato.gov.au>
to Alex Jones

Australian Government
Australian Taxation Office

Hi Alex,

- Your 2019 lodgement was received on 14 April 2020 at 06.20pm AEST.
- Your receipt number is 7111977864778.

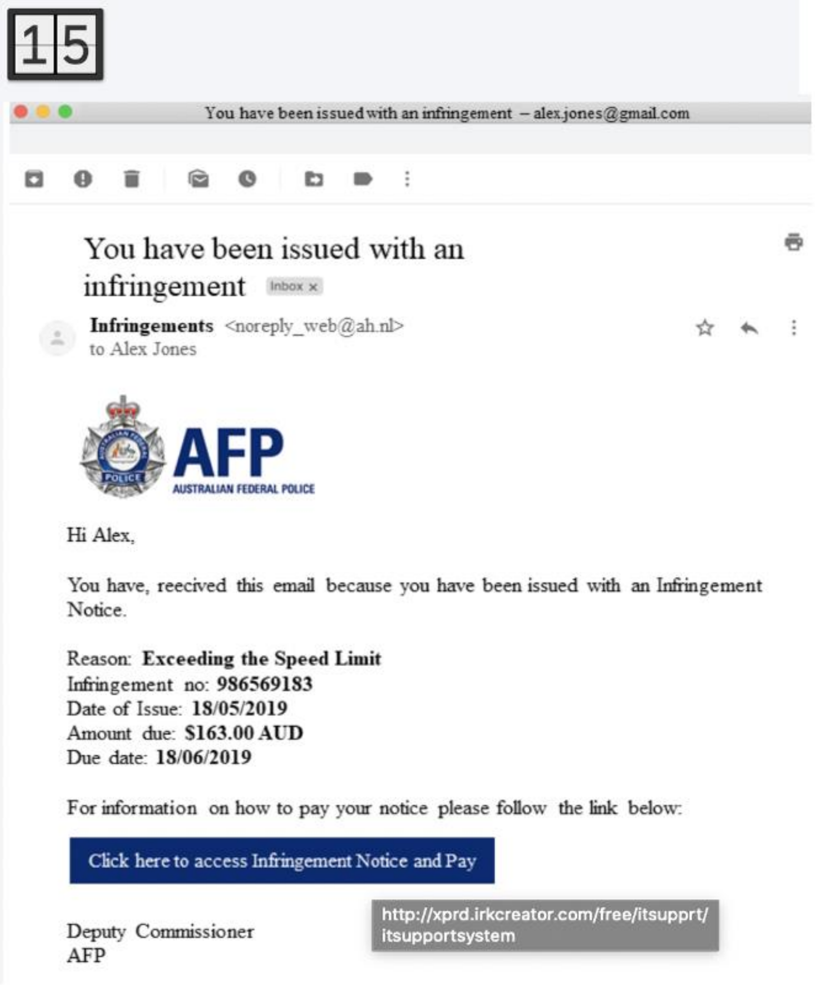
Thanks for your lodgement. Your notice of assessment will be available in your myGov Inbox when your lodgement is processed. You'll receive an email or SMS notification when it's available.

It takes about two weeks to process your lodgement. The quickest and easiest way to check the progress of your lodgement is online.

Track your refund or fix a mistake using our online services via myGov.

Track or fix

https://www.ato.gov.au/Individuals/Lodging-your-tax-return/Tracking-your-refund-or-fixing-a-mistake/



You have been issued with an infringement – alex.jones@gmail.com

You have been issued with an infringement Inbox ×

Infringements <noreply_web@ah.nl>
to Alex Jones

AFP
AUSTRALIAN FEDERAL POLICE

Hi Alex,

You have, reecived this email because you have been issued with an Infringement Notice.

Reason: **Exceeding the Speed Limit**
Infringement no: **986569183**
Date of Issue: **18/05/2019**
Amount due: **$163.00 AUD**
Due date: **18/06/2019**

For information on how to pay your notice please follow the link below:

Click here to access Infringement Notice and Pay

http://xprd.irkcreator.com/free/itsupprt/itsupportsystem

Deputy Commissioner
AFP

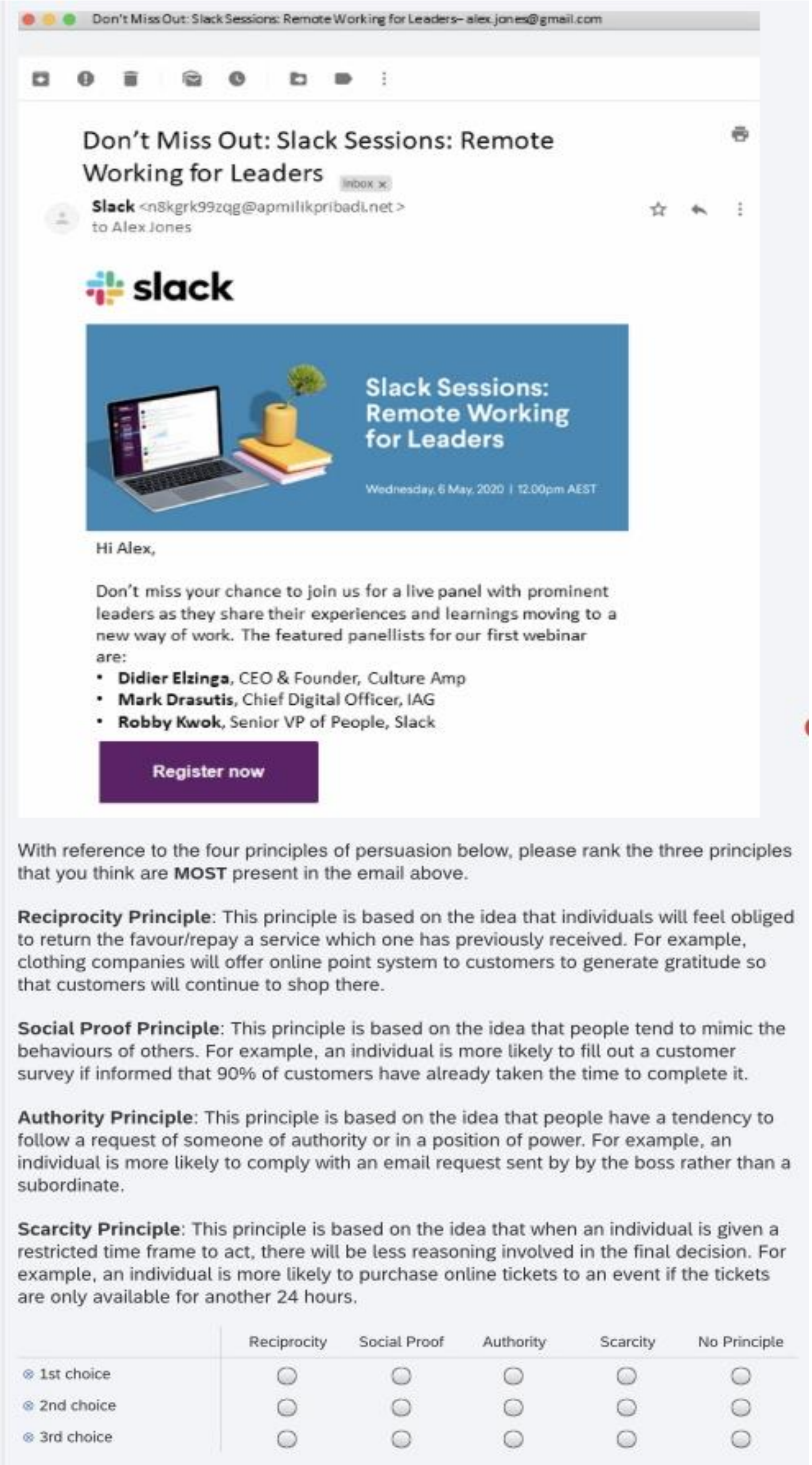
Figure 1. Examples of emails used. Left: A genuine email, using the 'Authority" social persuasion strategy, containing a genuine sender address, and URL with no spelling and grammatical errors. Right: A phishing email, using the 'Authority' persuasion strategy containing three phishing features. There is a suspicious URL (http://xprd.irkcreator.com/free/itsupprt/itsupportsystem), an illegitimate sender address (noreply_web@ah.nl), and spelling and grammatical errors on "reecived" and a comma after "you have,". The emails were presented in both short (7 seconds) and long (15 seconds) Email Exposure Times. It is important to note that participants were able to hover over the emails to view the URL (The above URL is for illustrative purposes only).

H4, a contrast-test was conducted to examine the effects. Data were analysed using IBM Statistical Package for Social Sciences (Version 25).

Data reduction. The data concerning the email management task underwent data reduction. To assess participants' capacity to discriminate phishing emails from genuine emails, the signal detection paradigm was utilised. This paradigm is important because it takes into account both hits and false alarms, compared to other paradigms which only accounts for hits. Hits are defined as the proportion of correctly identified phishing emails. False alarms are defined as the proportion of genuine emails identified as phishing emails. The signal detection framework has been widely accepted by decision-making researchers **in** numerous other contexts including baggage screening (Wolfe, Brunelli, Rubinstein, & Horowitz, 2013), medical decision making (Mohan, Rosengart, Farris, Fischhoff, & Angus, 2012), and phishing detection (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010; Mayhorn & Nyeste, 2012; Welk et al., 2015).

The hit rate and the false alarms were calculated across all the five persuasion strategies (Jones et al., 2019). A discrimination score for each persuasion strategy was obtained by subtracting hit rates from false alarms. For example, if a participant's hit rate for authority emails was 0.75, and their false alarm rate for authority emails was 0, then their discrimination score would be 0.75. The discrimination scores could range from -1 to 1. Given this, it is interpreted such that a greater, positive discrimination score indicate that the participants were better able to discriminate between the phishing and the genuine emails compared to those with lower a discrimination score.

Analysis of persuasion strategies, exposure time, and phishing susceptibility (H1, H2). Hypotheses 1, 2, and 3 were examined using a 2 x 5 (Email Exposure Time [Shorter, Longer] x Persuasion Strategy [Scarcity, Reciprocity, Social Proof, Authority, No Principle]) mixed-design Analysis of Variance (ANOVA) with Email Exposure Time as the between-subjects variable. Discrimination scores comprised the dependent variable. To confirm that the assumption of ANOVAs was met, an examination of the histograms revealed that the dependent variable of



Don't Miss Out: Slack Sessions: Remote Working for Leaders– alex.jones@gmail.com

Don’t Miss Out: Slack Sessions: Remote Working for Leaders

Slack <n8kgrk99zqg@apmilikpribadi.net>
to Alex Jones

slack
Slack Sessions: Remote Working for Leaders
Wednesday, 6 May, 2020 | 12.00pm AEST

Hi Alex,

Don’t miss your chance to join us for a live panel with prominent leaders as they share their experiences and learnings moving to a new way of work. The featured panellists for our first webinar are:

- **Didier Elzinga**, CEO & Founder, Culture Amp
- **Mark Drasutis**, Chief Digital Officer, IAG
- **Robby Kwok**, Senior VP of People, Slack

With reference to the four principles of persuasion below, please rank the three principles that you think are **MOST** present in the email above.

Reciprocity Principle: This principle is based on the idea that individuals will feel obliged to return the favour/repay a service which one has previously received. For example, clothing companies will offer online point system to customers to generate gratitude so that customers will continue to shop there.

Social Proof Principle: This principle is based on the idea that people tend to mimic the behaviours of others. For example, an individual is more likely to fill out a customer survey if informed that 90% of customers have already taken the time to complete it.

Authority Principle: This principle is based on the idea that people have a tendency to follow a request of someone of authority or in a position of power. For example, an individual is more likely to comply with an email request sent by by the boss rather than a subordinate.

Scarcity Principle: This principle is based on the idea that when an individual is given a restricted time frame to act, there will be less reasoning involved in the final decision. For example, an individual is more likely to purchase online tickets to an event if the tickets are only available for another 24 hours.

	Reciprocity	Social Proof	Authority	Scarcity	No Principle
1st choice	○	○	○	○	○
2nd choice	○	○	○	○	○
3rd choice	○	○	○	○	○

Figure 2. The second part of the pilot study. Participants were given definitions of Cialdini’s social persuasion strategies and were required to rank up the three most apparent strategies in each email. Participants were also provided with the “no principle” option.

discrimination was approximately normally distributed for each condition. Additionally, Levine’s test indicated that the assumption of equal variance was met for each of the persuasion strategy.

More so, Mauchly's test statistic showcased that the assumption for sphericity was met for each condition, X^2(9) = 13.50, P = 0.14. Therefore, sphericity-assumed values are reported.

There was a statistically significant main effect of persuasion strategies on discrimination scores *F*(4, 536) = 22.39, *p* < .001, η^2 = .14. This result supports H1 as it proposes that there was a significant difference in the discrimination scores across the different persuasion strategies (*M*=0.11, *SD*=0.17). Given the significant results obtained from the ANOVA, follow-up analyses were conducted yielding notable findings. These analyses revealed the discrimination scores between common persuasion strategies (authority, scarcity) (*M* = 0.21, *SD* = 0.21) and no persuasion strategies (*M* = 0.20, *SD* = 0.24) were similar. In comparison, the analyses also revealed that uncommon persuasion strategies (reciprocity, social proof) were associated with lower discrimination (*M* = 0.09 *SD* = 0.18) compared to no persuasion strategies (*M* = 0.20, *SD* = 0.24). It produced a statistically significant effect, *t(*135) = -5.91, *p* < .001.

There was a statistically significant main effect of email exposure time on discrimination scores *F*(1, 134) = 15.09, *p* < .001, η^2 = .10. This result supports H2, suggesting that participants who were given a longer duration to view each email were better able to discriminate between phishing and genuine emails (*M*=0.21, *SD*=0.02) compared to those who were given a shorter time to view each email (*M*=0.10, *SD*=0.02).

Analysis of the interaction between persuasion strategies, and exposure time (H3). There was a non-significant interaction effect between email exposure time, persuasion strategies and their discrimination scores *F*(4, 536) = 0.73, *p*= 0.57, η^2 = .01. This result indicates a non-support for H3, suggesting that participants' ability to discriminate between phishing and genuine emails incorporating commonly used persuasion strategies was not greater in the shorter email exposure time. Instead, participants' discrimination was similar in both seven seconds, short email-exposure time condition as well as 15 seconds, long exposure- time condition. Refer to Figure 3 showcasing a visual representation of the effect of persuasion strategy (H1), and exposure time (H2) on phishing susceptibility as well as the interaction effect between the varying effectiveness of each persuasion strategies relative to email exposure time (H3).

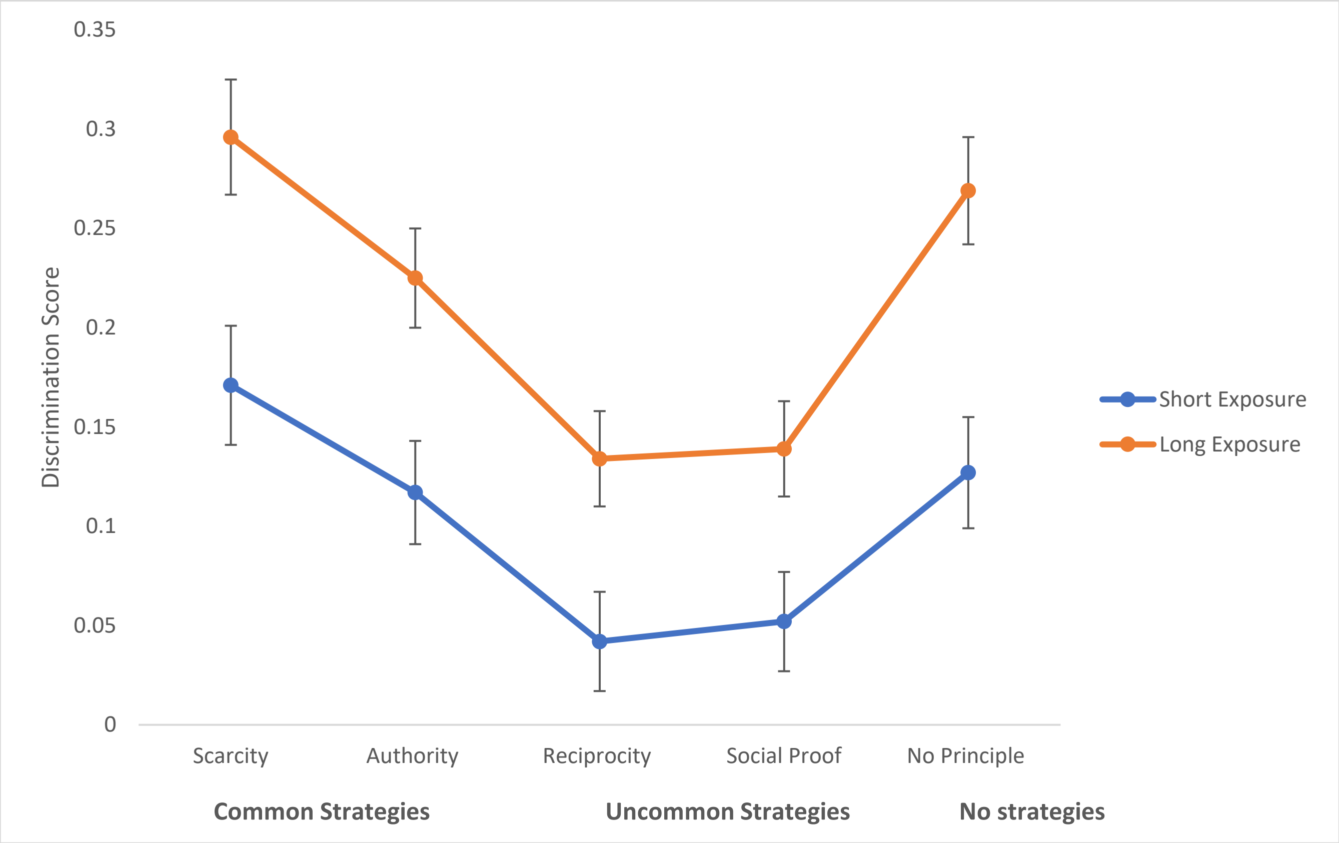


Figure 3. The effects of persuasion strategy and phishing detection rate (H1), exposure time, and phishing detection rate (H2) and interaction between exposure time and persuasion strategies (H3).

Analysis of the number of phishing features and phishing detection rate (H4). To examine H4, a paired samples t-test was conducted comparing the detection rate of emails containing one phishing feature and emails containing three phishing features. Here, the detection rate is being utilised instead of discrimination scores, because the hypothesis is examining phishing features, which are embedded only in phishing emails. Hence, the means of one and three phishing features that are from the same individual, for all the individuals were compared. This was sufficient to examine whether there was a difference between the detection rate of one versus three phishing features. A statistically significant result was evident for this effect $t(135) = -7.24$, $p < .001$. Providing support for H4, this indicates that participants are better at detecting phishing emails when they contain three phishing features (*M*=0.40, *SD*=0.38) compared to one phishing feature (*M* = 0.15, *SD* = 0.14).

Discussion

The purpose of the current study was to investigate whether the characteristics of emails (namely, persuasion strategies, number of features, and email exposure time) affects participants' capacity to discriminate between phishing and genuine emails. Overall, the study highlighted several significant results. It suggests that individuals are more likely to detect phishing emails when they have a greater time to view the email (H2). Individuals are also more likely to detect phishing emails when phishing emails contain common persuasion strategies (authority and scarcity) (H1) and a greater number of phishing features (H4). This provided support for H1, H2, and H4. Additionally, it was noted that participants' ability to detect phishing emails with commonly used persuasion strategies was not greater in short exposure time. Instead during both time conditions (short and long email exposure time) participants were equally better at identifying phishing emails with both commonly used persuasion strategies, and uncommonly used persuasion strategies.

Social persuasion strategies and phishing susceptibility. The outcomes of this study add to the literature and aids in the understanding of phishing email detection, enabling to assist in future training and/or awareness campaigns. It conveys that phishing training programs and campaigns need to tailor their approach to provide more knowledge regarding uncommon persuasion strategies (reciprocity, social proof). These uncommon strategies are possibly unfamiliar to people and hence they might see it as less threatening. Yet, phishers may begin to embed these uncommon persuasion strategies more frequently, to increase susceptibility. For example, in 2018, businesses were targeted by a fake invoice or billing scams. Here, phishers took advantage of a business's existing relationship with a particular service or product asking to update their banking information, which led to the money being paid to the scammer rather than the existing supplier (Australian Competition and

Consumer Commission, 2018). In this example, they are appealing to the reciprocity principle by using previous relations and giving a sense of obligation to pay for a service the recipient had received. Furthermore, the follow-up findings between common persuasion strategies and no persuasion strategies were notable. It proposes that a phisher could utilise no persuasion strategies in their phishing emails and individuals would still be able to discriminate between phishing and genuine emails the same as if phishers utilise common persuasion strategies (authority, scarcity). Also, the follow-up findings between uncommon persuasion strategies and no persuasion strategies reflect that individuals will be better able to detect the difference between phishing and genuine emails if phishers utilised uncommon strategies. A replication study is required to further strengthen and support these findings.

Exposure time and phishing susceptibility. This hypothesis aimed to replicate conditions where individuals view an email quickly and with a lack of attention due to the sheer amount of emails received per day. The findings of this hypothesis suggest that it is important to view an email for a longer period, potentially benefiting in detecting suspicious phishing features. It also highlights that users who view their emails for a short amount of time are more likely to be phished. Therefore, it is necessary to educate participants through interactive awareness campaigns and training programs on the dangers associated with a quick response to phishing emails. One such campaign is “Take Five” (a UK Government campaign encouraging users to stop and think before making decisions around personal data and financial information: https://takefive-stopfraud.org.uk) and the results of the current study support these kinds of campaigns (Jones et al., 2019).

Exposure time and the effectiveness of persuasion strategies. The findings of this interaction hypothesis conveyed that the performance for identifying phishing emails containing common persuasion strategies does not vary across the shorter or longer email exposure time condition. Two possible explanations can account for this incongruent finding. The first explanation could be that the discrimination score was used instead of looking at only hits and only false alarms by itself. This is because, system 1 lends itself to making errors as individuals partake in fast, intuitive, and autonomous thinking. Additionally, in the longer email exposure time-condition, individuals possibly did not use the extra time to make deliberate decisions. This may have affected the hit and false alarm rate such that there were greater false alarms and lesser hit rates. Hence, future research should examine the hits and false alarms separately to analyse this effect. A second explanation could be that, even though inoculation theory and dual-process theory make a logical argument to deduce that the effect of the common persuasion strategies would be greater in a shorter exposure time, other theories or variables such as fatigue, the cognitive load may be at play to explain this effect. So, future studies should continue to investigate inoculation theory and information processing theory further but also examine other variables such as fatigue and cognitive load and its role in phishing susceptibility. This finding also emphasises the need for educating people to utilise a deliberate system 2 processing rather than intuitive system 1 processing. Meaning that individuals should stop and think about responding to or clicking on any email.

The number of phishing features and phishing susceptibility. The findings of this hypothesis are consistent with previous research in other domains such as chess (Stokes, Kemper, & Marsh, 1992) and weather-related decision making (DeGroot, 1966). It reinforces the notion that, in potentially harmful and complex situations (phishing attacks), having more features allows for quick recognition engagement of the appropriate responses. Given, the lack of research on the number of features in the phishing context, this finding provides a basis for future research. Additionally, this finding provides a positive practical implication of aiding in the development of more cue-based training such as weather-wise (see below for more details) (Wiggins & O’Hare, 2003), which could be utilised in phishing to reduce phishing susceptibility.

For weather-related decision making in the aviation environment, Wiggins and O’Hare (2003) introduced a cue-based training program called WeatherWise. This training program demonstrated that utilising numerous features enhances learner-performance in quickly recognising and responding to problems in busy and probabilistic environments such as during deteriorating weather conditions whilst flying (Wiggins & O'Hare, 2003). From an applied point of view, cue-based training programs such as this would be a highly cost-effective means of improving human performance in the organisational settings. This is because it could be utilised individually or within a group setting to provide knowledge regarding phishing features to increase detection. And so, a greater understanding in such an area has the potential to aid in cue-based training which could be utilised in phishing to reduce phishing susceptibility.

In order to develop quality, cue-based training programs, this study opens up a window into examining other cues as well such as legal disclaimers, logos, and greetings. This is because spelling, sender address, and URL are not absolute or infallible. For example, it is common to find poor spelling or grammar in genuine emails, and not all phishing emails contain mistakes. From a practical point of view, this has a devastating effect on both organisations and individuals as it can ruin customer trust as well as lead to an individual missing out on important information.

However, whilst these training and awareness campaigns on phishing emails might help raise the awareness concerning cybersecurity threat, Kumaraguru et al. (2008) highlight that users spend a less amount of time engaging in security-related tutorials and programs. Therefore, future studies regarding phishing susceptibility should look to make the above anti-phishing training programs and campaigns more interactive. For example, individuals could be given immediate feedback, allowing them to learn by trial and error. Training programs and anti-phishing campaigns should also create more platforms like PishGuru, which incorporates anti-phishing training materials in form of comic strips and providing questions along the way for participants to answer (Kumaraguru et. al., 2008). This directs individuals to learn and acquire appropriate responses while mitigating unwanted and consequence-driven behaviour. Besides, since scammers continually improve the sophistication of phishing emails (Arachchilage et al., 2014) it is imperative that any training is regularly updated to reflect current trends.

Strengths of the current study. One of the strengths of the current study is that participants were exposed to a larger number of emails (40 genuine and 20 phishing) from a range of sources and industries such as finance, government officials, and social media platforms. This is beneficial because it overcomes the shortcomings of existing literature in creating and examining email-stimuli based on a narrow subset of industries, lacking generalisability (Parsons, Butavicius, Delfabbro, & Lillie, 2019; Vishwanath, Herath, Chen, Wang, & Rao, 2011; Williams et al., 2018; Zielinska, Welk, Mayhorn, & Murphy-Hill, 2016). Consequently, this provides a more comprehensive assessment of the influence of the email category on people's phishing susceptibility than the previous research. This is also beneficial because it reflects the current trends and findings concerning the fact that phishers are also targeting diverse industries. This may also have implications for the design of future phishing studies and how researchers interpret the results of their study.

Similarly, another strength is that the emails in this study contained both, a greater and a lesser number of phishing features. This is a strength because the existing phishing literature only examines the effect of sophisticated phishing emails containing only one phishing feature, specifically URL, on phishing susceptibility (Bayl-Smith, Sturman, & Wiggins, Cue Utilization, Phishing Feature, and Phishing Email Detection, 2020; Parsons et al., 2019). Hence, varying the number of phishing features allowed valuable investigation into how the level of phishing email sophistication determines its effectiveness and association with phishing susceptibility. Additionally, it also needs to be noted that all the URLs in this study were actual URLs obtained from previous verified phishing emails, aiding in ecological validity.

Furthermore, this study was originally planned to be conducted in a lab-based setting. However, due to COVID-19, it was adapted to be an online survey-study. This presents both benefits and limitations. One of the benefits of an online survey-study is that it is convenient for the participants to complete at their own pace, time, and preferences, which can increase response rates. However, researchers do not have the control over how the individuals’ completed the study, like they have during lab settings (they could have been distracted, lacked attention decreasing the reliability of results). Additionally, an online survey allows researchers to reach a wider audience by sharing it on the social media platform, and it reduces administration costs and effort (Evans & Mathur, 2005).

Limitations and future directions. One of the limitations of the study is that participants may have possessed different levels of familiarity with the types and sources of emails used. The study sample contained several mature and older audiences who may not use platforms such as Spotify, Ezibuy, Twitter, or Slack. This may have caused variations in discrimination ability as older individuals may be unfamiliar with the 'look' of a genuine email from these organisations. Future research could attempt to assess this through a questionnaire. The questionnaire could include items such as asking the individuals about their familiarity with relevant organisations and services before the study. This will enable the creation of a more personalised sample of phishing and genuine emails that both the younger and older individuals could recognise quickly and effectively (Parsons et al., 2019; Vishwanath et al., 2011; Williams et al., 2018.; Zielinska et al., 2016).

Another limitation that needs to be considered is gender-bias. Out of 136 participants, a large proportion of the sample, 74.3% are females. This is beneficial as it provides valuable knowledge regarding discrimination ability among young females who utilise technology more often compared to mature individuals. Nevertheless, this is a limitation as it skews the data and reduces the external validity of the study. This is because the sample is unrepresentative and does not represent all the key interest groups in the population in terms of age, education level, technology, and phishing familiarity. It therefore cannot be generalised to the wider population. Future research should replicate this research study with a more representative sample and an even proportion of genders.

Additional future directions that would assist in understanding this area are to look into taking a mixed-methods approach by aiding quantitative data with qualitative data, establishing a more in-depth insight. Qualitative data could be attained by conducting interviews where individuals can provide feedback after the study. During the interview, researchers could ask questions such as what things an individual specifically paid attention to distinguish between a phish or a genuine email. Additionally, researchers can enquire the participant to describe their own phishing experiences and what sort of messages they have come across in their everyday life. Even more, participants could be encouraged to provide feedback about the specific types of programs, strategies, or ideas that they think are needed in the work field to personalise the experience and improve training programs (Luo, Zhang, Burd, & Seazzu, 2013).

Even more, this study focused specifically on phishing attacks via emails and did not address phishing through other different mediums such as online social media platforms. Future research should investigate specific features utilised in social media (such as greeting, design, and look, language, and personalisation) and see its effects on phishing susceptibility (Frauenstein & Flowerday, 2020; Goel, Williams, & Dincelli, 2017).

Conclusion

The current study aimed to contribute to the phishing literature by examining the email characteristics of persuasion strategies, the number of phishing features, and the amount of time to read an email and its effect on phishing susceptibility. Several significant results were attained. It suggested that individuals are better able to identify phishing emails if they contain common persuasion strategies. Individuals are also more likely to recognise and identify phishing emails if they are given more time to view an email. Furthermore, if phishing emails are obvious and contain several phishing features, it is more likely to be easier to discriminate between the phishing emails out of the genuine emails. Hence, these findings have practical implications on training and awareness programs such that it highlights the need for more tailored training programs where they target uncommon strategies and more sophisticated phishing emails. It also emphasizes the need to educate individuals regarding the dangers associated with impulsive, and autonomous system 1 decision making by teaching them to stop and partake in more deliberative, system 2 processing.

This research also might aid in cue-based programs such as Weatherwise. Importantly, as phishing attacks continue to become more frequent and sophisticated, there is a continued need for future research to examine those most at risk and the strategies that can help improve detection.

References

ACCC. (2019). *Australian Competition & Consumer Commission: Targeting scams: Report of the ACCC on scams activity 2018.* Canberra: accc.gov.au.

Akbar, N. (2014). *essay.utwente.* Retrieved from the University of Twente: https://essay.utwente.nl/66177/1/Akbar_MA_EEMCS.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.

Atkins, B., & Huang, W. (2013). A study of social engineering in online frauds. *Open Journal of Social Sciences*, *1(*3*),* 23-32.

Bayl-Smith, P., Sturman, D., & Wiggins, M. (2020). Cue Utilization, Phishing Feature, and Phishing Email Detection. In J. Bonneau, *Financial Cryptography and Data Security* (pp. 56-70). Malaysia: Springer International Publishing.

Bissell, K., LaSalle, R., & Dal Cin, P. (2019). *The Cost of Cybercrime.* Michigan: Accenture security.

Blythe, M., Petrie, H., & Clarke, F. J. (2011). F for fake: four studies on how we fall for phish. *CHI'11 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 3469-3478). Vancouver BC, Canada: Association for Computing Machinery.

Chen, J., Mishler, S., Hu, B., Li, N., & Proctor, R. W. (2018). The description-experience gap in the effect of warning reliability on user trust and performance in a phishing-detection context. *International Journal of Human-Computer Studies, 119*, 35–47. Retrieved from https://doi.org/10.1016/j.ijhcs.2018.05.010.

Compton, J., Jackson, B., & Dimmock, J. A. (2016). Persuading Others to Avoid Persuasion: Inoculation Theory and Resistant Health Attitudes. *Frontier Psychology, 7(*122*),* 1-9.

DeGroot, A. D. (1966). Perception and memory versus thought: Some old ideas and recent findings. In B. Kleinmuntz, *Problem-solving: Research, method, and theory* (pp. 19-50). New York: Wiley Publications.

Evans, J. S. B. T. (2008). Dual-processing accounts of reasoning, judgment, and social cognition. *Annual Review of Psychology, 59*, 255–278. Retrieved from https://doi.org/10.1146/annurev.psych.59.103006.093629.

Fellner, C. (2019, June 17). *Australian Catholic University staff details stolen in the fresh data breach.* Retrieved from The Sunday Morning Herald: https://www.smh.com.au/national/australian-catholic-university-staff-details-stolen-in-fresh-data-breach-20190617-p51yif.html.

Frauenstein, E. D., & Flowerday, S. (2020). Susceptibility to phishing on social network sites: A personality information processing model. *Computers and Security*, *94*. 1-18. Retrieved from https://doi.org/10.1016/j.cose.2020.101862.

Gaba, D. M., Howard, S. K., & Small, S. D. (1995). Situation awareness in anesthesiology. *Human Factors*, *37(*1*)*, 20-31.

Goel, S., Williams, K., & Dincelli, E. (2017). A I S, Association for Information Systems: Got Phished? Internet Security and Human Vulnerability. *Journal of Associations of Information Systems*, *18(*1*)*, 22–44.

Radicati Group. (2015). *Email Statistics Report, 2015-2019.* California: A Technology Market Research Firm. Retrieved from https://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf

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

Hong, K. W., Kelley, C. M., Tembe, R., Murphy-Hill, E., & Mayhorn, C. B. (2013). Keeping Up With The Joneses. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 57*(1), 1012-1016.

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems, 34*(2*)*, 597-626.

Jones, H. S., Towse, J. N., Race, N., & Harrison, T. (2019). Email fraud: The search for psychological predictors of susceptibility. *PLoS ONE, 14*(1), 1-15. Retrieved from https://doi.org/10.1371/journal.pone.0209684

Kim, D., & Kim, J. H. (2013). Understanding persuasive elements in phishing e-mails: A categorical content and semantic network analysis. *Online Information Review, 37*(6), 835-850.

Klein, G. A. (1998). *Sources of power: How people make decisions.* Cambridge: MIT Press.

Kumaraguru, P., Sheng, S., Acquisti, A., & Cranor, L. (2008). Lessons From a Real-World Evaluation of Anti-Phishing Training. *eCrime Researchers Summit*, 1-15. Atlanta, doi: 10.1109/ECRIME.2008.4696970.

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

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

McGuire, W. J. (1961). Resistance to persuasion conferred by the active and passive prior refutation of the same and alternative counter-arguments. *Journal of Abnormal Social Psychology, 63(2),* 326-332.

Muncaster, P. (2020). *COVID19 Drives Phishing Emails Up 667% in Under a Month.* Retrieved from: InfoSecurity Magazine: https://www.infosecurity-magazine.com/news/covid19-drive-phishing-emails-667/.

Muniandy, L., & Muniandy, B. (2013). Phishing: Educating Internet users – a practical approach using email screenshots. *Journal of Research & Method in Education, 2(*3*),* 33-41.

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. Retrieved from https://doi.org/10.1016/j.ijhcs.2019.02.007.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. *Computers and Securit*y, *52*, 194–206. Retrieved from https://doi.org/10.1016/j.cose.2015.02.008.

Pattinson, M., Butavicius, M., Parsons, K., & Mccormac, A. (2016). Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails Human Aspects of Cyber Security. *The Australasian Conference on Information Systems Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails*, 1-10. Retrieved from https://www.researchgate.net/publication/303812216.

Rehman, I., Mahabadi, N., & Rehman, C. I. (2020). Classical Conditioning. *StatPearls*, 1-5.

Robson, S., Searston, R., & Edmond, G. (2020). An expert-novice comparison of feature choice. *Applied Cognitive Psychology, 34(*5*)* , 1-30.

Ryan, T., Wen Tay, S., Ryan, P., & Anthony Ryan, C. (2016). Canadian Medical Education Journal Major Contribution Systems 1 and 2 thinking processes and cognitive reflection testing in medical students. *Canadian Medical Education Journal, 7*(2*),* 97-103. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5344059/.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, F. L., & Downs, J. (2010). Who Falls for Phish? A demographic analysis of phishing susceptibility and effectiveness of Interventions.

Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1, 373-382. Atlanta.

Simons, H. W. (1976). *Persuasion: Understanding, Practice, and Analysis.* Addison-Wesley Publication Cooperation.

Stokes, A. F., Kemper, K. L., & Marsh, R. (1992). *Time-stressed decision making: A study of expert and novice aviators.* Illinois: Aviation Research Laboratory, Institute of Aviation, University of Illinois.

Sturman, D., Wiggins, M. W., & Helton, W. S. (2019). Cue utilisation predicts control room operators' performance in a sustained visual search task. *Journal Ergonomics, 63(*1*),* 48-60.

Taib, R. (2019). Social Engineering and Organisational dependencies. In D. Lamas, *Human-Computer Interaction – INTERACT 2019: 17th IFIP TC 13 International Conference, Paphos, Cyprus, September 2–6, 2019, Proceedings, Part I* (pp. 565-583). Cyprus: Spring Nature.

Verizon. (2019). *2019 Data investigations Report*. Retrieved from Verizon- business ready: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support System*s, *51*(3), 576–586. Retrieved from https://doi.org/10.1016/j.dss.2011.03.002.

Welk, A. K., Hong, K. W., Zielinska, O. A., Tembe, R., Murphy-Hill, E., & Mayhorn, C. B. (2015). Will the "Phisher-men" reel you in? assessing individual differences in a phishing detection task. *International Journal of Cyber Behavior, Psychology, and Learning*, *5(*4*),* 1–17. Retrieved from https://doi.org/10.4018/IJCBPL.2015100101.

White, C. (2017, March 28). *Email Attention Spans Are Growing!* Retrieved from SalesForce.com: https://www.salesforce.com/blog/2017/03/email-attention-spans-are-growing.html#:~:text=The%20average%20time%20spent%20reading,emails%20using%20Litmus%20Email%20Analytics.

Wiggins, M., & O’Hare, D. (2003). Weatherwise: Evaluation of a cue-based training approach for the recognition of deteriorating weather conditions during flight. *Human Factors, 45(*2*),* 337–345. Retrieved from https://doi.org/10.1518/hfes.45.2.337.27246.

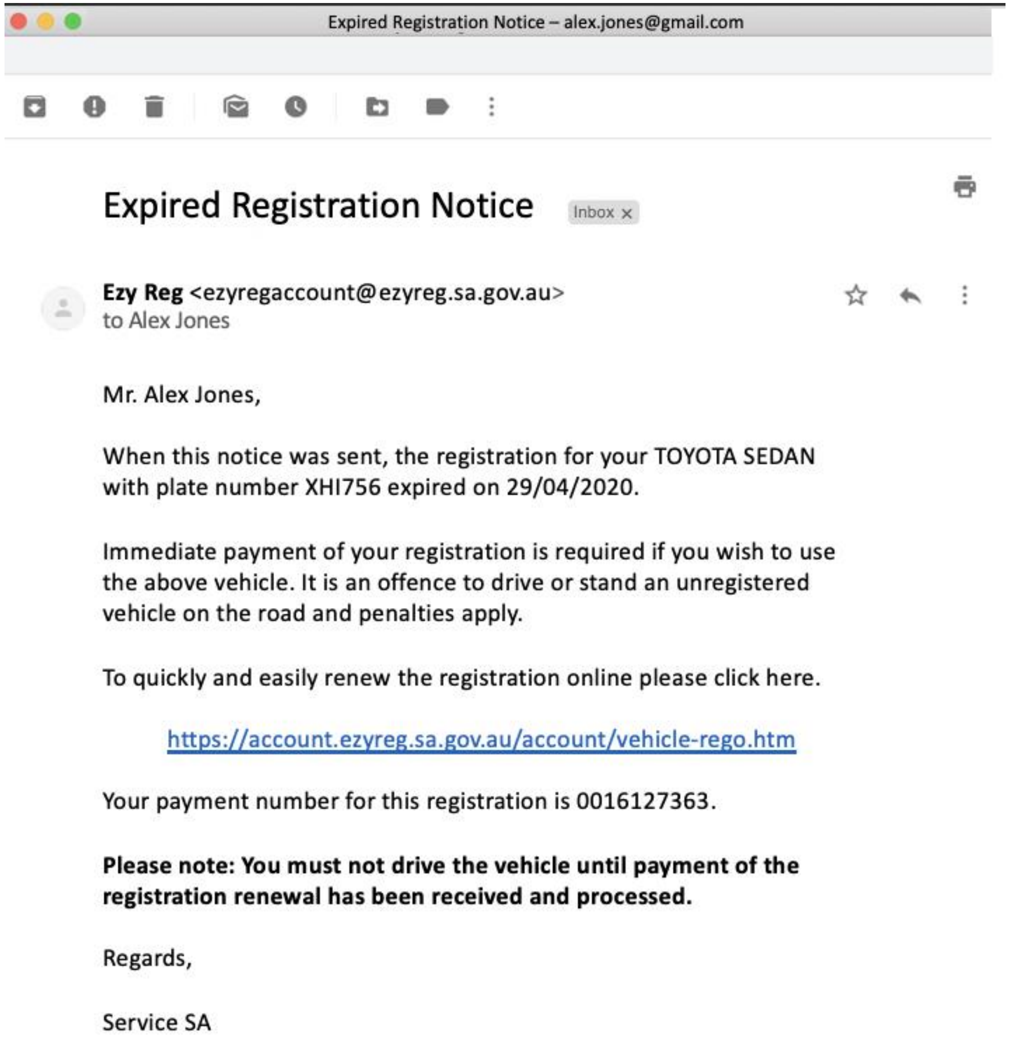
Williams, E. J., Hinds, J. & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies. 120*, 1–13. Retrieved from https://doi.org/10.1060/j.ijhcs.2018.06.004.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Influence techniques in phishing attacks: An examination of vulnerability and resistance. *Information Systems Research, 25(*2*)*, 385–400. Retrieved from https://doi.org/10.1287/isre.2014.0522.

Zielinska, O. A., Tembe, R., Hong, K. W., Ge, X., Murphy-Hill, E., & Mayhorn, C. B. (2014). One phish, two phish, how to avoid the internet phish: Analysis of training strategies to detect phishing emails. In *Proceedings of the Human Factors and Ergonomics Society, 58,* (pp. 1466–1470). Human Factors and Ergonomics Society Inc. Retrieved from https://doi.org/10.1177/1541931214581306.

Appendix A: Examples of Email Stimuli.

Scarcity (genuine) Email and Scarcity (phishing) Email containing Three Phishing Features (URL, Spelling and Grammatical Errors, Sender Address).



Expired Registration Notice

Ezy Reg <ezyregaccount@ezyreg.sa.gov.au>
to Alex Jones

Mr. Alex Jones,

When this notice was sent, the registration for your TOYOTA SEDAN with plate number XHI756 expired on 29/04/2020.

Immediate payment of your registration is required if you wish to use the above vehicle. It is an offence to drive or stand an unregistered vehicle on the road and penalties apply.

To quickly and easily renew the registration online please click here.

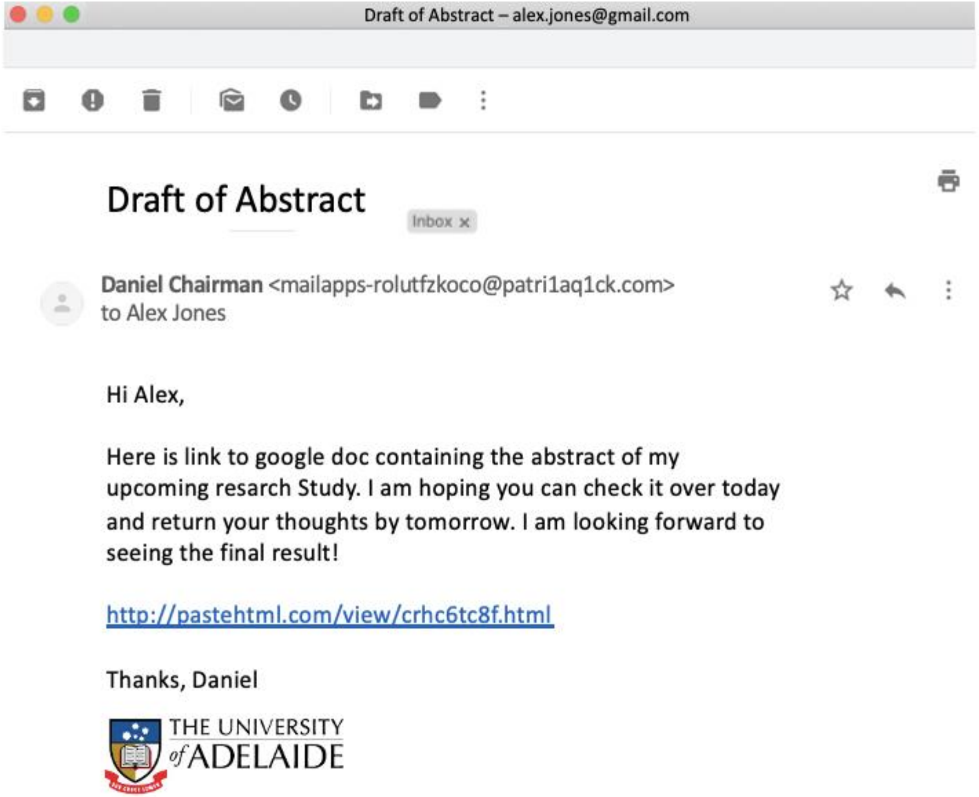
https://account.ezyreg.sa.gov.au/account/vehicle-rego.htm

Your payment number for this registration is 0016127363.

Please note: You must not drive the vehicle until payment of the registration renewal has been received and processed.

Regards,

Service SA


Draft of Abstract – alex.jones@gmail.com
Inbox ×
THE UNIVERSITY of ADELAIDE

Draft of Abstract

Daniel Chairman <mailapps-rolutfzkoco@patri1aq1ck.com>
to Alex Jones

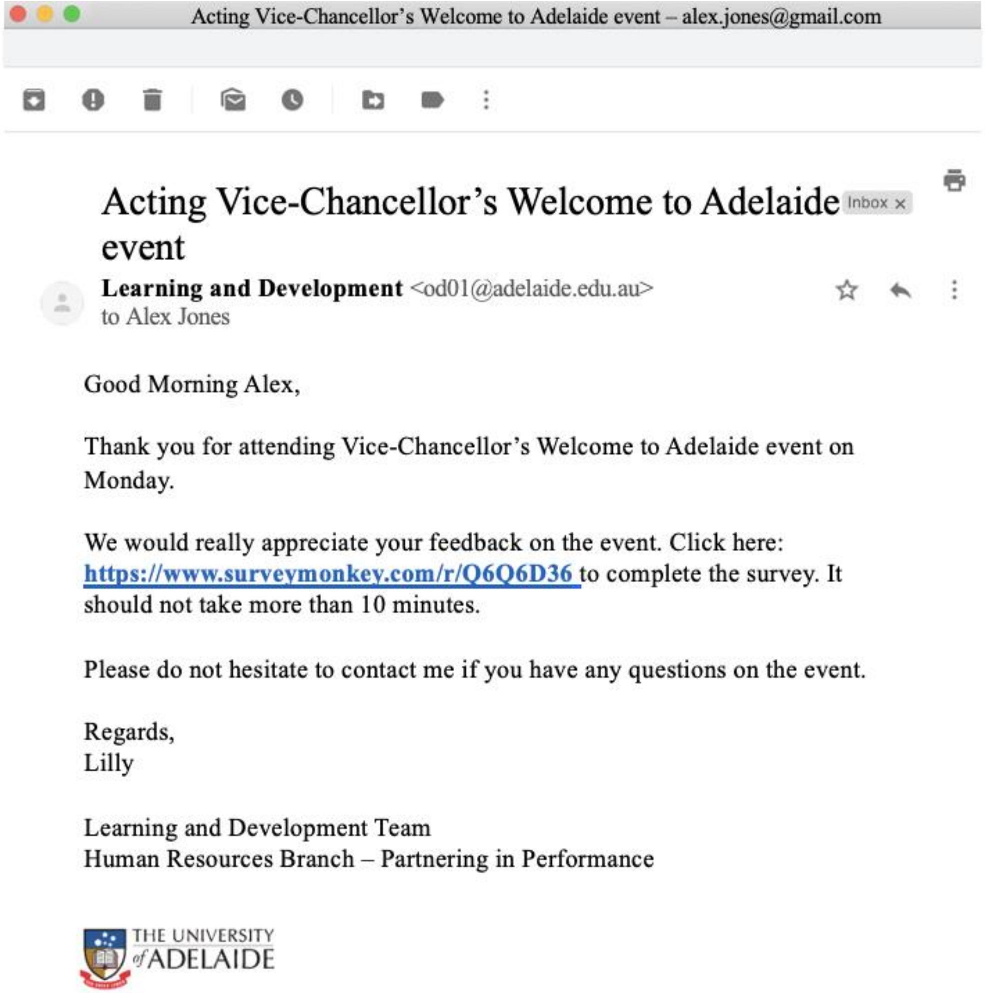
Hi Alex,

Here is link to google doc containing the abstract of my upcoming resarch Study. I am hoping you can check it over today and return your thoughts by tomorrow. I am looking forward to seeing the final result!

http://pastehtml.com/view/crhc6tc8f.html

Thanks, Daniel

Authority (genuine) Email and, Authority (phishing) Email containing One Phishing Feature (URL).



Acting Vice-Chancellor’s Welcome to Adelaide event – alex.jones@gmail.com

Acting Vice-Chancellor’s Welcome to Adelaide event

Learning and Development <od01@adelaide.edu.au>
to Alex Jones

Good Morning Alex,

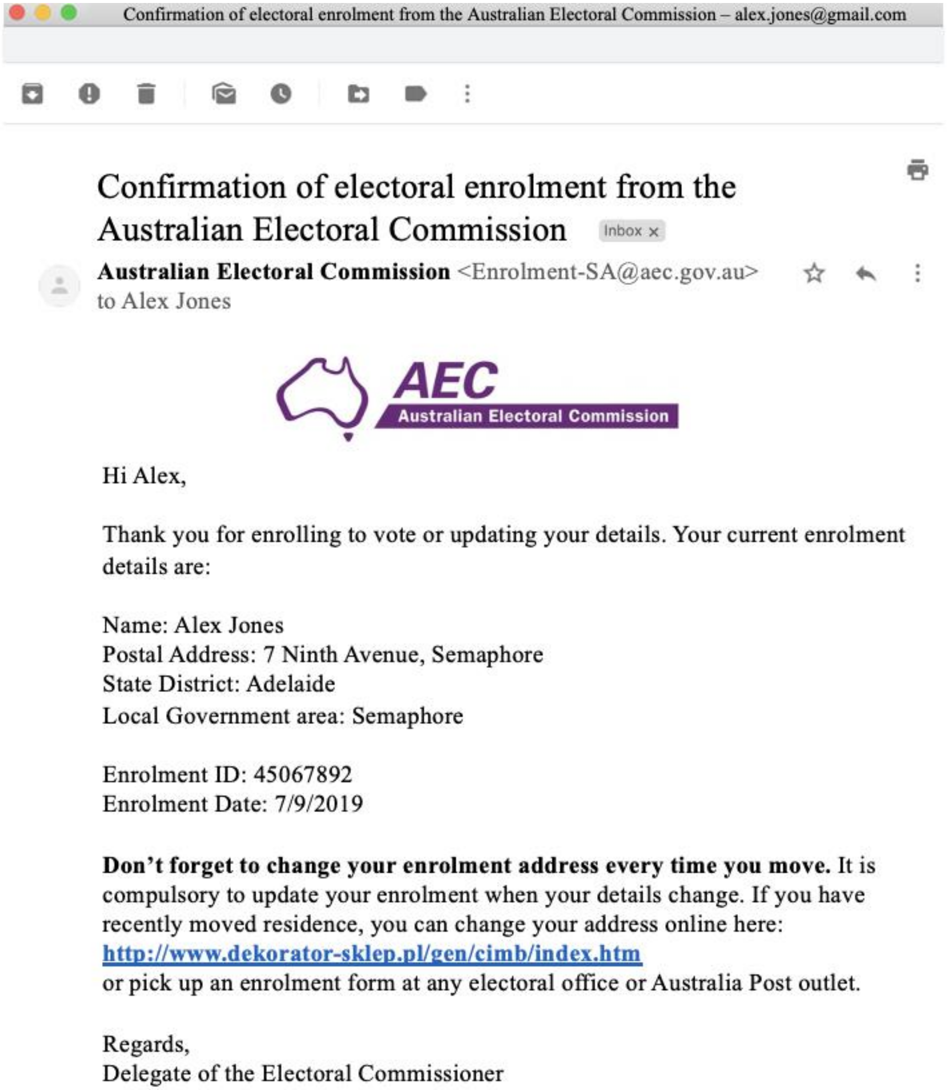
Thank you for attending Vice-Chancellor’s Welcome to Adelaide event on Monday.

We would really appreciate your feedback on the event. Click here: https://www.surveymonkey.com/r/Q6Q6D36 to complete the survey. It should not take more than 10 minutes.

Please do not hesitate to contact me if you have any questions on the event.

Regards,
Lilly

Learning and Development Team
Human Resources Branch – Partnering in Performance



Confirmation of electoral enrolment from the Australian Electoral Commission – alex.jones@gmail.com

Confirmation of electoral enrolment from the Australian Electoral Commission

Australian Electoral Commission <Enrolment-SA@aec.gov.au>
to Alex Jones

Hi Alex,

Thank you for enrolling to vote or updating your details. Your current enrolment details are:

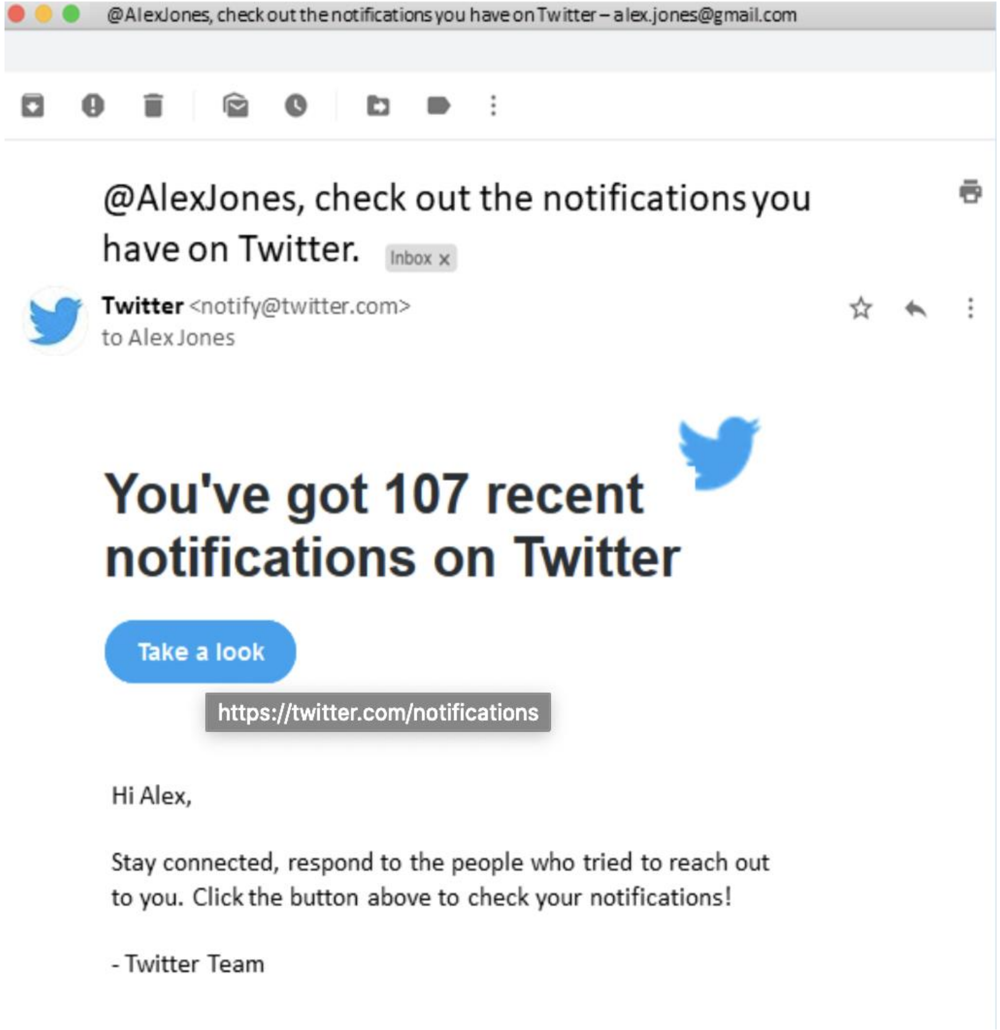
Name: Alex Jones
Postal Address: 7 Ninth Avenue, Semaphore
State District: Adelaide
Local Government area: Semaphore

Enrolment ID: 45067892
Enrolment Date: 7/9/2019

Don’t forget to change your enrolment address every time you move. It is compulsory to update your enrolment when your details change. If you have recently moved residence, you can change your address online here: http://www.dekorator-sklep.pl/gen/cimb/index.htm
or pick up an enrolment form at any electoral office or Australia Post outlet.

Regards,
Delegate of the Electoral Commissioner

Reciprocity (genuine) Email and, Reciprocity (phishing) Email with Three Phishing Features (URL, Spelling and Grammatical Errors, Sender Address).



@AlexJones, check out the notifications you have on Twitter – alex.jones@gmail.com

@AlexJones, check out the notifications you have on Twitter. Inbox ×

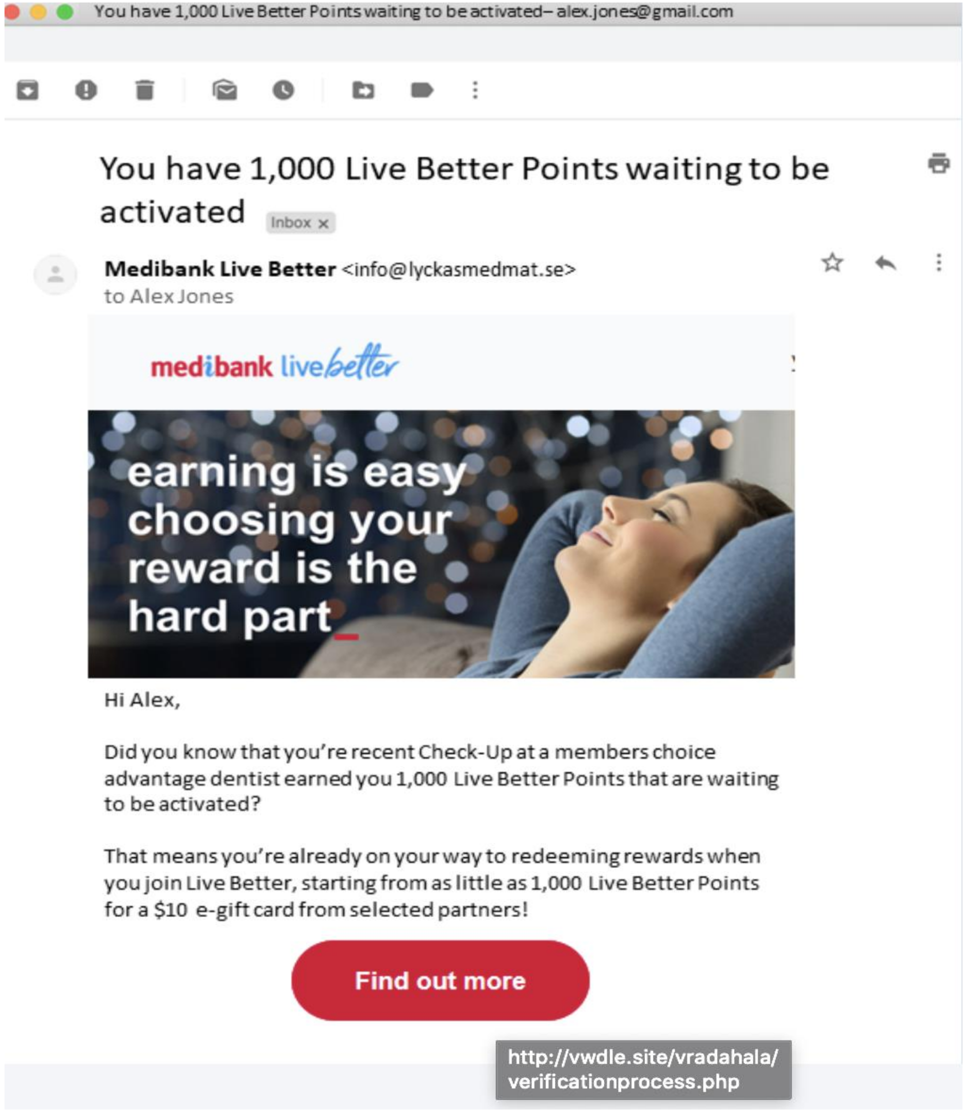
Twitter <notify@twitter.com>
to Alex Jones

You've got 107 recent notifications on Twitter

Hi Alex,

Stay connected, respond to the people who tried to reach out to you. Click the button above to check your notifications!

- Twitter Team



You have 1,000 Live Better Points waiting to be activated– alex.jones@gmail.com

You have 1,000 Live Better Points waiting to be activated Inbox ×

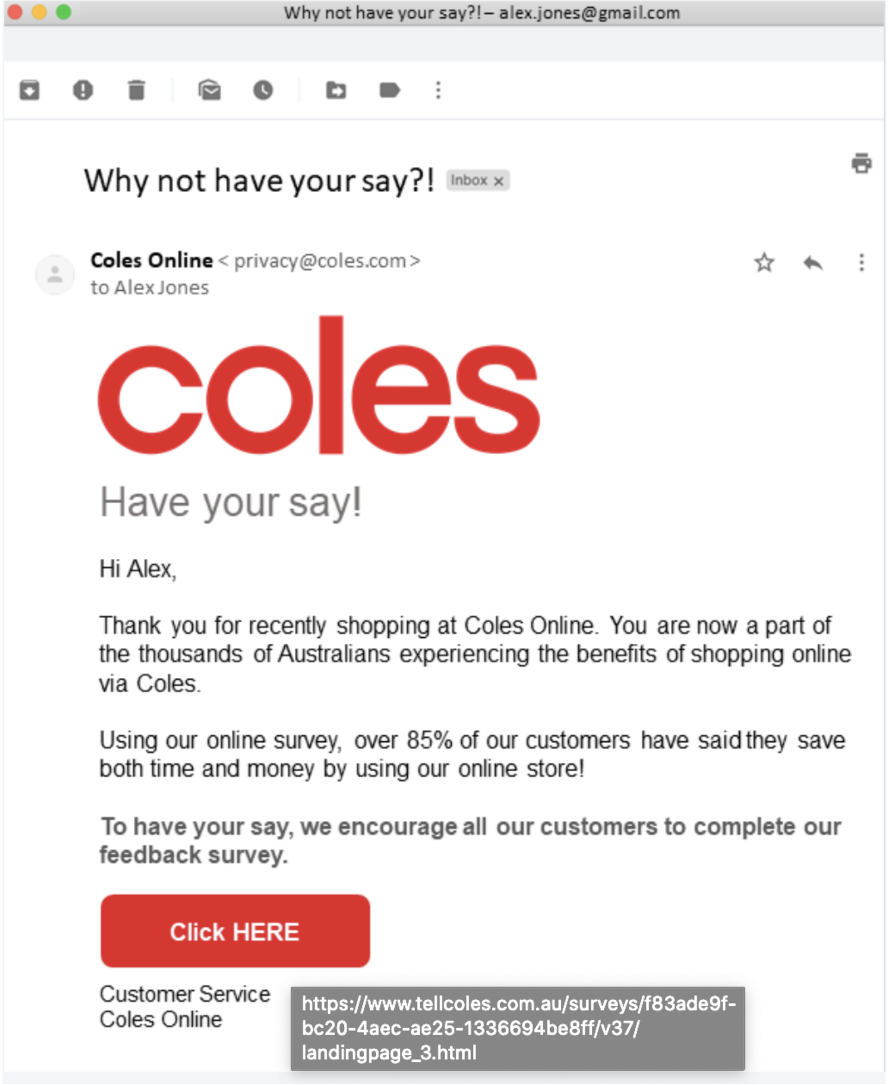
Medibank Live Better <info@lyckasmedmat.se>
to Alex Jones

Hi Alex,

Did you know that you're recent Check-Up at a members choice advantage dentist earned you 1,000 Live Better Points that are waiting to be activated?

That means you're already on your way to redeeming rewards when you join Live Better, starting from as little as 1,000 Live Better Points for a $10 e-gift card from selected partners!

Social Proof (genuine) Email and, Social Proof (phishing) Email with Three Phishing Features (URL, Spelling, and Grammatical Errors, Sender Address).



Why not have your say?! – alex.jones@gmail.com

Why not have your say?!

Coles Online < privacy@coles.com >
to Alex Jones

Have your say!

Hi Alex,

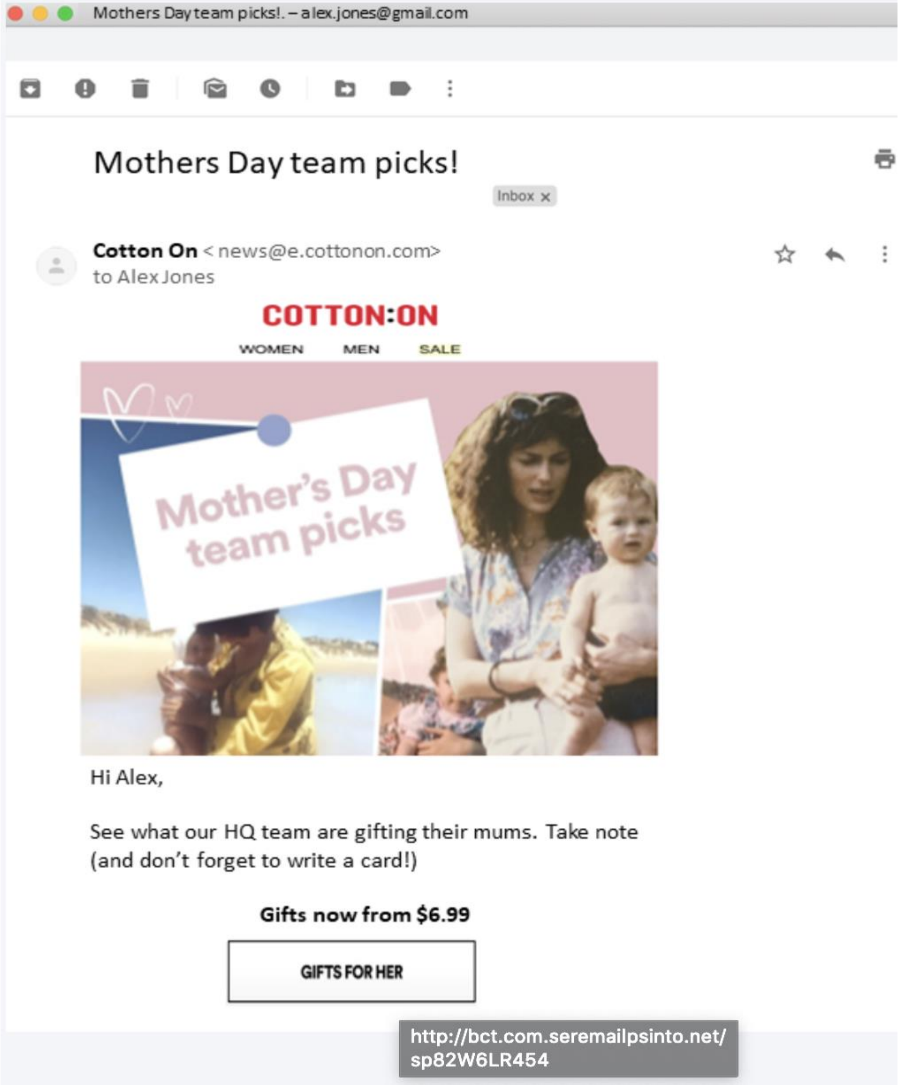
Thank you for recently shopping at Coles Online. You are now a part of the thousands of Australians experiencing the benefits of shopping online via Coles.

Using our online survey, over 85% of our customers have said they save both time and money by using our online store!

To have your say, we encourage all our customers to complete our feedback survey.

Customer Service
Coles Online

https://www.tellcoles.com.au/surveys/f83ade9f-bc20-4aec-ae25-1336694be8ff/v37/landingpage_3.html



Mothers Day team picks!. – alex.jones@gmail.com

Mothers Day team picks!

Cotton On < news@e.cottonon.com>
to Alex Jones

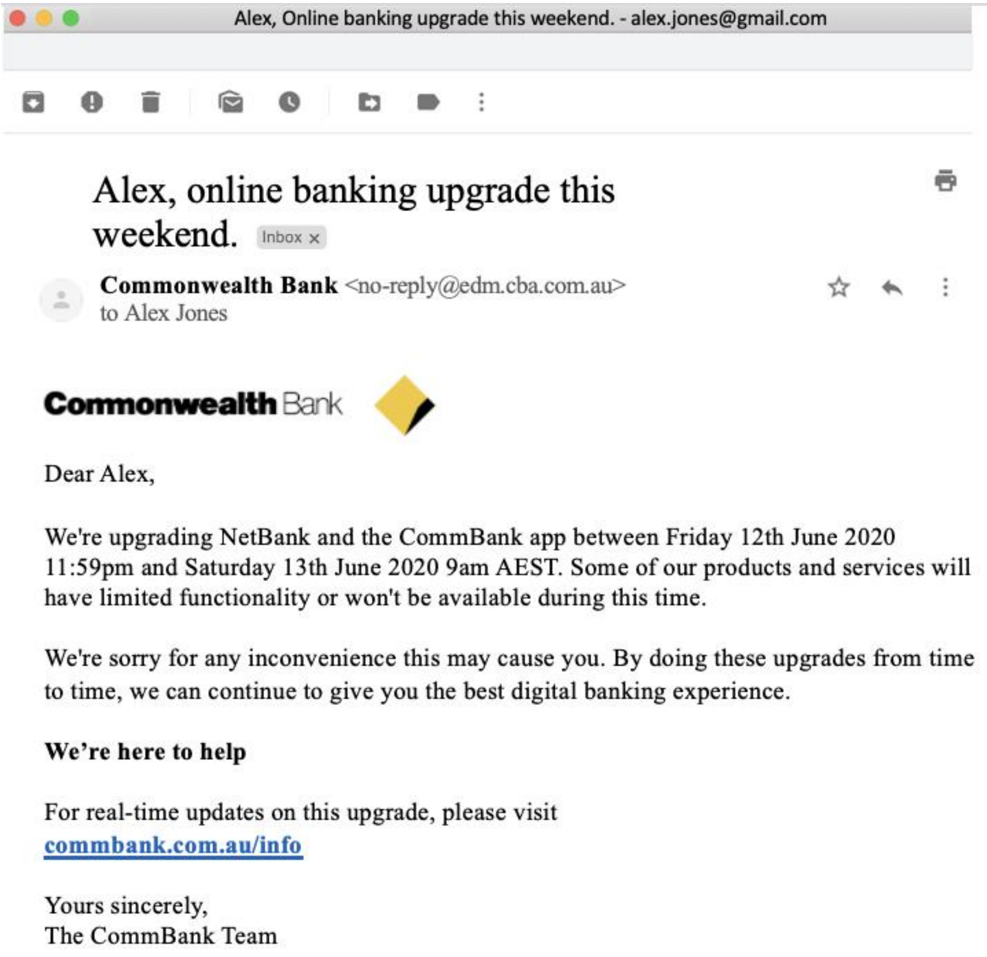
Hi Alex,

See what our HQ team are gifting their mums. Take note (and don't forget to write a card!)

Gifts now from $6.99

http://bct.com.seremailpsinto.net/sp82W6LR454

No Strategy (genuine) Email and, No Strategy (phishing) Email with Three Phishing Features (URL, Spelling and Grammatical Errors, Sender Address).



Alex, Online banking upgrade this weekend. - alex.jones@gmail.com

Alex, online banking upgrade this weekend. Inbox ×

Commonwealth Bank <no-reply@edm.cba.com.au>
to Alex Jones

Dear Alex,

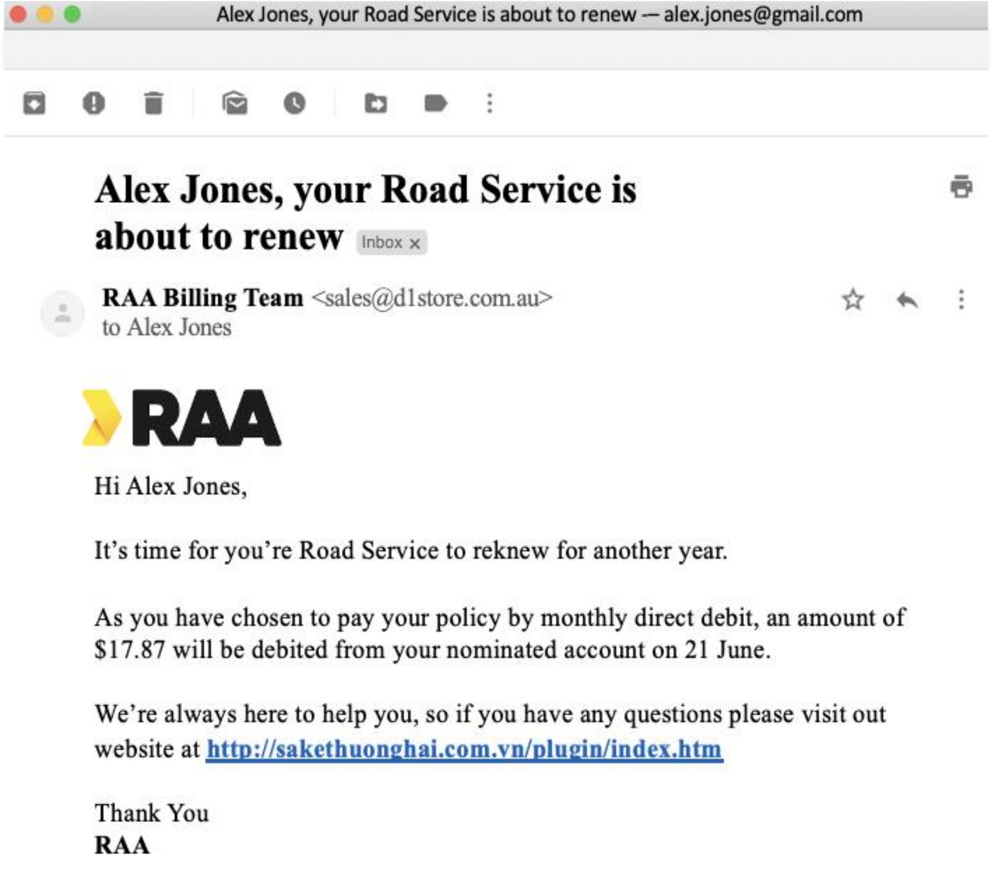
We're upgrading NetBank and the CommBank app between Friday 12th June 2020 11:59pm and Saturday 13th June 2020 9am AEST. Some of our products and services will have limited functionality or won't be available during this time.

We're sorry for any inconvenience this may cause you. By doing these upgrades from time to time, we can continue to give you the best digital banking experience.

We're here to help

For real-time updates on this upgrade, please visit commbank.com.au/info

Yours sincerely,
The CommBank Team



Alex Jones, your Road Service is about to renew — alex.jones@gmail.com

Alex Jones, your Road Service is about to renew Inbox ×

RAA Billing Team <sales@d1store.com.au>
to Alex Jones

Hi Alex Jones,

It's time for you're Road Service to reknew for another year.

As you have chosen to pay your policy by monthly direct debit, an amount of $17.87 will be debited from your nominated account on 21 June.

We're always here to help you, so if you have any questions please visit out website at **http://sakethuonghai.com.vn/plugin/index.htm**

Thank You
RAA

Appendix B: Pilot Study Results.

Table 1

The cumulative total of intended principle across first, second, and third choice for 20 phishing emails.

Social Persuasion Principle	Embedded Phishing Feature(s)	% of participants who identified the intended principle as first, second, or third choice
Scarcity	Email Sender Address	63%
Scarcity	Sender address, URL, spelling and grammatical errors	95%
Scarcity	Spelling and grammatical errors	84%
Scarcity	URL	89%
Reciprocity	Sender address, URL, spelling and grammatical errors	89%
Reciprocity	Email Sender Address	84%
Reciprocity	URL	95%
Reciprocity	Spelling and grammatical errors	89%
Authority	Sender address, URL, spelling and grammatical errors	100%
Authority	URL	89%
Authority	Email Sender Address	100%
Authority	Spelling and grammatical errors	100%
Social Proof	Email Sender Address	89%
Social Proof	Spelling and grammatical errors	95%
Social Proof	Sender address, URL, spelling and grammatical errors	100%
Social Proof	URL	84%
No Principle	Email Sender Address	42%
No Principle	Spelling and grammatical errors	68%
No Principle	Sender address, URL, spelling and grammatical errors	68%
No Principle	URL	79%

Note: N=19