The Role of Time Pressure, Cue Utilisation, and Information Security Awareness on Phishing Email Susceptibility

Oliver Plate

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

Formatted per the 6th edition of the APA Publication Manual.

School of Psychology

University of Adelaide

September 2020

Word Count: 9499

Table of Contents

List of Figures

List of Tables

Abstract

Phishing emails are emails which attempt to solicit sensitive information from unsuspecting users. Phishing represents a major threat to information security. To develop interventions aimed at reducing phishing susceptibility, an understanding of how emails are evaluated to determine their legitimacy, and individual differences that may predict phishing email susceptibility is required. The current study aims to examine the relationship between phishing susceptibility and time pressure, along with individual differences in cue utilisation and information security awareness (ISA). In an online study, 127 participants were randomly assigned to either a 7-second or 15-second time condition and were presented with 60 emails (40 genuine and 20 phishing). Emails were presented one at a time for the duration corresponding with each participant's time condition. Participants were required to sort each email into one of ten categories. The 'phishing' category was considered a hit when chosen following a phishing email, and a false alarm when following a genuine email. Participants also completed an assessment of cue utilisation in the domain of phishing, and the Human Aspects of Information Security Questionnaire (HAIS-Q). Statistical analyses revealed that a higher level of cue utilisation, a shorter email exposure duration and higher ISA resulted in reduced ability to differentiate between phishing and genuine emails. Furthermore, a positive correlation was found between cue utilisation and ISA, however, there was no interaction between time pressure and cue utilisation on phishing susceptibility. This study's outcomes may aid in the development of training and education programs aimed at reducing phishing susceptibility.

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

For this thesis, I collaborated with another honours student when creating the email stimuli, but different aspects of the project and different research questions were addressed. In writing this thesis, my supervisors, the other honours student, and I collaborated to generate research questions of interest and design the appropriate methodology. The other student and I completed the ethics application, then selected and recreated all 60 emails used within the email management task. I, alone, created the email management task on the Qualtrics platform and inserted the appropriate pre-existing questionnaires (HAIS-Q and EXPERTise 2.0). I was responsible for all participant recruitment and testing, and I allocated credit to students upon the studies completion, while my supervisors provided all participation incentives for the public. I, alone; collected, collated, and formatted all data that was retrieved from the experiment and reported in this thesis. My supervisors and I collaborated to analyse the data using SPSS. I wrote up all aspects of the thesis.

Acknowledgements

I would like to thank my supervisors Jaime Auton and Daniel Sturman, you have both been incredibly supportive to me this year. I could always expect prompt email responses filled with great advice, I have learnt a lot from you both and I am grateful for the time you have given me.

I also would like to thank fellow honours student Tazin Tanvir, who I worked closely with when creating the experiment, it was great to have someone to bounce ideas off.

Finally, I thank my family and friends who have further supported me through the writing of this thesis, giving me motivation when I needed it most.

The Role of Time Pressure, Cue Utilisation, and Information Security Awareness on Phishing Email Susceptibility

Phishing refers to a type of cyber-attack that derives its name from its aim; to ‘phish’ for sensitive information. Phishing attacks take many forms, with the most common method being an email disguised as legitimate to fool recipients into clicking on a malicious link or attachment (Australian Competition & Consumer Commission, 2020a; Luo, Zhang, Burd, & Seazzu, 2013). Phishing attacks usually target a large group of people at once, where the objective is to gather personal details, login credentials or gain access to a computer system (Luo et al., 2013; Parsons, Butavicius, Delfabbro, & Lillie, 2019; Xu & Zhang, 2012).

Phishing has been identified as one of the greatest threats to organisational information security (Parsons et al., 2019). Between 2014 and 2018 cyber-attacks to businesses increased by 67% (Biselle, LaSalle, & Dal Cin, 2017), and phishing was the top form of scam reported to the Australian Competition & Consumer Commission in 2019 (Australian Competition & Consumer Commission, 2020b). The estimated loss to Australian individuals from those reported phishing attacks was over $1.5 million, and in 2020 the number of phishing reports for January-April is almost half the number of reports for the entirety of 2019 (Australian Competition & Consumer Commission, 2020a; 2020c). In addition to financial loss, phishing attacks can cause negative psychological effects, as phishing victims have indicated feelings of embarrassment, anger, devastation, and sadness (Jansen & Leukfeldt, 2018). They also experienced reduced feelings of safety online, reduced trust in themselves and others, and physical symptoms including sleepless nights (Jansen & Leukfeldt, 2018).

In recent years, as technology has become more sophisticated and internet usage has grown, phishing attacks have also increased in frequency and sophistication making them increasingly difficult to detect (Australian Cyber Security Centre, 2020; Vishwanath, Herath, Chen, Wang, & Rao, 2011; Xu & Zhang, 2012). Contemporary email applications and internet browsers have begun implementing technological solutions to prevent potential phishing emails being passed on to users. For example, many email applications have email-filtering technology installed automatically filtering out suspected phishing emails (Luo et al., 2013; Xu & Zhang, 2012). While such technologies are an extremely useful barrier to phishing emails, they are not infallible. As such, technological solutions alone cannot provide adequate safeguards against ever evolving phishing attacks (McCormac et al., 2018; Vishwanath et al., 2011).

Phishing emails rely on human error to succeed, as their content oftentimes aims to exploit cognitive weaknesses and biases (Ferreira & Teles, 2019; Parsons et al., 2019; Vishwanath et al., 2011). This can be illustrated in a study conducted by IBM, where it was found over 95% of security breaches were due to human error (IBM, 2015). Therefore, as human users are the last defense against phishing attacks, a greater understanding of individual differences that may increase phishing email susceptibility is warranted. Thus, psychologists endeavour to determine how best to minimise errors in email judgement to gain a greater understanding of individual differences influencing phishing susceptibility (Vishwanath et al., 2011).

Individual Differences and Phishing Email Susceptibility

Phishing emails originated in 1995 (Rekouche, 2011) and were first observed in Australia in 2003 (Australian Cyber Security Centre, 2020), therefore, phishing literature is a relatively new field of research. To gain understanding of their influence on phishing susceptibility, the phishing literature has typically focused on demographic information such as computer-usage, gender and age (Moody, Galletta, & Dunn, 2017; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010). This literature has produced inconsistent findings. For instance, some researchers found females were more susceptible to phishing emails, compared to males (e.g., Halevi, Lewis, & Memon, 2013; Jagatic, Johnson, Jakobsson, & Menczer, 2007; Sheng et al., 2010), while several studies found no difference in phishing susceptibility between genders (e.g., Butavicius et al., 2017; Parsons et al., 2019). Additionally, studies have demonstrated phishing susceptibility decreases with age (Parsons et al., 2019; Sheng et al., 2010), while others have found age to have no effect (Moody et al., 2017). Similarly, some researchers have shown possessing a higher familiarity with computers resulted in increased ability to detect phishing emails (Parsons et al., 2019), while others found increased frequency of internet usage was associated with a higher likelihood to click on phishing email links (Moody et al., 2017).

These inconsistent findings demonstrate it is unknown which individual differences reliably influence phishing susceptibility. Therefore, further research is required to solidify these relationships, or to identify alternative individual differences that may demonstrate an increased effect. Potential alternative differences include cue utilisation, information security awareness and decision-making processes, which are yet to be investigated and may arguably influence an individual's ability to detect phishing emails.

Cues

When determining email legitimacy, effective decision-making relies on an accurate and timely evaluation of the email (Klein, 2008), which is facilitated by feature-event/object associations stored in memory, known as cues (Wiggins, 2014a; 2014b). For example, in a situation wherein an individual aims to determine whether an email is legitimate or phishing, the presence of certain features (e.g., spelling/grammar mistake or unrecognised URL) are associated with an event (whether said email is phishing or legitimate). These specialised associations are formed through repeated application to become a cue, which, when encountered, is retrieved from long-term memory, and activated (Brunswik, 1955; Wiggins, 2014a).

Every situation is comprised of unique features that can become cues which inform appropriate situational behaviour (Brouwers, Wiggins, Helton, O'Hare & Griffin, 2016). Cues function to increase the ease with which a decision can be made and implemented, enabling rapid recognition and response to a situation with minimal cognitive effort (Brouwers et al., 2016; Brunswick, 1955; Wiggins, 2014a). Depending on the stimulus complexity, multiple cues can be activated at once at the unconscious level of information processing (Wiggins, 2014a).

Cues commonly associated with phishing emails include links or senders addresses that do not appear legitimate, along with spelling/grammar errors (Parsons, et al., 2015). Brunswik's (1955) Lens Model attempts to explain how individuals make judgements using cues in a variety of situations. The Lens Model (Figure 1) can be applied to decision making in a phishing context, wherein the 'true state' represents whether the email is legitimate or phishing, and the 'judged state' represents whether an individual thinks the email is legitimate or phishing.

When observing a phishing email, several cues will be available (spelling/grammar mistake, unrecognised URL etc.), all differently weighted regarding how diagnostic they are of the event (the email is phishing). To aid their decision, an individual could choose to use any of these cues. Therefore, if fewer diagnostic cues are used, their judgement accuracy may be reduced, thus concluding the email is not phishing. Consequently, in such a case where the individual's 'judged' and 'true' state differ, they will have an increased likelihood of falling victim to phishing compared to individuals whose states correlate and, therefore, more effectively judge phishing emails. Judgement was based on this lens of information (cues) to determine whether an email is legitimate or not (Parsons et al., 2015; Wang, Herath, Chen, Vishwanath, & Rao, 2012).

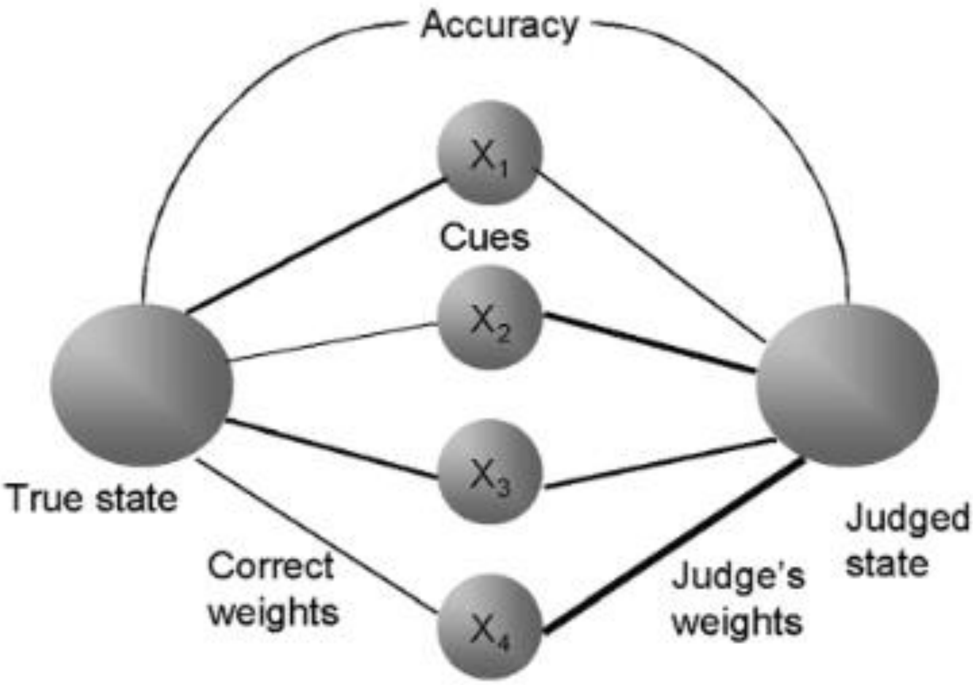


Figure 1: The Lens Model

Cue Utilisation. When assessing situations, everyone has a different inherent capability to extract key environmental features and form cues, and may possess a different level of necessary environmental experience for task-related features to become apparent (McCormack, Wiggins, Loveday & Festa, 2014; Yuris ,Wiggins, Auton, Gaicon, & Sturman, 2019). Additionally, individuals differ in propensity to acquire patterns that make up cues (Brouwers, Wiggins & Griffin, 2018) and cue-based decision making is prone to errors that delay or prevent accurate recognition of the event/object (Brouwers et al., 2018). This differing capacity to identify and apply cues is known as cue utilisation and is thought to be a key individual difference influencing individuals' ability to discriminate between genuine and phishing emails.

A higher capacity for cue utilisation depends on several factors, firstly, capacity to identify task-related features from an assortment of features (e.g., an environmental scene; Wiggins, 2014b). Furthermore, it is necessary to understand how different features and events/objects constituting an operating environment are related and a capacity to discriminate between the relevance of different cues in solving the situation-specific problem (Wiggins, 2014b). Finally, cue utilisation is reliant on a capacity to prioritise the acquisition of feature information best suited to the resolution of a task-related problem (Wiggins, 2014b).

Cue utilisation has been found to differentiate more-effective from less-effective operators in a variety of contexts. During a novel train control task, lower levels of cue utilisation resulted in significantly greater response latency and significantly lower accuracy than higher levels of cue utilisation (Brouwers et al., 2016). This indicates participants' effectiveness and efficiency in recognising cues was influenced by their cue utilisation level (Brouwers et al., 2016). Furthermore, during a simulated driving task, participants with higher cue utilisation experienced significantly fewer errors, collisions, fixations, and visual saccades compared to those with lower levels of cue utilisation (Yuris et al., 2019). This result occurred despite completing the task at a faster mean rate, indicating environmental cues were identified and applied with higher efficiency and effectiveness (Yuris et al. 2019).

To date, one study has examined the relationship between phishing detection and cue utilisation, wherein higher cue utilisation resulted in improved identification of phishing features within emails, compared to lower cue utilisation (Bayl-Smith, Sturman & Wiggins, 2020). However, this improved ability to identify phishing features did not translate to an improved ability to discriminate between phishing and genuine emails (Bayl-Smith et al., 2020). The researchers indicated this may have been due to the study's small email sample (5 phishing, 5 genuine), containing multiple phishing features and consequently being too easy to detect (Bayl-Smith et al., 2020). Furthermore, these did not operate as a real email would, they were merely images (e.g., no ability to hover-over hyperlinks to reveal more information), and had no personal import to participants', therefore, reducing motivation

(Bayl-Smith et al., 2020). This small email sample reduced the studies statistical power, increasing likelihood of type II errors, additionally, lack of sophistication within the emails and the ease with which they could be detected may have reduced ecological validity. Future research could remedy these issues with a larger sample of more sophisticated emails, resembling and operating more closely to real emails, representing a wider variety of subject types, and email formats.

Modes of Decision Making

When making decisions, individuals may differ in how they assess situation-related information. According to dual processing theory, in a decision-making situation such as evaluating an email for legitimacy, two processing systems are accessed: system 1 and system 2 (Kahneman, 2003). Processing within these two systems is distinct from one another; system 1 constitutes fast and effortless processing, utilising automatic heuristics such as environmental cues to allow for efficient decision making (Kahneman, 2003). While system 2 processing is slow, controlled, and effortful, and has been linked to choices determined by considering consequences of actions (Evans & Stanovich, 2013; Kahneman, 2003), such as when evaluating an email for legitimacy.

Most behaviour will use system 1 processing, and system 2 will provide intervention when difficulty, novelty, and motivation combine to command mental resources and consider an alternate decision (Evans & Stanovich, 2013). Arguably, in a typical situation when answering emails, a computer-user will use system 1 processing. This may be due to the need for quick decision making when answering many commonplace emails received daily. Regular cues may be identified and accessed within these predictable emails, and the appropriate situational action becomes apparent. However, if the email appears abnormal due to the presence of a potential phishing cue, or is entirely new, assessment difficulty and novelty may increase, motivating the computer-user to access system 2’s deliberative processes. In such a case, the email is effortfully observed, and intuitions suggested initially by system 1 will be reflected upon to come to a decision (Chowdhury, Adam & Skinner, 2019). However, situational factors could interrupt this process, such as time pressure, therefore, necessitating a decision to be made before this process can complete, increasing reliance on system 1 (Chowdhury et al., 2019).

The Effect of Time Constraints on Decision Making. Time-pressure has been identified as a structural influence affecting the decision mode used in a situation (Allen, 2011). Previous research suggests, under time pressure, decision makers increase their decision speed, or switch to simpler strategies (Chowdhury et al., 2019). Furthermore, it has been suggested that time pressure results in reliance on intuition (system 1) as a surrogate for exhaustive search strategies (system 2) (Allen, 2011; Chowdhury et al., 2019). For example, if an individual is about to have a collision while driving, they are under time pressure to avoid catastrophe. Therefore, they are far more likely to engage in quick system 1 processing, rather than slower system 2 processing. (Kahneman, 2003).

Individuals have reported increasingly experiencing time pressure in their professional and personal lives as they are loaded with multiple tasks and aim to meet deadlines (Chowdhury et al., 2019). Oftentimes, such time pressure is generated when answering emails, as many may be received daily coupled with an expectation of a prompt response. A higher email load has been linked to an increased likelihood to respond to phishing emails (Vishwanath et al., 2011). Furthermore, habitual media use, which results in automatic responses to patterned stimuli, has been linked to phishing susceptibility (Vishwanath et al., 2011). This illustrates that increased reliance on quick cue-based system 1 decisions, resulting from time pressure, could increase phishing susceptibility. If every email was verified with system 2 processing, time pressure would compound, as the act of verifying security cues in emails has been identified as a task that generates time pressure (Chowdhury et al., 2019).

In a systematic review examining time pressure's effect on various cybersecurity activities, two studies examined phishing (Chowdhury et al., 2019). These studies looked at participants' responses to time pressure implied through urgency cues in emails (Chowdhury et al., 2019). Both demonstrated when email content implied urgency, participants were more likely to respond to the phishing email (Marett & Wright, 2009; Wang et al., 2012). However, neither study directly applied time-pressure to participants when they were viewing the emails.

In Chowdhury et al.'s (2019) review, of the studies that did not examine phishing, four explicitly measured time pressure, as participants had a certain amount of time in which the task was to be completed. Only one compared a low and high time pressure condition, in this case, low time pressure participants completed 91% of the tasks, while participants' under high time pressure only completed 74% of tasks (Chowdhury et al., 2019; McNab, Hess, & Valacich, 2009). Additionally, time pressure was compared to no-time-pressure in three studies. In all three cases, time pressure was implied, and not explicit, and led to a non-secure information security behaviour (Chowdhury et al., 2019). These results demonstrate, compared with lesser or no time pressure, higher levels of time pressure reduced performance on a variety of cybersecurity tasks.

This review evidences time pressure increases the likelihood of unsafe information security behaviours, but examination of time pressure's influence on phishing detection is lacking. In future research, to ensure time pressure is directly applied to participants, explicit time pressure should be enacted by allocating a certain amount of time for responses. This will place a guaranteed level of time pressure on participants and allow for direct measurement of its effects. Furthermore, varying time pressure conditions are necessary to allow for a comparison of performance. This review, along with the effects of time pressure on decision making processes, illustrate time pressure may be a determining influence on individual's phishing susceptibility. As email information may be inadequately processed thus reducing ability to discriminate between phishing and genuine emails.

Interaction between cue utilisation and time pressure. Higher levels of cue utilisation indicate more effective and efficient identification and accessing of environmental cues (Bayl-Smith et al., 2020; Sturman, Wiggins, Auton & Loft, 2019a). Additionally, time pressure may change the decision mode, causing increased reliance on system 1 processing, which uses cues to facilitate decision making (Allen, 2011; Kahneman, 2003). Consequently, under time pressure, individuals with relatively higher levels of cue utilisation should be able to more efficiently assess and act upon cues. While those with relatively lower levels of cue utilisation will attempt the same process, with lower efficiency, resulting in poorer discrimination between phishing and genuine emails. However, with reduced time pressure, individuals should have sufficient time to recognise important features in phishing emails regardless of their level of cue utilisation. Consequently, with reduced time pressure, cue utilisation is likely to have less impact on phishing email detection.

Information Security Awareness

Information security awareness (ISA) is the extent to which people understand safe information security behaviours, and extent to which individuals are committed to, and behave in accordance with, best practice of these behaviours (Parsons et al., 2017). This difference may influence phishing detection, as information security refers to processes and methodologies designed to protect information or data from unauthorized access (SANS, 2020). Therefore, phishing is an information security issue, as phishers aim to obtain information illegally. ISA serves as an operationalisation of individuals' cyber-risk beliefs, allowing insight into knowledge, attitudes, and behaviour regarding email-use (Parsons et al., 2017).

Individuals' beliefs are formed through prior experience, exposure to media and other internal factors (Bandura, 1989). Additionally, when situational actions are considered, the most readily accessed cognitions are previously held beliefs corresponding with that situation (e.g., consideration of risk-related actions correspond with risk-related beliefs; Griffin, Neuwirth, Giese & Dunwoody, 2002). These beliefs were formed previously, and when a similar situation arose, they were accessed and applied. Therefore, when assessing an email and considering the next action, individuals will access previously established cyber-risk beliefs.

It is likely an individual with higher ISA will indicate better knowledge, attitude, and behaviour towards email-related information security issues. These cyber-risk beliefs have been previously established (Bandura, 1989) and, due to higher ISA, are better understood. Consequently, individuals with a higher ISA more readily consider related risks (Griffin et al., 2002), resulting in safer email-related information security behaviours than those with lower ISA. Previous research has found employee's ISA is vital in mitigating risks associated with information security breaches (Arachchilage & Love, 2014; Sohrabi Safa, Von Solms & Furnell, 2016). Additionally, higher ISA has been found to correlate with an improved ability to detect illegitimate email links (Parsons et al., 2017), however, whether this translates to other phishing cues is yet to be examined.

ISA represents knowledge, attitude, and behaviour towards information security, measured using a self-report. To develop cues that identify an email as phishing, some knowledge of potential phishing features is necessary, therefore, some degree of ISA is required to identify such features. Cues will develop through exposure to information security environments, and increased exposure may result in increased understanding of these environments, and therefore, higher ISA. Increased ISA corresponds with safe information security behaviours (Parsons et al., 2017), and therefore, may result in better developed cues that can be applied with greater effectiveness. Furthermore, while ISA indicates an understanding of rules regarding safe information security behaviours, cue utilisation can demonstrate this understanding in an operative environment. Therefore, these individual differences may be closely related, with one able to predict the other.

The Current Study

Aims and Operationalisation. The aim of the current study was to understand how time pressure, cue utilisation, and ISA influence the ability to discriminate between phishing and genuine emails. Discrimination was measured based on a novel email management task, which required participants to view a series of email stimuli, that were either genuine, or had a phishing cue inserted into them. These stimuli were presented in two email exposure durations (7 secs or 15 secs), and once shown, were required to be sorted into a choice of ten possible categories (e.g. Banking, Urgent, Phishing).

Hypotheses

H1: It was hypothesised that participants with a relatively higher level of cue utilisation would be better able to discriminate between genuine and phishing emails, compared to those with a relatively lower level of cue utilisation.

H2: It was hypothesised that participants in the longer email exposure duration would be better able to discriminate between genuine and phishing emails, compared to participants in the shorter email exposure duration.

H3*:* It was hypothesised that differences in ability to discriminate between genuine and phishing emails based on cue utilisation will be significantly greater in the shorter exposure duration, compared to the longer exposure duration.

H4: It was hypothesised that higher ISA would be positively associated with participants' ability to discriminate between genuine and phishing emails.

H5: It was hypothesised that participants with a relatively higher level of cue utilisation will have higher ISA, compared to those with a relatively lower level of cue utilisation.

Method

Participants

One hundred twenty-seven participants were recruited for the experiment (94 Females, 33 Males), aged between 17 and 54 years (*M* = 22.10, *SD* = 7.21), and required to be fluent in English. Of these, 109 participants were recruited using the SONA system from the pool of first year psychology students at the University of Adelaide. In these cases, students received credit upon completion of the study as compensation for their time. Eighteen participants were recruited from the public using snowball and convenience sampling via social media and word of mouth. As incentive and compensation, these participants could enter in a draw to win a $20 gift card.

Design

The present study used a 2 x 2 quasi-experimental design, with participants' ability to correctly discriminate phishing from genuine emails serving as the dependent variable. Exposure time (7 vs 15 seconds) and cue utilisation typology (higher vs lower) were between-subjects independent variables and ISA was included as a continuous covariate.

Materials

Demographic Questions. Demographic questions included gender, age (in years), and participants' confidence in using a computer (measured using a Likert scale from 1 [no confidence] to 5 [very confident]). Furthermore, participants were asked to indicate the approximate number of emails received per day and time spent on the computer each day.

Email Management Task. The Qualtrics platform was used to create and host this online task, in which participants are told to roleplay as personal assistant to “Professor Alex Jones”. They are tasked with examining emails sent to his inbox and sorting them into one of ten categories. Before commencing the task, participants are given instructions; along with an image demonstrating how to hover-over links in the stimuli.

The email management task consists of 60 emails (see Appendix A). Emails replicated genuine non-phishing emails previously received by the researchers, representing a mix of personal and work-related emails. Emails contained between 15 and 100 words; this upper limit was chosen to ensure participants were able to adequately assess each email within the given time. Emails were selected to contain a balance of Cialdini’s (2009) persuasion strategies. These strategies aim to place a perceived pressure on the reader through the email’s writing and content. Twelve emails contained the authority persuasion strategy, 12 contained the scarcity persuasion strategy, 12 contained the reciprocity persuasion strategy, 12 contained the social proof persuasion strategy and 12 contained no persuasion strategy. This was chosen to remain consistent with emails received in a typical inbox, as both genuine and phishing emails usually contain persuasion strategies (Parsons et al., 2019). All emails contained a URL. In 17 stimuli this URL was displayed in the body of the email, while in 43 stimuli, the URL was embedded in a prompt button (e.g., “CLICK HERE”). In the latter case, the mouse could be used to hover-over the prompt button and display said URL (see Appendix B). In either instance it was ensured each stimulus remained consistent with the email serving as its basis.

Of the 60 emails, 20 were converted into phishing emails by inserting phishing cues. The stimuli were randomly assigned into one of four phishing conditions, determining which phishing cue was embedded. Five emails included one spelling and one grammar mistake inserted within the first two lines of text to maintain consistency. Furthermore, five emails included a phishing sender's address, five included a phishing URL and five included all three of these (see Appendix A). These features were balanced across persuasion strategies and were selected to best emulate the range of phishing cues present in real world phishing emails, and to be of equal salience. Each phishing URL and phishing senders address used was a genuine example, found online or within a real phishing email received by the researchers.

Participants were presented with all 60 stimuli for either 7 seconds or 15 seconds depending on the allocated email exposure duration. When viewing each email, a count-down timer was displayed, indicating the time remaining in which they could view the email. This manipulation allowed effects of the email exposure duration to be directly observed and for comparison of these durations. Following each presentation, the stimulus was removed, and participants were asked to categorise the email. This categorisation question contained ten options, aiming to obfuscate the "phishing" option, and reduce the chance of any priming effects. These options were urgent, teaching, research, banking, online purchases, social media accounts, official, spam, phishing and miscellaneous. Each was paired with a description, informing participants of email types which should be sorted into the respective category (see Appendix C). If the phishing option was chosen after viewing a stimulus with a phishing cue, this was considered a hit. Choosing any other option after the presentation of a phishing stimulus was considered a miss. Genuine stimuli (no phishing cue present) sorted into the phishing category were considered a false alarm, and genuine stimuli classified as any other option was a correct rejection. This process was completed for all 60 stimuli, and the task was estimated to take between 30-60 minutes.

The study's description informed participants that the study would be investigating "User Behaviour and the Management of Emails". Consequently, participants were misinformed about the study's true nature, ensuring they were unaware the experiment related to phishing email detection. This approach was chosen to avoid any subject expectancy bias and priming effects (Parsons, McCormac, Pattinson, & Butavicius, 2015). Past research has found that if participants are aware a study is phishing-related they act unnaturally, resulting in an increase in false alarms (identifying genuine emails as phishing; Lawson, Zielinska, Pearson, & Mayhorn, 2017; Parsons et al., 2015).

Pilot Study

A pilot study was run to assist in determining the time (in seconds) allocated to the shorter and longer time condition in the main study. This was achieved by examining the confidence rating that participants gave their email categorisation decision, along with performance on the task. The confidence rating was made on a 5-point Likert scale from 1 (not confident) to 5 (very confident), while performance was measured using the same methodology as the main study.

Twenty participants were recruited using the SONA system from the pool of University of Adelaide first-year psychology students (15 females, 4 males, 1 other). Participants who completed the pilot study were excluded from completing the main study. This pilot study was conducted prior to the main study, and the email management task used the same 60 stimuli used in the main study. These stimuli were allocated into one of four time conditions (5, 7, 10 and 15 seconds), resulting in 15 stimuli in each condition. Each condition contained 10 genuine emails and five phishing emails. Phishing features were consistent with the main study (spelling/grammar mistake, phishing senders address, phishing URL and all three), and were evenly distributed across time conditions. The pilot study used a within-subjects design, whereby participants viewed all 60 emails and therefore experienced all time conditions. Consistent with the main study, participants experienced the same role-playing scenario and were informed the task was investigating "User Behaviour and the Management of Emails".

The results indicated performance in the 5 second condition was no better than chance, and the categorisation decision was consistently made with low confidence. Performance in the 7 second condition was above chance, and rating confidence was moderate, and therefore 7 seconds was selected as the duration for the shorter time condition, and to maximise the difference between the two conditions, 15 seconds was selected to be the longer time condition.

Human Aspects of Information Security Questionnaire (HAIS-Q). To measure participant's ISA, the present study used the Human Aspects of Information Security Questionnaire (HAIS-Q; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014). This intends to capture individuals' knowledge, attitude, and behaviour regarding information security (Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2013). Underpinning this measure is the Knowledge-Attitude-Behaviour (KAB) Model (Baranowski, Cullen, Nicklas, Thompson, & Baranowski, 2003), which had been previously established in an information security context (Kruger & Kearny, 2006). This model was decided upon due to a hypothesis formed from results of interviews with a company's management, and an exploratory survey completed by 203 employees of the same company (Parsons et al., 2013). This hypothesis posited that as computer users' knowledge of information security policy and procedure rises, attitudes will improve, resulting in improved information security behaviours (Parsons et al., 2017).

The HAIS-Q centres around 7 focus areas; internet use, email use, social networking site use, password management, incident reporting, information handling and mobile computing (Parsons et al., 2014; 2017). These focus areas were decided using results from the previously mentioned interviews and survey (Parsons et al., 2013), and reviews of organisational information security policies (Parsons et al., 2014). The resulting focus areas were determined to be areas of information security "relevant to employers and computer users and most prone to non-compliance" (Parsons et al., 2014). There are three representative areas within each focus area, and in each of these is a knowledge, attitude, and behaviour statement.

The email use focus area of the HAIS-Q was solely used in the present study. Modular use of the HAIS-Q has been suggested previously, to allow isolation of relevant aspects to the specific project (Parsons et al., 2017). The 3 representative areas in the email use focus area are, "Clicking on links in emails from known senders", "Clicking on links in emails from unknown senders", and, "Opening attachments in emails from unknown senders"; and each are measured via a separate knowledge, attitude and behaviour statement (Parsons et al., 2017). Therefore, the email use subscale used in the present study contains 9 statements, for example, "it's risky to open an email attachment from an unknown sender" (of these statements, 5 are negatively worded; Parsons et al., 2017). Participants are asked to respond to each statement on a five-point Likert scale, from 1 (Strongly Disagree) to 5 (Strongly Agree). All items within each set of questions, are presented in a fixed random order.

The HAIS-Q has been used on many large groups of working Australians, demonstrating its ability to measure ISA (Parsons et al., 2017). A higher score on the email use focus area has been found to correlate with improved ability to detect phishing emails (Parsons et al., 2017). The HAIS-Q has high internal reliability, evidenced by consistently high alpha levels for knowledge, attitude, behaviour, and overall ISA; ranging from .84 to .96 (McCormac, Calic, Parsons, Zwaans & Butavicius, 2016; McCormac, Calic, et al., 2017a;

McCormac, Zwaans, et al., 2017b; Parsons et al., 2014; 2017; Wiley, McCormac & Calic, 2020).

Additionally, the measure has shown high test-retest reliability (McCormac et al., 2016; McCormac, Calic et al., 2017a), and content validity has been established on multiple occasions (Calic, Pattinson, Parsons, Butavicius & McCormac, 2016; Pattinson, Butavicius, Parsons, McCormac & Jerram, 2015). Convergent validity has been demonstrated, as the HAIS-Q was found to correlated with phishing detection, which is a behavioural measure expected to correlate with ISA (Parsons et al., 2017). Furthermore, the form of construct validity known as 'known-groups validity' has been established (Pattinson, Butavicius, Parsons, McCormac, Calic & Jerram, 2016). This looks at how the measure is sensitive to similarities and differences between groups (Hattie & Cooksey, 1984). The present experiment aims to solidify use of the HAIS-Q in a phishing context, and the viability of its modular use.

EXPERT Intensive Skills Evaluation (EXPERTise 2.0) – Phishing Edition. To measure cue utilisation, the EXPERT Intensive Skills Evaluation 2.0 (EXPERTise; Wiggins, Loveday, & Auton, 2015) phishing edition (Bayl-Smith et al., 2020) was used. This is a customisable shell software package able to assess participants' utilisation of cues during task-related activities. EXPERTise has demonstrated good construct validity (Small, Wiggins & Loveday, 2014; Wiggins, Azar, Hawken, Loveday & Newman, 2014), predictive validity (Watkinson, Bristow, Auton, McMahon & Wiggins, 2018), and test-retest reliability (Loveday, Wiggins, Festa, Schell & Twigg, 2013a; Watkinson et al., 2018). EXPERTise has been used in varied contexts, including power control (Loveday, Wiggins, Harris, O'Hare & Smith, 2013b), aviation decision making (Wiggins et al., 2014) and audiology (Watkinson et al., 2018). In the current study, the phishing variant of EXPERTise 2.0 is completed by participants, comprising of four tasks of domain-specific stimuli: The Feature Identification Task, Feature Recognition Task, Feature Association Task and Feature Discrimination Task.

Feature Identification Task (FIT). In the FIT, participants are required to identify key features, as quickly as possible, within a complex scene. In the phishing edition, participants are presented with 16 scenarios, each consisting of a single phishing email. Using a mouse, participants must select the area of the email which they consider the greatest concern (e.g., a suspicious URL) as quickly as possible. The first two scenarios are practice trials and were not included when calculating mean response times. Participants response speed is recorded in milliseconds and mean response latency was determined over the 14 scenarios. Higher cue utilisation has been associated with lower mean response latency (Loveday, Wiggins, & Searle, 2014; Schriver, Morrow, Wickens, & Talleur, 2017).

Feature Recognition Task (FRT). In the FRT, participants are presented with domain-related stimuli for short periods and then must categorise them. The phishing edition has participants view 22 scenarios, 10 with genuine emails, 10 with phishing emails, and two practice trials. Each email is presented for 1000ms, after which participants classify the emails as “trustworthy”, “untrustworthy” or “impossible to tell”. Participants accuracy was summed over the 20 scenarios, greater accuracy is indicative of higher levels of cue utilisation (Brouwers et al., 2018; Wiggins & O’Hare, 2003).

Feature Association Task (FAT). In the FAT, participants are presented with two domain-related stimuli, and must rate their perceived relatedness. In the phishing edition, 16 pairs of words are shown for 1500 milliseconds (e.g. email & task). Using a 7-point Likert scale, participants must indicate how related they perceive the words to be, from 1 (extremely unrelated) to 7(extremely related). Participants mean variance over mean response time was calculated into a single discrimination metric. A greater mean variance to response time is indicative of their capacity to rapidly distinguish related from unrelated features and events/objects, and hence, higher cue utilisation (Morrison, Wiggins, Bond, & Tyler, 2013; Wiggins et al., 2014).

Feature Discrimination Task (FDT). In the FDT participants are presented with two email scenarios with information relating to a specific problem (e.g. a colleague is expecting a delivery). Based on information presented in the email, participants select a course of action from a list of four options (e.g. ignore the email). Following their response, participants are provided with a list of features from the scenario and must rate the perceived importance of each feature to their decision on a 10-point Likert scale from 1 (Not important at all) to 10 (Extremely important). Ratings are aggregated to calculate a variance score, whereby greater variance is indicative of more discriminant ratings of importance between cues in the scenario, and therefore, higher cue utilisation (Loveday et al., 2014; Pauley, O'Hare, & Wiggins, 2009; Weiss & Shanteau, 2003).

Procedure

Ethics approval was obtained from the subcommittee in the School of Psychology at the University of Adelaide (Ref No: 20/39). Participants accessed the link to the online study through the SONA system, or through snowball and convenience sampling. Participants read the participant information sheet and provided electronic consent, followed by completion of the demographic questionnaire. This was followed by random assignment into either the shorter (7 seconds) or the longer (15 seconds) time condition, instructions were displayed to participants and Email Management Task was completed. Both time conditions viewed the same stimuli in the same randomised order. After completing the task, participants completed the email-use module of the HAIS-Q and then were redirected to EXPERTise 2.0. The HAIS-Q and EXPERTise tasks, which focus on phishing emails, were completed after the email management task to ensure no priming effects occurred regarding study's true nature. Once

EXPERTise was completed, participants were displayed a message informing them of the studies completion.

Results

Overview of Analyses

The aim of this experiment was to investigate whether two individual differences (cue utilisation capacity and ISA) and one email characteristic (email exposure duration) affected participants' ability to discriminate between phishing and genuine emails. The data was analysed in two stages using IBM Statistical Package for Social Sciences (Version 26). During the first stage, participants were categorised as having a lesser or greater capacity for cue utilisation (based on performance in the EXPERTise 2.0 tasks). Second, a discrimination score was created based on performance on the Email Management Task, followed by examination of the hypotheses with the appropriate statistical tests.

Data Reduction

Data from the phishing edition of EXPERTise 2.0 and the Email Management Task underwent data reduction. The EXPERTise 2.0 data were used to classify participants into cue utilisation typologies reflecting a relatively higher or lower capacity for cue utilisation (Sturman et al., 2019a). The data across the four EXPERTise 2.0 tasks were reduced in a manner consistent with the standard approach for categorising participants into the two typologies (e.g., Brouwers, Wiggins, Griffin, Helton, & O'Hare, 2017; Loveday et al., 2013b).

Participants' performance in the Email Management Task represented one of the dependent variables. Data reduction for this task relied on Signal Detection Theory (Green & Swets, 1966) to ascertain a discrimination score for each participant. This score represented participants' capacity to discriminate between genuine and phishing emails. It was decided a discrimination score would be more appropriate than an alternative that examined only phishing email detection ability. This allowed for a distinction between participants with a bias towards cautious behaviour, and those most effective at discriminating between phishing and genuine emails. Previous research demonstrates individuals with higher attentional bias towards threat-related stimuli mistook genuine links as phishing more often than those with less attentional bias towards threats (Falkenberg, Auton, & Parsons, 2019).

During the Email Management Task, participants categorised 60 emails (20 phishing; 40 genuine) into one of ten categories (e.g., work, spam, phishing etc.). If participants categorised a phishing email correctly into the phishing category, this was considered a hit, and if this option was chosen in response to a genuine email, this was considered a false alarm. From this, each participants' hit, and false alarm scores were calculated into a proportion score. The proportion of false alarms was subtracted from the proportion of hits, to create a discrimination score. For example, if a participant chose the 'phishing' option ten times in response to phishing emails, this would result in a hit score of ten. This would then be divided by the total number of phishing emails (10/20) to create the hit proportion score (0.5). This same process would then be completed for the genuine emails, for example, if the phishing option was chosen after ten of these, a false alarm score of ten was given. This would then be divided by the total number of genuine emails (10/40) to create a false alarm proportion score (0.25). These scores would then be subtracted from one another (0.5-0.25 = 0.25). Discrimination scores can theoretically range between -1 and 1. A discrimination score of 0 indicates the individual has no ability to discriminate between phishing and genuine emails. A negative score indicates an inability to recognise phishing emails and a tendency to judge genuine emails as phishing, while a more positive score represents a better discrimination ability, with a greater ratio of hits to less false alarms.

Data Analysis

Stage 1: Establishing Typologies. A k-means cluster analysis was conducted to determine whether participants could, based on performance in the four tasks, be categorised into a higher or lower typology representing relative levels of cue utilisation in the phishing domain (Sturman et al., 2019a; Wiggins et al., 2014). Before the cluster analysis could be conducted, the scores for each task were converted to z-scores. The cluster analysis using these standardised scores yielded two distinct typologies representing relatively higher and lower levels of cue utilisation. The higher cue utilisation typology contained 66 participants who recorded relatively lower response latencies on the FIT, relatively greater accuracy on the FRT, relatively higher mean variance to response latency in the FAT and relatively higher mean variance in the FDT. This is the expected pattern of responses for participants who possess a higher level of cue utilisation. The remaining 61 participants were classified in the lower cue utilisation typology. These participants recorded the opposite pattern of responses across the 4 tasks, consistent with performance associated with a lower level of cue utilisation. Table 1 summarises the results of the cluster analysis.

Table 1.

Participant Cluster Means for the EXPERTise 2.0 Measures Across the Two Cue Utilisation Typologies.

	Typology	
EXPERTise 2.0 Tasks	Higher (*n* = 66)	Lower (*n* = 61)
Feature Identification Task (response latency)	-.36	.40
Feature Recognition Task (accuracy)	.59	-.67
Feature Association Task (variance/response latency)	.29	-.32
Feature Discrimination Task (variance)	.57	-.61

Stage 2: Hypothesis Testing. In the present study, hypotheses 1, 2, 3 and 4 were examined using a 2 x 2 between-subjects analysis of covariance (ANCOVA). This ANCOVA used cue utilisation (higher, lower) and email exposure duration (shorter, longer) as between-subjects variables, with ISA as a continuous covariate. These served as the independent variables, while the discrimination score of participants served as the dependent variable.

Examination of histograms revealed the dependent variable was normally distributed for each condition, indicating the assumption of normality was met. Levene's test revealed there was no significant difference in each group's variance, indicating the assumption of equal variance was met. The assumption of independence was met by the design of the study, with no participant tested twice.

There was a statistically significant main effect of cue utilisation typology on participants' discrimination scores, $F(1, 122) = 19.73$, $p < .001$, $\eta^2 = .14$. This result supports H1, indicating that participants with higher cue utilisation demonstrated greater discrimination ($M = 0.214$, $SD = 0.152$), compared to participants with lower cue utilisation ($M = 0.094$, $SD = 0.152$).

There was a statistically significant main effect of email exposure duration on participants' discrimination scores, $F(1, 122) = 11.91$, $p = .001$, $\eta^2 = .089$. This result supports H2, indicating that participants in the longer email exposure duration ($M = 0.200$, $SD = 0.144$), were better able to discriminate between phishing and genuine emails, compared to those in the shorter email exposure duration ($M = 0.108$, $SD = 0.152$).

H3 was not supported, as there was no statistically significant interaction between the participants' cue utilisation typology and the email exposure duration on their discrimination score, $F(1, 122) = 0.353$, $p = .553$. This result suggests that difference in ability to discriminate genuine from phishing emails between participants with a relatively higher and lower capacity for cue utilisation, was not affected by the email exposure duration. Therefore, compared to participants in the longer email exposure duration, participants in the shorter email exposure duration did not have a significantly greater difference in discrimination scores between participants with a higher and lower capacity for cue utilisation.

There was a statistically significant main effect of HAIS-Q score on discrimination scores, *F*(1, 122) = 8.425, *p* = .004, η^2 = .065. This finding supports H4, demonstrating that higher level of ISA, as indicated by HAIS-Q scores, is associated with a greater ability to discriminate between phishing and genuine emails. See Figure 2 for a visual representation of results

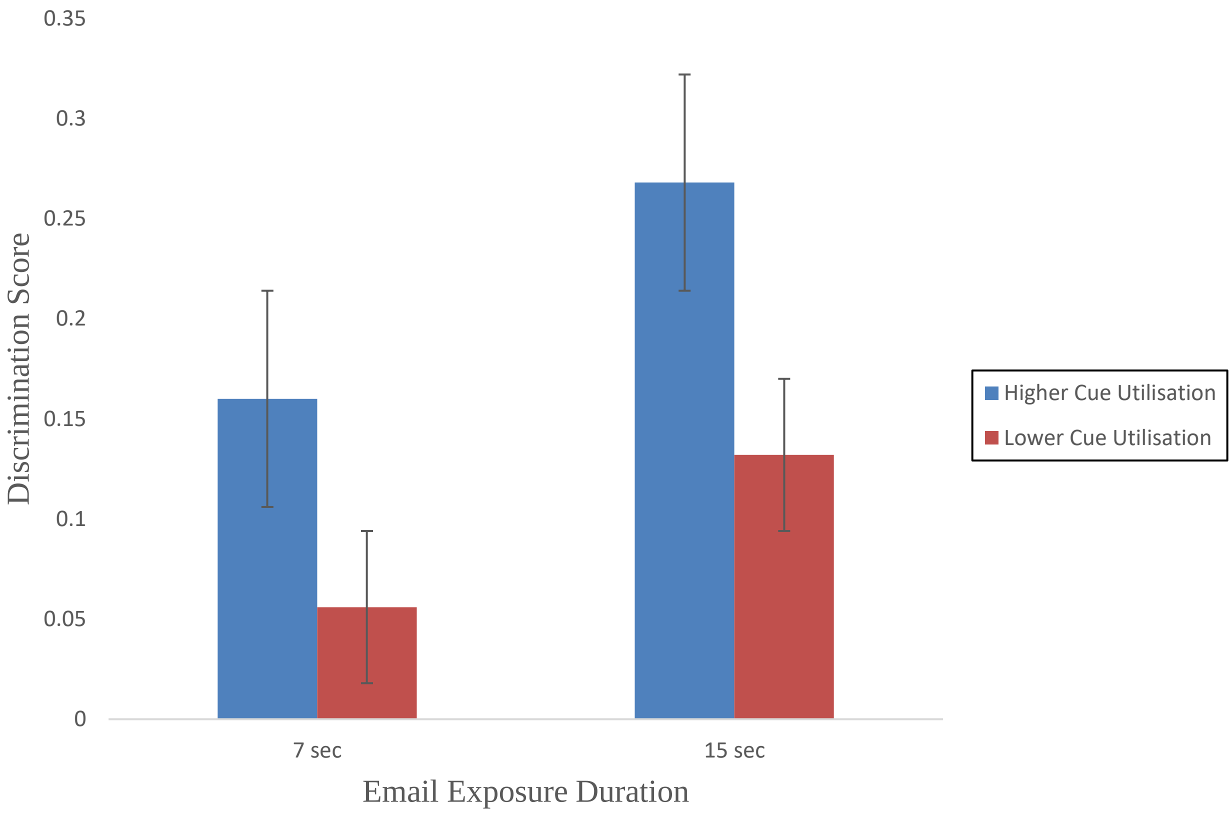


Figure 2. Participants' marginal mean discrimination scores for the higher and lower cue utilisation typology, in the shorter and longer email exposure duration. All means are controlled for the covariate HAIS-Q score at 35.50. Error bars represent standard error.

An independent samples t-test was conducted to investigate whether participants in the two cue utilisation typologies differed in their HAIS-Q scores. Results indicated a statistically significant difference in HAIS-Q scores for the higher (*M* = 36.71, *SD* = .687) compared to the lower (*M* = 34.18, *SD* = .653) cue utilisation typology; *t*(125) = 2.661, *p* = .009. This result suggests that participants with a relatively higher level of cue utilisation had a higher level of ISA, compared to those with a relatively lower level of cue utilisation.

Discussion

Overview

The current experiment aimed to examine the main effects of time pressure, cue utilisation, and ISA on participants' ability to discriminate between phishing and genuine emails. Cue utilisation, exposure time, and ISA were all found to be statistically significant predictors of discrimination ability. However, there was no statistically significant interaction between cue utilisation and exposure time. Cue utilisation was also found to be a statistically significant predictor of ISA.

Individual Differences and Discrimination Ability

Cue Utilisation and Discrimination Ability. H1 was supported, indicating that phishing cues present within illegitimate emails are more effectively accessed by individuals with a relatively higher level of cue utilisation. The effect size for this relationship was moderate, highlighting that cue utilisation is a relatively good predictor of phishing susceptibility.

This result was predicted, as higher cue utilisation represents improved ability to apply environmental cues (Sturman et al., 2019a), and has been shown to distinguish between more-effective and less-effective operators in varied environments (Brouwers et al., 2016; Sturman et al., 2019a; 2019b; Yuris et al., 2019). Therefore, higher cue utilisation was expected to result in effective assessment of a phishing situation. This expands the cue utilisation literature as phishing is affected by differences in cue utilisation and this individual difference can determine an individual’s phishing susceptibility.

This differs from previous research which found higher levels of cue utilisation did not translate to improved discrimination ability (Bayl-Smith et al., 2020). This difference could be explained by the current experiment’s email stimuli. Stimuli in the present study encompassed a wide range of subject and email types, to represent email variety within a real inbox. These exactly replicated real-world emails, and functioned as expected, as participants had the ability to hover-over and display hyperlinks. These factors improved the ecological validity of the present experiment as email stimuli represented their real-world counterparts as closely as possible, allowing participants to respond as they would in a natural setting. Furthermore, in the previous study, emails contained multiple phishing cues, causing those stimuli to possibly be too easy to detect (Bayl-Smith et al., 2020). While the current experiment’s stimuli varied in number and type of cues, allowing for varied results.

Information Security Awareness and Discrimination Ability. H4 was supported, indicating that participants with a higher score on the HAIS-Q, representing a higher level of ISA, had a greater ability to discriminate between phishing and genuine emails. This bolsters the previously established relationship between higher ISA and safe information security behaviours, as increased discrimination ability is an example of a safe information security behaviour.

This result was expected, as ISA is an operationalisation of cyber-risk beliefs (Parsons et al., 2017) formed through previous experience, that are accessed when a relevant situation occurs (Griffin et al., 2002). The results demonstrate that these beliefs were more effectively accessed by individuals with higher levels of ISA. Moreover, higher levels of ISA have previously been linked to reduced information security breaches (Sohrabi Safa et al., 2016). Therefore, improved discrimination ability results in more efficient identification of phishing emails, thus allowing for mitigation of such breaches. Previous research has demonstrated a relationship between higher ISA and detection of phishing links within emails (Parsons et al., 2017). The current experiment expands this relationship to include other phishing cues, additionally, higher ISA results in improved discrimination ability.

These findings strengthen the suggestion that the email-use focus area of the HAIS-Q can be used in a phishing context, separate from the rest of the questionnaire, and that the HAIS-Q can be used modularly (Parsons et al., 2017). Additionally, the HAIS-Q could be used in workplaces to identify individuals lacking in relevant knowledge, possessing a worse attitude, and potentially demonstrating unsafe information security behaviours.

Cue Utilisation and Information Security Awareness. H5 was supported, indicating individuals with better self-reported knowledge, attitude, and behaviour regarding information security, will have an improved objective ability to discriminate between phishing and genuine cues within emails.

This result was expected as greater knowledge of safe email-related information security behaviours will logically increase awareness of potential email phishing features. Previous results from the current experiment demonstrate higher levels of ISA result in better discrimination of environmental features, which is a necessary factor for cue utilisation (Wiggins, 2014a). Additionally, an understanding of the relatedness of features and events within operating environments, and the ability to prioritise correct features, are needed for cue utilisation (Wiggins, 2014a). Understanding of these factors will increase with knowledge of safe information security behaviours, resulting in better development of environmental cues and indicating a higher capacity for cue utilisation. Furthermore, these results indicate that safer self-reported information security behaviours translate to safer objectively measured behaviours in an operative environment. This provides a basis for future research into the relationship between these two variables, wherein one could predict the other.

Time Pressure and Discrimination Ability

H2 was supported, indicating the shorter email exposure duration, which aimed to apply time pressure to participants, resulted in a reduced ability to discriminate between phishing and genuine emails compared to those exposed to the email for longer. This suggests increased time pressure necessitates faster, less deliberative decision making, resulting in worse discrimination ability.

This was expected as novel or abnormal situational information necessitates the use of system 2 processing to reflect on system 1's initial intuitions, to determine if a change in decision is needed (Evans & Stanovich, 2013). Introducing time pressure may increase decision speed, possibly changing the decision mode and necessitating fast system 1 processing that utilises cues (Allen, 2011; Chowdhury et al., 2019; Kahneman, 2003). Previous research demonstrated habitual decision making, which is present in system 1, has caused increased phishing susceptibility (Vishwanath et al., 2011). Furthermore, a systematic review demonstrated that time pressure reduced safe cybersecurity behaviours in several contexts (Chowdhury et al., 2019). Therefore, an abnormal email feature may have been noticed, initiating the use of system 2, but this process was interrupted by the short time limit in the short email exposure duration, changing the decision mode and reducing discrimination ability.

Alternatively, participants may not have been able to identify all critical features within the email in the allocated time. Consequently, participants may not be changing the way the decision is made in the shorter email exposure duration, but instead the accessible information is reduced, and a decision is forced. In either case, this result emphasizes the need to reduce situational time pressure placed upon email-users, to reduce the number of people victimised by phishing attacks.

Chowdhury et al. (2019) identified three time pressure forms used in cyber-security literature; explicit, implicit, and self-referred. Explicit refers to a deadline being placed upon participants, while implicit implies this without explicitly enforcing a time limit. Self-referred time pressure involves a self-report of perceived time pressure, and the resultant consequences. The current experiment demonstrates the effect of explicit time pressure; however, future research could compare this to other identified forms, to determine differences in influence on discrimination ability.

Interaction between Cue Utilisation and Time Pressure on Discrimination Ability

H3 was not supported, indicating the difference in discrimination ability between relatively higher and lower cue utilisation individuals, was not affected by the email exposure duration. Relatively higher cue utilisation participants were expected to assess and apply cues within the emails at a faster rate than those with a relatively lower level (Sturman et al., 2019a). Moreover, higher cue utilisation would be more advantageous for participants in the shorter email exposure duration, as time pressure may result in reliance on cue-based intuitive decision making (Allen, 2011; Chowdhury et al., 2019; Kahneman, 2003). Thus, resulting in a greater difference in discrimination ability between higher and lower cue utilisation participants under time pressure, as higher cue utilisation participants could complete this process within the time limit.

However, this difference in discrimination ability between higher and lower cue utilisation individuals when under time pressure was not greater than when time pressure is reduced. Therefore, possessing higher levels of cue utilisation is not just advantageous when under time pressure but is beneficial when given longer to examine emails. This demonstrates that advantages associated with cue utilisation are not merely due to information processing speed, but increased effectiveness of processing producing better decisions when time pressure is reduced.

Furthermore, the longer email exposure duration (15 seconds) may, for some participants, still represent time pressure. Future research could include a wider range of email exposure durations, to determine whether an alternative duration may reveal a difference. Alternatively, including a no-time-pressure condition to examine whether cue utilisation continues to be advantageous when a decision can be made without a time limit. Otherwise, an unidentified factor could have resulted in participants within the shorter email exposure duration to have better than expected discrimination ability.

Implications of the Findings

The findings suggest reducing time pressure may reduce phishing susceptibility and improve cybersecurity behaviours. Consequently, workplaces could introduce interventions aiming to inform individuals of the risks associated with assessing emails while under time pressure. Policies could be enacted that reduce the number of received emails, allowing more time to review potentially illegitimate emails.

Furthermore, governmental awareness campaigns focusing on phishing could inform individuals about the dangers of time pressure and upon improving discrimination ability, instead of increasing bias towards risk-averse behaviour. A clear distinction should be made, as bias towards risk-averse behaviour causes genuine emails to be considered suspicious (Falkenberg et al., 2019), while improved discrimination will reduce these false alarms.

These results support the use of EXPERTise within workplaces to identify individuals with greater phishing susceptibility, improving the efficiency of workplace training allocation. This was an inaugural examination of the relationship between time pressure and discrimination ability, providing a basis for future research in this area. This experiment bolsters the existing phishing literature regarding individual differences, providing a possible design to be adapted and further applied.

Strengths

This experiment’s design, whereby participants were unaware the task was examining responses to phishing emails, is novel in phishing research examining individual differences. The design aimed to make the email assessment process as close as possible to how participants would assess their own emails, whilst remaining experimental. The roleplay aspect helped ensure participants remained unaware of the phishing-related nature, reduced subject-expectancy bias and added context to the categorisation decisions. Furthermore, the email stimuli exactly replicated real received emails and encompassed a large range of email and subject types. The large stimuli sample allowed the phishing to genuine email ratio to be akin to a real inbox while producing sufficient data points. Moreover, as the experiment was online, it remained closer to a natural email answering environment, allowing for similar distractions.

All these aspects lent ecological validity to the experiment; thus, increasing generalisability of the results. Similar role-play designs have been used previously (Parsons et al., 2015; 2019), and the current experiment follows suggestions for a large and diverse (in content) email sample (Parsons et al., 2015). Previous studies have involved sending crafted phishing emails to the real inbox of unknowing participants (Parsons et al., 2015), and while these provide useful indications of response rates, generalisability is reduced as only one email type can be sent. Moreover, the large participant sample recruited from student and public sources allowed for responses from a varied set of individuals, resulting in a wide age-range of participants. This furthered result generalisability, increased statistical power, and decreased the likelihood of type II errors, allowing more valid results to be produced.

Limitations and Future Directions

This experiment's time pressure conditions aimed to replicate time pressure that individuals may experience when responding to multiple emails each day. This manipulation was necessary to maintain experimental control and ensure study length did not extend beyond feasibility. However, it is unclear whether participants used all allocated time to assess the emails. For instance, participants in the 15 second condition may have only used 10 seconds to assess the email. Consequently, this manipulation may not capture real world responses, where individuals are free to vary the email assessment time. For example, an individual may quickly determine an email is genuine and not phishing but may require several minutes to determine whether a potential phishing email is phishing. Future research could include naturalistic experimental conditions where unlimited time is given to assess and categorise emails. Alternatively, participants could be given a block of time to classify multiple emails.

Future uses of a similar experimental design may benefit from including an open-ended question as a check near the study's conclusion, ensuring participants have not realised the true nature of the study. This would allow responses where participants realised the study was examining phishing to be identified and not included, to avoid invalid data. Additionally, a lab-based version of this experiment could be conducted, allowing examination of outcomes when potential variances are further controlled. This may also allow the studies length to be increased.

As time pressure is a novel variable to consider in conjunction with phishing susceptibility, future research could attempt to determine which individual differences best lessen its effects. Training could be designed aiming to teach individuals how to best minimise email assessment errors and minimise time pressure's effect by increasing email assessment efficiency. A wider variety of time pressure conditions could be examined, i.e. a low, high, and no-time-pressure context, to determine differences when reducing, compared to removing, time pressure.

Conclusion

The current study aimed to further the understanding of how time pressure, cue utilisation, and ISA influence the ability to discriminate between phishing and genuine emails. Time pressure was found to result in poorer discrimination ability. Furthermore, a relatively higher level of cue utilisation and a higher level of ISA resulted in improved discrimination ability. These two individual differences were found to be positively associated with each other. However, no interaction was found between cue utilisation and time pressure on discrimination ability. Future research is required to further examine these relationships to determine who is most at risk of phishing attacks, and how to minimise errors that cause people to fall susceptible to phishing.

References

Allen, D. (2011). Information behavior and decision making in time-constrained practice: A dual-processing perspective. *Journal of the American Society for Information Science and Technology*, *62*(11), 2165–2181. https://doi.org/10.1002/asi.21601

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

Australian Competition and Consumer Commission. (2020a). Scam statistics: Phishing 2019. Retrieved from: https://www.scamwatch.gov.au/scam-statistics?scamid=31&date=2019

Australian Competition and Consumer Commission. (2020b). Scam statistics: All scam types 2019. Retrieved from: https://www.scamwatch.gov.au/scam-statistics?scamid=all&date=2019

Australian Competition and Consumer Commission. (2020c). Scam statistics: Phishing 2020. https://www.scamwatch.gov.au/scam-statistics?scamid=31&date=2020

Australian Cyber Security Centre. (2020). Phishing. Retrieved from: https://www.staysmartonline.gov.au/protect-yourself/recover-when-things-go-wrong/phishing

Bandura, A. (1989). Human agency in Social Cognitive Theory. *American Psychologist*, *44*(9), 1175–1184. https://doi.org/10.1037/0003-066X.44.9.1175

Baranowski, T., Cullen, K. W., Nicklas, T., Thompson, D., & Baranowski, J. (2003). Are current health behavioral change models helpful in guiding prevention of weight gain efforts? *Obesity Research*, *11*(S10), 23S-43S. https://doi.org/10.1038/oby.2003.222

Bayl-Smith, P., Sturman, D., & Wiggins, M. (2020). Cue utilization, phishing feature and phishing email detection. *AsiaUSEC Conference 2020*. Retrieved from http://www.usablesecurity.net/USEC/asiausec20/papers/AsiaUSEC20_paper_8.pdf

Biselle, K., LaSalle, R., Dal Cin, P. (2019). The cost of cybercrime. Retrieved from: https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

Brouwers, S, Wiggins, M. W., Helton, W., O'Hare, D., & Griffin, B. (2016). Cue utilization and cognitive load in novel task performance. *Frontiers in Psychology*, 7(435), 1-12. https://doi.org/10.3389/fpsyg.2016.00435

Brouwers, S., Wiggins, M. W., Griffin, B., Helton, W. S., & O'Hare, D. (2017). The role of cue utilisation in reducing the workload in a train control task. *Ergonomics*, *60*(11), 1500–1515. https://doi.org/10.1080/00140139.2017.1330494

Brouwers, S., Wiggins, M., & Griffin, B. (2018). Operators who readily acquire patterns and cues, risk being miscued in routinized settings. *Journal of Experimental Psychology: Applied*, *24*(2), 261–274. https://doi.org/10.1037/xap0000151

Brunswik, E. (1955). Representative design and probabilistic theory in a functional psychology. *Psychological Review*, *62*(3), 193–217. https://doi.org/10.1037/h0047470

Butavicius, M., Parsons, K., Pattinson, M., Mccormac, A., Calic, D., & Lillie, M. (2017). Understanding susceptibility to phishing emails: Assessing the impact of individual differences and culture. *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017)* , *2016*(Haisa), 12–22.

Calic, D., Pattinson, M., Parsons, K., Butavicius, M., & McCormac, A. (2016). Naïve and accidental behaviours that compromise information security: What the experts think. In *Proceedings of the 10th International Symposium on Human Aspects of*

Information Security and Assurance, HAISA 2016 (pp. 12–21). University of Plymouth

Chowdhury, N. H., Adam, M. T. P., & Skinner, G. (2019). The impact of time pressure on cybersecurity behaviour: A systematic literature review. *Behaviour and Information Technology*, *38*(12), 1290–1308. https://doi.org/10.1080/0144929X.2019.1583769

Cialdini, R.B. (2009). Influence: Science and Practice. William Morrow, New York.

Evans, J. S. B. T., & Stanovich, K. E. (2013). Dual-process theories of higher cognition: Advancing the debate. *Perspectives on Psychological Science*, *8*(3), 223–241. https://doi.org/10.1177/1745691612460685

Falkenberg, A., Auton, J. C., Parsons, K. (2019). *The role of cue utilisation and anxiety on phishing email susceptibility.* Unpublished manuscript, School of Psychology, University of Adelaide, Adelaide, Australia.

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

Green, D. M., & Swets, J. A. (1966). Signal Detection Theory and Psychophysics. New York, NY: Wiley

Griffin, R. J., Neuwirth, K., Giese, J., & Dunwoody, S. (2002). Linking the heuristic-systematic model and depth of processing. *Communication Research*, *29*(6), 705-732+733. https://doi.org/10.1177/009365002237833

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. In *WWW 2013 Companion - Proceedings of the 22nd International Conference on World Wide Web* (pp. 737–744). Association for Computing Machinery. https://doi.org/10.1145/2487788.2488034

Hattie, J., & Cooksey, R. W. (1984). Procedures for assessing the validities of tests using the “Known-Groups” method. *Applied Psychological Measurement*, *8*(3), 295–305. https://doi.org/10.1177/014662168400800306

IBM Global Technology Services. (2015). IBM security services 2014 cyber security intelligence index.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94–100. https://doi.org/10.1145/1290958.1290968

Jansen, J., Leukfeldt, R. (2018). Coping with cybercrime victimization: An exploratory study into impact and change. *Journal of Qualitative Criminal Justice and Criminology*, *6*(2), 205–228.

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. https://doi.org/10.1080/07421222.2017.1334499

Kahneman, D. (2003, September). A perspective on judgment and choice: Mapping bounded rationality. *American Psychologist*, *58*(9), 697-720. https://doi.org/10.1037/0003-066X.58.9.697

Klein, G. (2008, June). Naturalistic decision making. *Human Factors*, *50*(3), 456-460. https://doi.org/10.1518/001872008X288385

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, *25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Lawson, P., Zielinska, O., Pearson, C., & Mayhorn, C. B. (2017). Interaction of personality and persuasion tactics in email phishing attacks. In *Proceedings of the Human*

Factors and Ergonomics Society (Vol. 2017-October, pp. 1331–1333). Human Factors an Ergonomics Society Inc. https://doi.org/10.1177/1541931213601815

Loveday, T., Wiggins, M. W., & Searle, B. J. (2014). Cue utilization and broad indicators of workplace expertise. *Journal of Cognitive Engineering and Decision Making*, *8*(1), 98–113. https://doi.org/10.1177/1555343413497019

Loveday, T., Wiggins, M. W., Harris, J. M., O'Hare, D., & Smith, N. (2013b). An objective approach to identifying diagnostic expertise among power system controllers. *Human Factors*, *55*(1), 90–107. https://doi.org/10.1177/0018720812450911

Loveday, T., Wiggins, M., Festa, M., Schell, D., & Twigg, D. (2013a). Pattern recognition as an indicator of diagnostic expertise. *Advances in Intelligent Systems and Computing*, *204*(Jan), 1–11. https://doi.org/10.1007/978-3-642-36530-0_1

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. https://doi.org/10.1016/j.cose.2012.12.003

Marett, K., & Wright, R. (2009). The effectiveness of deceptive tactics in phishing. In *AMCIS 2009 Proceedings*. Paper 340. http://aisel.aisnet.org/amcis2009/340

McClanahan, W., van der Linden, S., & Ruggeri, K. (2019). Decision-making style mediates the relationship between trait self-control and self-reported criminal behavior. *Personality and Individual Differences*, *151*, 109537. https://doi.org/10.1016/j.paid.2019.109537

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., & Pattinson, M. (2017a). A reliable measure of Information Security Awareness and the identification of bias in responses. *Australasian Journal of Information Systems*, *21*. https://doi.org/10.3127/ajis.v21i0.1697

McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., & Lillie, M. (2018). The effect of resilience and job stress on information security awareness. *Information and Computer Security*, *26*(3), 277–289. https://doi.org/10.1108/ICS-03-2018-0032

McCormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M., & Pattinson, M. (2016). Test-retest reliability and internal consistency of the human aspects of information security questionnaire (HAIS-Q). In *Proceedings of the 27th Australasian Conference on Information Systems, ACIS 2016*. University of Wollongong, Faculty of Business.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017b). Individual differences and Information Security Awareness. *Computers in Human Behavior*, *69*, 151–156. https://doi.org/10.1016/j.chb.2016.11.065

McCormack, C., Wiggins, M. W., Loveday, T., & Festa, M. (2014). Expert and competent non-expert visual cues during simulated diagnosis in intensive care. *Frontiers in Psychology*, *5*(949). https://doi.org/10.3389/fpsyg.2014.00949

Mcnab, A. L., Hess, T. J., & Valacich, J. S. (2009). Designing emergency response applications for better performance. In *ICIS 2009 Proceedings - Thirtieth International Conference on Information Systems*.

Moody, G. D., Galletta, D. F., & Dunn, B. K. (2017). Which phish get caught? An exploratory study of individuals′ susceptibility to phishing. *European Journal of Information Systems*, *26*(6), 564–584. https://doi.org/10.1057/s41303-017-0058-x

Morrison, B. W., Wiggins, M. W., Bond, N. W., & Tyler, M. D. (2013). Measuring relative cue strength as a means of validating an inventory of expert offender profiling cues. *Journal of Cognitive Engineering and Decision Making*, *7*(2), 211–226. https://doi.org/10.1177/1555343412459192

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

Parsons, K., Butavicius, M., Pattinson, M., McCormac, A., Calic, D., & Jerram, C. (2015). Do users focus on the correct cues to differentiate between phishing and genuine emails? In *ACIS 2015 Proceedings - 26th Australasian Conference on Information Systems*. Association for Information Systems.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers and Security*, *66*, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). An analysis of information security vulnerabilities at three Australian government organisations. In *Proceedings of the European Information Security Multi-Conference, EISMC 2013* (pp. 34–44). Plymouth University.

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

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Jerram, C. (2015). Examining attitudes toward information security behaviour using mixed methods. In *Proceedings* *of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015* (pp. 57–70). University of Plymouth.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., Calic, D., & Jerram, C. (2016). The information security awareness of bank employees. In *Proceedings of the 10th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2016* (pp. 189–198). University of Plymouth.

Pauley, K., O'Hare, D., & Wiggins, M. (2009). Measuring expertise in weather-related aeronautical risk perception: The validity of the Cochran-Weiss-Shanteau (CWS) index. *International Journal of Aviation Psychology*, *19*(3), 201–216. https://doi.org/10.1080/10508410902979993

Rekouche, K. (2011) Early Phishing. Retrieved from: https://arxiv.org/ftp/arxiv/papers/1106/1106.4692.pdf

SANS Institute (2020) Information Security References. Retrieved from: https://www.sans.org/information-security/#free

Schriver, A. T., Morrow, D. G., Wickens, C. D., & Talleur, D. A. (2008). Expertise differences in attentional strategies related to pilot decision making. In *Proceedings of the Human Factors and Ergonomics Society* (Vol. 1, pp. 21–25). https://doi.org/10.4324/9781315095080-25

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Conference on Human Factors in Computing Systems - Proceedings* (Vol. 1, pp. 373–382). https://doi.org/10.1145/1753326.1753383

Small, A. J., Wiggins, M. W., & Loveday, T. (2014). Cue-based processing capacity, cognitive load and the completion of simulated short-duration vigilance tasks in power transmission control. *Applied Cognitive Psychology*, *28*(4), 481–487. https://doi.org/10.1002/acp.3016

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, *56*, 1–13. https://doi.org/10.1016/j.cose.2015.10.006

Sturman, D., Wiggins, M. W., Auton, J. C., & Loft, S. (2019a). Cue utilization differentiates resource allocation during sustained attention simulated rail control tasks. *Journal of Experimental Psychology: Applied*, *25*(3), 317–332. https://doi.org/10.1037/xap0000204

Sturman, D., Wiggins, M. W., Auton, J. C., Loft, S., Helton, W. S., Westbrook, J. I., & Braithwaite, J. (2019b). Control room operators' cue utilization predicts cognitive resource consumption during regular operational tasks. *Frontiers in Psychology*, *10*(AUG). https://doi.org/10.3389/fpsyg.2019.01967

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 Systems*, *51*(3), 576–586. https://doi.org/10.1016/j.dss.2011.03.002

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/TPC.2012.2208392

Watkinson, J., Bristow, G., Auton, J., McMahon, C. M., & Wiggins, M. W. (2018). Postgraduate training in audiology improves clinicians' audiology-related cue utilisation. *International Journal of Audiology*, *57*(9), 681–687. https://doi.org/10.1080/14992027.2018.1476782

Weiss, D. J., & Shanteau, J. (2003, March). Empirical assessment of expertise. *Human Factors*. https://doi.org/10.1518/hfes.45.1.104.27233

Wiggins, M. W. (2014a). The role of cue utilisation and adaptive interface design in the management of skilled performance in operations control. *Theoretical Issues in Ergonomics Science*, *15*(3), 283–292. https://doi.org/10.1080/1463922X.2012.724725

Wiggins, M. W. (2014b). Measuring diagnostic skills through the utilization of cues. In *Proceedings of the Human Factors and Ergonomics Society* (Vol. 2014-January, pp. 2345–2349). Human Factors an Ergonomics Society Inc. https://doi.org/10.1177/1541931214581488

Wiggins, M. W., & O'Hare, D. (2003). Expert and novice pilot perceptions of static in-flight images of weather. *International Journal of Aviation Psychology*, *13*(2), 173–187. https://doi.org/10.1207/S15327108IJAP1302_05

Wiggins, M. W., Azar, D., Hawken, J., Loveday, T., & Newman, D. (2014). Cue-utilisation typologies and pilots' pre-flight and in-flight weather decision-making. *Safety Science*, *65*, 118–124. https://doi.org/10.1016/j.ssci.2014.01.006

Wiggins, M.W., Loveday, T., Auton, J.C.: EXPERT Intensive Skills Evaluation (EXPERTise) Test. Macquarie University, Sydney (2015).

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers and Security*, *88*. https://doi.org/10.1016/j.cose.2019.101640

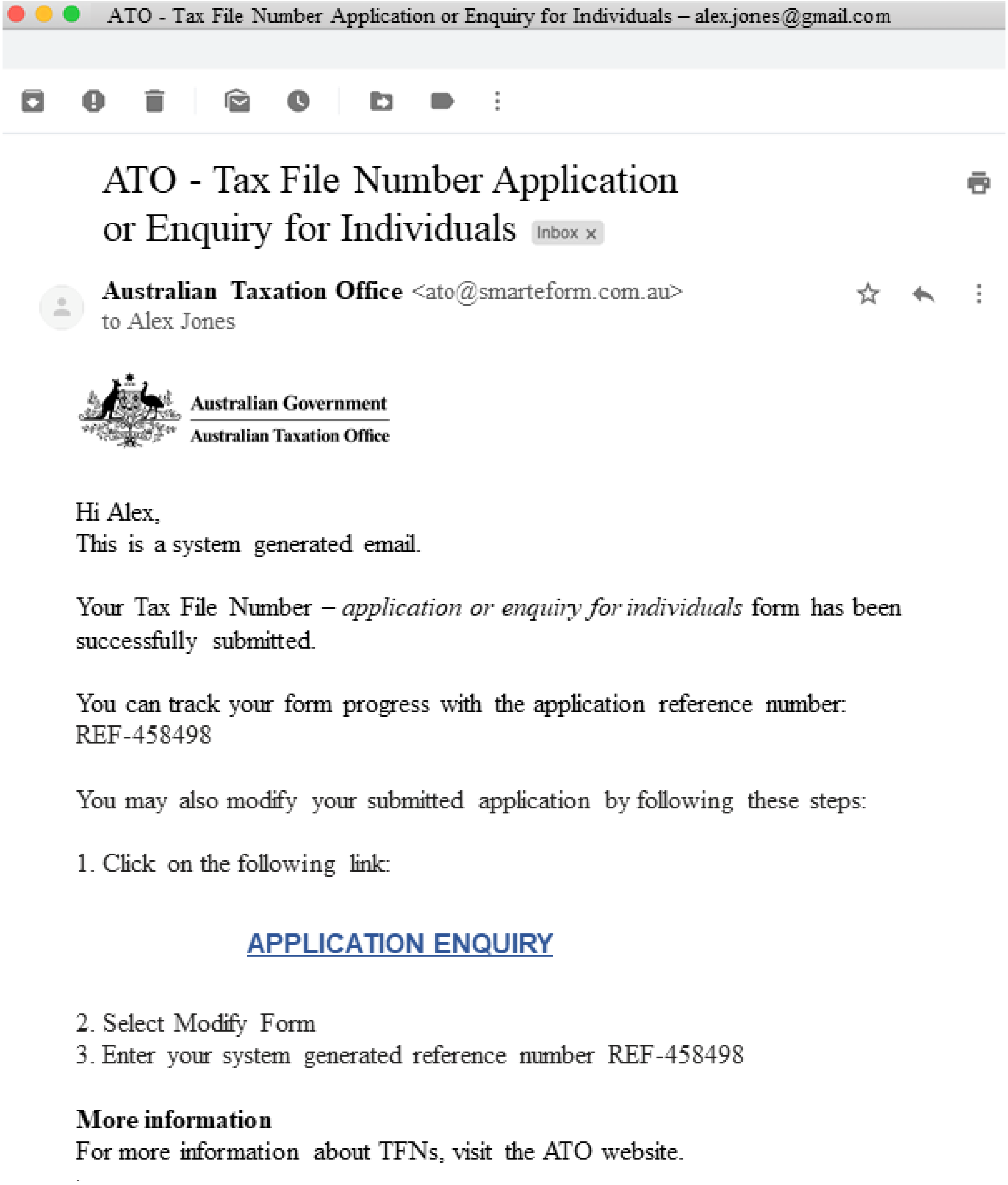
Xu, Z., & Zhang, W. (2012). Victimized by phishing: A heuristic-systematic perspective. *The Journal of Internet Banking and Commerce*, 17, 1-16.

Yang, H., & Thompson, C. (2016). Capturing judgement strategies in risk assessments with improved quality of clinical information: How nurses' strategies differ from the ecological model. *BMC Medical Informatics and Decision Making*, *16*(1). https://doi.org/10.1186/s12911-016-0243-1

Yuris, N. C., Wiggins, M. W., Auton, J. C., Gaicon, L., & Sturman, D. (2019). Higher cue utilization in driving supports improved driving performance and more effective visual search behaviors. *Journal of Safety Research*, *71*, 59–66. https://doi.org/10.1016/j.jsr.2019.09.008

Appendix A: Email Stimuli Examples

Genuine Email Stimulus



ATO - Tax File Number Application or Enquiry for Individuals – alex.jones@gmail.com

ATO - Tax File Number Application or Enquiry for Individuals

Australian Taxation Office <ato@smarteform.com.au>
to Alex Jones

Hi Alex,
This is a system generated email.

Your Tax File Number – *application or enquiry for individuals* form has been successfully submitted.

You can track your form progress with the application reference number:
REF-458498

You may also modify your submitted application by following these steps:

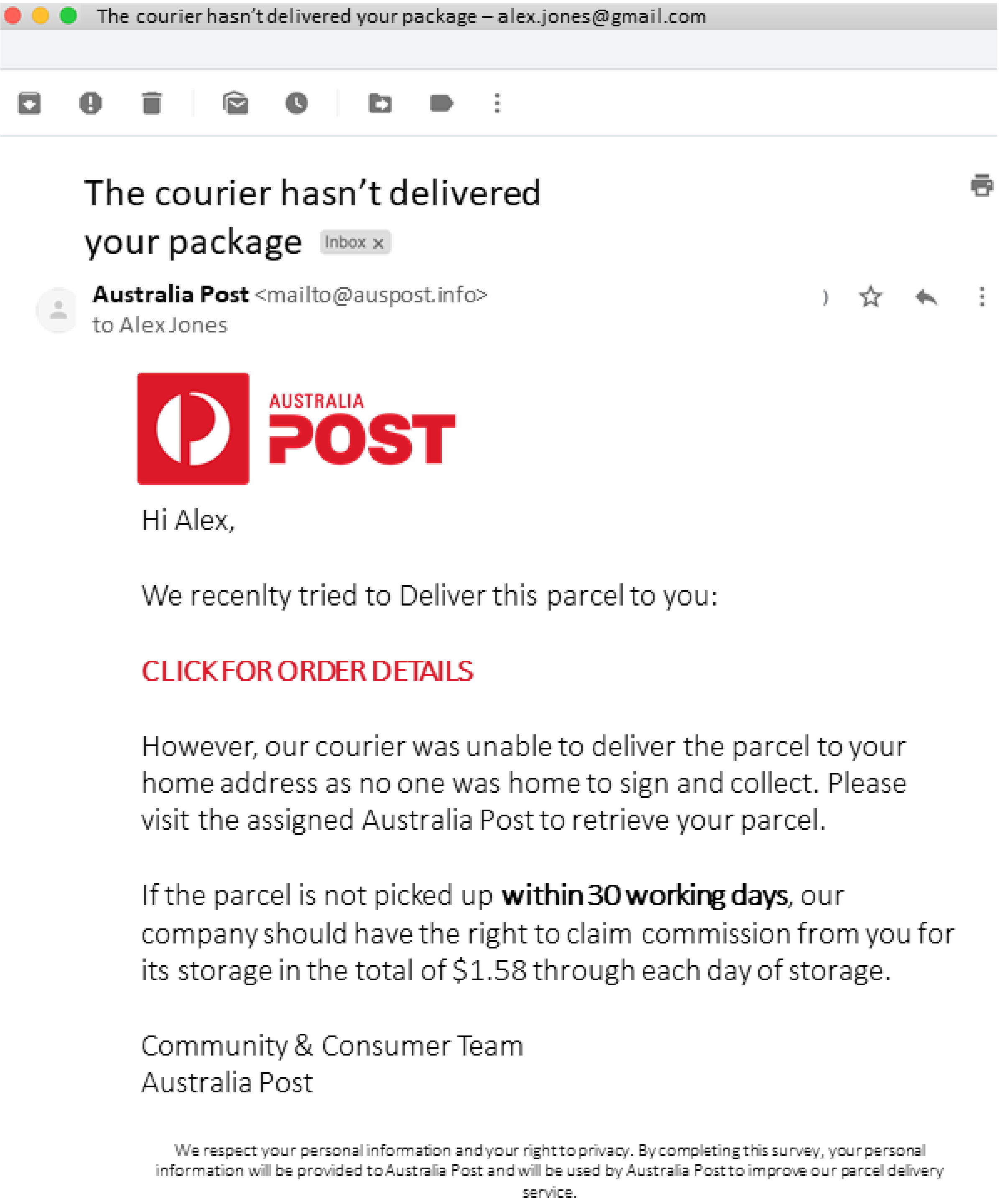
1. Click on the following link:

APPLICATION ENQUIRY

2. Select Modify Form
3. Enter your system generated reference number REF-458498

More information
For more information about TFNs, visit the ATO website.

Phishing Email Stimulus: Cue - Spelling/Grammar Mistake



The courier hasn't delivered your package – alex.jones@gmail.com

The courier hasn't delivered your package

Australia Post <mailto@auspost.info>
to Alex Jones

Hi Alex,

We recenlty tried to Deliver this parcel to you:

CLICK FOR ORDER DETAILS

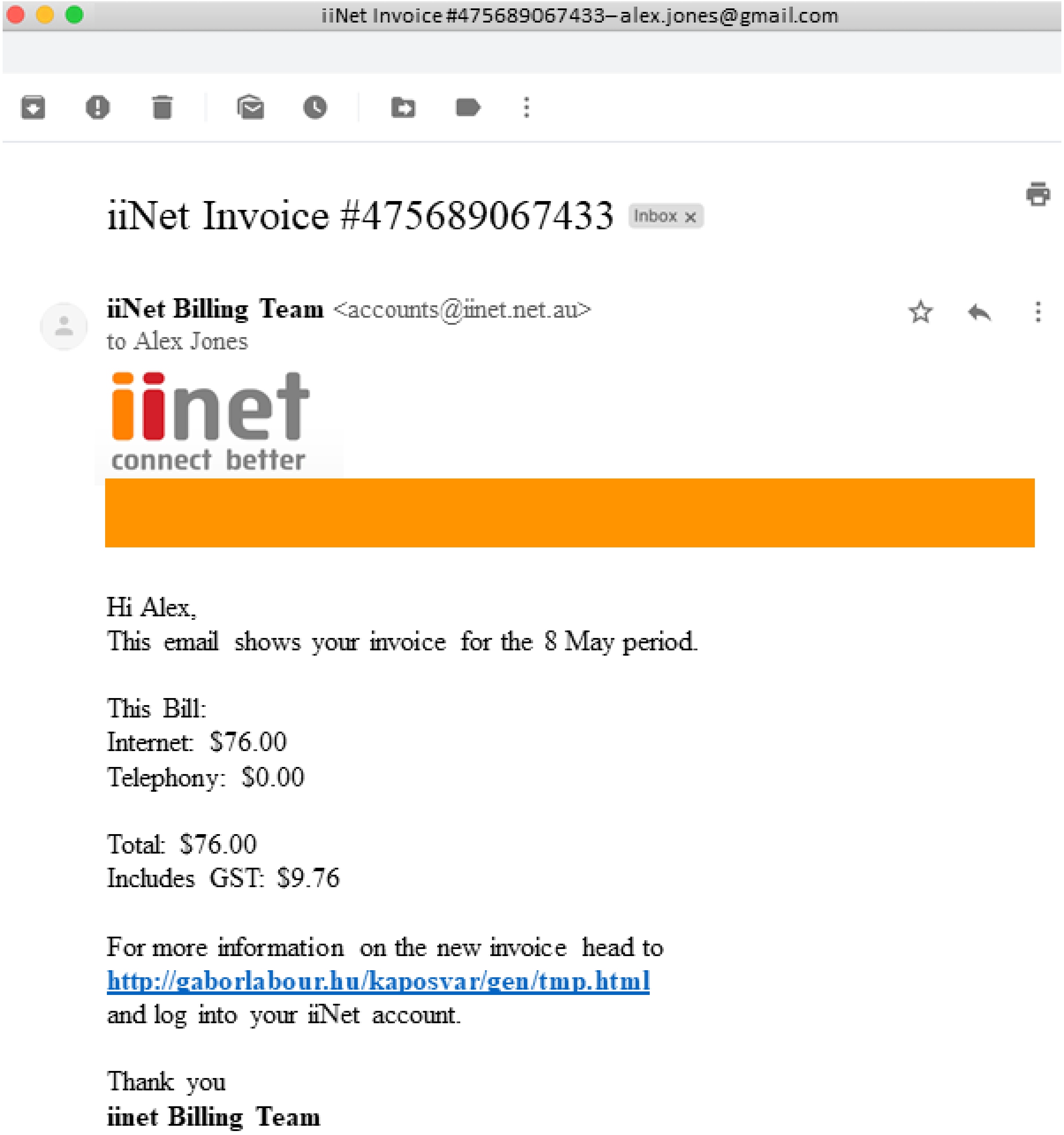
However, our courier was unable to deliver the parcel to your home address as no one was home to sign and collect. Please visit the assigned Australia Post to retrieve your parcel.

If the parcel is not picked up **within 30 working days**, our company should have the right to claim commission from you for its storage in the total of $1.58 through each day of storage.

Community & Consumer Team
Australia Post

We respect your personal information and your right to privacy. By completing this survey, your personal information will be provided to Australia Post and will be used by Australia Post to improve our parcel delivery service.

Phishing Email Stimulus: Cue – Illegitimate URL



iiNet Invoice #475689067433

iiNet Billing Team <accounts@iinet.net.au>
to Alex Jones

Hi Alex,
This email shows your invoice for the 8 May period.

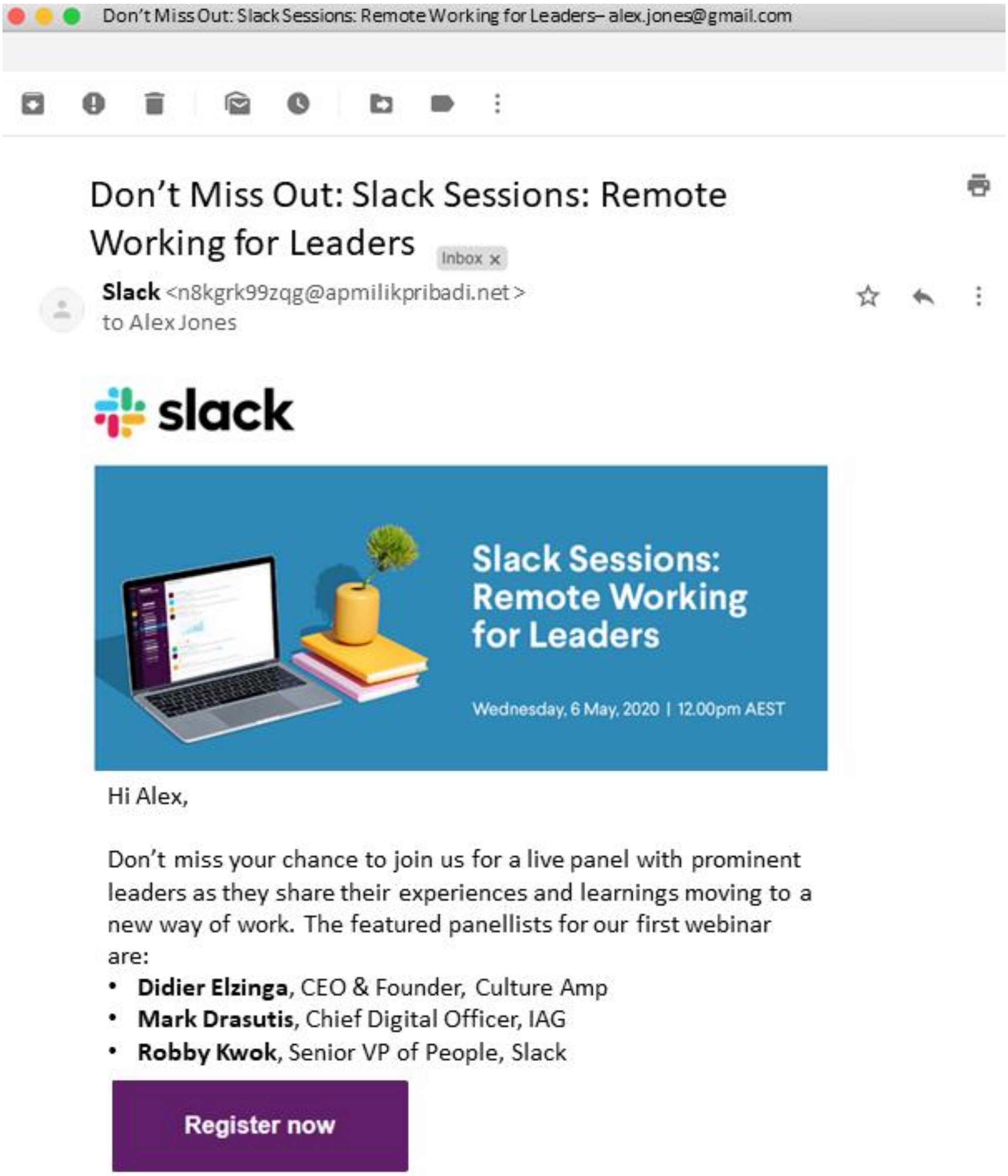
This Bill:
Internet: $76.00
Telephony: $0.00

Total: $76.00
Includes GST: $9.76

For more information on the new invoice head to
http://gaborlabour.hu/kaposvar/gen/tmp.html
and log into your iiNet account.

Thank you
iinet Billing Team

Phishing Email Stimulus: Cue – Illegitimate Sender's Address



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

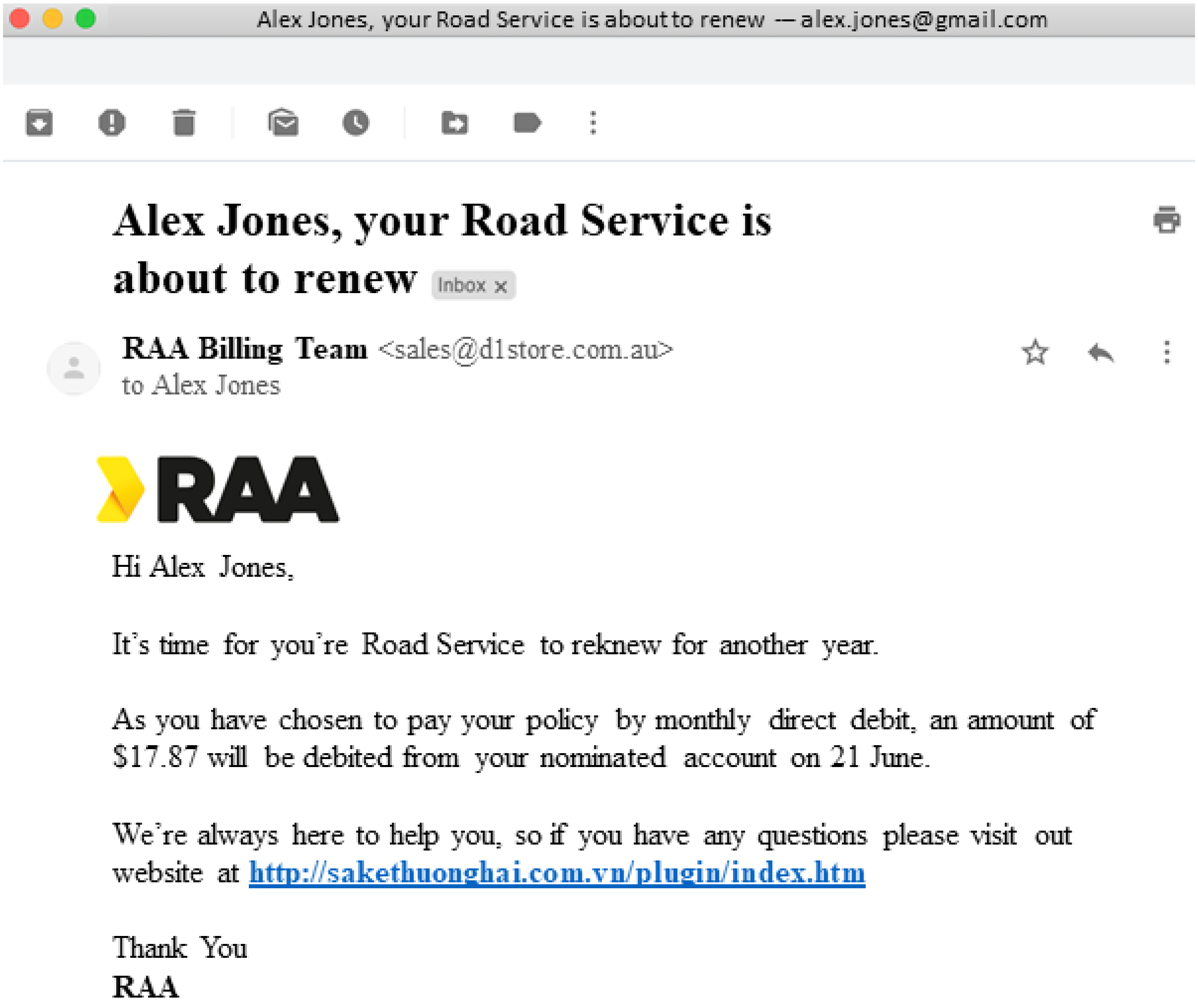
slack
Slack Sessions: Remote Working for Leaders
Wednesday, 6 May, 2020 | 12.00pm AEST

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

Phishing Email Stimulus: Cue – All 3 Phishing Cues



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

Alex Jones, your Road Service is about to renew

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

Hi Alex Jones,

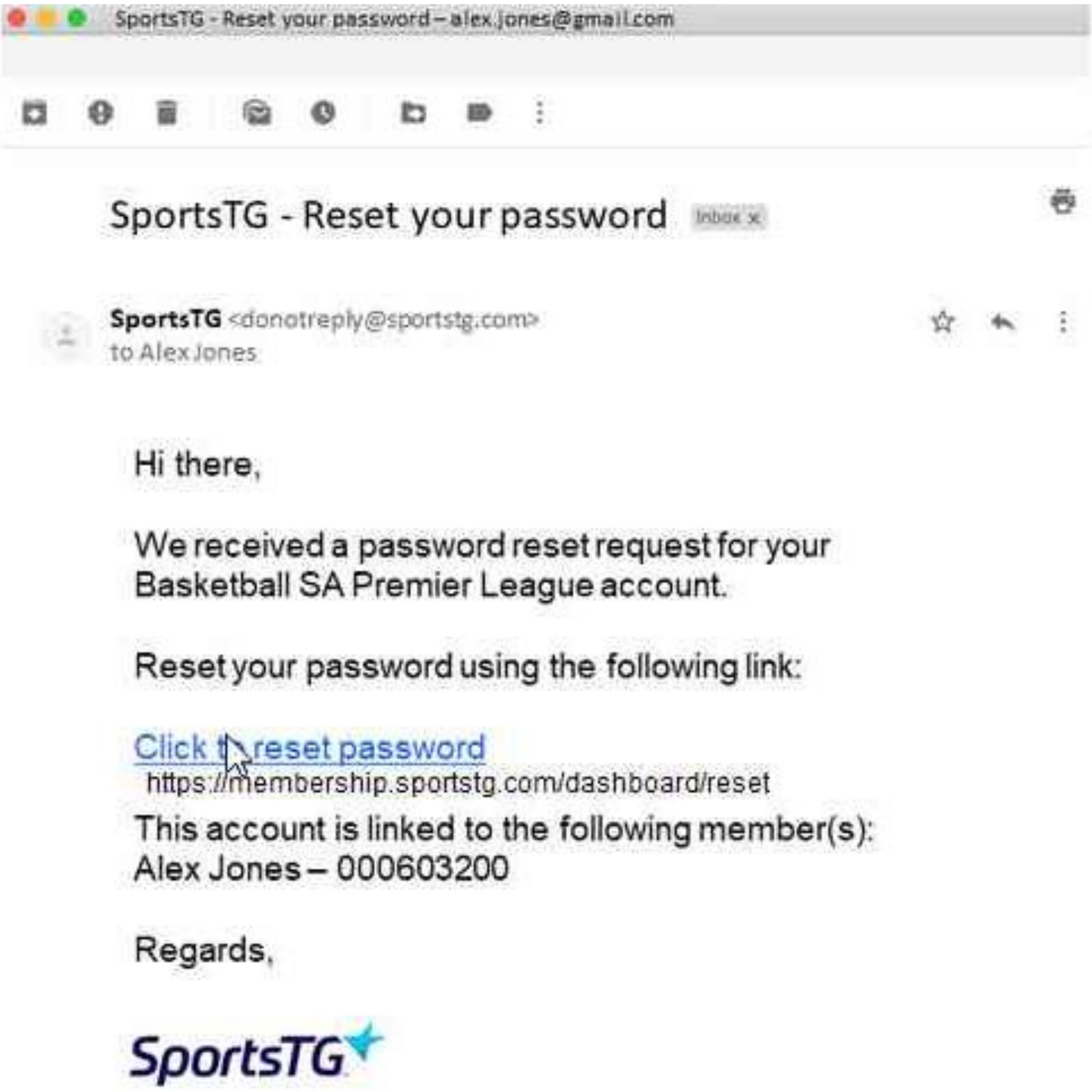
It’s time for you’re Road Service to reknew for another year.

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: Hover-over Function within an Email Stimulus



SportsTG - Reset your password – alex.jones@gmail.com

SportsTG - Reset your password

SportsTG <donotreply@sportstg.com>
to Alex Jones

Hi there,

We received a password reset request for your Basketball SA Premier League account.

Reset your password using the following link:

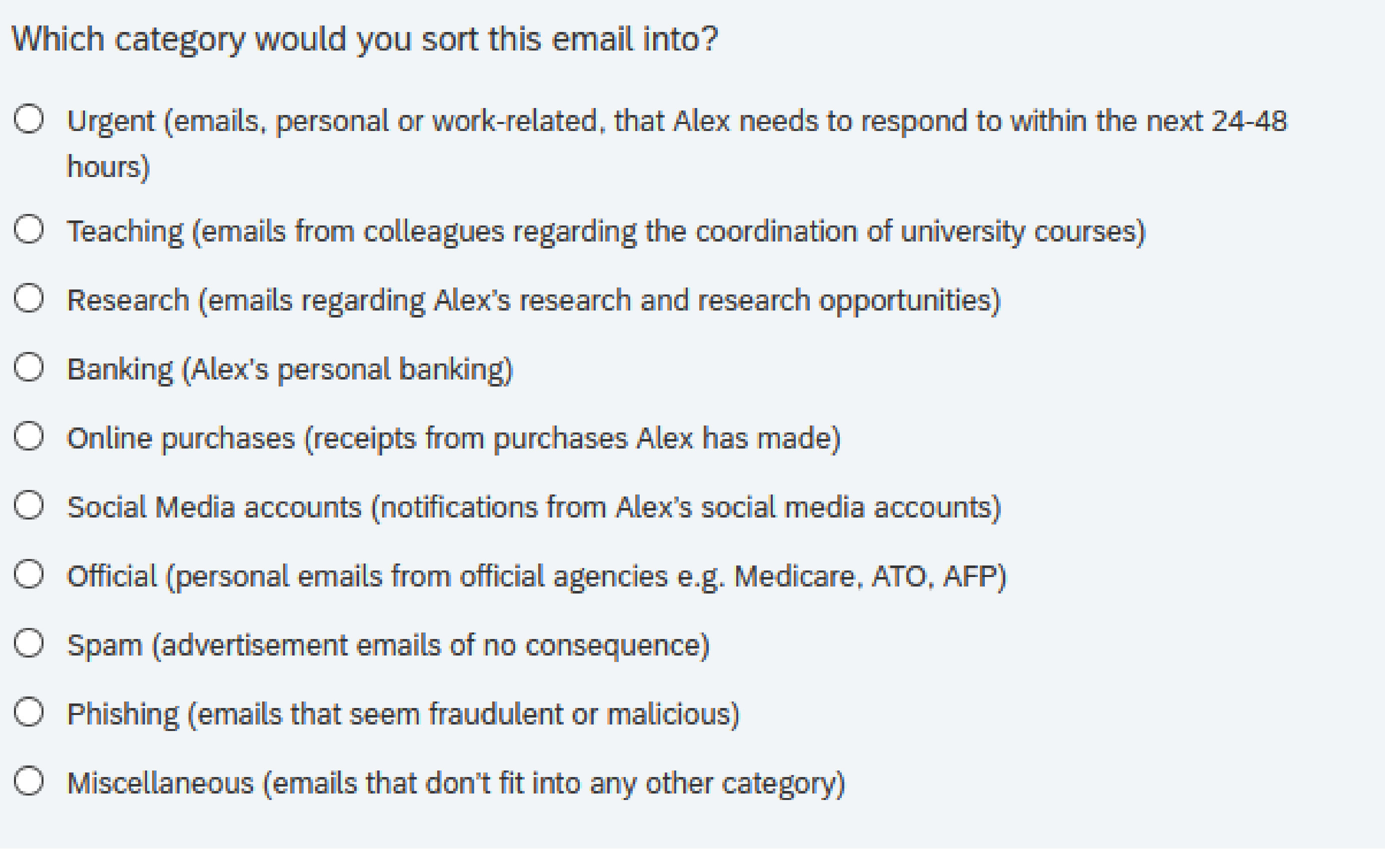
Click to reset password
https://membership.sportstg.com/dashboard/reset

This account is linked to the following member(s):
Alex Jones – 000603200

Regards,

SportsTG

Appendix C: Descriptions for Email Categorisation Options



Which category would you sort this email into?

○ 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)