

The Individual Differences in Cue Utilisation, Decision Making, and Time Pressure on Phishing
Susceptibility

Chelsea Valenzuela

Word Count: 9,036

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

School of Psychology

University of Adelaide

September 2021

Table of Contents

List of Figures.....	5
List of Tables.....	6
Abstract.....	7
Declaration.....	8
Contribution Statement.....	9
Acknowledgements.....	10
The Individual Differences in Cue Utilisation, Decision Making, and Time Pressure on Phishing Susceptibility.....	11
Background.....	11
Individual Differences in Phishing Susceptibility.....	14
Cue Utilisation.....	14
Cue Utilisation in Phishing.....	16
Decision-Making Styles.....	17
Decision Making Styles and Phishing Detection.....	19
Time Pressure and Decision Making Style.....	19
Cue Utilisation and Decision Styles.....	20
Current Study.....	21
Hypotheses.....	22
Method.....	23

Participants.....	23
Materials	23
<i>Demographic Questions</i>	23
<i>Email Sorting Task</i>	23
Measures	25
<i>Decision Making Style Scale</i>	25
<i>EXPERTise 2.0 (Phishing Edition)</i>	26
<i>Procedure</i>	27
Results	28
Overview of Analyses.....	28
Data Reduction.....	28
Decision Making Style Preferences.....	28
Phishing Detection Scores	29
Data Analysis	29
Discussion.....	33
Cue Utilisation and Phishing Detection.....	33
Decision Making Preferences and Phishing Detection.....	34
Interaction Between Decision Making Preference and Cue Utilisation on Phishing Detection.....	35
Implications of Findings	38

Strengths	40
Limitations and Future Direction	42
Conclusion	43
Appendix A: Email Stimuli Examples	51
Genuine Email Stimulus	51
Phishing Email Stimulus: Cue – Phishing/Illegitimate URL	52
Phishing Stimuli: Cue – All 3 Phishing Cues	53
Appendix B: Function to hover-over link button to reveal URL within email stimulus	54
Appendix C: Email categorisation options and their descriptions in the Email-Sorting Task	55
Appendix D: Adapted Decision-Making Scale Items (Hamilton et al., 2016)	56
Email-Specific (Clicking on a Link) Scale:	56

List of Figures

Figure 1: Participants' performance on phishing detection for the higher and lower cue utilisation typology, in the shorter and longer email exposure duration.....31

List of Tables

Table 1: Participant Cluster Means for the EXPERTise 2.0 Measures Across the Two Cue
Utilisation Typologies.....29

Abstract

Phishing attacks rely on human error to successfully scam individuals. To avoid being scammed, individuals must identify features of an email which indicate that the email is not genuine. These features include spelling and grammatical mistakes, suspicious URL links, and unrecognisable sender addresses. Through repeated exposure, relationships between these features are developed and stored in long-term memory as cues. Cue utilisation is the individual difference in the capacity to identify and apply cues. Additionally, time constraints and decision-making preferences (rational vs intuitive) may impact phishing email detection. The current study investigates the role of individual differences in phishing susceptibility by examining the relationships between phishing detection and cue utilisation, time pressure, and decision-making preferences. Undergraduate psychology students ($N = 200$) were tested on their ability to detect phishing emails. Participants were randomly assigned to either a short (7-second) or long (15-second) time condition and were presented with 60 emails (50 genuine and 10 phishing). After each email was presented, participants sorted the email into one of ten categories. They were then asked about how safe they thought it would be to click on the link. Participants also completed an email version of the decision-making preference scale and a software to measure cue utilisation in the domain of phishing emails. Results revealed higher cue utilisation, a preference for rational decision-making, and lower time pressure all predicted greater detection of phishing emails. Outcomes of this study may help organisations with the development of cybersecurity training that aims to reduce phishing susceptibility.

Keywords: Phishing Susceptibility, Cue Utilisation, Decision-Making Styles, Time Pressure

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 2021

Contribution Statement

For this thesis, my supervisors and I collaborated to formulate the research questions and variables of interest. I developed and adapted a decision making scale to be relevant to the context of emails. I was responsible for completing all of the data collection including recruitment of participants, testing, and allocation of credit. I collated and formatted all of the data from the experiment. My supervisor and I collaborated to analyse the data in SPSS.

I wrote up all aspects of this thesis.

Acknowledgements

I would like to express my deepest gratitude for my supervisors, Dr. Daniel Sturman and Dr. Jaime Auton. Their continuous guidance and productive conversations have inspired me to reach my potential and produce my best work. Thank you, Daniel, for guiding me. I appreciate your patience, quick email responses, and consistent reliability. I have gained so much knowledge from your insight and feedback and will always appreciate all that I have learned this year.

I also want to thank my partner Zac for his continuous loving support and encouragement every step of the way. I wouldn't be where I am today without your reassurance and emotional support. I want to express my gratitude to the Holmes family for making a home for me here in Australia, and especially Shayne and Bettie for their pep talks and words of wisdom to keep me motivated.

I would also like to thank Linda, for being such a kind and empathetic friend during these stressful times. I would also like to thank Maddie for her tokens of advice. I am so grateful to have such great friends to have gone through this honours year with.

Thank you to my family and friends back home in California for their support. This is dedicated to my sweet childhood dog ChaCha, who left us during the writing of this thesis.

The Individual Differences in Cue Utilisation, Decision Making, and Time Pressure on Phishing Susceptibility

Background

Phishing is a cyber-attack, usually delivered via email, that attempts to access personal and confidential information from individuals or organisations. Phishing perpetrators use social engineering techniques to trick email recipients into providing this information (Ferreira et al., 2015). Social engineering techniques are ways that perpetrators psychologically manipulate individuals into performing an action or sharing private information (Ferreira et al., 2015). An action is typically a response to an email from the phishing perpetrator containing private information or the user clicking on a fraudulent link. If a victim clicks on a fraudulent link, phishers may prompt the user for their login details or can also install malware onto a user's device, giving them access to personal information including usernames, passwords, bank details, and other identifying information (Aleroud & Zhou, 2017).

Phishing can lead to financial losses at individual or organisational levels from data breaches that expose the victim's private or classified information (Vishwanath et al., 2011). Successful phishing attacks have also been shown to erode trust in the security of online payment systems (Vishwanath et al., 2011). Consequently, with the increasing prevalence of electronic commerce, consumer mistrust in online payment systems can result in large financial losses. Data breaches will not only cause financial losses from a decrease in electronic commerce traffic but can also result in the theft of large sums of money from private individuals or organisations as well. Such consequences of successful phishing attacks have been associated with a financial

loss of almost \$3 million AUD in 2021 (Australian Competition & Consumer Commission, 2021) and up to \$1 trillion USD to date worldwide (Bose et al., 2008).

Alongside financial losses, phishing can result in psychological, social, and physical impacts from the threat to identity security (Jansen & Leukfeldt, 2018). Victims of phishing can exhibit a reduction in confidence of their online security, self-trust in navigating tasks online, and the trust held in those around them (Jansen & Leukfeldt, 2018). Psychological and physical effects can include anxiety, difficulties in concentrating, a lowered self-esteem, and difficulty in sleeping or sleep loss (Jansen & Leukfeldt, 2018).

Given the negative financial and psychological impacts of phishing attacks, considerable resources have been devoted towards developing anti-phishing software (Luo et al., 2013; Xu & Zhang, 2012). Phishing perpetrators are constantly improving their baiting techniques to penetrate such software. As a result, they are quickly evolving to circumvent updated security measures and exploit weaknesses in the software to create emails that appear more realistic (Vishwanath et al., 2011). These applications and technologies designed specifically to filter phishing emails before they reach the user are unable to identify and suppress every attempt (McCormac et al., 2018; Vishwanath et al., 2011). Perpetrators take advantage of this by exploiting human error and cognitive biases to successfully scam individuals (Parsons et al., 2019; Vishwanath et al., 2011). A report from IBM's Cyber Security Index revealed that 95 percent of cyber security incidents were ultimately caused by human error (IBM, 2014). Consequently, humans must act as the last line of defence by discerning between genuine emails and phishing attempts.

Phishing emails take advantage of human error and cognitive biases by invoking a sense of urgency and appeal to authority. This exploits the primary reasons that may cause an individual to fall victim to a phishing email: limited amount of time, and inattention to various features and signifiers within the phishing email (Chowdhury et al., 2019; Wang et al., 2012). In this way, a phishing email is designed to cause the email user to panic and rush their decisions, influencing them to perform an action like clicking on a malicious link (Chowdhury et al., 2019; Wang et al., 2012). If individuals were able to relieve time pressures and were better equipped to identify critical features of phishing attempts to discriminate legitimate from fraudulent emails, they might have a better chance at detecting when an email is a potential phishing attempt (Allen et al., 2011; Chowdhury et al., 2019).

Phishing emails take advantage of human error and cognitive biases by invoking a sense of urgency and appeal to authority. This exploits the primary reasons that may cause an individual to fall victim to a phishing email: limited amount of time, and inattention to various features and signifiers within the phishing email (Chowdhury et al., 2019; Wang et al., 2012). Phishing perpetrators use social engineering techniques to design their emails to cause the email user anxiety or panic and rush their decisions (Ferreira et al., 2015; Gupta et al., 2017), influencing them to perform an action like clicking on a malicious link (Chowdhury et al., 2019; Wang et al., 2012). This reduces the amount of time the user has to examine or question the email, in turn reducing their likelihood of noticing inconsistencies or atypical features that reveal the email to be a phishing attack. If individuals were able to relieve time pressures and were better equipped to identify critical features of phishing attempts to discriminate legitimate from fraudulent emails, they might have a better chance at detecting when an email is a potential phishing attempt (Bayl-Smith et al., 2020; Nasser et al., 2020).

Individual Differences in Phishing Susceptibility

Research conducted on phishing susceptibility has generally centred around demographic information such as age, gender, and internet usage (Sheng et al., 2010; Moody et al., 2017); however, conclusions drawn in the literature were found to contradict each other. For example, investigations into gender differences (Halevi et al., 2013; Jagatic et al., 2007; Sheng et al., 2010) concluded that women were more susceptible to phishing attacks, which was contradicted by the findings of negligible differences in susceptibility between men and women by Butavicius et al. (2017) and Parsons et al. (2019). Phishing susceptibility with age has yielded a similar occurrence. Some studies found a decreased susceptibility with age (Parsons et al., 2019; Sheng et al., 2010), while others found no difference (Moody et al., 2017). In the case of internet usage, Parsons et al. (2019) found that those who are more familiar with computers can better detect phishing emails. On the contrary, Moody and colleagues (2017) found that a higher frequency in internet usage made it more likely for an individual to be susceptible to phishing. While there is little difference found in phishing susceptibility based on age, gender, and internet usage, there is evidence to suggest that individual differences in cognitive processing, such as cue utilisation and decision-making preferences, may be better predictors of phishing susceptibility (Bayl-Smith et al., 2020; Downs et al., 2006; Musuva et al., 2019).

Cue Utilisation

A cognitive process that can help with recognising a phishing email is the ability to develop and identify patterns or cues from memory (Klein, 2008). Cues develop when features and events/objects are observed simultaneously on multiple occasions (Wiggins, 2012). When regularly exposed to associations between features and events/objects, the developed cues are

stored in long term memory and ready to be accessed once a feature is present, which allows for less demand on working memory (Brouwers et al., 2016).

Cue utilisation is an individual difference in the ability to develop and use cues (Bayl-Smith et al., 2020). Individual differences in cue utilisation have been examined in several domains where quick and accurate identification of cues and their application are vital, such as driving and air traffic control (Sturman et al., 2019; Wiggins et al., 2012). Individuals with higher cue utilisation were found to more often correctly identify features related to a task from an array, such as an environmental scene, and recognise various related features and objects in an environment, as compared to individuals with lower cue utilisation (Wiggins, 2014). Higher cue utilisation also enables better discrimination between relevant and irrelevant cues to solve domain-specific problems and prioritise features essential to a related problem (Wiggins, 2014). Cue utilisation assists in reducing demands on cognitive load to help individuals make quicker and more accurate decisions (Brouwers et al., 2016).

More importantly, cue utilisation assists in the rapid identification of important features (Brouwers et al., 2016; Wiggins, 2014). This would be particularly effective in time-pressured situations because individuals tend to rely less on information and more on critical features (Bayl-Smith et al., 2020). When individuals are rushed, they do not have as much time to fully evaluate all of the features in an email (Chowdhury et al., 2019). Consequently, this leads to overlooking critical features that make a phishing email detectable. As speed is an essential feature of successful identification in time-pressured situations, those with higher cue utilisation may be able to identify the critical features and patterns that comprise a phishing email in a shorter period of time than individuals with lower cue utilisation (Chowdhury et al., 2019).

Therefore, individuals who have higher cue utilisation should not be as negatively impacted by time pressure compared to those with lower cue utilisation.

Cue Utilisation in Phishing

In detecting phishing emails, features such as spelling and grammatical mistakes, suspicious URL links, and unrecognisable sender addresses may unconsciously activate the cues for identifying potential phishing emails (Parsons et al., 2019). An individual with higher cue utilisation should be able to better discriminate between relevant and irrelevant features that may lead to the successful detection of a phishing email (Klein, 1993; Nasser et al., 2020). Cue utilisation aids in the process of identifying important features (e.g., suspicious URL or sender's address, spelling/grammatical mistakes) and matching this pattern of features with those seen previously in phishing emails. This process typically results in more timely and accurate judgements (Bayl-Smith et al., 2020). For example, a feature in a phishing email may be a phishing URL link in the form of a link button that can include prompts such as 'click here' or 'read more' that leads to the next stage of the phishing attack. This next stage could be malware that is automatically downloaded onto the computer, or the user might be taken to a website appearing to be the organisation's genuine website with a prompt for their login details. Higher cue utilisation could detect these features from past experience and prevent the next stage from being initiated.

In phishing, cue utilisation should be able to aid the ability to rapidly identify features that are characteristic of phishing emails. This should also be able to help in situations where time pressure is an issue. Individuals may receive large numbers of emails daily, which increases the pressure to read and classify emails in short periods of time. In order to address this time pressure, users might need to rely on a limited number of features when categorising emails.

Cue-based processing facilitates quick and accurate evaluations based on a limited number of features (Lansdale et al., 2010). Cue utilisation should be able to aid in more accurate recognition of phishing emails when under time pressure situations.

Decision-Making Styles

Individuals differ in how they prefer to make decisions. Some may prefer to rely on their gut instincts or feelings, while others may prefer to consider all of the information before making a decision. The process of decision-making depends on situational factors and individual differences. A useful distinction between the different modes of decision-making was proposed by Kahneman (2003) as a dual processing theory. This theory labels the rapid, instinctual, subconscious decisions associated with automatic heuristics as being made by System 1, or intuition, and slower, deliberate, conscious decisions by System 2, or rationality (Kahneman, 2003).

Intuitive Decision Style

System 1, which will be referred to as intuition, is an automatic response that is processed through feelings and first impressions. Intuitive processing uses heuristics or cognitive shortcuts that are used to simplify complexities (Kahneman & Tversky, 1973; Shiloh et al., 2002). While Kahneman argues that intuition uses these heuristics that are prone to errors from bias, Klein discusses intuition in the domain of expert intuition (Kahneman & Klein, 2009). Experts are fast, require less information, demonstrate a superior working memory, and have an awareness of meaningful patterns of information (Persky & Robinson, 2017). According to both Kahneman

and Klein, intuition comes from learning from past experiences and is applied when similar experiences are presented (Pachur, 2015; Kahneman & Klein, 2009). Kahneman (2003) has discussed that intuition is formed when there are rules in an environment that can be learned, when being continuously exposed to the environment and practice is reinforced, and by receiving immediate feedback. The disadvantage of an intuitive decision style is that the heuristics that are used could be prone to bias and trusting our initial instincts can lead us to make poor or error-prone decisions (Kahneman & Tversky, 1973). Kahneman (2003) argues that because the world has many inconsistencies, it is difficult to predict or have a correct intuition about it.

Rational Decision Style

System 2 processing, which will be referred to as rationality, is a deliberate, effortful, and conscious form of processing that allows for more thought to be placed on making a decision (Kahneman, 2003). With rationality, more mental effort, time, and attention is needed when attending to a task (Kahneman & Tversky, 1973). Rational processing is useful for tasks that require more mental effort, such as solving a mathematical equation or problem-solving. A person with a preference for a rational decision style may be able to notice details of an environment or event that may be missed by an intuitive decision style. The disadvantage of System 2 processing is that at times, there may not be enough time or information available to be able to make a deliberate decision. This can be the case if there is an emergency or a quick reaction time is needed, such as a fire or a medical emergency. In time-pressured scenarios just like these, System 2 processing would not be as helpful but could instead be detrimental because a quick decision needs to be made.

Decision Making Styles and Phishing Detection

The quick processing of information is handled by intuition, allowing the user to perform tasks while spending less time reading and sorting emails. Phishing perpetrators depend on users to disregard a rational decision-making style (Xu et al., 2012). A person with a preference for intuitive decision-making may be less likely to examine all features of an email before making a decision, and therefore may be more likely to overlook irregularities or suspicious features. If a user notices irregularities in an email, a person with a preference for rational decision-making might be more likely to investigate the email further. An individual may prefer a rational decision-making style when more deliberate or conscious processing of a situation is needed. For instance, in the event of a detection of novel or suspicious features in an email, a careful consideration of a response will be necessary (Evans & Stanovich, 2013).

Rational decision-making is more useful when checking for biases that enter with intuitive decision-making. However, because much effort is needed when utilising a rational decision-making style, more time may be needed and fewer distractions can take place for it to be effective. This may not be possible, though, if an individual is looking through a large number of emails in a short period of time (Chowdhury et al., 2019).

Time Pressure and Decision Making Style

Individuals who use email frequently to communicate with colleagues or external organisations may receive a multitude of emails every day. Each email may need to be tended to in short periods of time due to the high volume of emails and the expectation of a quick response. An individual who prefers a more intuitive decision-making style can make decisions quickly without having to consciously think about it; however, that does not mean that they do so effectively. Individuals who prefer a more rational approach may notice important features of a

phishing email if given a sufficient amount of time. The more deliberate and slow nature of rational decision-making may therefore be affected by time pressure. On the other hand, using this style of decision-making with more time should result in greater accuracy in the detection of phishing emails.

When under time pressure, all participants, regardless of whether they have more or less of a preference for a decision style, should be forced to use an intuitive decision-making style. If this is the case, with a shorter time condition and greater time pressure, decision-making preference should not have an impact on performance because everyone is using the same decision-making style. When there is more time and less pressure, individuals should be able to use their preferred decision-making style. Thus, individuals with a preference for rational decision-making should be able to detect phishing emails with greater accuracy than those who prefer intuitive decision-making when given more time, whereas, individuals would be expected to perform similarly with a shorter time condition. Training programs may use the influence of time pressure on decision-making styles by influencing those who prefer intuition to use a more rational style.

Cue Utilisation and Decision Styles

Herbert Simon (1992) defines intuition as the recognition of patterns and the ability to make use of them in relevant contexts. Some individuals prefer an intuitive decision style even though they may have a limited amount of information, while others prefer to think about possible alternatives before making a decision. Cue utilisation is an individual's capacity to develop and use cues, which can be helpful when needing to make quick decisions (Brouwers et al., 2018). One can prefer an intuitive decision-making style but may not have developed the cues or patterns in memory to be able to make accurate decisions.

Intuition may only operate effectively by relating features and patterns to cues stored in long-term memory from past experiences, as proposed in the recognition-primed decision model (Klein, 1993; Pachur et al., 2015). If an individual were to see an email that appears to be from a genuine organisation, someone who prefers an intuitive decision-making style may not question its legitimacy if they do not have phishing cues stored in their memory. While on the other hand, someone who prefers a rational decision-making style might have a closer look at the details of the email to assess its legitimacy. However, if they do have cues related to phishing detection, those with higher cue utilisation should be able to detect the most important features and therefore make more accurate decisions if they prefer intuition (Nasser et al., 2020).

Previous research has examined decision-making styles in domain-specific settings, however, they were not able to evaluate participants' ability to make accurate decisions (Parchur et al., 2015). Therefore it may be useful to examine the relationship between whether a person has a preference for intuitive decision-making and whether they are able to accurately make decisions using that type of processing.

Current Study

The aim of the current study is to examine how cue utilisation, decision style preferences, and time pressure will influence an individual's ability to detect phishing emails. Phishing detection performance was measured with an email sorting task where participants viewed a sequence of email stimuli that were either genuine or had features of a phishing email embedded within them. The email stimuli were shown with two different time durations, where participants were shown the sequence of email stimuli for either 7 seconds or 15 seconds. After each time sequence was complete, participants were then required to sort the email into 1 of 10 categories, with one of the categories being phishing. Decision style preferences were measured on a

continuum for a preference of intuition when deciding to click on a link within an email. Cue utilisation was measured by a platform designed to test participants' abilities to detect features through identification, recognition, association, and discrimination.

Hypotheses

Hypothesis 1: It is hypothesised that participants with higher cue utilisation will have a greater preference for intuitive decision-making over rational decision-making compared to participants with lower cue utilisation.

Hypothesis 2: It is hypothesised that participants who score higher on cue utilisation will be better able to detect phishing emails than those with lower cue utilisation.

Hypothesis 3: It is hypothesised that participants with higher cue utilisation will be able to detect phishing emails more accurately than those with lower cue utilisation when emails are presented for 7 seconds, whereas when emails are presented for 15 seconds there will be a smaller difference in performance between those with higher and lower cue utilisation.

Hypothesis 4: It is hypothesised that for participants with higher cue utilisation, a preference for intuitive decision-making will be positively associated with the ability to detect phishing emails, whereas for participants with lower cue utilisation a preference for intuitive decision-making will be negatively associated with the ability to detect phishing emails.

Hypothesis 5: It is hypothesised that for participants in the 7 second time condition, there will be no significant relationship between decision-making preference and the ability to detect phishing emails, whereas, in the 15 second time condition, there will be a negative association between a preference for intuitive decision-making and phishing detection performance.

Method

Participants

A total of 200 participants took part in the study. Participants who did not complete the second part of the study, EXPERTise 2.0 (Phishing Edition), were excluded from the data analyses. The final sample consisted of 188 participants (141 Female, 47 Male), from ages 17 to 55 ($M = 20.41$, $SD = 5.25$). Participants were first-year psychology students enrolled in Semester 1 2021 at the University of Adelaide recruited using the SONA system and were required to be fluent in English. Students who participated in the study were granted course credit upon completion.

Materials

Demographic Questions

Demographic questions included age in years, gender (Female, Male, Other/Prefer Not to Say), and the length of time spent using a computer per day in hours.

Email Sorting Task

The email sorting task and EXPERTise 2.0 were completed remotely on participants' personal devices. The email sorting task was hosted on the Qualtrics platform. Participants were told to imagine that they were the personal assistant to a "Professor Alex Jones" from the Department of Psychology at the University of Adelaide. As Professor Alex Jones' personal assistant, participants were to examine emails that he received and assigned them to one of ten categories. These categories included Urgent, Teaching, Research, Banking, Online Purchases, Social Media accounts, Official, Spam, Phishing, and Miscellaneous.

Before the task began, participants were given instructions, including an image that demonstrates how to hover over the links given in the stimuli. Participants were shown 60 emails

in total. The emails contained 15-100 words and all contained a URL for consistency. Seventeen of the stimuli had URLs in the body of the email and 43 of the stimuli had a URL embedded in a 'prompt button' (e.g., 'CLICK HERE'). Participants were able to hover over the 'prompt button' to display the associated URL. Eleven out of 60 emails were phishing. The 10 phishing emails were created by replacing the URL from the original emails with a URL from an actual phishing email. For 5 of the phishing emails, spelling and grammatical errors and unusual sender's addresses were added. For 6 of the phishing emails, the email appeared genuine, only the phishing URL replaced the original URL.

Participants were randomly assigned to either a short or long time condition. Participants in the short time condition were presented with each email for 7 seconds, while those in the long time condition were presented with each email for 15 seconds. During the email stimuli presentation, a countdown timer indicated how much time they had left to view the email. Once the time interval was completed, the email stimulus was removed and participants were prompted to sort the email into one of ten categories, with one of the categories being phishing. The other nine categories were included as a distraction to reduce priming effects. The ability to detect phishing emails was operationalised as the number of correctly classified phishing emails.

Control Measures

Below the instructions, participants were told that 1 in 6 of the emails they encounter would be a phishing email (an email that is fraudulent or malicious). On the following page, they were quizzed on whether they read the instructions carefully by asking how many of the emails they were told would be phishing. This was done to ensure that participants did not presume that every email would be phishing in the case that they recognised the intention of the study and to reduce priming effect.

Measures

Decision Making Style Scale

Participants were asked to rate their decision making styles when deciding to click on a link in an email. This was done on a Likert Scale (1= Strongly Disagree, 5= Strongly Agree). There were 10 statements, where 5 of the statements indicated an intuitive preference and the other 5 statements indicated a rational preference.

The decision making style scale used in this study was adapted from a scale developed and validated by Hamilton and colleagues (2016), which resulted in 10 items that captured a range of rational to intuitive styles of decision making. The scale has support for dimensionality and reliability which was demonstrated by a factor structure and high internal consistency (Hamilton et al., 2016).

The decision making scale in this current study was adapted to create a version tailored to deciding whether to click on a link in an email. There were 10 statements in total, 5 relevant to rational decision making and 5 relevant to intuitive decision making. An example of a rational decision making item is, "I prefer to gather all the necessary information before deciding whether to click on a link in an email", while an example of an intuitive decision making item is, "When deciding whether to click on a link in an email, I rely mainly on my gut feelings". Each statement was rated on a Likert Scale ranging from 1 (Strongly disagree) to 5 (Strongly agree). The final scores were out of a total of 25 for rational and a total of 25 for intuitive. For example, if a participant scored 19 out of 25 for the rational items and 5 out of 25 for the intuitive items, they would be considered having a high preference for rational decision making. To account for decision making as part of a range of a preference for a certain style, the final scores were standardised and added on a continuum of intuitive decision making, with a score of -5 having a

greater preference for rational decision making and a score of 5 having a greater preference for intuitive decision making.

EXPERTise 2.0 (Phishing Edition)

The EXPERT Intensive Skills Evaluation (EXPERTise 2.0) Phishing Edition was used to measure cue utilisation (Bayl-Smith et al., 2020; Wiggins et al., 2015). The phishing edition of EXPERTise consists of 4 tasks: a Feature Identification Task (FIT), a Feature Recognition Task (FRT), a Feature Discrimination Task (FDT), and a Feature Association Task (FAT).

Feature Identification Task (FIT). In the FIT, participants are instructed to identify features in an email as quickly as possible. Participants were presented with 10 scenarios that included a phishing email in each scenario. When the email was presented, participants were required to click on the area that peaked their suspicion or click on a button labelled “Trustworthy Email”. This task was measured based on response latency, where lower mean response latency is associated with higher cue utilisation (Bayl-Smith et al., 2020; Loveday et al., 2014; Wiggins et al., 2003).

Feature Recognition Task (FRT). In the FRT, participants are presented with phishing stimuli for short periods of time and must categorise them. This task included 20 email stimuli, 10 being genuine emails and 10 being phishing emails. Each email was presented for 1000ms and participants were immediately asked to categorise the email as either “Trustworthy”, “Untrustworthy”, or “Impossible to tell”. FRT measures the ability to extract important information in an extremely short amount of time. A greater number of correct classifications is generally associated with higher cue utilisation (Bayl-Smith et al., 2020; Loveday et al., 2014; Wiggins et al., 2003).

Feature Discrimination Task (FDT). In the FDT, participants are presented with two email scenarios relating to a problem and based on that information, they must select a course of action, with one of the options being ignoring the email. Participants are shown a list of 11 features from the scenario and are then asked to rate the importance of each feature when deciding on their response. The features included factors that are related to a work environment and email such as “your boss’ anger” or “the sender’s email address”. The rating of importance ranged from 1 (Not important at all) to 10 (Extremely important). Greater variance in feature ratings is generally associated with higher cue utilisation (Bayl-Smith et al., 2020; Weiss et al., 2003; Pauley, 2009).

Feature Association Task (FAT). In the FAT, participants are shown two phishing-related phrases or words and must rate their perceived relatedness. Participants are shown 14 pairs of phrases/words that relate to computers and phishing such as “Email” and “Malware”. Each stimuli pair is presented simultaneously for 2000ms, and after, participants are asked to rate the perceived relatedness of the phrases/words on a scale ranging from 1 (Extremely unrelated) to 6 (Extremely related). Greater mean-variance in ratings by being able to select the perceived relatedness in a short amount of time is generally associated with higher cue utilisation (Bayl-Smith et al., 2020; Morrison et al., 2013).

Procedure

This current study received ethics approval from the subcommittee in the School of Psychology at the University of Adelaide (Ref no: 20/39). The study was posted in the SONA Research Participation System for first-year psychology students to access the link to the online study. Participants were presented with the information sheet and provided electronic consent to participate in the research and were informed that they could withdraw from further participation

in the research at any time without consequence. Participants completed the email sorting task, followed by the decision making scale, and completed the study with EXPERTise 2.0 (Phishing Edition).

Results

Overview of Analyses

This study used a 2x2 quasi-experimental design. The dependent variable was participants' ability to detect phishing emails, while the between-subject independent variables were cue utilisation typology (higher vs lower) and time pressure (7 vs 15 seconds). Additionally, decision making preference (rational vs intuitive) was the continuous independent variable. The data analyses were conducted on the IBM Statistical Package for Social Sciences (SPSS Statistics), Version 27.

Data Reduction

The data from the Email Management Task and EXPERTise 2.0 (phishing edition) was reduced. The cue utilisation typologies indicate either a higher or lower ability for cue utilisation (Sturman et al., 2019). The data from the four EXPERTise 2.0 tasks (FIT, FAT, FDT, FRT) were reduced per the standard method of categorising participants into two typologies (Brouwers et al., 2017, Loveday et al., 2013). The standard method of classifying the two typologies is done by conducting a cluster analysis using standardised z -scores for each of the four EXPERTise tasks.

Decision Making Style Preferences

The scores for each of the two decision making style scales were converted to standardised z -scores, and the difference between intuitive and rational z -scores was calculated.

More positive scores indicated a greater preference for intuitive decision making, while more negative scores indicated a greater preference for rational decision making.

Phishing Detection Scores

The phishing detection performance was the dependent variable that measured participants' ability to recognise a phishing email. Phishing detection performance was operationalised as the ability to identify the emails that contained a phishing URL as well as all 3 features of a phishing email (illegitimate sender address, spelling/grammar mistakes, and a phishing URL) which can both be seen in Appendix A. The measures evaluated the number of phishing emails participants' correctly categorised with scores ranging from 0 to 10.

Data Analysis

Establishing Typologies

To establish cue utilisation typologies, a *k*-means cluster analysis was conducted to classify participants into a higher or lower typology based on performance on the four EXPERTise tasks (Sturman et al., 2019; Wiggins et al., 2014). Prior to the cluster analysis, the scores for each task were first converted into standardised *z*-scores. With the standardised scores, the cluster analysis created two separate typologies for higher and lower cue utilisation. The results yielded 100 participants in the higher typology and 88 participants in the lower typology. Those with higher cue utilisation had greater mean-variance and faster time in FAT, greater variance in FDT, lower mean response latency in FIT, and greater accuracy in FRT. Table 1 shows the summary of the cluster analysis for cue utilisation typologies.

Table 1.

Participant cluster means for tasks from EXPERTise 2.0 (Phishing Edition).

Typology

EXPERTise 2.0 (Phishing Edition) Tasks	Higher (<i>n</i> = 100)	Lower (<i>n</i> = 88)
Feature Identification Task	-.32*	.37*
Feature Recognition Task	.51*	-.58*
Feature Association Task	.52*	-.60*
Feature Discrimination Task	.53*	-.61*

Significance level * $p < 0.001$

Hypothesis Testing

A 2x2 between-subjects Analysis of Covariance (ANCOVA) was used to examine Hypotheses 2, 3, 4, and 5 and an independent samples t-test was used to examine Hypothesis 1. The between-subject variables in the ANCOVA were cue utilisation (higher vs lower), exposure time (7 vs 15 seconds), and the continuous variable of decision making style preference (rational to intuitive). The dependent variable measured was performance on correct phishing detection.

The assumptions of normality were met when looking at the histograms of residuals, supported by non-significant Shapiro-Wilk tests. Levene's Test of Equal Variance also revealed no significant difference in each group's variance, which shows that the assumption of equal variance was met.

Hypothesis 1: Participants who scored higher on cue utilisation ($M = -0.29$, $SD = 1.78$) have a greater preference for rational decision making, whereas, those who scored lower on cue utilisation ($M = 0.33$, $SD = 1.33$) have more of a preference for intuitive decision making, $t(189) = -2.702$, $p = .008$. This does not support the hypothesis that those with higher cue utilisation

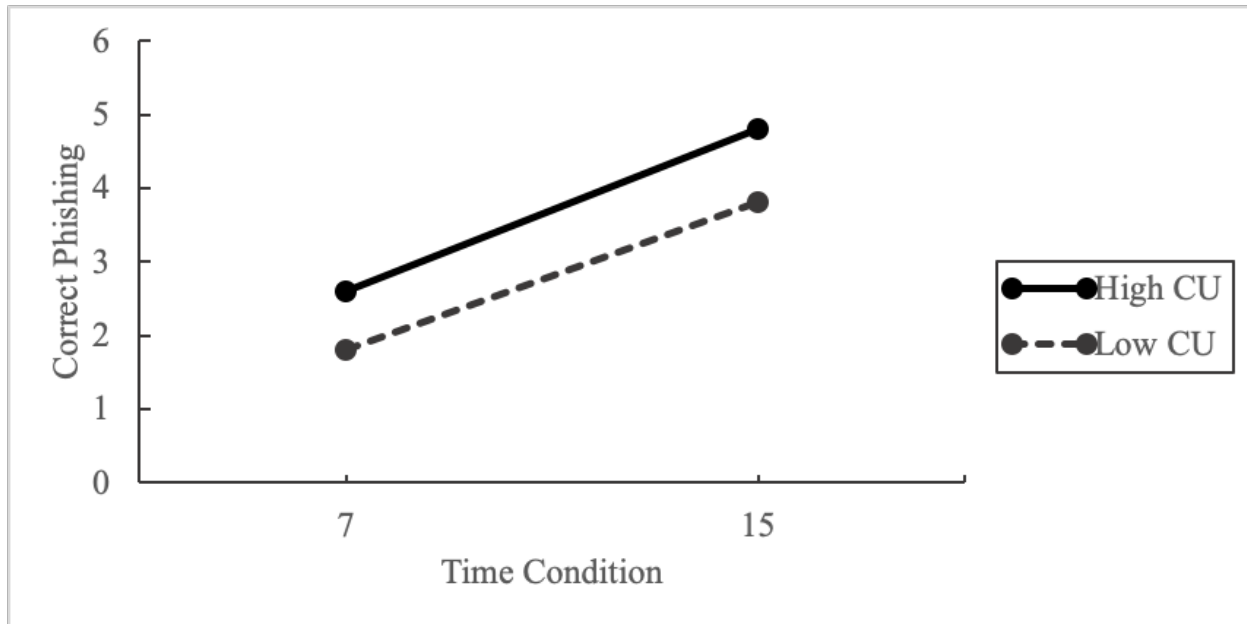
would have more of a preference for intuitive decision making, however, this indicates that there is a significant relationship between higher cue utilisation and rational decision making.

Hypothesis 2: There was a statistically significant main effect of cue utilisation on phishing detection scores, $F(1, 177) = 5.037, p = .026, \eta^2 = .028$. Averaged across time conditions, participants who scored higher on cue utilisation ($M = 3.74, SD = 2.67$) were better able to detect phishing emails than those who scored lower on cue utilisation ($M = 2.76, SD = 2.65$). This supports the main effect hypothesis of cue utilisation on phishing scores.

Hypothesis 3: There was no significant interaction found between high cue utilisation and time conditions in phishing performance, $F(1, 177) = 0.090, p = .765, \eta^2 = .001$. The absence of an interaction can be seen in Figure 1. However, the main effect of time pressure was found to be significant $F(1, 177) = 29.57, p < .001, \eta^2 = .143$. Participants in the 15 second time condition ($M = 4.34, SD = 3.00$) were better able to detect phishing emails than participants in the 7 second time condition ($M = 2.24, SD = 1.86$), indicating that having more time to assess an email is beneficial in detecting if it is phishing.

Figure 1.

Results for an interaction effect between cue utilisation and time pressure on correct phishing detection.



Hypothesis 4: There was no significant interaction found between cue utilisation and decision making preference in phishing detection performance, $F(1, 177) = 0.244$, $p = .622$, $\eta^2 = .001$. However, decision making preference had a significant main effect $F(1, 177) = 3.993$, $p = .047$, $\eta^2 = .022$. There is a negative association between an intuitive preference and correct phishing detection ($B = -.21$), indicating that a greater preference for intuitive decision making was associated with a decreased ability to detect phishing emails.

Hypothesis 5: There was no significant interaction found between time pressure and decision making preference in phishing detection performance, $F(1, 177) = .320$, $p = .572$, $\eta^2 = .000$. This suggests that the difference in phishing detection performance between participants with more of a preference for intuition or more of a preference for rationality was not affected by which time condition they were in. Thus, participants in the longer time condition did not have a significantly greater difference in phishing detection scores between those who prefer intuitive or rational decision making.

Discussion

Overview

The aim of this study was to examine whether exposure to different levels of time pressure and individual differences in both cue utilisation and decision making style preferences would affect an individual's ability to detect phishing emails. The results revealed that the main effects of cue utilisation, decision making preference, and time pressure have a significant impact on phishing detection performance. However, there were no interactions found between cue utilisation and decision making, cue utilisation and time pressure, and time pressure and decision making on phishing detection performance.

Cue Utilisation and Phishing Detection

Hypothesis 2 was supported with the main effect being found for cue utilisation on phishing detection performance. This finding aligns with research conducted by Bayl-Smith and colleagues (2020), where they found that having higher cue utilisation would be a significant predictor of identifying features of a phishing email. These findings support the notion that individuals who have higher cue utilisation are better able to identify features that are not typical of expected patterns in a genuine email, which enables them to generate accurate assessments of a situation (Bayl-Smith et al., 2020). Finding a main effect for cue utilisation on phishing detection performance indicates that there are individual differences in cognitive processes in how users approach emails (Bayl-Smith et al., 2020). Phishing perpetrators rely on users to create inaccurate mental representations of the situation for them to successfully perpetrate a phishing attack, therefore developing accurate mental models through cue utilisation is beneficial. Accurate mental models can be developed through training such as Klayman's (1988) cue discovery, which facilitates the acquisition of domain-specific cues with the use of

simulation training. This type of cue-based training may assist in the attainment of features and patterns to develop cues related to phishing emails.

Decision Making Preferences and Phishing Detection

The main effect of decision making preferences on phishing detection performance showed having more of a preference for intuitive decision making resulted in a decreased ability to detect phishing emails. This decrease in performance by showing a preference for intuitive decision making is supported by Kahneman's theory on heuristics and biases, where quick, automatic thought processes may have a greater tendency to result in error (2003). An example of this is the "fast and frugal" heuristic that allows for making decisions with limited information (Kahneman & Tversky, 1973). By taking advantage of this heuristic, an individual may develop a skewed view of reality with the presence of biases. In the case of phishing emails, phishing perpetrators will design emails to imitate genuine emails, which is then able to skew the world view of an email recipient and trick them into believing the email is genuine (Zhang et al., 2017). Vishwanath and colleagues (2011) have also shown that this type of intuitive decision making can cause an increase in phishing susceptibility. Klein (1993) argues that expert intuition would result in the ability to quickly process and identify relevant information, this is likely not the case in the current study because participants, being undergraduate students, have likely not been exposed to high volumes of emails on a frequent basis to develop a sense of expert intuition. Even if they had, it may be the case that they have not been exposed to many phishing emails and they may not know what features or patterns to look for to intuitively identify a phishing email.

Although Kahneman argues for scepticism in intuition, Kahneman (2003) supports the idea that intuition could be developed from effortful practise and exposure. However, that

effortful practice would initially require an effortful and rational decision-style before being able to use an automatic and intuitive decision-style to achieve greater accuracy (Kahneman, 2003). Kahneman (2003) also argues that intuition needs to be delayed for as long as possible to gather as much information as possible, and only when enough information has been gathered to move forward with the decision. It is also suggested to act on intuition alone when the evidence has been carefully considered (Kahneman, 2003). In other words, it is more beneficial to use a more deliberate mode of decision making such as the rational decision making preference in the scenarios presented in this study (Kahneman, 2003).

Cue Utilisation and Decision Making Styles

Previously, it was thought that, due to the ability to rapidly detect features, individuals who have higher cue utilisation would prefer the automaticity that comes with an intuitive decision making style. However, a significant relationship was found between cue utilisation and decision making style, which showed that those who scored higher on cue utilisation have a greater preference for rational decision making. Although this does not support the initial hypothesis, this is an interesting relationship as the participants who score higher on cue utilisation still prefer a more careful and deliberate style of decision making despite having the capacity to quickly identify features that would be expected with a preference for intuitive decision making.

Interaction Between Decision Making Preference and Cue Utilisation on Phishing

Detection

A hypothesis was made that there would be an interaction between having a preference for intuitive decision making and exhibiting higher cue utilisation, since those who have higher cue utilisation should be able to identify and apply relevant and irrelevant cues quickly and possibly intuitively (Kahneman & Klein, 2009). However, the results did not support this

hypothesis and no significant relationship was found. The lack of a significant relationship indicated that there was no difference in phishing detection performance regardless of the cue utilisation typology and decision making preference. Although individuals may prefer to make decisions quickly and with less consideration, they may not have the necessary skills or feature-recognition available to rely on their intuition to make correct judgements.

Intuition may be useful in situations with less time to make a decision, however, it does not mean the decision will be accurate. Cue utilisation may be useful in such time-sensitive situations. If individuals are better able to develop their cue utilisation through cue-based training, perhaps their intuition could be used more effectively. Better cue utilisation could be achieved through training with frequent exposure to examples of phishing emails among authentic emails, similar to what is done in this study.

Furthermore, an individual's self-reported preference for a decision making style is not an indication of their effectiveness with that style being applied to certain tasks. An individual may even be aware of their poor performance at certain tasks with a style of decision making, and yet still prefer that style. They may even have a preference and be aware of their poor performance, and deliberately enacted an alternate style when performing the email sorting task.

Time Pressure and Phishing Detection

The main effect of time pressure was also found to be significant. This supports the hypothesis that participants in the shorter time condition had a reduced ability to detect phishing emails compared to those who were exposed to the longer time condition. This suggests that imposing time pressure makes it more difficult to detect a phishing email because there is less time to discern all the features. Specifically, the participants in the shorter time condition may

not have been able to correctly identify the phishing emails with high accuracy due a lack of time available to inspect the URL link embedded in the emails.

The finding of time pressure significantly affecting phishing detection performance is supported by previous research done by Chowdhury and colleagues (2019). They found that a greater time pressure with a shorter time interval leads to poorer decision making with regards to cybersecurity behaviours (Chowdhury et al., 2019), suggesting that allocating a sufficient amount of time and minimising time pressure when reading emails is vital in reducing phishing susceptibility.

Interaction Between Cue Utilisation and Time Pressure on Phishing Detection

Despite hypothesising that an interaction would be found with participants who score higher on cue utilisation performing better at detecting phishing emails in the shorter time condition, no significant relationship was found. The main effect of cue utilisation across both time conditions indicates that participants with higher cue utilisation are better able to detect phishing emails. Similarly, the main effect of time pressure reveals that having more time is more advantageous than less time in detecting phishing emails. However, participants with higher cue utilisation and lower cue utilisation performed the same as they usually would, regardless of which time condition they were in. This suggests that although having higher cue utilisation is expected to be particularly useful in time pressure situations, it was found that there is no difference in how they usually perform compared to those with lower cue utilisation.

Interaction between Decision Making Preference and Time Pressure on Phishing Detection

It was hypothesised that participants in the 7 second time condition would show no significant difference between decision making styles and the ability to detect phishing emails, whereas in the 15 second time condition participants would show a negative association between

a preference for intuitive decision making and phishing detection performance. The main effect of intuitive decision preference on phishing detection performance indicates there was a negative relationship across both the shorter and longer time conditions. However, the interaction between decision making preferences and time pressure was not found to be significant. A preference for intuitive decision making has a negative impact on all participants, regardless of time conditions. While this supports the second half of the hypothesis, the overall hypothesis is not supported and the previously assumed idea that rational decision-makers may be forced to use an intuitive decision making style in the 7-second time condition is not supported. It may be the case that those who prefer a rational decision style were still able to use their preference in deliberative processing, despite not having the time to think slowly.

Individuals who demonstrate a preference for rational decision making may rely on their conscientious and deliberate nature to make decisions, while having a limited amount of time (Evans et al., 2013; Hamilton et al., 2016; Kahneman, 2003). Although it was previously assumed that having less time would force intuitive processing to initiate, despite their reported preferences, participants have seemingly not changed the way their decisions were made. Regardless of the decision making style used, their final decision was forced to be made within their allocated time limit.

Implications of Findings

The findings of this study suggest that it is vital to take the time to use a slow, deliberate, and rational mode of decision making when approaching emails. Therefore, it could be beneficial for organisations to enact decision training where individuals are encouraged to use a more proactive approach (Siebert et al. 2021). This study has also confirmed that there are indeed

individual differences in the way that people approach emails and make decisions about what features are important and unimportant when looking at emails.

The findings of this study could also be used to promote safe email sorting within organisations by implementing training that demonstrates the consequences of falling victim to a phishing attack and preventative measures that individuals can take. Training can include the use of EXPERTise 2.0 (Phishing Edition) and the adapted decision making scale to reveal a person's susceptibility through their cue utilisation typology as well as their decision making preference when approaching emails. Email sorting training can then be tailored toward users' level of cue utilisation and preference in decision making style relevant to phishing detection. As this study also reveals that time pressure of a matter of seconds can lead to poor phishing detection, the time condition can be factored into training. Since it is in an email user's best interest to ensure enough time before taking action within an email (i.e., clicking on a link), training can condition users to be patient and ensure they use more time.

Organisations can further promote greater cyber security by focusing on a two-way understanding between email senders and receivers. Cue utilisation can become more effective if receivers are familiar with features and patterns from legitimate emails within the organisation and senders can ensure their emails do not contain features of potential phishing emails like spelling/grammatical errors or suspicious URLs that trigger cues. An example of this could be the inclusion of a footnote required in emails sent from the organisation with statements that they never ask for bank details or confidential information. Receivers could also be encouraged to confirm the authenticity of the email with an independent source. Secure emailing practice can be promoted in this way through the implementation of decision making training and educating users about the use of cues. Greater security can also be promoted with frequent reminders of

important features to pay attention to in an email, such as looking at the sender address, inspecting for spelling and grammar mistakes, if there is a link attached to the email with a prompt to click on it, and importantly to be sceptical of the link before clicking.

A reason for less accurate email sorting for users with a preference for intuitive decision making is that participants were not experts at emailing. In other words, as undergraduate students, they are likely to not have been exposed to high volumes of emails on a daily basis with a great deal of time pressure. As Klein (1993) suggests, expert intuition stems from domain-specific experience, and because participants may not have developed expert intuition in the domain of emailing, this may explain the result of inaccurate phishing detection for those with a preference for intuition over rational. Including a larger, more diverse sample of participants from different educational domains such as information technology or computer science, where they may have a better understanding of what features and patterns to pay attention to and have developed the relevant cues, may yield different results. It could also be helpful to have a team of experts send out an email that is suspicious and monitor responses and actions to it, which is done in large organisations to test cyber security. However, human error can also occur in professionals that are meant to be experts or at least highly exposed to a certain activity, and they too can benefit from additional education and training as phishing perpetrators evolve in their attempts.

Strengths

The strength of the study is found in its design, which led to its ecological validity. The email sorting task was created to be as close to an authentic email environment as possible by including a wide variety of email categories and subjects as well as having a large number of stimuli to replicate the multitude of emails an individual may receive in their inbox. Additionally,

since participants were not in an actual email application, they were still given the freedom to explore important features of an email such as hovering over a link to see where a URL button may be leading to. This feature was added to give the user more information in their decision making process regarding the validity of an email to further add to its authenticity. Furthermore, the online nature of the study allowed for comparable engagement and distractions to a real-life email sorting environment. Previous studies have designed and sent out real-world phishing emails to participants without their prior knowledge, as discussed in a review of phishing studies (Parsons et al., 2015). Although this was useful for assessing responses to phishing emails, the generalisability of those responses were limited to the one category of email, being phishing. Therefore, this current study's use of a variety of features and email subjects allowed for the evaluation of participant's attention to the critical features within the phishing email.

Another strength of the study was that participants were told at the beginning when reading instructions for the email sorting task that 1 in 6 of the emails would be phishing, in order to prevent a priming effect if participants knew the true intention of the study and thought every email was a phishing email. Parsons and colleagues (2015) found that when participants are primed for phishing emails, they are more likely to pay attention to cues relevant to phishing. This is also supported by Kahneman & Tversky's (1973) notion of the framing effect where information is influenced by the context or environment in which it is presented. This suggests that anti-phishing training programs should continuously prime individuals in their personal and professional lives to consider phishing when assessing emails until they have developed higher cue utilisation towards phishing detection.

The addition of the decision making scale adapted for emails is a novel contribution to research conducted on phishing susceptibility. Although Downs et al. (2006) also examined the

relationship between decision making and phishing susceptibility, a decision making scale was not used to measure decision making. Furthermore, the sample size in the study was relatively small which affected its generalisability (Parsons et al., 2015). Whereas, this current study had a large sample size of 200 participants, which further adds to the generalisability of the research outcomes of this study. This current study provided a decision making scale influenced by a dual-processing theory with the use of intuitive and rational decision making which can be used to guide future research as well as training in how to influence individuals to make more rational decisions when assessing emails.

Limitations and Future Direction

Although the ecological validity of the study made it realistic, the limitations of the study include the generalisability to the wider populations. The participants included in this current study were first-year psychology students at the University of Adelaide. There are many factors that may play into the results of the study including the fact that university students are trained in their studies to use a more rational decision making style instead of intuitive (Hamilton et al., 2016). As a consequence, we may not have been able to see a more effective use of intuition. Those with majors more versed in computers, such as computer science or IT, may have performed differently than the current participants as a result of their program structures. Therefore, future research can benefit from recruiting more diverse samples. Future studies can also examine the use of anti-phishing training tools that use the results from cue utilisation and decision making, as well as how to sustain the knowledge gained from training. Furthermore, future research may also benefit from examining the misidentification of genuine emails as phishing. It has been shown that exposure to genuine emails that include

phishing features such as spelling and grammar mistakes, as well as unknown sender addresses could assist in reducing the chances of misidentification (Brouwers et al., 2018).

Conclusion

The impact of clicking on a single phishing link can not only cause a loss of millions of dollars but can also lead to psychological distress and physical symptoms. As a result, it is vital to look into what makes individuals susceptible to phishing. This study investigated the individual differences of phishing susceptibility by examining cue utilisation typologies and decision making preferences in the context of phishing emails, as well as the role of time pressure. Results found that having higher cue utilisation, having a more rational decision making style, and having more time to look at an email can greatly increase the chances of successfully detecting a phishing email. The results of this study can be used to guide anti-phishing training as well as promote cyber security culture.

References

- Akdemir, N., & Yenil, S. (2021). How phishers exploit the coronavirus pandemic: A content analysis of covid-19 themed phishing emails. *SAGE Open*, *11*(3), 215824402110318. <https://doi.org/10.1177/21582440211031879>
- Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, *68*, 160–196. <https://doi.org/10.1016/j.cose.2017.04.006>
- 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>
- Australian Competition and Consumer Commission. (2021). Scam statistics: Phishing 2021. Retrieved from: <https://www.scamwatch.gov.au/scam-statistics?scamid=31&date=2021>
- 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
- Bose, A.C.M. Leung, Assessing anti-phishing preparedness: a study of online banks in Hong Kong, *Decision Support Systems* *45* (4) (2008) 897–912.
- 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>

- 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>
- Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. *ACM International Conference Proceeding Series*, 149, 79–90. <https://doi.org/10.1145/1143120.1143131>
- 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>
- Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. *Lecture Notes in Computer Science*, 36–47. https://doi.org/10.1007/978-3-319-20376-8_4
- Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2017). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems*, 67(2), 247–267. <https://doi.org/10.1007/s11235-017-0334-z>
- Hamilton, K., Shih, S.-I., & Mohammed, S. (2016). The development and validation of the rational and intuitive decision styles scale. *Journal of Personality Assessment*, 98(5), 523–535. <https://doi.org/10.1080/00223891.2015.1132426>
- 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>

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

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.

Kahneman, D. & Tversky, A. (1973). Judgment under Uncertainty: Heuristics and Biases. <https://doi.org/10.21236/ad0767426>

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>

Kahneman, D., & Klein, G. (2009). Conditions for intuitive expertise: A failure to disagree. *American Psychologist*, 64(6), 515–526. <https://doi.org/10.1037/a0016755>

Klayman, J. (1988). Cue discovery in probabilistic environments: Uncertainty and experimentation. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 14(2), 317–330. <https://doi.org/10.1037/0278-7393.14.2.317>

Klein, G. A. (1993). In *A recognition-primed decision (RPD) model of rapid decision making* (pp. 138–147). Ablex Publishing Corp. *Psychologist*, 58(9), 697-720. <https://doi.org/10.1037/0003-066X.58.9.697>

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

- Klein, G. (2015). A naturalistic decision making perspective on studying intuitive decision making. *Journal of Applied Research in Memory and Cognition*, 4(3), 164–168.
<https://doi.org/10.1016/j.jarmac.2015.07.001>
- Lansdale, M., Underwood, G., & Davies, C. (2010). Something Overlooked? How experts in change detection use visual saliency. *Applied Cognitive Psychology*, 24(2), 213–225.
<https://doi.org/10.1002/acp.1552>
- Loveday, T., Wiggins, M., Festa, M., Schell, D., & Twigg, D. (2013). 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
- 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>
- 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>
- 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>
- 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>
- Musuva, P. M. W., Getao, K. W., & Chepken, C. K. (2019). A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility. *Computers in Human Behavior*, 94, 154–175. <https://doi.org/10.1016/j.chb.2018.12.036>
- Nasser, G., Morrison, B. W., Bayl-Smith, P., Taib, R., Gayed, M., & Wiggins, M. W. (2020). The role of cue utilization and cognitive load in the recognition of phishing emails. *Frontiers in Big Data*, 3, 1–10. <https://doi.org/10.3389/fdata.2020.546860>
- Pachur, T., & Spaar, M. (2015). Domain-specific preferences for intuition and deliberation in decision making. *Journal of Applied Research in Memory and Cognition*, 4(3), 303–311.
<https://doi.org/10.1016/j.jarmac.2015.07.006>
- 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>
- 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>
- 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>

- 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>
- Shiloh, S., Salton, E., & Sharabi, D. (2002). Individual differences in rational and intuitive thinking styles as predictors of heuristic responses and framing effects. *Personality and Individual Differences*, 32(3), 415–429. [https://doi.org/10.1016/s0191-8869\(01\)00034-4](https://doi.org/10.1016/s0191-8869(01)00034-4)
- Siebert, J. U., Kunz, R. E., & Rolf, P. (2021). Effects of decision training on individuals' decision-making proactivity. *European Journal of Operational Research*, 294(1), 264–282. <https://doi.org/10.1016/j.ejor.2021.01.010>
- Simon, H. A. (1992). What is an “Explanation” of Behavior? *Psychological Science*, 3(3), 150–161. <https://doi.org/10.1111/j.1467-9280.1992.tb00017.x>
- Sturman, D., Wiggins, M. W., Auton, J. C., & Loft, S. (2019). 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>
- 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>

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., & 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. (2014). 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>

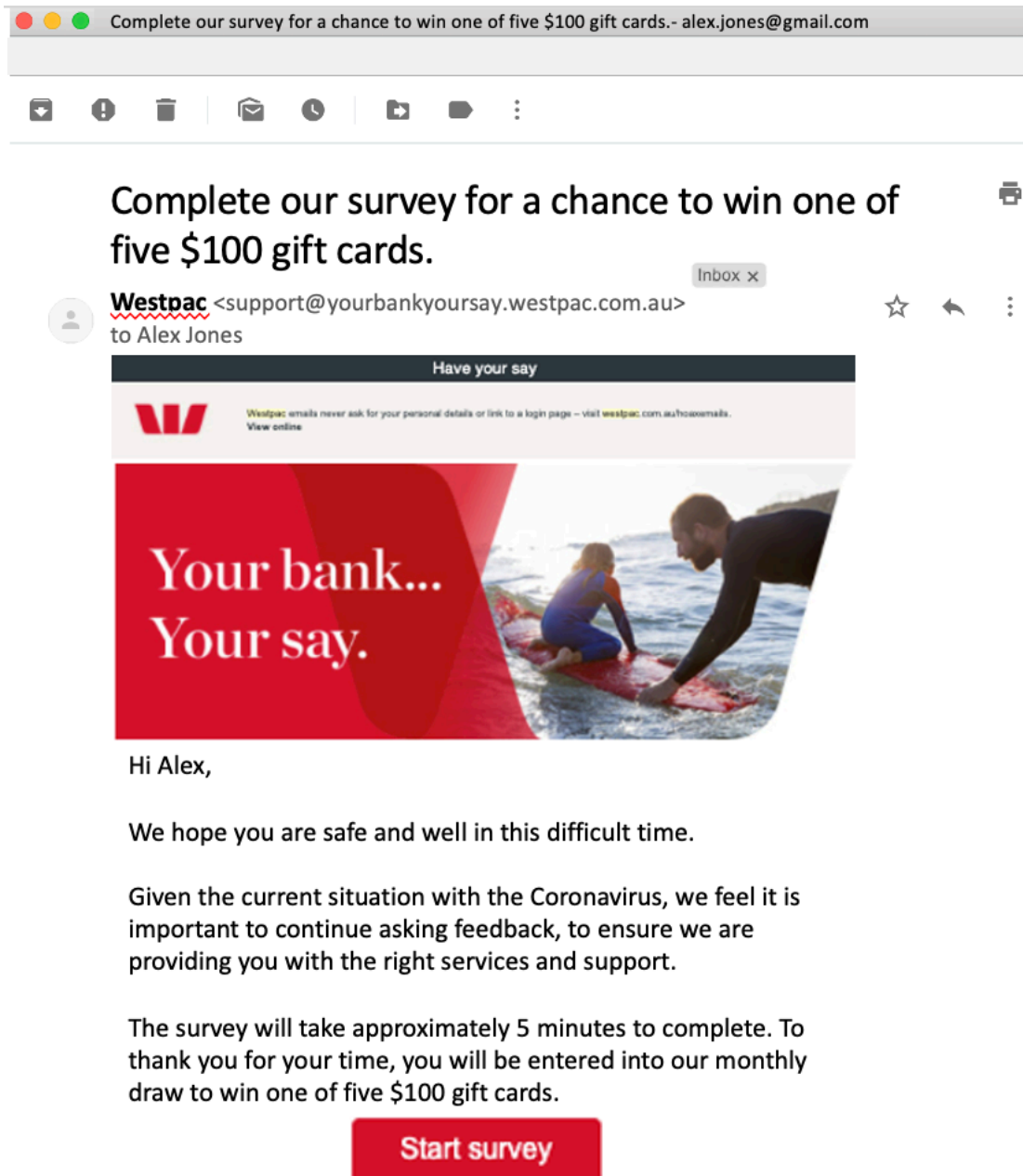
Wiggins, M. W. (2014). Measuring diagnostic skills through the utilization of cues. In *Proceedings of the Human Factors and Ergonomics Society* (Vol. 2014-January, pp. 2345–2349). Human Factors and Ergonomics Society Inc.

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

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

Appendix A: Email Stimuli Examples

Genuine Email Stimulus



Complete our survey for a chance to win one of five \$100 gift cards.- alex.jones@gmail.com

Complete our survey for a chance to win one of five \$100 gift cards.

Westpac <support@yourbankyoursay.westpac.com.au> to Alex Jones

Have your say

W Westpac emails never ask for your personal details or link to a login page – visit westpac.com.au/hozonemails.
View online

Your bank...
Your say.

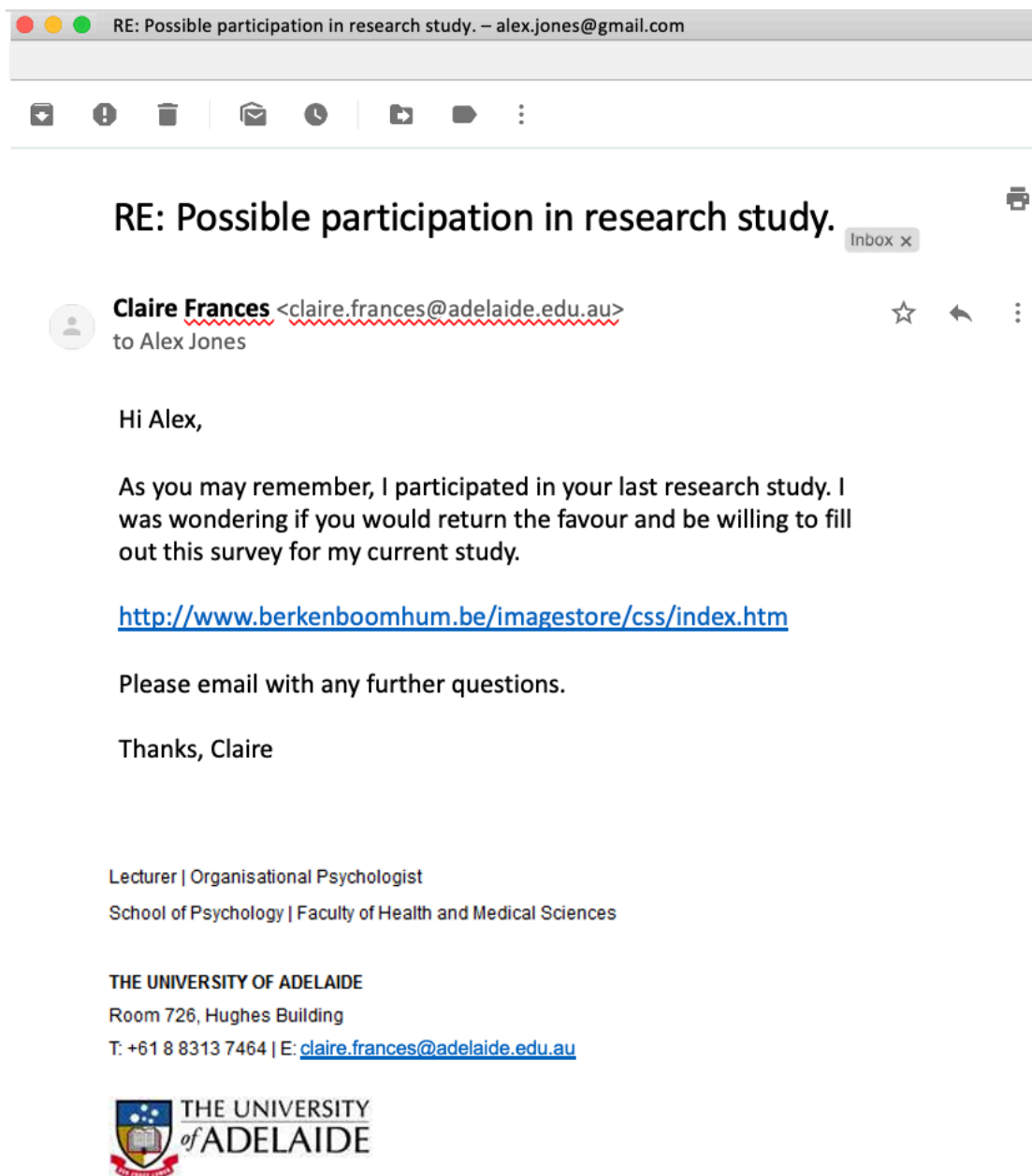
Hi Alex,

We hope you are safe and well in this difficult time.

Given the current situation with the Coronavirus, we feel it is important to continue asking feedback, to ensure we are providing you with the right services and support.

The survey will take approximately 5 minutes to complete. To thank you for your time, you will be entered into our monthly draw to win one of five \$100 gift cards.

[Start survey](#)

Phishing Email Stimulus: Cue – Phishing/Illegitimate URL

RE: Possible participation in research study. – alex.jones@gmail.com

RE: Possible participation in research study. Inbox x

Claire Frances <claire.frances@adelaide.edu.au>
to Alex Jones

Hi Alex,

As you may remember, I participated in your last research study. I was wondering if you would return the favour and be willing to fill out this survey for my current study.


<http://www.berkenboomhum.be/imagestore/css/index.htm>

Please email with any further questions.

Thanks, Claire

Lecturer | Organisational Psychologist
School of Psychology | Faculty of Health and Medical Sciences

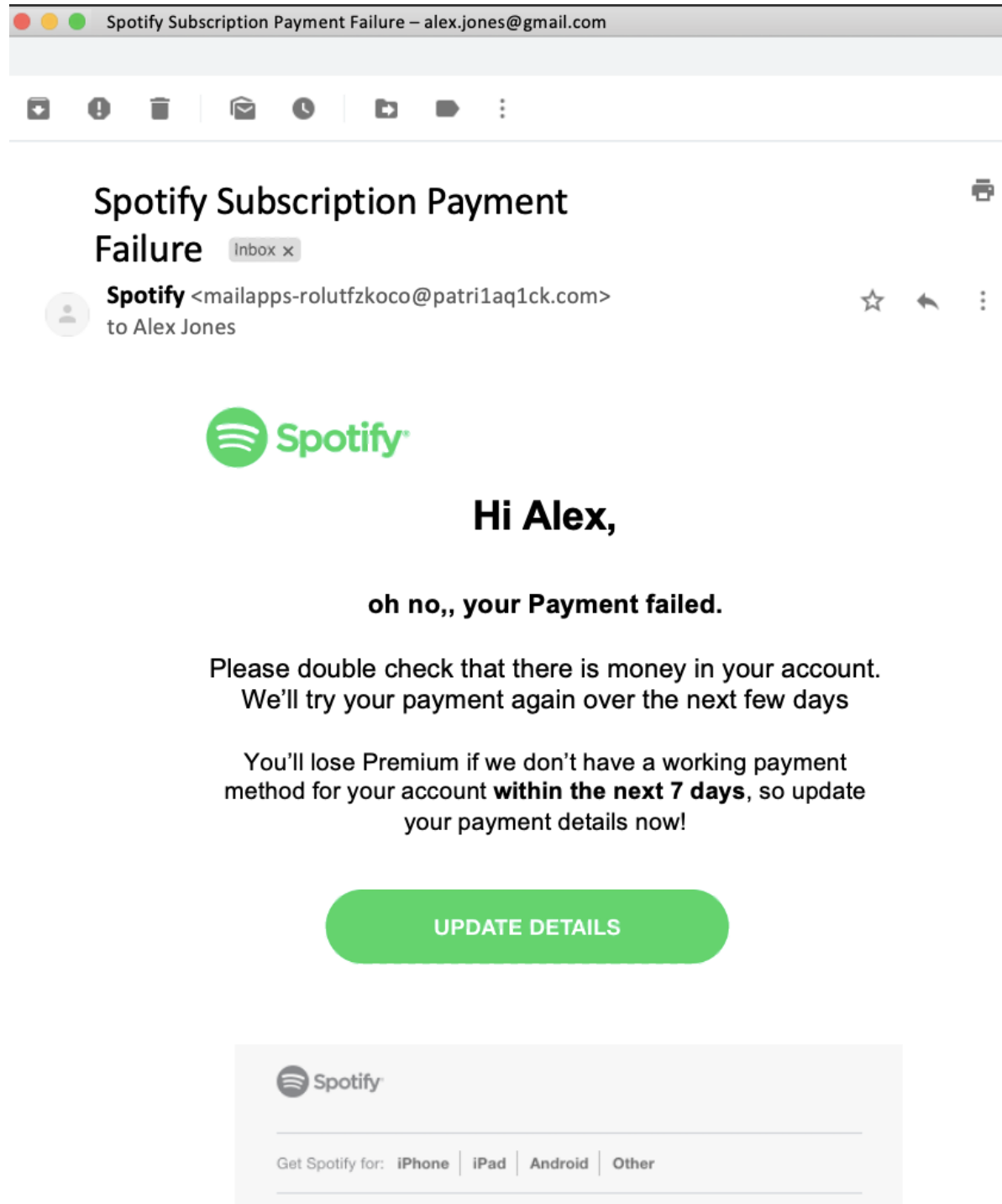
THE UNIVERSITY OF ADELAIDE
Room 726, Hughes Building
T: +61 8 8313 7464 | E: claire.frances@adelaide.edu.au



Phishing Stimuli: Cue – All 3 Phishing Cues

When hovering over the “update details” button, it leads to a phishing link:

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



The image shows a screenshot of an email client interface. The browser tab at the top reads "Spotify Subscription Payment Failure – alex.jones@gmail.com". The email header shows the subject "Spotify Subscription Payment Failure" with an "Inbox x" tag. The sender is "Spotify <mailapps-rolutfzkoco@patri1aq1ck.com>" and the recipient is "to Alex Jones". The email body features the Spotify logo, a greeting "Hi Alex,", and a message: "oh no,, your Payment failed. Please double check that there is money in your account. We'll try your payment again over the next few days. You'll lose Premium if we don't have a working payment method for your account **within the next 7 days**, so update your payment details now!". A prominent green button labeled "UPDATE DETAILS" is centered below the text. At the bottom, a footer contains the Spotify logo and the text "Get Spotify for: iPhone | iPad | Android | Other".

Spotify Subscription Payment Failure

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

Hi Alex,

oh no,, your Payment failed.

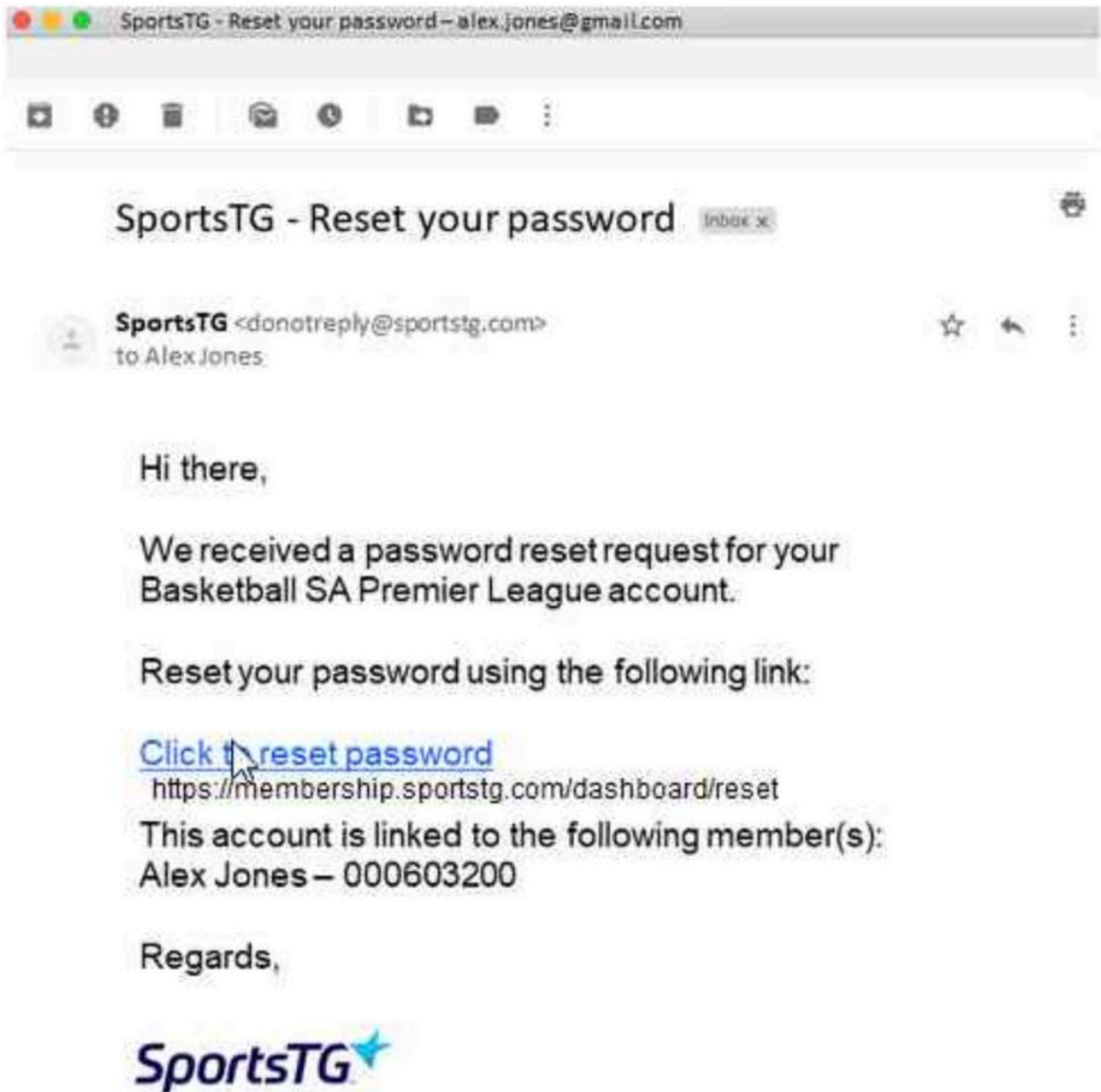
Please double check that there is money in your account.
We'll try your payment again over the next few days

You'll lose Premium if we don't have a working payment method for your account **within the next 7 days**, so update your payment details now!

UPDATE DETAILS

Spotify

Get Spotify for: iPhone | iPad | Android | Other

Appendix B: Function to hover-over link button to reveal URL within email stimulus

Appendix C: Email categorisation options and their descriptions in the Email-Sorting Task

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)

Appendix D: Adapted Decision-Making Scale Items (Hamilton et al., 2016)**Email-Specific (Clicking on a Link) Scale:*****Rational items***

1. I prefer to gather all the necessary information before deciding whether to click on a link in an email.
2. I thoroughly evaluate an email before deciding whether to click on a link in the email.
3. When deciding whether to click on a link in an email, I take time to contemplate the pros/cons or risks/benefits.
4. Investigating the facts is important when deciding whether to click on a link in an email.
5. I weigh a number of different factors when deciding whether to click on a link in an email.

Intuitive items

1. When deciding whether to click on a link in an email, I rely mainly on my gut feelings.
2. My initial hunch about deciding whether to click on a link in an email is generally what I follow.
3. I decide whether to click on links in emails based on intuition.
4. I rely on my first impressions when deciding whether to click on a link in an email.
5. I weigh feelings more than analysis when deciding whether to click on a link in an email.