

The Role of Cue Utilisation and Anxiety on Phishing Email Susceptibility

Annastasia Falkenberg

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

School of Psychology

University of Adelaide

October 2019

Word Count: 9,492

Table of Contents

List of Figures.....	v
List of Tables.....	vi
Abstract.....	vii
Declaration.....	viii
Acknowledgments.....	ix
Student Contribution to the Experimental Design.....	x
Introduction.....	1
Phishing Emails.....	1
Social persuasion in phishing emails.....	2
Individual Differences and Susceptibility to Phishing Emails.....	3
Cue utilisation.....	4
<i>Cues and Brunswik's Lens Model.....</i>	4
<i>System 1 and system 2 processing.....</i>	7
<i>Cues utilisation and cognitive load.....</i>	7
Anxiety and decision-making performance.....	8
<i>State and trait anxiety.....</i>	9
The Current Study.....	9
Aim and operationalisation.....	10
Hypotheses.....	9
Method.....	11

Participants.....	11
Design.....	11
Materials.....	11
Demographic questionnaire.....	11
Phishing Email Task (PET).....	12
Manipulation checks.....	15
Railroad task.....	16
State-Trait Anxiety Inventory (STAI).....	19
EXPERT Intensive Skills Evaluation (EXPERTise 2.0)	19
<i>Feature Identification Task (FIT)</i>	20
<i>Feature Recognition Task (FRT)</i>	20
<i>Feature Association Task (FAT)</i>	21
<i>Feature Discrimination Task (FDT)</i>	21
<i>Feature Prioritisation Task (FPT)</i>	22
National Aeronautics and Space Administration Task Load Index (NASA- TLX)	24
Procedure.....	24
Results.....	26
Overview of Analysis.....	26
Data Reduction.....	26
Data Analysis.....	29
Stage 1: Establishing Typologies.....	29
<i>Cue Utilisation</i>	29
<i>Anxiety</i>	30

Stage 2: Hypothesis Testing.....	31
<i>H1: Participants could discriminate between genuine and phishing emails.....</i>	31
<i>H2. Participants with higher levels of cue utilisation will have a higher capacity to discriminate phishing emails from genuine emails, relative to those with lower levels of cue utilisation.....</i>	31
<i>H3. Participants with higher levels of cue utilisation would perceive a phishing email task as less cognitive demanding, relative to those with lower levels of cue utilisation.....</i>	32
<i>H4a. Participants with higher levels of trait anxiety will have a lower capacity to discriminate between genuine and phishing emails, relative to those with lower levels of trait anxiety.....</i>	32
<i>H4b: Participants with higher levels of state anxiety will have a lower capacity to discriminate between genuine and phishing emails, relative to those with lower levels of state anxiety.....</i>	34
Discussion.....	35
Overview.....	35
Cue Utilisation and Phishing Susceptibility (H2).....	35
Subjective Workload and Cue Utilisation (H3).....	36
Anxiety and Phishing Susceptibility (H4a and H4b).....	37
Implications of the Findings.....	38
Strengths.....	39
Limitations and Future Directions.....	40
Conclusion.....	41
References.....	42

Footnotes.....	47
Appendix A: Advertisement Flyer.....	48
Appendix B: Demographic questionnaire.....	49
Appendix C: Example of Emails.....	50
Appendix D: Social Persuasion Definitions and Rating Scale.....	57
Appendix E: Manipulation Check 1 Results.....	58
Appendix F: Amendment to Consistency Email.....	59
Appendix G: Manipulation Check 2 Results.....	60
Appendix H: Paper-and-pencil version of the NASA-TLX.....	61
Appendix I: Online Participant Information and Consent Form.....	62
Appendix J: Instruction page for the PET.....	64
Appendix K: Summary of the email click-ability ratings from the PET for anxiety and cue utilisation typologies.....	65

List of Figures

Figure 1: The Lens Model.....	6
Figure 2: Examples of Emails Used.....	14
Figure 3: Experimental set up as viewed by participants displaying the PET (monitor 1: left) and the RRT (monitor 2: right).....	17
Figure 4: Simulated RRT as viewed by participants.....	18
Figure 5: EXPERTise 2.0 Cybersecurity Feature Prioritisation Task as viewed by participants.....	23
Figure 6: Experimental set up of participant completing both tasks simultaneously.....	25
Figure 7: Experimental workflow of the current study.....	25
Figure 8: Discrimination scores for individuals categorised with levels of high and low cue utilisation.....	32
Figure 9: Discrimination scores for individuals categorised with levels of high and low trait anxiety.....	33
Figure 10: Discrimination scores for individuals categorised with levels of high and low state anxiety.....	34

List of Tables

Table 1: Centroid Values for EXPERTise Task Clusters.....30

Abstract

A 'phishing email' is an attempt to solicit personal or sensitive information from an unsuspecting user. Phishing emails currently represent a major threat to cybersecurity, and as such, researchers have begun to recognise the importance of identifying various individual differences that might predict phishing email susceptibility. The current study aimed to further understand individual differences and examine the relationship between an individual's capacity for cue utilisation and levels of state/trait anxiety with phishing email susceptibility. Thirty-two participants completed a lab-based study where they were presented with a series of emails (phishing and genuine) and rated the extent to which they felt it was 'okay' to click on a link embedded within the email. Participants were then classified into typologies of cue utilisation and state/trait anxiety. While it was hypothesised that those categorised as having higher cue utilisation would be better able to discriminate between phishing and genuine emails, analyses did not support this prediction. However, it was found that those categorised as having higher levels of trait anxiety were less able to discriminate between phishing and genuine emails compared to their less anxious counterparts. The theoretical findings of the present study could help inform phishing education, training and awareness programs.

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.”

October 2019

Acknowledgements

I would first like to thank my supervisor, Dr. Jaime Auton. I feel very greatly to have learnt from such a passionate and dedicated mentor whose expertise inspired me to go that extra mile throughout this year. You have been such a genuine supervisor who was always there to reply to my last-minute emails and give me support when I needed it most. I am very fortunate to have worked with you and will be forever grateful for your time.

To my mum, thank you for being my biggest support this year. You were always there when times were tough and for that, I am so lucky. I know you will always be proud of me. I would also like to thank my friend, Mikaela, who has been there since my first year studying psychology. She has motivated me to get this far with my studies and I can't wait to see where the future takes us both.

I would also like to thank those who participated in my study and took time out of their day to complete it. This research would not have been possible without you.

Student Contribution to the Experimental Design

While the Honours research project is inevitably a collaborative process between the student and the supervisor, it is also important to highlight the aspects of the experimental design that were largely the product of the student's efforts. It would like to be acknowledged that all stimuli used for the 'Phishing Email Task' were created, and subsequently validated, by the student researcher. The Railroad Task and the measure of cue utilisation within the domain of cybersecurity used in this study were pre-existing measures. Furthermore, all data reported in this thesis, including the data reported within the two manipulation checks, was collected in full by the student researcher.

The Role of Cue Utilisation and Anxiety on Phishing Email Susceptibility

Susceptibility to phishing emails is an emerging body of research in psychological literature. Previous studies have begun to investigate the strategies used by ‘phishers’ to exploit individuals and identify the individual differences (such as age and gender) which might make some users more susceptible to such attacks (Akbar, 2014; Butavicius, Parsons, Pattinson, & McCormac, 2016; Ferreira & Teles, 2019; Parsons, Butavicius, Delfabbro, & Lillie, 2019; Parsons et al., 2016). However, there has been a dearth of research that has examined the individual differences of cue utilisation and state/trait anxiety and their relationship with phishing email susceptibility. As phishing email research is still relatively young, the current study aims to investigate these specific individual differences to contribute to the understanding of susceptibility to phishing emails. A greater understanding of this domain will likely lead to more tailored awareness campaigns and/or training programs to aid in development of phishing email detection skills.

Phishing Emails

Commonly engineered via email, phishing is the fraudulent practice of mimicking trustworthy or legitimate institutions in an attempt to solicit personal or sensitive information from online users (Akbar, 2014; Parsons et al., 2019). Phishing emails often request the recipient to reveal personal information (e.g., passwords) and/or inadvertently provide access to their computer network (e.g., through the installation of malware) (Butavicius et al., 2016). This can be achieved by asking the recipient to click on a seemingly routine email attachment such as an invoice or receipt (Telstra Corporation Limited, 2019), or a link embedded within the email (Parsons et al., 2019).

However, phishing attacks are now becoming more sophisticated, going beyond the usual indicators of visual deception and typographical errors, requiring recipients to pay attention to the plausibility of the message (Rajivan & Gonzalez, 2018). Consequently,

existing procedures and security tools which aim to detect these emails are becoming ineffective and potentially obsolete (Rajivan & Gonzalez, 2018). The Australian Competition and Consumer Commission (ACCC) stated ‘phishing’ was the highest reported method of scamming in 2018, with scams committed via email costing AU\$25.3 million in losses. More recently, a successful cyberattack on one of Australia’s leading universities, Australian Catholic University (ACU), saw phishers trick ACU staff with a falsified email prompting them to click on a link, or open an attachment related to an ACU login page. As a result, staff login details were comprised and used to successfully breach email accounts, calendars and back account details (Bastian, 2019). With the number of phishing emails predicted to increase in 2019 (Telstra Corporation Limited, 2019), there is an urgent need for future research to extend the understanding of how phishing emails can be recognised and who might be most vulnerable to these attacks.

Social persuasion in phishing emails. Phishing attacks continue to be so successful as they usually contain an element of social persuasion to assist in user compliance (Akbar, 2014; Rajivan & Gonzalez, 2018). Social persuasion is the scientific study of attitude or behaviour change due to real or imagined pressure (Guadagno, Muscanell, Rice, & Roberts, 2013). Within psychology, the most widely accepted classification of social persuasion is Cialdini’s six principles of influence; authority, reciprocity, consistency, liking, social proof, and scarcity (Akbar, 2014; Cialdini, 2007). The *authority* principle is used to engender fear, to influence people to obey commands to avoid negative consequences. The *reciprocity* principle is used to make people feel obliged to repay an act of kindness, or a favour. Under the *consistency* principle, people become psychologically vested to commit to a decision they have made. The *liking* principle is used to create trust and compliance with others they find attractive or perceive as credible. The *social proof* principle is used to make individuals feel the need to model the behaviour of their peer group, or important others.

Finally, the *scarcity* principle is based upon reactance, whereby people respond to perceived shortages of scarce items (Akbar, 2014). In the domain of phishing emails, phishers have used the authority principle to impersonate government organisations, such as the Australian Tax Office, to influence individuals to disclose personal details (Parsons et al., 2019). In an example of the scarcity principle, email phishers have masqueraded as delivery companies regarding a package that could not be picked up to encourage users to follow their requests (Parsons et al., 2019).

These principles have been directly manipulated in real-world phishing research to evaluate how people's susceptibility to social influence principles affects their response to phishing emails. In a novel, online study by Parsons et al. (2019), participants were presented with a series of genuine and phishing emails, each consisting of one social influence principle. The only indication of illegitimacy within each email was a link embedded in the content of the email. After reading each email, participants were asked to respond to the statement, 'It is okay to click on the link in this email' on a five-point Likert scale from 1(*Strongly disagree*) to 5(*Strongly agree*). Susceptibility was measured based on performance of whether participants were more likely to click on the link when embedded in phishing emails compared to genuine emails. Results indicated that different persuasion strategies had different effects on the likelihood participants would click on either a genuine or phishing email. Therefore, these strategies should be considered in future phishing research.

Individual Differences and Susceptibility to Phishing Emails

In addition to examining the effects of social persuasion principles on phishing email susceptibility, Parsons et al. (2019) also examined the role of various individual differences. Age and percentage of time spent on a computer were significant contributors in people's ability to detect phishing emails. Additionally, individuals with higher impulsivity were more likely to click on a phishing link embedded within an email, compared to a genuine link

(Parsons et al., 2019). In other research, the personality traits of conscientiousness (Lawson, Zielinska, Pearson, & Mayhorn, 2017), neuroticism and individualism (Butavicius et al., 2017), have also been linked to an increased detection of phishing emails. These findings highlight that individual differences play a role in phishing susceptibility. However, the individual differences of cue utilisation and anxiety have yet to be considered.

Cue utilisation. Conceptually, cues are thought to be unconscious associations in memory between features/s of an environment with an object/event (Wiggins, 2012). For example, as a result of extensive driving experience, it would be expected that motor vehicle drivers would have developed the cue association that a brake light on a car ahead (feature) usually means that the car ahead is stopping (event). This association is activated from long-term memory (LTM), which is a relatively permanent and unlimited storage for information acquired from past experiences. Therefore, a driver with an extensive experience in this domain should have a reservoir of cue patterns that pertain to different events (Croskerry, 2009). These patterns facilitate a more efficient process of interpretation, resulting in less deliberation (Wiggins, 2012).

Cues and Brunswik's Lens Model. Brunswik's (1955) Lens Model suggests individuals base their judgements on probabilistic cues, or attributes to evaluate elements in the environment (Mosier & Kirlik, 2004). The model characterises judgements as both a facet of the environment, and the mediator within it (Mosier & Kirlik, 2004). To understand judgement, the model requires three important concepts; ecological validity, cue utilisation validity, and achievement (Yang & Thompson, 2016). Ecological validity refers to the correlation between the proximal cues and an ecological criterion. Cue utilisation validity refers to the correlation between the proximal cues and the individual's judgements. Achievement refers to the correlation between the ecological criterion and the individual's judgement (Yang & Thompson, 2016).

The characteristics pertaining to the Lens Model can help us understand how individuals detect phishing emails. It has been empirically recognised that users often identify phishing emails as having more spelling or grammatical errors, and less personalisation or links that appear legitimate (Parsons et al., 2016). Consistent with the Lens Model, individuals base their judgements on a “lens” of information (or weighted cues) to infer the true state of an email (Parsons et al., 2019; Wang, Herath, Chen, Vishwanath, & Rao, 2012).

For example, using the Lens Model (see Figure 1), the ‘true state’ represents how much a proximal cue (e.g., a suspicious link) is correlated with an actual phishing email (i.e., ecological validity). The ‘judged state’ represents the importance an individual weights the suspicious link as representative of the true state of a phishing email (i.e., cue utilisation validity). ‘Accuracy’ represents how well the judged state (e.g., I think this is a phishing email) correlates with the true state (i.e., achievement). However, the judged state may not always be the same as the true state (Yang & Thompson, 2016). Thus, judges who weight cues appropriately, are more likely to be successful than individuals who make trade-offs among cues (Mosier & Kirlik, 2004). Arguably, cue utilisation may be a necessary precursor for phishing email detection.

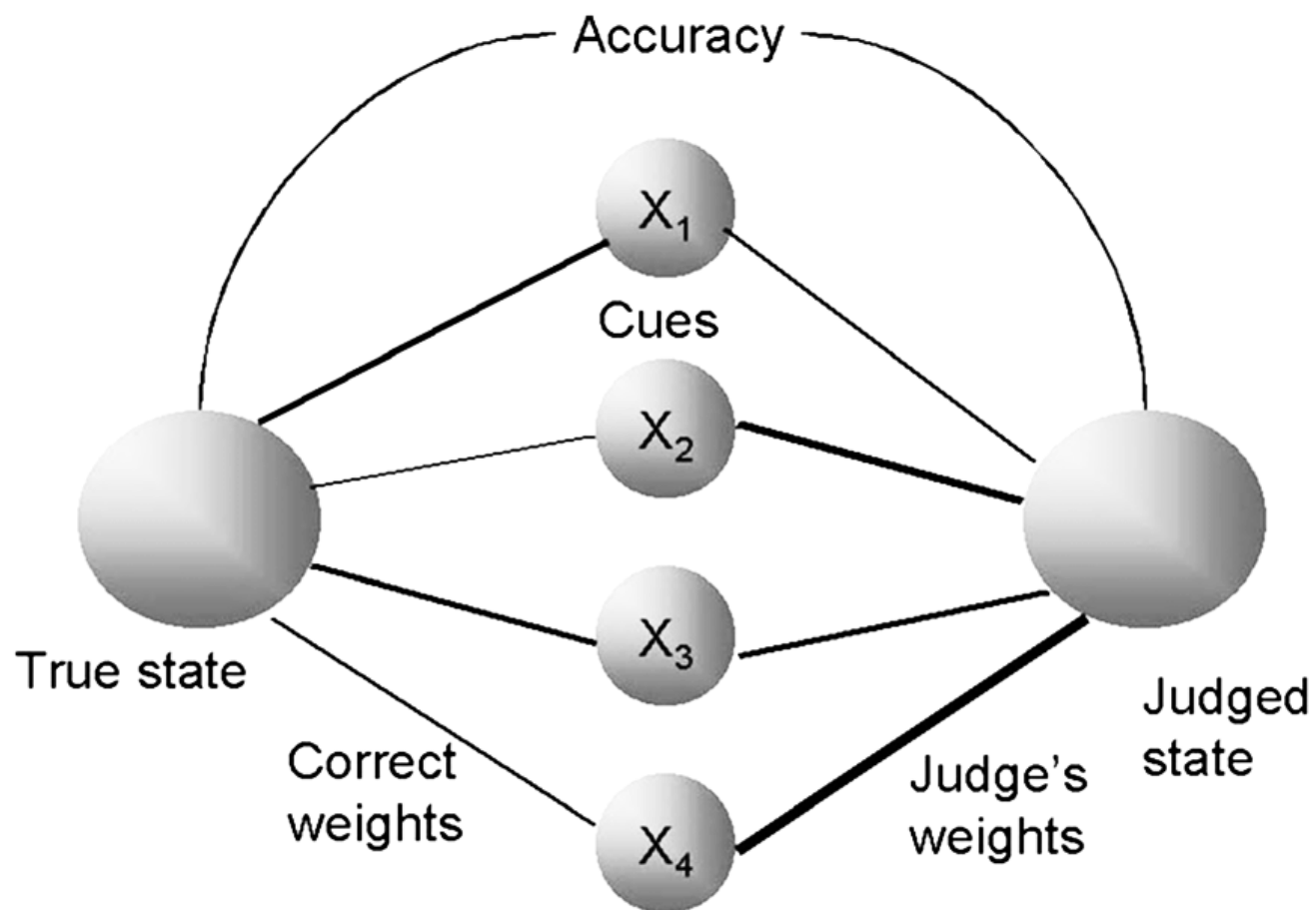


Figure 1. The Lens Model. Adapted from "Capturing judgement strategies in risk assessments with improved quality of clinical information: How nurses' strategies differ from the ecological model" by Yang, H., & Thompson, C. (2016). *BMC Medical Informatics and Decision Making*, 16(1)

System 1 and system 2 processing.

Additional to the Lens Model, the application of cues when recognising developing situations can be explained by two fundamental approaches to reasoning, System 1 and System 2 processing. System 1 involves automatic and unconscious mental shortcuts to help understand situations (Chen, Duckworth, & Chaiken, 1999). In uncertain and dynamic environments, System 1 facilitates the rapid assessment of information. On the other hand, System 2 involves slower, more systematic and analytical treatment of information to help understand situations (Croskerry, 2009). Therefore, individuals who do not possess the relevant cue associations stored in LTM, must engage in System 2 processing. For example, in a driving situation that requires a rapid response (e.g., a car switches lane unexpectedly), a less experienced driver who does not have relevant cues stored in LTM must engaged in System 2 processing to evaluate the situation. The driver may therefore crash due to the inability to engage in System 1.

Cue utilisation and cognitive load. One of the advantages associated with the application of cues (and System 1 processing) is that their activation imposes relatively fewer demands on cognitive load (Wiggins, Brouwers, Davies, & Loveday, 2014). Cognitive load refers to “the total amount of mental activity imposed on working memory at an instance in time” (Brouwers, Wiggins, Griffin, Helton, & O’hare, 2017, p. 1503). A reduction in cognitive load means that there are more resources available in working memory, thereby enabling individuals to undertake complex tasks with relatively consistent levels of accuracy. For example, in a novel pattern recognition task using simulated train control, Brouwers et al. (2017) demonstrated that under increased workload conditions, those with higher levels of cue utilisation demonstrated reduced response latencies and increased accuracy during a novel rail control task. This study suggests that for participants with higher cue utilisation, the imposition of increased workload did not affect their performance during the novel task.

Drawing on the above concepts, individuals with a relatively higher capacity for cue utilisation are expected to more rapidly and accurately differentiate between a phishing and genuine email, compared to those with a relatively lower capacity for cue utilisation.

Anxiety and decision-making performance. Currently, there is no research that has examined the relationship between state/trait anxiety and phishing email susceptibility. Of the literature that does exist, anxiety has been associated with detrimental effects on performance, particularly when tasks are demanding (Leon & Revelle, 1985). According to Leon and Revelle (1985), less anxious subjects allocate all their attentional resources to the designed task, whereas more anxious subjects divide their attention by allocating only part of their attentional resources to that task, and the remainder to self-relevant (i.e., task-irrelevant) concerns.

This can be understood by the Attentional Control Theory which postulates that anxious individuals have a processing bias towards threat-related information, and the negative interpretation of ambiguous stimuli (Hartley & Phelps, 2012). This has been observed across a variety of studies where anxious individuals recorded faster response times in detecting or identifying a threat-stimuli, and slower response times in reporting neutral information (Eysenck, Derakshan, Santos, & Calvo, 2007). This theory also asserts that anxious individuals have a tendency to negatively frame stimuli, even at the cost of missing potential gains (Hartley & Phelps, 2012). With this in mind, it would be expected that individuals with higher levels of anxiety would be better at identifying phishing emails due to their ability to engage in threat-related stimuli more readily than non-anxious individuals. However, by perceiving all ambiguous stimuli as a potential threat, anxious individuals might be more likely to perceive genuine emails as more threatening too. Arguably, this would suggest that individuals who are relatively more anxious might be less able to discriminate phishing from genuine emails compared to their less anxious counterparts.

State and trait anxiety. In an attempt to capture the multiple facets of anxiety, Cattell (1966) introduced two concepts of anxiety, state and trait, later elaborated by Spielberger (1983). *State anxiety* refers to “a transitory emotional response involving unpleasant feelings of tension and apprehensive thoughts” (Caci, Baylé, Dossios, Robert, & Boyer, 2003, p. 395). In contrast, *trait anxiety* refers to “individual differences in the likelihood that a person would experience state anxiety in a stressful situation” (Caci et al., 2003, p. 395). Studies have found that the impacts of anxiety on attention is an interactive function of both state and trait anxiety (Quigley, Nelson, Carriere, Smilek, & Purdon, 2012). Therefore, the relative roles of trait and state anxiety in attentional biases cannot be determined from studies that examine only trait or state, as both tend to confound each other (Quigley et al., 2012). As a result, it is unclear whether state and trait anxiety play a similar or different role in the context of phishing email susceptibility.

The Current Study

Aims and operationalisation. The aim of the current study was to understand how the individual differences of cue utilisation and state/trait anxiety relate to phishing email susceptibility. In line with the method used in Parsons et al. (2019), susceptibility was measured based on performance in a novel phishing email task. This task was lab-based and required participants to appraise a series of incoming emails which were created as either genuine or phishing. Each email was designed using a direct manipulation of one of Cialdini’s (2007) six social persuasion principles.

Cue utilisation was operationalised using a software package (EXPERTise 2.0; Wiggins, Loveday, & Auton, 2015) which is customised to record performance in response to cues within the domain of cybersecurity. Performance on EXPERTise 2.0 classified participants into two ‘typologies’ representing participants with relatively higher and lower levels of cue utilisation. Anxiety was measured using the State-Trait Anxiety Inventory

(Spielberger, 1983) classifying participants as having either high or low levels of state and trait anxiety. The NASA-Task Load Index was also administered as a subjective measure of perceived workload of the phishing email task-

Hypotheses.

H1: It was hypothesised that participants would be able to discriminate between genuine and phishing emails.

H2: It was hypothesised that participants with higher levels of cue utilisation would have a higher capacity to discriminate between phishing emails and genuine emails, relative to those with lower levels of cue utilisation.

H3: It was hypothesised that participants with higher levels of cue utilisation would perceive the phishing email task as less cognitive demanding, relative to those with lower levels of cue utilisation.

H4a: It was hypothesised that participants with higher levels of trait anxiety would have a lower capacity to discriminate between genuine and phishing emails, relative to those with lower levels of trait anxiety.

H4b: It was hypothesised that participants with higher levels of state anxiety would have a lower capacity to discriminate between genuine and phishing emails, relative to those with lower levels of state anxiety.

Method

Participants

Thirty-two participants were recruited for the current study (11 males, 21 females). Fifteen participants were recruited from the general public using snowball and convenience sampling via social media, word of mouth and advertisement flyers (see Appendix A). Additionally, seventeen first-year psychology students from the University of Adelaide were recruited using SONA Systems, the University's online participant pool. Participants were aged between 18 and 54 years old ($M = 23.38$, $SD = 7.63$). Participants were required to be 18 years or older and fluent in English.

Design

The current study was a face-to-face lab-based study. The study comprised two, 2 x 2 mixed, experimental designs. The first 2 x 2 design had two cue utilisation typologies (higher, lower) as the between groups factor, and email condition (phishing, genuine) as the within-groups factor. Participants were classified with either higher or lower cue utilisation based on an assessment of cue utilisation within the context of cybersecurity. The dependent variable was performance in a phishing email task and a measure of subjective workload.

The second 2 x 2 design had two anxiety typologies (high, low) as the between groups factor, and email condition (phishing, genuine) as the within-groups factor. Participants were classified with high and low levels of state and trait anxiety using an assessment that captured both state-trait anxiety. The dependent variable was performance in a phishing email task.

Materials

Demographic questionnaire. Participants were asked to complete a series of demographic questions indicating their age, gender, time spent using a computer per day, confidence with computer use, level of English fluency, and number of emails received per day (see Appendix B).

Phishing Email Task (PET). As per the recommendations of Parsons et al. (2019), it was important to ensure that participants partaking in the current study were unaware that they were signing up for an experiment related to phishing email detection. This approach was taken to avoid subject expectancy bias. Indeed, previous research has found that if participants are informed they are involved in a phishing study they tend to err on the side of false alarms (classifying a legitimate email as phishing) rather than misses (classifying a phishing email as legitimate) (Lawson et al., 2017). To avoid priming participants as to the true nature of the study, participants were informed that they were electing to participate in a study on ‘how people manage their emails, and the factors that may affect email use’.

An online experimental platform was used to deliver the novel phishing email task (PET) which was largely consistent with that described in Parsons et al. (2019). During the PET, participants were asked to read and respond to a randomised series of 21 emails (plus two practice emails); 14 genuine emails and 7 phishing emails. A greater number of genuine email stimuli, compared to phishing, was used in an effort to reflect real-world email correspondence (Parsons et al., 2019). All personal details within each email were modified to that of a fictitious individual with a gender-neutral name (i.e., Alex Jones). Participants were instructed that all emails were taken from the inbox of ‘Alex Jones’ and to assume that they were deliberately sent and of relevance to them. Participants were exposed to each email for 30 seconds after which they were automatically directed to answer the statement, ‘It is okay to click on the link in this email’. Participants selected the extent to which they agreed with the statement on a five-point Likert scale from 1(*Strongly Disagree*) to 5(*Strongly Agree*).

The nature of the emails used were adapted emails either found online or received by the researchers which all appeared to be sent from large national or international organisations. These emails were representative of the types of topics that would be expected

in a typical inbox as well as types of institutions commonly targeted for phishing attacks (Parsons et al., 2019), such as Australia Post, the Australian Federal Police, and Facebook. In line with Parsons et al. (2019), the series of emails were constructed using a direct manipulation of Cialdini's (2007) social persuasion principles (i.e., authority, consistency, liking, reciprocity, scarcity and social proof). Of the 14 genuine emails that comprised this task, there were two emails that incorporated each of the six principles and two that were constructed with no social principle. Of the seven phishing emails that comprised this task, there was one email that incorporated each of the six principles and one that was constructed with no social principle. The distribution of social principles across the emails was in line with Parsons et al. (2019). Examples of emails used are provided in Appendix C.

The only cue that an email was a 'phish' was the embedded link within the email text displayed next to a prompt button 'Click Here'. During real-world email activity, individuals can hover over a prompt button to see the link associated with the prompt. However, the online experimental platform that was used in the current study was limited as such that displaying the link adjacent or below to the 'Click Here' button was the best alternative to this real-world experience. Emails created as 'genuine' showed a legitimate link taken from legitimate emails (e.g., a genuine email from National Crime Check included the link https://www.nationalcrimecheck.com.au/consumer/start_form), whereas emails created as 'phishing' showed a link that had previously been included in a verified phishing email (e.g., a phishing email from the Australian Federal Police included the link <http://www.dekurator-sklep.pl/gen/cimb/index.htm>) (see Figure 2). All phishing links were directly taken from Parsons et al. (2019) with permission.

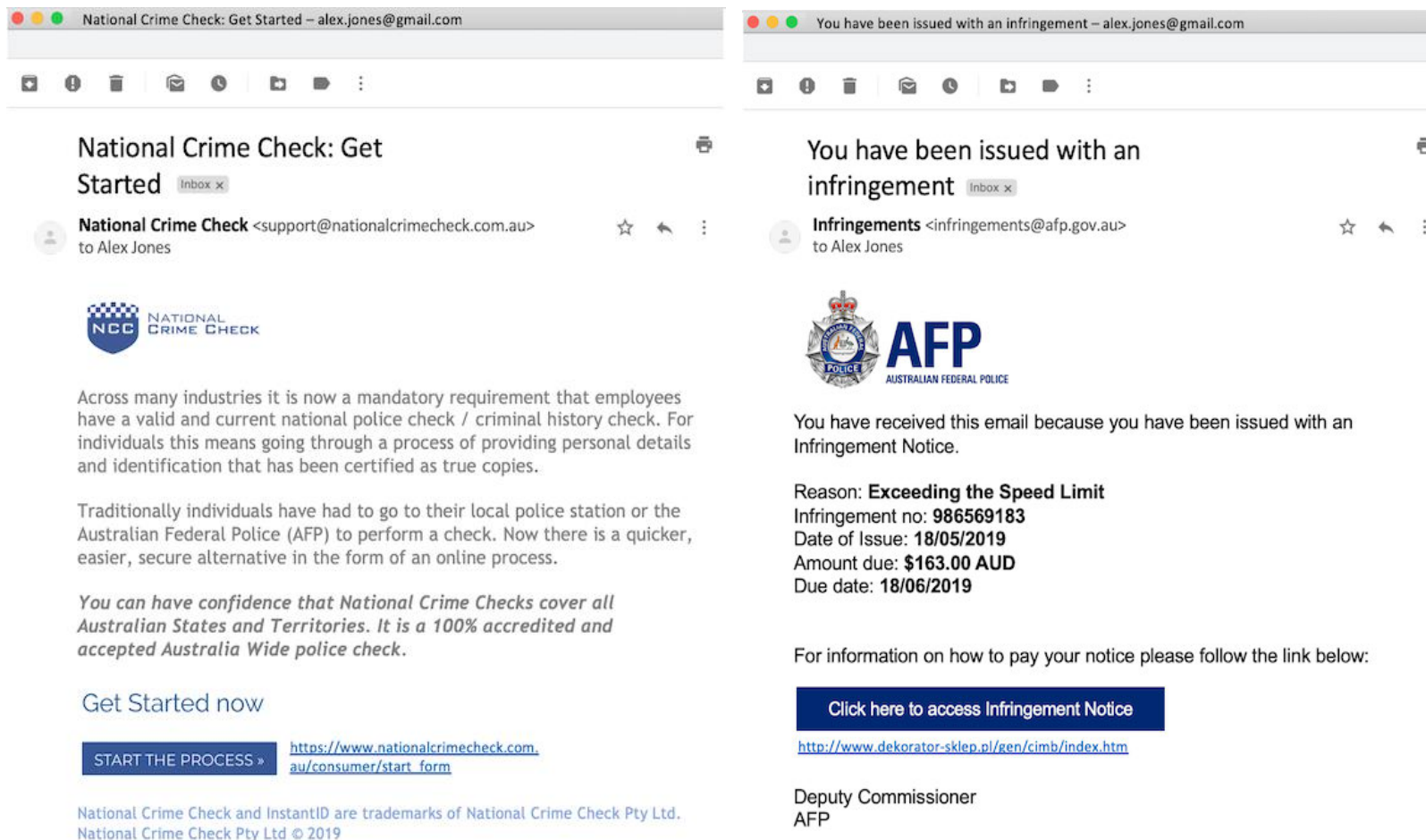


Figure 2. Example of Emails Used. Left: A genuine email, using the ‘authority’ social persuasion principle, with prompt button ‘Start the Process’ and corresponding adjacent link. Right: A phishing email, also using the ‘authority’ social persuasion principle, with prompt button ‘Click here to access Infringement notice’ and corresponding link below.

Manipulation checks. Two manipulation checks pertaining to the email stimuli were conducted. Manipulation check 1 aimed to assess whether the affiliated Cialdini (2007) social persuasion principles embedded within each email were recognised accordingly.

Manipulation check 2 aimed to assess whether participants could discriminate between the genuine and phishing emails to ensure there were no ceiling or floor effects. This manipulation check was conducted as previous studies have found that individuals are quite naive in judging the legitimacy of a link, regardless of whether the email was phishing or genuine (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010; Parsons et al., 2019).

Both manipulation checks followed the same procedure. Specifically, they were conducted through an online experimental platform and took participants less than 20 minutes to complete. Consistent with the main study, all participants were informed that they were taking part in a study on ‘how people manage their emails, and the factors that may affect email use’ and hence were not explicitly told they would be responding to phishing emails. Participants were recruited through social media announcements within the researchers’ networks and required to be fluent in English and be 18 years or older.

Eleven participants were recruited for manipulation check 1. In line with the strategy by Parsons et al. (2019), participants were presented with definitions of each principle and asked to rank up to three principles that were most apparent in each email (see Appendix D for definitions). Participants were also provided with a ‘no-principle’ option. For 18 of the 21 emails, the principle that was *most* frequently selected to be *most* present, matched the intended principle. For example, for the emails that were manipulated to contain the ‘liking’ principle, ‘liking’ was ranked as the most present principle by 73% of participants; see full table of results in Appendix E. In two emails where the intended principle was not ranked as most present, participants still recognised the principle in their second or third rank. An amendment to one email was made, as its intended principle ‘consistency’ was not

recognised by participants (see Footnote 1). These results provided sufficient evidence to suggest that the emails that were manipulated to emulate a specific social persuasion principle were in fact perceived in line with their intended principle.

Twelve participants were recruited for manipulation check 2. Participants were exposed to the 21 emails used in the main study for 30 seconds and on the subsequent screen asked to respond to the statement 'It is okay to click on the link in this email'. Responses were measured on a five-point Likert scale from 1(*Strongly disagree*) to 5(*Strongly Agree*). On average, participants reported significantly lower ratings to click on the link of phishing emails ($M = 2.00$, $SD = .72$) compared to genuine emails ($M = 3.72$, $SD = .52$), $t(11) = -6.42$, $p < .001$, $r = -.11$. This was consistent across all principles of social persuasion except social proof; see full table of results in Appendix G. These results were sufficient enough to indicate that overall, individuals were able to discriminate between genuine and phishing emails.

Railroad task. The use of a simulated railroad task was introduced as a concurrent, secondary task to increase cognitive workload while completing the PET. This task was completed simultaneously, but on a separate monitor (see Figure 3). The purpose of this secondary task was to maximise the cognitive resources needed to complete both tasks to a satisfactory level. This ensured that participants did not have enough time or cognitive resources available to use System 2 processing and analyse the email content in detail. This strategy 'forced' participants to activate System 1 processing and use any available cues related to phishing email detection. Participants were not told which task was the primary task and thus expected to allocate the necessary cognitive resources to complete each task satisfactorily.

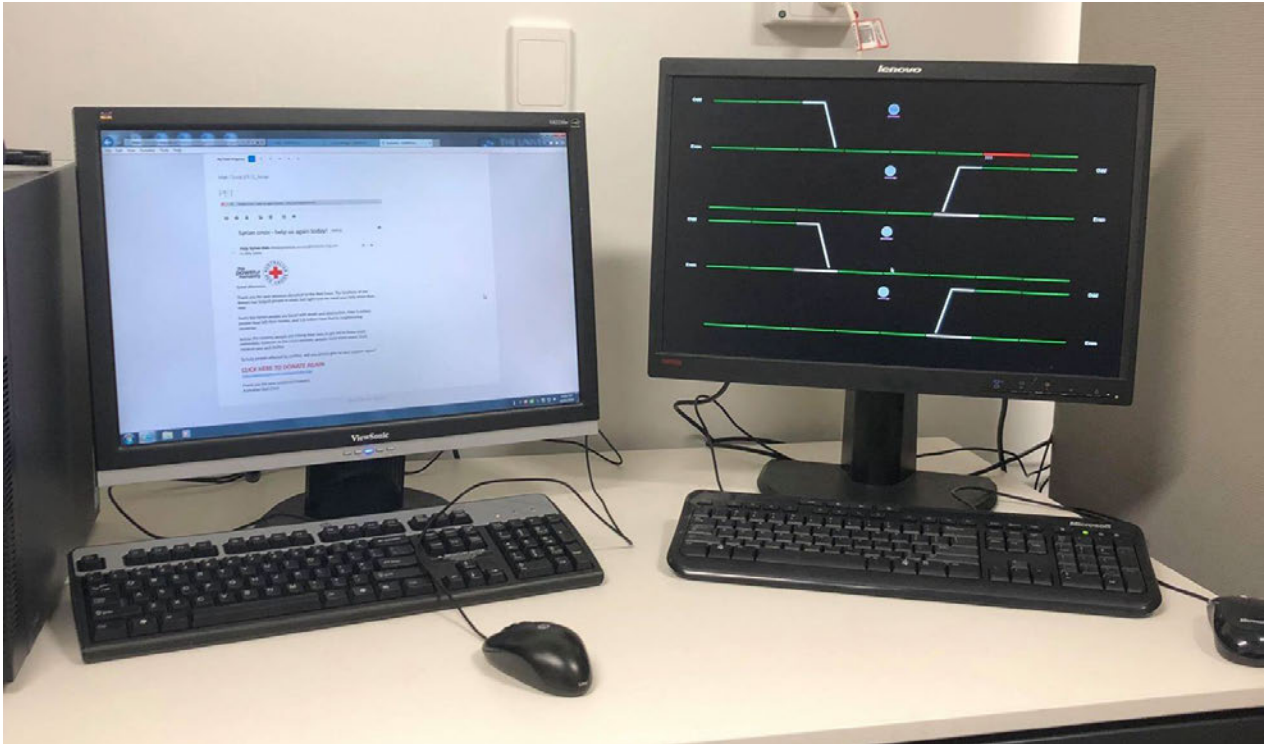


Figure 3. Experimental set up displaying the PET (Monitor 1: left) and the railroad task (Monitor 2: Right).

The railroad task required participants to re-route trains that periodically required diversion, ensuring each train arrived at its appropriate destination. Four green railway tracks ran horizontally across the screen, each with an intersection to form ODD and EVEN endpoints (see Figure 4). The intersection was marked by a white portion of the track and indicated the point in which a diversion was required. The train was represented as a red line, which moved either from right to left of screen, or vice versa, allocated with a recurring three-digit number. Odd numbered trains were to arrive at endpoints labelled 'ODD', and even numbered trains were to arrive at endpoints labelled 'EVEN'. If the train was on a misrouted track (i.e., an ODD train moving towards an EVEN endpoint), participants were required to click a grey icon, positioned adjacent to the intersection track, labelled 'change' to divert the train to its correct route.

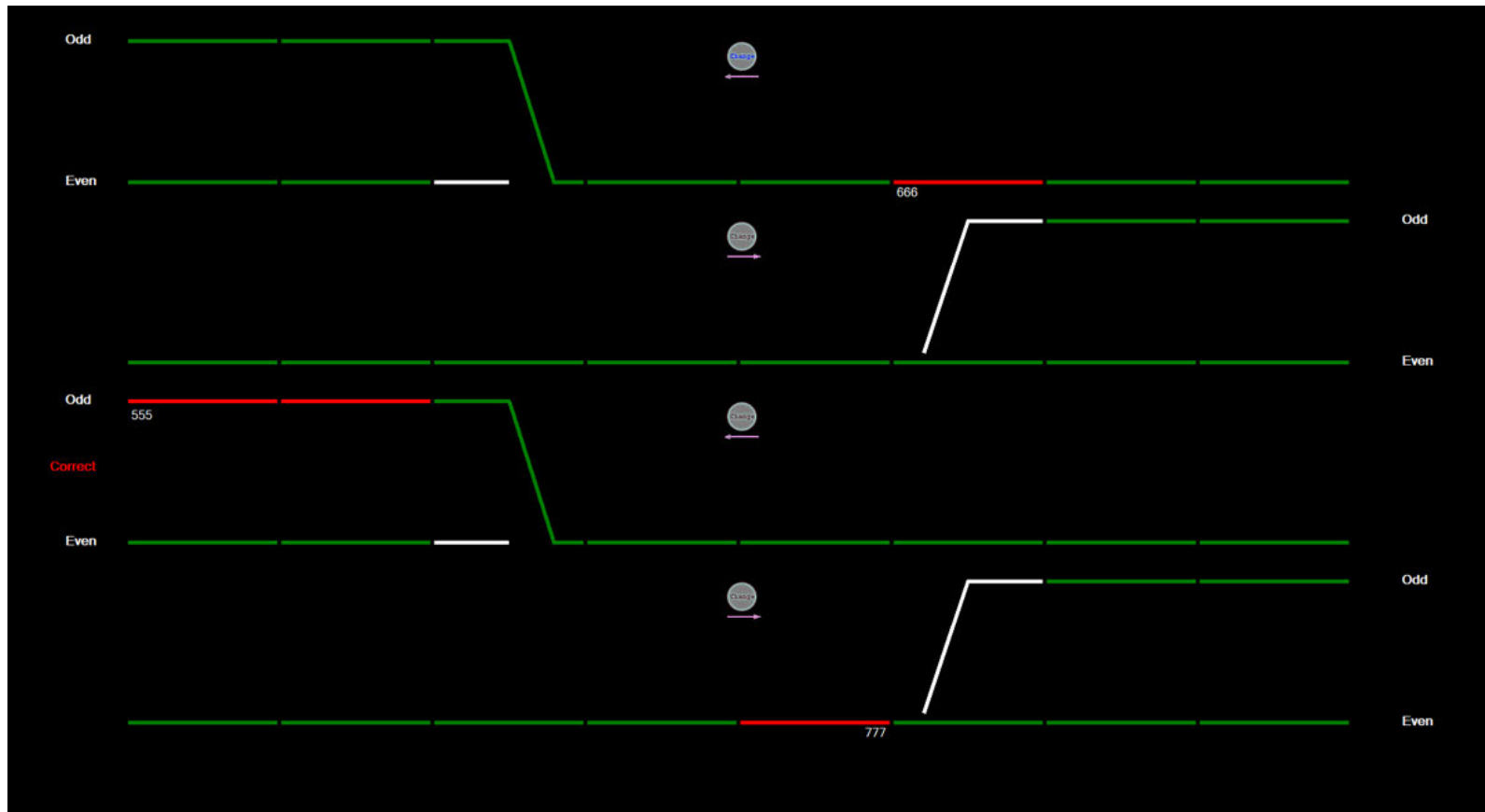


Figure 4. Simulated railroad task as viewed by participants. The green lines represent the railroad, while the red lines represent the train accompanied with either an EVEN or ODD number. For example, the top track has a train labelled with an EVEN number moving towards the left of screen; however, it is programmed to continue on the ODD track. Therefore, it requires diversion by clicking 'change' before reaching the white line intersection point.

The railroad task was set up so that every 7 seconds, a new train would enter the screen requiring a decision to be made by participants. Based on the duration of the PET, this task ran for 15 minutes to ensure participants did not complete this task prior to finishing the PET. This was consistent for all participants to keep workload controlled.

State-Trait Anxiety Inventory (STAI). To measure state and trait anxiety, participants completed the STAI (Form Y; (Spielberger, 1983). The STAI uses two bipolar and unidimensional scales containing state–trait “anxiety present” items and state–trait “anxiety absent” items (Caci et al., 2003). This type of item pool is referred to as ‘balanced’ as items are polarised either towards anxiety or the opposite pole of anxiety. All items are self-reported on a 4-point Likert scale ranging from 1(*Not at all*) to 4(*Very much so*).

The S-Anxiety scale consists of 20 self-report items, provided as short statements, with instructions “how you *feel* right now, *at this moment*”. Half of these items are worded positively to measure the absence of S-anxiety (e.g., “I feel calm”), whilst the other half are worded negatively to measure the presence of S-anxiety (e.g., “I feel tense”). This scale was designed to be sensitive to the conditions under which the test is administered (Spielberger, 1983). The T-Anxiety scale also consists of 20 self-report items however are answered based on “how do you *generally* feel”. Seven of these items are worded positively to measure the absence of T-anxiety (e.g., “I feel pleasant”), whilst the remaining 13 are worded negatively to measure to presence of T-anxiety (e.g., “I worry too much over something that really doesn’t matter”). This scale is relatively impervious to conditions under which it is given, rather, capturing the personality trait of anxiety (Spielberger, 1983).

EXPERT Intensive Skills Evaluation (EXPERTise 2.0). EXPERTise 2.0 (Wiggins, Loveday, & Auton, 2015) is a shell software package that can be customised to assess participants’ utilisation of cues during task-related activities within a specific domain. Typologies of behaviour that reflect higher or lower levels of cue utilisation are calculated,

the validity of which has been established in power control (Loveday, Wiggins, Harris, O'Hare, & Smith, 2013) and aviation decision making (Wiggins, Azar, Hawken, Loveday, & Newman, 2014). EXPERTise 2.0 has also demonstrated satisfactory test-retest reliability (Watkinson, Bristow, Auton, McMahon, & Wiggins, 2018).

In the current study, participants completed the cybersecurity 'edition' of EXPERTise 2.0, which comprises five tasks of domain-specific stimuli: Feature Identification Task, Feature Recognition Task, Feature Association Task, Feature Discrimination Task and the Feature Prioritisation Task. The EXPERTise 2.0 assessment was completed after the PET to ensure that the cybersecurity related stimuli did not prime participants to the true nature of the study.

Feature Identification Task (FIT). Feature identification is based on the observation that experts are able to identify and utilise visual features in the environment that are more diagnostic of the system state compared to novices (Schriver, Morrow, Wickens, & Talleur, 2008). In the FIT, participants are required to identify key features within a complex scene. The FIT presents participants with 16 incoming emails (including two practice trails) in a random order, each taken from the inbox of fictional individuals. Using a mouse, participants select the area of the email which they consider the greatest concern (e.g., a suspicious email address). Participants speed of response is recorded in milliseconds, with lower response latencies associated with higher cue utilisation (Loveday, Wiggins, & Searle, 2013).

Feature Recognition Task (FRT). Feature recognition measures the accuracy in which participants can make a decision based on the recognition of critical features (Brouwers, Wiggins, & Griffin, 2018). In the FRT, participants are exposed to a series of 22 emails (including two practice trials) for 1000 milliseconds. Participants must decide whether they think that the email is 'trustworthy', 'untrustworthy' or 'impossible to tell' from the information available to them in the short period of exposure. It is thought that greater

accuracy on this task is indicative of higher levels of cue utilisation (Brouwers, Wiggins, & Griffin, 2018).

Feature Association Task (FAT). Feature association measures the extent to which participants are able to discriminate between relevant and less relevant associations between feature-event/object pairs (Wiggins et al., 2014). In the FAT, participants are shown 16 pairs of words presented for 1500 milliseconds (e.g., Email and Task). Using a 7-point Likert scale, participants are asked to indicate how related they perceive the words to be from 1(*extremely unrelated*) to 7(*extremely related*). The mean variance is calculated, with a greater mean variance indicative of their capacity to distinguish related from unrelated features and events/object, and hence, higher cue utilisation (Wiggins et al., 2014).

Feature Discrimination Task (FDT). Feature discrimination measures the capacity for individuals to discriminate between task-relevant and irrelevant features during a decision-making scenario. 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 the information presented within the email, participants must then select a subsequent course of action to take from a list of four (e.g., Ignore the Email). In addition, participants must rate the utility of the individual features within the email (e.g., 'Date of email' or 'Location of purchase') that influenced their decision using 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 utility between the cues in the scenario and hence, higher cue utilisation (Loveday, Wiggins, & Searle, 2013).

Feature Prioritisation Task (FPT). Feature prioritisation is based on the finding that expert and novice operators vary in their approach taken to access task-relevant information in the initial assessment of a situation (Wiggins & O'Hare, 1995). Novice operators tend to

acquire information based on their visual presentation, whilst experts are more discriminating in their approach extracting information on their basis of relevance (Wiggins & O'Hare, 1995). In the FPT, participants are presented with two incomplete email scenarios each with a small vignette (e.g., You have received an email from a colleague overseas). Participants are told that they can access further information pertinent to the scenarios from a list of dropdown tabs (see Figure 5). Participants are only given 30 seconds to access as much information as they deem necessary. After the time limit has elapsed, participants progress to a new page and asked, "How do you respond to this email?". Higher cue utilisation is associated with a greater proportion of pairs of information tabs accessed in the sequence they are presented, calculated as the proportion of the total number of pairs of information tabs accessed (Wiggins & O'Hare, 1995).

The screenshot shows a web interface for the EXPERTise 2.0 program. At the top, there is a navigation bar with a plus sign and a URL: `Participant/Project/Scenario?projectId=384&taskOrder=4&scenarioOrder=0&preview=True&scenarioPreview=False`. Below the navigation bar is the EXPERTise 2.0 logo, which includes the text "Expert Intensive Skills Evaluation Program".

The main content area is titled "My Task Progress" and shows a progress indicator with six numbered tabs (1-6). The current task is "Cybersecurity V2_Annie" and the specific task is "Feature Prioritisation Task".

The task description reads: "You have received an email from a colleague overseas. Access the information below that you think is necessary to establish whether the email content should be trusted."

A timer indicates "You have 0 seconds remaining to make your decision". Below the timer, a red text prompt says "Click on the tabs below to access the relevant information".

The interface lists 15 features for prioritization, each with a right-pointing arrow icon:

- Age and gender of colleague
- Relationship with colleague
- Country that colleague is in
- Time Email Sent
- Time the email was opened
- Sender's Email Address
- Email Subject
- Sender's Company
- Email Logo
- Email Greeting
- Email Content
- Hyperlink address
- Email Sign-off

At the bottom right, there is a blue button labeled "My Decision" and a small text prompt: "Click here only when you are ready to make your final decision".

Figure 5. EXPERTise 2.0 Feature Prioritisation Task as viewed by participants.

NASA-Task Load Index (TLX). The NASA-TLX is a subjective measure of workload using a multidimensional rating scale with six bipolar dimensions of workload: mental demand; physical demand; temporal demand; own performance; effort; frustration (Hart & Staveland, 1988). An item for each dimension was administered (e.g., mental demand: “how high were the *mental demands* of the task?”; own performance: “how *successful* do you think you were in accomplishing the task?”). Apart from ‘own performance’, which is responded to using a scale from 1(*not successful*) to 7(*successful*), all other dimensions are measured from 1(*low*) to 7(*high*). This index was administered using paper-and-pencil (see Appendix H) immediately after participants completed the PET and railroad task. The NASA-TLX is one of the most widely used measurement tools to assess subjective workload in high-risk, time sensitive industries (Tubbs-Cooley, Mara, Carle, & Gurses, 2018).

Procedure

Ethics approval was obtained from the subcommittee in the School of Psychology at the University of Adelaide (Ref No: 19/41). Upon arrival, participants were briefed and directed to two adjacent computer monitors. On monitor 1, participants were required to read an online participant information form and provide electronic consent (see Appendix I). Participants then completed the demographic questionnaire, followed by the STAI. During this section of the task, the researcher remained outside of the room. Upon completion, participants were notified to alert the researcher, after which the PET was loaded on monitor 1 and the railroad task was loaded on monitor 2. Instructions for the PET were displayed on screen in the pre-amble of the task, aided by an example (see Appendix J). Instructions for the railroad task were explained using standardised written instructions, with participants required to complete a 2-minute practice trial. Participants then commenced both tasks simultaneously on respective monitors (see Figure 6).



Figure 6. Experimental set up of participant completing both tasks simultaneously (PET on monitor 1: left) and the railroad task on monitor 2: right).

After completing the dual tasks, participants completed the paper-and-pencil version of the NASA-TLX. Participants then completed the EXPERTise 2.0 cue utilisation task battery on monitor 1. A debrief with participants took place immediately following the session to discuss any queries or concerns relating to the study. Experimental sessions took approximately 60 minutes. A summary of the experimental process can be seen in Figure 7.

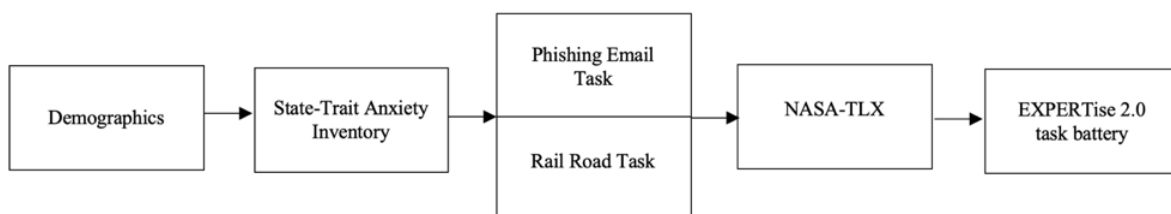


Figure 7. Experimental workflow of the current study.

Results

Overview of Analyses

The primary aim of the current study was to examine whether two typologies of participants, categorised on the basis of cue utilisation, differed in their discrimination of phishing from genuine emails and also their perception of cognitive workload during this task. A secondary aim was to examine whether two typologies of participants, categorised on the basis of state and trait anxiety, differed in their discrimination of phishing from genuine emails. Data was analysed in two stages using IBM Statistical Package for Social Sciences (Version 25). The first stage of analysis included establishing typologies of participants based on scores for the cue utilisation and anxiety measures to form the independent variables. The second stage of the analysis examined the hypotheses.

Data Reduction

Data pertaining to the EXPERTise 2.0 battery, the PET, the STAI, and the railroad task all underwent data reduction. The data reduction for the EXPERTise 2.0 tasks was consistent with the standard approach to the analysis of this data (Brouwers, Wiggins, Helton, O'Hare, & Griffin, 2016; Loveday, Wiggins, Harris, et al., 2013). For the Feature Identification Task, the mean response latency to identify the critical feature within the email was determined across the 16 scenarios. For the Feature Recognition Task, participants' summed accuracy in identifying phishing emails was calculated across the 22 scenarios. For the Feature Association Task, ratings of perceived association between feature-event pairs across the 16 scenarios were combined into a single discrimination metric to reflect a mean variance score of participants' responses. For the Feature Discrimination Task, the ratings of importance for each 10 features were recorded on a 10-point Likert scale, from 1(*not important at all*) to 10(*extremely important*) and the mean of variance of these ratings was created for the two scenarios. The two mean variances were combined to form one mean. Finally, for the Feature

Prioritisation Task, the ratio of pairs of features that were selected in sequence, compared to the total number of pairs of features available, were recorded to form a mean ration for the two scenarios.

Data reduction from the PET took place in two stages. Participants response to the statement ‘It is okay to click on the link in this email’ was considered for each email. In line with Parsons et al. (2019), a response of 1(*Strongly disagree*) was considered most appropriate when responding to a phishing email, and a response of 5(*Strongly Agree*) was considered most appropriate when responding to a genuine email. A response of 3(*Neither Agree nor Disagree*) was considered a neutral rating. In the first stage, a “click-ability” score for each email condition (genuine, phishing) was created as an average across the seven principles. Refer to Appendix K for a table summary of click-ability ratings for anxiety and cue utilisation typologies.

In the second stage, a discrimination score was calculated for each participant which subtracted his/her average click-ability rating for phishing emails from genuine emails. Establishing a discrimination score ensured that the current hypotheses were appropriately analysed regarding the capacity of participants to discriminate between genuine and phishing emails. For example, if a participant’s average genuine click-ability score was 4.2, and their average phishing click-ability score was 1.3, their discrimination score would be 2.9. A greater, positive discrimination score indicated that the participant was better able to discriminate between genuine and phishing emails, compared to those with a lower discrimination score. While the stimuli were created in line with Cialdini’s (2007) social persuasion principles, an analysis of these principles, as seen in Parsons et al. (2019), was beyond the scope of this thesis.

Data from State-Trait Anxiety Inventory was reduced consistent with Spielberger (1983) to form an added-weighted score for the S-Anxiety and the T-Anxiety scales. Using a

self-reported 4-point Likert scale ranging from 1(*Not at all*) to 4(*Very much so*), a rating of 4 indicates a high level of anxiety for anxiety-present items, whilst a rating of 1 indicates a low level of anxiety for anxiety-absent items, (Spielberger, 1983). Scoring weights on anxiety-present items remained the same, whilst the scoring weights on anxiety-absent items were reverse coded. The anxiety-absent items were provided by Spielberger (1983). For participants who omitted one or two items on either scale, the prorated full-scale score was obtained by determining the mean weighted score for items that the participant did respond, multiplied by 20. Total scores from each scale range between 20 and 80, with higher scores indicative of higher state/trait anxiety.

Data reduction from NASA-TLX was consistent with the method used by Hart and Staveland (1988). After completing the PET and the railroad task, participants completed the NASA-TLX to measure the six bipolar dimensions of workload: mental demand; physical demand; temporal demand; own performance; effort; frustration. Apart from 'own performance', which was responded using a scale from 1(*not successful*) to 7(*successful*) all other dimensions were measured from 1(*low*) to 7(*high*). A final score was calculated as the mean rating from each of the six dimensions, with 'own performance' scores reverse coded. Final scores ranged from 0 to 7, where higher scores indicated higher perceived workload.

Data from the railroad task was analysed separately for each participant. The aim of the railroad task was to impose additional cognitive resources to force participants to use cue associations while responding to the PET. Therefore, it was important to ascertain that each participant was at least attempting the task. Response rate on the task was measured as the amount of times participants attempted to divert a train. Of the 125 trains that were programmed to enter the tracks, 65 required diversion and 60 did not. All participants had a

response rate of 70% or more thus, it was clear that all participants were at least ascribing some cognitive resources to the secondary task.

Data Analysis

Stage 1: Establishing Typologies.

Cue Utilisation. A *k*-means cluster analysis was conducted to determine whether participants could be categorised into two typologies representing higher and lower levels of cue utilisation within the domain of cybersecurity based on their performance across the five distinct tasks (Wiggins et al., 2014; Sturman, Wiggins, Auton, & Loft, 2019). Before the cluster analysis could be performed, scores for each task were converted to z-scores. The cluster analysis yielded two distinct typologies that broadly represented higher and lower levels of cue utilisation. Cluster 1 contained 16 participants who recorded relatively lower response latencies on the FIT, relatively greater accuracy on the FRT, relatively greater variance in the FAT and FDT, and a relatively lower ratio of sequential information accessed in the FPT. Overall, this pattern of performance across the EXPERTise 2.0 tasks was reflective of a relatively higher level of cue utilisation. The remaining 16 participants comprised the second typology who recorded the opposite pattern of responses across the five tasks which is consistent with performance associated with a lower level of cue utilisation. Table 1 summarises the results of the cluster analysis.

Table 1.

Centroid Values for EXPERTise Task Clusters

EXPERTise 2.0 Tasks (DV in brackets)	Typology	
	Cluster 1 (Higher) (<i>n</i> = 16)	Cluster 2 (Lower) (<i>n</i> = 16)
Feature Identification Task (response latency)	-.37	.37
Feature Recognition Task (accuracy)	.61	-.61
Feature Association Task (variance)	.29	-.28
Feature Discrimination Task (variance)	.41	-.41
Feature Prioritisation Task (ratio)	-.54	.54

Anxiety. To establish anxiety typologies, scores from the State-Trait Anxiety Inventory were used to categorise participants into three groups for both state and trait anxiety, which follows the methodology described in Harris and Cumming (2003). The typologies for state anxiety were categorised as follows: low anxiety comprised people with scores between 20 and 26 (*n* = 16), moderate anxiety comprised people with scores between 37 and 45 (*n* = 7), and high anxiety comprised people with scores from 46 and higher (*n* = 9). The typologies for trait anxiety were categorised as follows: low anxiety comprised people with scores between 24 and 37 (*n* = 14), moderate anxiety comprised people with scores between 38 and 43 (*n* = 3), and high anxiety comprised people with scores 44 and higher (*n* = 15). High and low typologies were only included in the data analysis to ensure participants only represented extreme levels of anxiety.

Stage 2: Hypothesis Testing.

H1: Participants could discriminate between genuine and phishing emails. To examine H1, a dependent samples t-test was conducted between the mean click-ability ratings of the two email conditions (phishing, genuine). A statistically significant result was evident between the mean click-ability ratings of genuine and phishing emails, $t(31) = -5.53, p < .001, r = -.30$. Providing support for H1, this result indicates that on average, participants were significantly less likely to consider it ‘okay’ to click on the link of phishing emails ($M = 2.31, SD = .87$), compared to genuine emails ($M = 3.64, SD = .82$).

H2. Participants with higher levels of cue utilisation will have a higher capacity to discriminate phishing emails from genuine emails, relative to those with lower levels of cue utilisation. To examine H2, a discrimination metric was used between participants click-ability ratings for genuine and phishing emails. A higher discrimination score was indicative of a higher capacity to discriminate between genuine and phishing emails (described in more detail above). Using an independent samples t-test, cue utilisation typology (high, low) was the between-groups factor, with discrimination score as the dependent variable. There was no main effect of cue utilisation typology on discrimination scores, $F(1, 30) = .15, p = .62$. Failing to support H2, this result suggests that there was no statistically significant difference in discrimination ability between phishing and genuine email for those with a higher ($M = 1.45, SD = 1.38$), compared to those with a lower ($M = 1.21, SD = 1.37$) capacity for cue utilisation. Figure 8 summaries the discrimination scores for individuals categorised with levels of high and low cue utilisation.

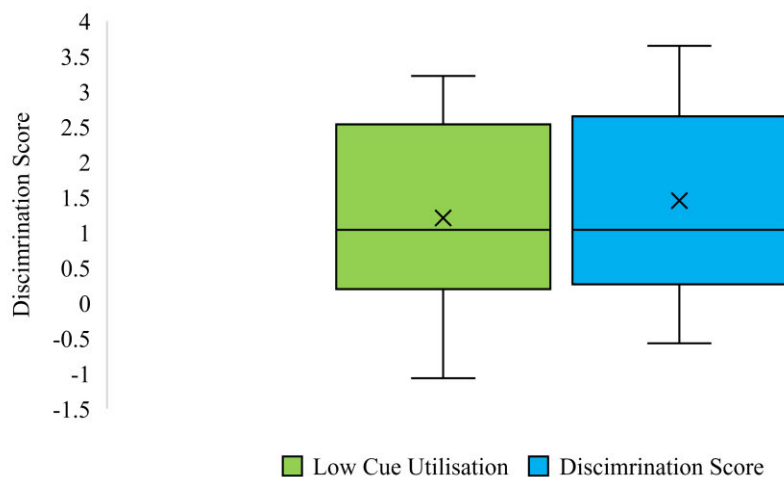


Figure 8. This boxplot illustrates the discrimination scores for individuals with levels of high and low cue utilisation. Each box contains the middle 50% of scores for each cue utilisation typology, where the middle line represents the median value. The upper and lower whiskers represent the top and bottom 25% of scores, respectively. The error bars represent the maximum and minimum scores, respectively. ‘X’ represents the mean discrimination score.

H3. Participants with higher levels of cue utilisation would perceive a phishing email task as less cognitive demanding, relative to those with lower levels of cue utilisation.

To examine H3, an independent samples t-test was conducted with cue utilisation typology (high, low) as the independent variable, whilst score on the NASA-TLX was the dependent variable. There was no main effect of cue utilisation typology on perceived workload ($p = .71$). Failing to support H3, this result suggests that there was no statistically significant difference in perceived workload on the PET for those with a higher ($M = 3.85$, $SD = 0.94$), compared to those with a lower ($M = 3.96$, $SD = 0.80$) capacity for cue utilisation.

H4a. Participants with higher levels of trait anxiety will have a lower capacity to discriminate between genuine and phishing emails, relative to those with lower levels of trait anxiety. To examine H3a, a discrimination metric was used between participants click-

ability ratings for genuine and phishing emails. A higher discrimination score was indicative of a greater capacity to discriminate between genuine and phishing emails. Using an independent samples t-test, trait anxiety typology (low, high) was the between-groups factor, whilst discrimination score was the dependent variable. A statistically significant between-groups effect was evident for trait anxiety typology on discrimination scores, $F(1, 28) = 4.32$, $p = .047$. Providing support for H4a, this result suggests that individuals with high trait anxiety had a lower capacity to discriminate between genuine and phishing emails ($M = .88$, $SD = 1.28$) compared to individuals with low trait anxiety ($M = 1.88$, $SD = 1.30$) Figure 9 summaries the discrimination scores for individuals categorised with levels of high and low trait anxiety.

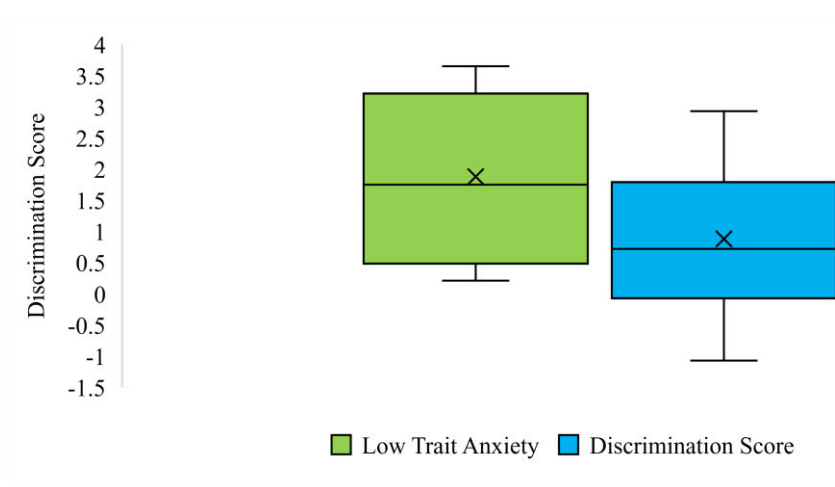


Figure 9. This boxplot illustrates the click-ability discrimination scores between phishing and genuine emails, for individuals with levels of high and low trait anxiety. Each box contains the middle 50% of scores for each trait anxiety typology, where the middle line represents the median value. The upper and lower whiskers represent the top and bottom 25% of scores, respectively. The error bars represent the maximum and minimum scores, respectively. 'X' represents the mean discrimination score.

H4b: Participants with higher levels of state anxiety will have a lower capacity to discriminate between genuine and phishing emails, relative to those with lower levels of state anxiety. To examine H4b, a discrimination metric was used between participants click-ability ratings for genuine and phishing emails. A higher discrimination score was indicative of a greater capacity to discriminate between genuine and phishing emails. Using an independent samples t-test, state anxiety typology (low, high) was the between-groups factor, whilst click-ability discrimination score was the dependent variable. There was no main effect of state anxiety typology on discrimination scores, $F(1, 23) = .17, p = .33$. Failing to support H3b, this result suggests that there was no statistically significant difference in discrimination ability between phishing and genuine email for individuals with high state anxiety ($M = 1.00, SD = 1.43$) compared to individuals with low state anxiety ($M = 1.59, SD = 1.44$). Figure 10 summaries the discrimination scores for individuals categorised with levels of high and low state anxiety.

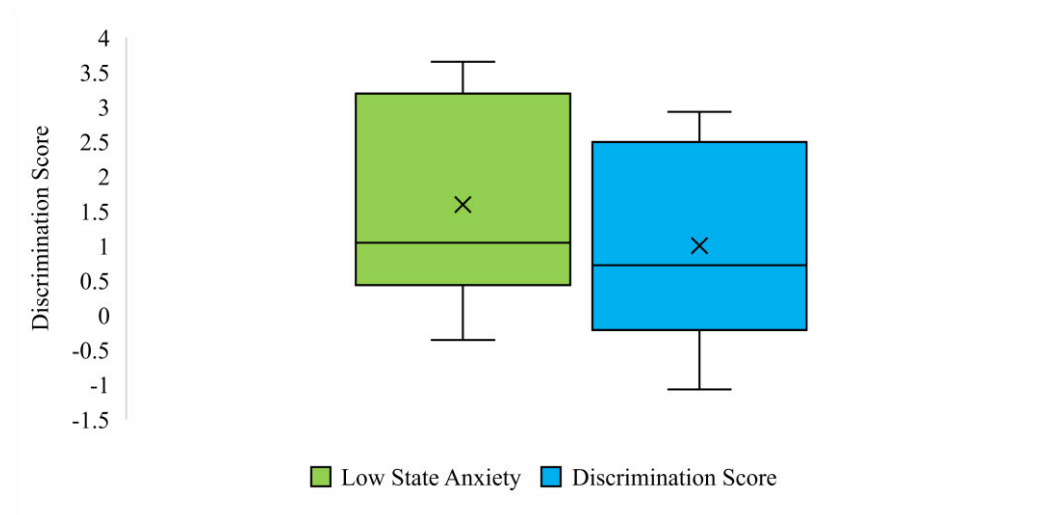


Figure 10. This boxplot illustrates the click-ability discrimination scores between phishing and genuine emails, for individuals with levels of high and low state anxiety. Each box contains the middle 50% of scores for each state anxiety typology, where the middle line represents the median value. The upper and lower whiskers represent the top and bottom 25%

of scores, respectively. The error bars represent the maximum and minimum scores, respectively. 'X' represents the mean discrimination score.

Discussion

Overview

The current study aimed to examine the individual differences of cue utilisation and state/trait anxiety and their association with phishing email susceptibility. The study further aimed to explore the effect of cue utilisation on subjective mental workload, which was yet to be explored in the context of a phishing email study. Overall, the findings from this study suggest that participants were significantly more likely to consider a link 'okay' to click on when viewing genuine emails, compared to phishing emails, providing support for H1. However, the *only* significant finding relating to individual differences was trait anxiety, indicating that individuals with higher levels of trait anxiety had a lower capacity to discriminate between genuine and phishing emails, compared to their less anxious counterparts.

Cue Utilisation and Phishing Susceptibility (H2)

According to Brunswik's (1955) Lens Model, making sense of a given situation is guided by the cues present in the environment and the meaning of those cues to the individual. This model assumes that individuals recognise a situation as typical by matching the cues in the current situation with a situation resident in LTM. Behaviour is thus guided by the cues in which an individual can identify to better anticipate and engage in a situation. Therefore, in the context of the current study, those with a higher capacity for cue utilisation were expected to have a greater capacity to discriminate between phishing and genuine emails in a novel phishing email task, compared to those with a lower capacity for cue utilisation (H2). However, this hypothesis was not supported; specifically, it was found that

having a higher capacity for cue utilisation did not give participants an advantage when discriminating phishing from genuine emails.

This result was surprising considering the use of the secondary task, alongside the phishing email task, was designed to ‘force’ participants to engage in cue-based reasoning as the dual task condition was intended to limit cognitive resources. As such, it was expected that those who had cue associations pertaining to phishing email detection in LTM would be able to apply them during the task to facilitate superior performance. In comparison, those participants who did not possess such cue associations, would not be able to engage in fast and automatic processes to assess the emails and hence, would not perform as well.

However, as there was only one cue of “phishiness” within the email stimuli (a link), it is possible that all participants were generally good at picking up on this cue. Indeed, H1 showed that in general, participants were able to discriminate between genuine and phishing emails. Therefore, future studies should perhaps look at more sophisticated phishing emails that then might tease out the difference between high and low cue utilisation.

Subjective Workload and Cue Utilisation (H3)

While an increase in task demands involves an increase in cognitive demands, cue utilisation is thought to reduce the number of task-related elements that need to be processed (Brouwers et al., 2017). Therefore, it was hypothesised that participants with higher levels of cue utilisation would perceive the phishing email task as less cognitive demanding, relative to those with lower levels of cue utilisation (H3). The findings did not support this hypothesis as the task was perceived as having the same level of workload for both low and high cue utilisation typologies. It is suggested that this result is due to the outcomes in H2, in that participants with high and low cue utilisation equally possessed the capacity to associate the email link with email discriminability. As a result, neither group had to evoke System 2 processing, supporting the finding that both typologies found the task equally challenging.

Alternatively, Brouwers et al. (2017) proposed that such a finding could be due to a dissociation between perceived workload and performance under dual task conditions. Dissociations between subjective measures of workload and performance often occur when the competition for resources results in distorted self-report estimates of workload (Yeh and Wickens, 1998 cited in Brouwers et al., 2017). Perception of workload thus becomes reliant on perceived success, rather than the fidelity of workload required across both tasks. Arguably, as there was no difference in performance across participants with high and low cue utilisation, both groups could have perceived similar outcomes of success.

Anxiety and Phishing Susceptibility (H4a and H4b)

Due to the processing bias towards threat-related information of individuals with high levels of anxiety (Hartley & Phelps, 2012), this study hypothesised that participants with high levels of trait (H4a)/state (H4b) anxiety would have a lower capacity to discriminate between genuine and phishing emails, relative to those with low levels of state/trait anxiety.

In support of H4a, results indicated that individuals with high trait anxiety had a lower capacity to discriminate between genuine and phishing emails, compared to their less anxious counterparts. This finding suggests that participants with high trait anxiety erred on the side of caution, even when responding to a genuine email. Such a response is consistent with the underlying mechanisms of the Attention Control Theory which postulates that anxious individuals have a tendency to negatively frame stimuli, even at the cost of missing potential gains (Hartley & Phelps, 2012). This finding has practical implications, discussed in the latter.

While there was a relationship found with trait anxiety and email discriminability, this result was not replicated with state anxiety, failing to support H4b. Specifically, individuals with high state anxiety were no different in their capacity to discriminate between genuine and phishing emails compared to individuals with low state anxiety. Two possible

explanations can account for this incongruent finding. The first explanation relates to the way in which state anxiety was measured. Despite administering the assessment of state anxiety directly prior to the commencement of the dual tasks, the conditions under which it was administered were considerably mild and non-threatening in comparison. Indeed, as state anxiety is sensitive to the current conditions an individual is in, (Spielberger, 1983) state anxiety levels may have changed whilst completing the dual tasks. Therefore, participants state anxiety under cognitively demanding conditions may not have been accurately captured. This explanation is not warranted for H4a, as trait anxiety is more inherent and relatively stable across conditions.

The second explanation relates to whether state anxiety was a derivative of the task itself. In threatening environments, the state of anxiety encourages a self-protective framing of problems to avoid large losses (Matthews, Panganiban, & Hudlicka, 2011). However, for this 'framing' to occur, the paradigm of the task itself must be considered threatening. On the basis that H4b was not supported, this suggests that individuals categorised with high state anxiety were no more affected by the conditions of the task compared to those with low state anxiety. Therefore, state anxiety was not a task-specific outcome.

Implications of the Findings

The outcomes of this study help in the understanding of phishing email detection, which aims to assist future training and/or campaigns. Whilst it was recognised that on average individuals could discriminate between genuine and phishing emails, this was on the basis of only one cue (a link). Accordingly, it is assumed that using a cue to establish email discriminability is a relatively frugal task, even under cognitively demanding conditions. However, as phishing emails are becoming more sophisticated in their disguise, it is encouraged that future studies investigate into other, more nuanced cues (e.g., email greetings). This can be achieved by embedding a range of cues in the email stimuli to

determine what cues individuals use to better discriminate between genuine and phishing emails. This would provide extensive findings to form training and/or campaigns.

However, while campaigns on phishing emails may help raise awareness about this cybersecurity threat, it is recommended that future training focus on improving phishing discrimination rather than simply biasing people towards more risk-averse behaviour (Parsons et al., 2019). This is pertinent considering the current findings highlight that individuals with an attentional bias towards threat-related stimuli (i.e., high trait anxiety) had a lower capacity to discriminate between genuine and phishing emails. This can be detrimental to work/life productively if everything is deemed as suspicious. For example, incorrectly identifying a phishing email can result in an individual missing out on valuable or useful information, or, from an organisational perspective, affect customer trust and reputation (Parsons et al., 2019).

Strengths

The design of the current study sought to maximise cognitive resources using a dual task condition to induce participants to rely on cues to assess emails. Adopting this design strengthened the applicability of the findings to real-world settings, as individuals are often having conversations, looking at their phone, or engaging in other work whilst reading emails.

Another strength of the study was that it was lab-based. Often phishing studies are administered online, lending themselves to a number of uncontrolled variances in experimental conditions. However, as the current study was administered face-to-face, this ensured the experimental conditions were consistent across participants. In addition, this was an inaugural study investigating the individual differences of cue utilisation and anxiety in the context of phishing email susceptibility. This research forms a foundation for future research.

Limitations and Future Directions

The current study was not without limitations. First and foremost, the study was limited in sample size. This limited statistical power and potentiality for main effects and interactions relating to phishing susceptibility. It is recommended that the study be replicated to obtain a larger sample.

Using a role-play design, participants were to assume that all emails were of relevance to 'Alex Jones'. This may have disoriented participants in their appraisal of each email. Parsons et al. (2019) recognised that the appeal or click-ability of emails are much more effective if they reflect a real ongoing relationship. To address this limitation, Parsons et al. (2019) suggested future research target a specific university or organisation and present them with a series of genuine and phishing emails which are targeted directly at them (e.g., an email distributing an online student newsletter). In this context, the likelihood of appeal to existing relations could better represent an individual's phishing susceptibility (Parsons et al., 2019). Furthermore, while the statement 'It is okay to click on the link in this email' was used as an indirect measure of phishing susceptibility, this could have primed participants to more cautious behaviour. In real life email correspondence, susceptibility to phishing emails may be higher. It is suggested that future research use a statement less likely to prime participants, such as 'would you follow up with this email?'.

According to Kumaraguru et al. (2010) users are unlikely to spend a considerable amount of time engaging in security-related tutorials. Therefore, in future studies regarding phishing susceptibility, a more interactive methodology is recommended using learning-by-doing or immediate feedback tasks (Kumaraguru et al., 2010). For example, individuals will be provided with immediate feedback if they incorrectly judge a genuine email as phishing, or a phishing email as genuine. This aims to guide individuals towards correct behaviour and the reduction of unproductive behaviour.

Conclusion

The current study aimed to further understand how the individual differences of cue utilisation capacity and state/trait anxiety influence phishing email susceptibility. Higher trait anxiety was associated with a lower capacity to discriminate between phishing and genuine emails, presumably due to an attentional bias to threat-related stimuli. However, this relationship was not evident for state anxiety. No associations were evident between cue utilisation typology and phishing email susceptibility, and subjective mental workload.

Overall, this research makes a meaningful contribution to the combined literature of individual differences and phishing susceptibility. As phishing attacks continue to become more frequent and sophisticated, future research needs to continue to examine those most at risk and the strategies that can help improve detection.

References

- Akbar, N. (2014). *Analysing Persuasion Principles in Phishing Emails*. (Master Thesis), University of Twente, Enschede.
- Bastian, D. (2019). ACU hit by cyber attack, staff emails compromised.
- 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. doi:10.3389/fpsyg.2016.00435
- 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. doi:10.1037/xap0000151
- 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. doi:10.1080/00140139.2017.1330494
- Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016). Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails.
- Butavicius, S., 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*, 12-23.
- Caci, H., Baylé, F. J., Dossios, C., Robert, P., & Boyer, P. (2003). The Spielberger trait anxiety inventory measures more than anxiety. *European Psychiatry*, 18(8), 394-400. doi:10.1016/j.eurpsy.2003.05.003
- Cattell, R. B. (1966). *Patterns of Change: Measurement in relation to state dimension, trait change, liability, and process concepts*. *Handbook of Multivariate Experimental Psychology*. Chicago: Rand McNally & Co.

- Chen, S., Duckworth, K., & Chaiken, S. (1999). Motivated Heuristic and Systematic Processing. *Psychological Inquiry*, 10(1), 44-49. doi:10.1207/s15327965pli1001_6
- Cialdini, R. B. (2007). *Influence: The Psychology of Persuasion*. New York: Harper Collins.
- Croskerry, P. (2009). A universal model of diagnostic reasoning. *Academic medicine : journal of the Association of American Medical Colleges*, 84(8), 1022. doi:10.1097/ACM.0b013e3181ace703
- Eysenck, M. W., Derakshan, N., Santos, R., & Calvo, M. G. (2007). Anxiety and cognitive performance: attentional control theory. *Emotion*, 7(2), 336-353. doi:10.1037/1528-3542.7.2.336
- Ferreira, A., & Teles, S. (2019). Persuasion: How phishing emails can influence users and bypass security measures. *International Journal of Human-Computer Studies*, 125, 19-31. doi:10.1016/j.ijhcs.2018.12.004
- Guadagno, R. E., Muscanell, N. L., Rice, L. M., & Roberts, N. (2013). Social influence online: The impact of social validation and likability on compliance. *Psychology of Popular Media Culture*, 2(1), 51-60. doi:10.1037/a0030592
- Harris, L. M., & Cumming, S. R. (2003). An Examination of the Relationship Between Anxiety and Performance on Prospective and Retrospective Memory Tasks. *Australian Journal of Psychology*, 55(1), 51-55.
- Hart, S., & Staveland, L. (1988). Development of NASA-TLX (Task Load Index): Results of Empirical and Theoretical Research. *Advances in Psychology*, 52, 139-183.
- Hartley, C. A., & Phelps, E. A. (2012). Anxiety and decision-making. *Biological Psychiatry*, 72(2), 113. doi:10.1016/j.biopsych.2011.12.027
- Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, 10(2), 1-31.

- Lawson, P., Zielinska, O., Pearson, C., & Mayhorn, C. B. (2017). Interaction of Personality and Persuasion Tactics in Email Phishing Attacks. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 61(1), 1331-1333.
doi:10.1177/1541931213601815
- Leon, M. R., & Revelle, W. (1985). Effects of Anxiety on Analogical Reasoning: A Test of Three Theoretical Models. *Journal of Personality and Social Psychology*, 49(5), 1302-1315.
- Loveday, T., Wiggins, M. W., Harris, J. M., O'Hare, D., & Smith, N. (2013). An objective approach to identifying diagnostic expertise among power system controllers. *Human Factors*, 55(1), 90-107. doi:10.1177/0018720812450911
- Loveday, T., Wiggins, M. W., & Searle, B. J. (2013). Cue Utilization and Broad Indicators of Workplace Expertise. *Journal of Cognitive Engineering and Decision Making*, 8(1), 98-113.
- Matthews, G., Panganiban, A. R., & Hudlicka, E. (2011). Anxiety and selective attention to threat in tactical decision-making. *Personality and Individual Differences*, 50(7), 949-954. doi:10.1016/j.paid.2010.09.005
- Mosier, K., & Kirlik, A. (2004). BRUNSWIK'S LENS MODEL IN HUMAN FACTORS RESEARCH: MODERN APPLICATIONS OF A CLASSIC THEORY. *PROCEEDINGS of the HUMAN FACTORS AND ERGONOMICS SOCIETY 48th ANNUAL MEETING*, 350-354.
- Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2019). Predicting susceptibility to social influence in phishing emails. *International Journal of Human-Computer Studies*, 128, 17-26. doi:10.1016/j.ijhcs.2019.02.007

Parsons, K., Butavicius, M., Pattinson, M., Calic, D., McCormac, A., & Jerram, C. (2016).

Do Users Focus on the Correct Cues to Differentiate Between Phishing and Genuine Emails?

Quigley, L., Nelson, A. L., Carriere, J., Smilek, D., & Purdon, C. (2012). The effects of trait and state anxiety on attention to emotional images: An eye-tracking study. *Cognition & Emotion*, 26(8), 1390-1411. doi:10.1080/02699931.2012.662892

Rajivan, P., & Gonzalez, C. (2018). Creative Persuasion: A Study on Adversarial Behaviors and Strategies in Phishing Attacks. *Frontiers in Psychology*, 9, 135. doi:10.3389/fpsyg.2018.00135

Schriver, A. T., Morrow, D. G., Wickens, C. D., & Talleur, D. A. (2008). Expertise Differences in Attentional Strategies Related to Pilot Decision Making. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 50(6), 864-878.

Spielberger, C. D. (1983). State-Trait Anxiety Inventory for Adults. Sampler Set Manual, Instrument and Scoring Guide.

Telstra Corporation Limited. (2019). *Telstra Security Report 2019*. Retrieved from

Tubbs-Cooley, H., Mara, C., Carle, A., & Gurses, A. (2018). The NASA Task Load Index as a measure of overall workload among neonatal, paediatric and adult intensive care nurses. *Intensive and Critical Care Nursing*, 46, 64-69.

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*, 55, 345-362.

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.

doi:10.1080/14992027.2018.1476782

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. doi:10.1016/j.ssci.2014.01.006

Wiggins, M., & O'Hare, D. (1995). Expertise in Aeronautical Weather-Related Decision Making: A Cross-Sectional Analysis of General Aviation Pilots. *Journal of Experimental Psychology: Applied*, 1(4), 305-320.

Wiggins, M. W. (2012). 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. doi:10.1080/1463922x.2012.724725

Wiggins, M. W., Brouwers, S., Davies, J., & Loveday, T. (2014). Trait-based cue Utilization and initial skill acquisition: implications for models of the progression to expertise. *Frontiers in Psychology*, 5. doi:10.3389/fpsyg.2014.00541

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). doi:10.1186/s12911-016-0243-1

Footnotes

¹The subject line of the email was modified to include a stronger presence of the consistency principle (see Appendix F). As a result, 100% of the participants ($n = 5$) recruited following the amendment selected ‘consistency’ as the most present principle within that email.

Appendix A: Advertisement Flyer

User Behaviour and Management of Emails



Online communication is fundamental in our daily lives and **we need you** to help us understand more about this growing body of research!

You are invited to participate in an **honours level thesis** study regarding user behaviour and emails. This study aims to investigate how people manage their emails, and the factors that may affect email use!

Participants have the chance to win 1 of 5 \$20 Coles/Myer Gift Cards!

Detailed Description:	This is a face-to-face lab-based study that will take place in the Hughes Building at the University of Adelaide. If you decide to participate, you will be asked to make judgments on several emails sent to the inbox of a fictitious person. At the same time, you will be asked to complete a simulated rail control task. You will also provide some basic demographic information and answer questions regarding decision styles and mental workload.
Reimbursement	If you are a first-year psychology student at the University of Adelaide, you will receive 1 credit in exchange for participation. For all other students, or members of the general public, you can elect to go into the draw to win 1 of 5 \$20 Coles/Myer Gift Cards.
Eligibility Requirements:	Over the age of 18; English as your first language (or be fluent in English)
Duration:	Up to 60 minutes
Ethics Approval No.:	██████

If you are interested in participation, please contact one of the following researchers:



Appendix B: Demographic questionnaire.

Demographic Questions

Pre-Session Survey 1

Please complete the following demographic questions.

What is your age? * years

Please indicate your gender *

- Male
- Female
- Other
- Prefer not to say

How would you rate your English fluency/proficiency?

- Native
- Fluent
- Very good
- Average
- Poor

How long do you spend using a computer per day? *

- Less than 1 hour
- 1-3 hours
- 3-5 hours
- 5+ hours

How confident are you using a computer? *

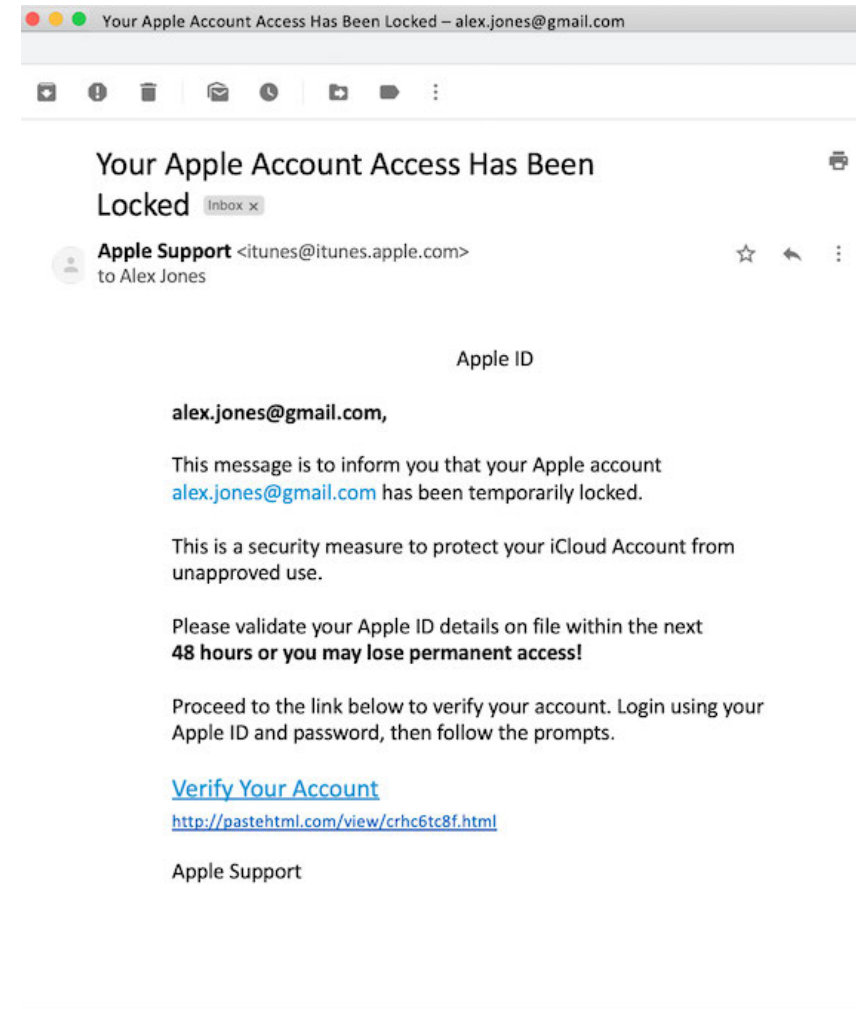
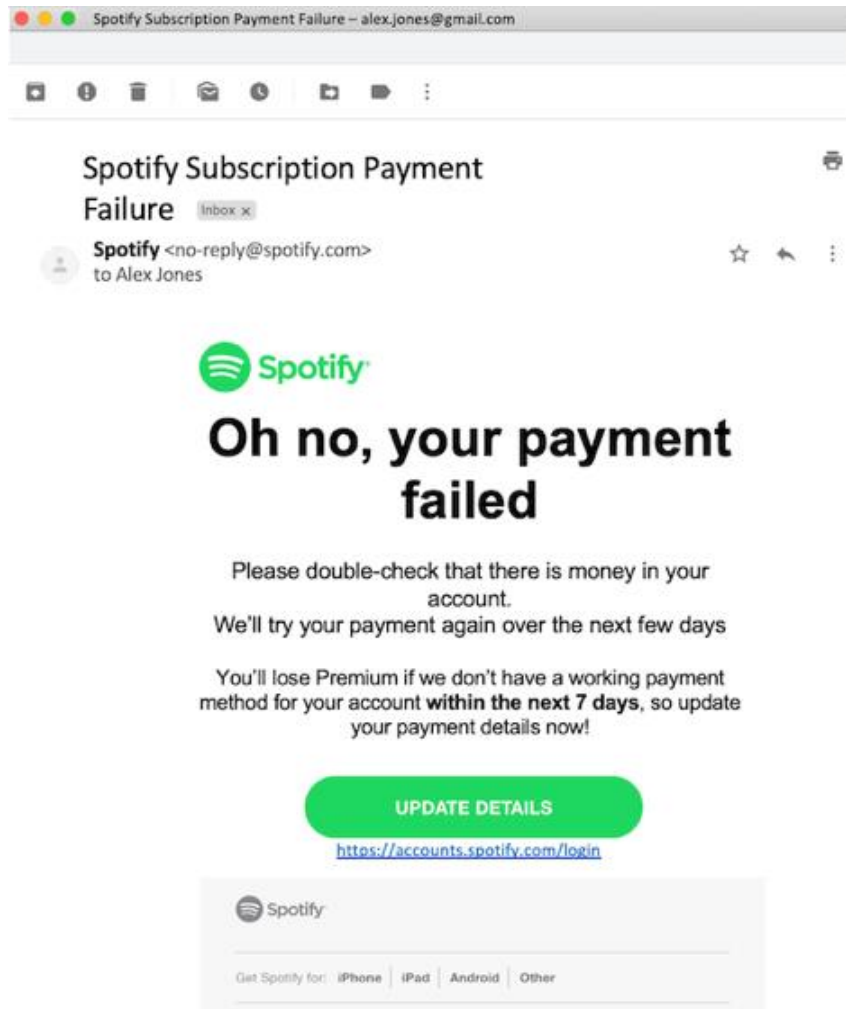
No Confidence	Low Confidence	Neutral	Confident	Very Confident
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

How many emails do you typically receive per day? Type number (eg. 40)

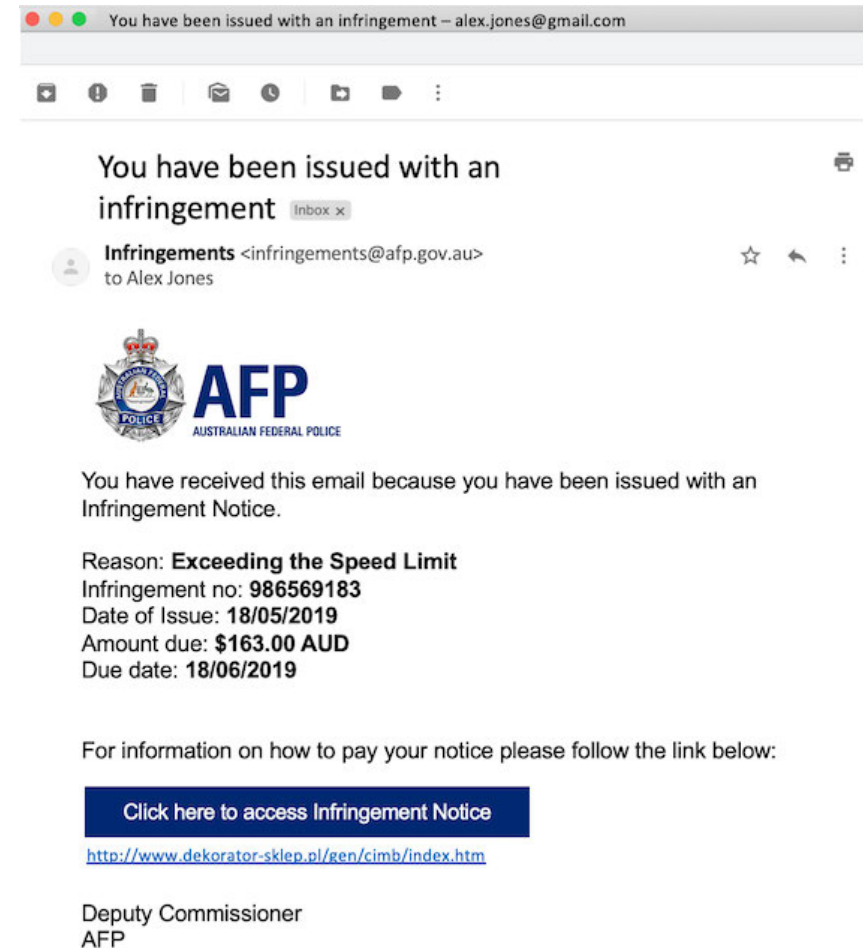
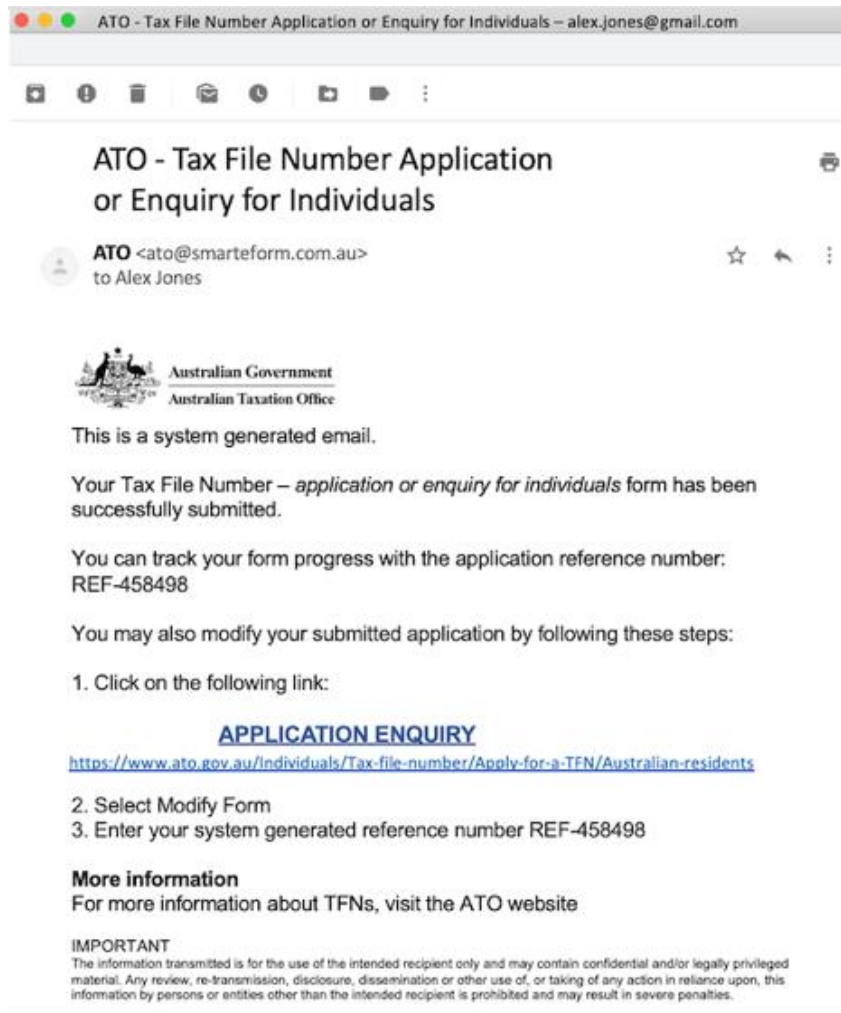
Next

Appendix C: Example of Emails.

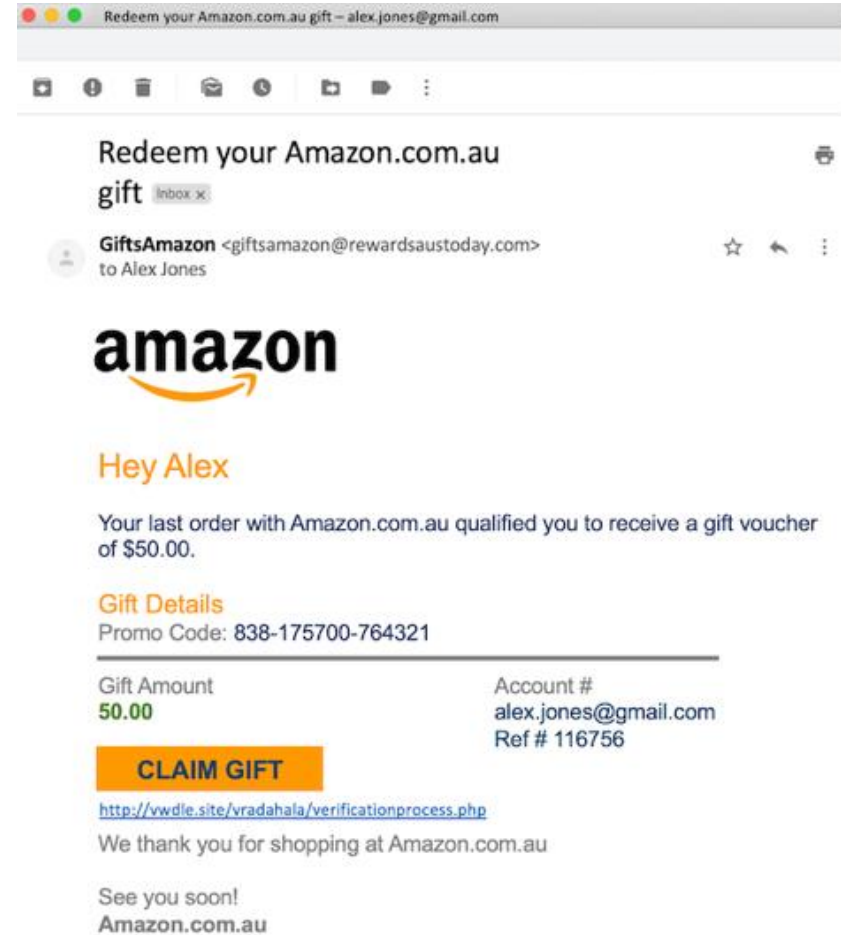
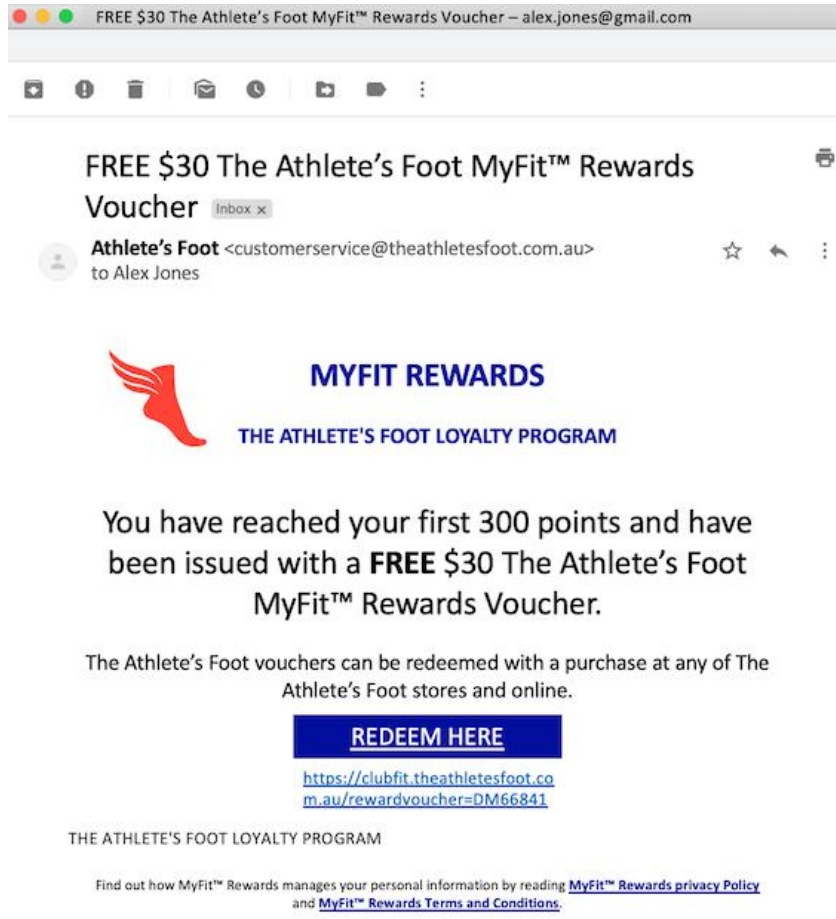
Scarcity (genuine) and Scarcity (phishing) Emails



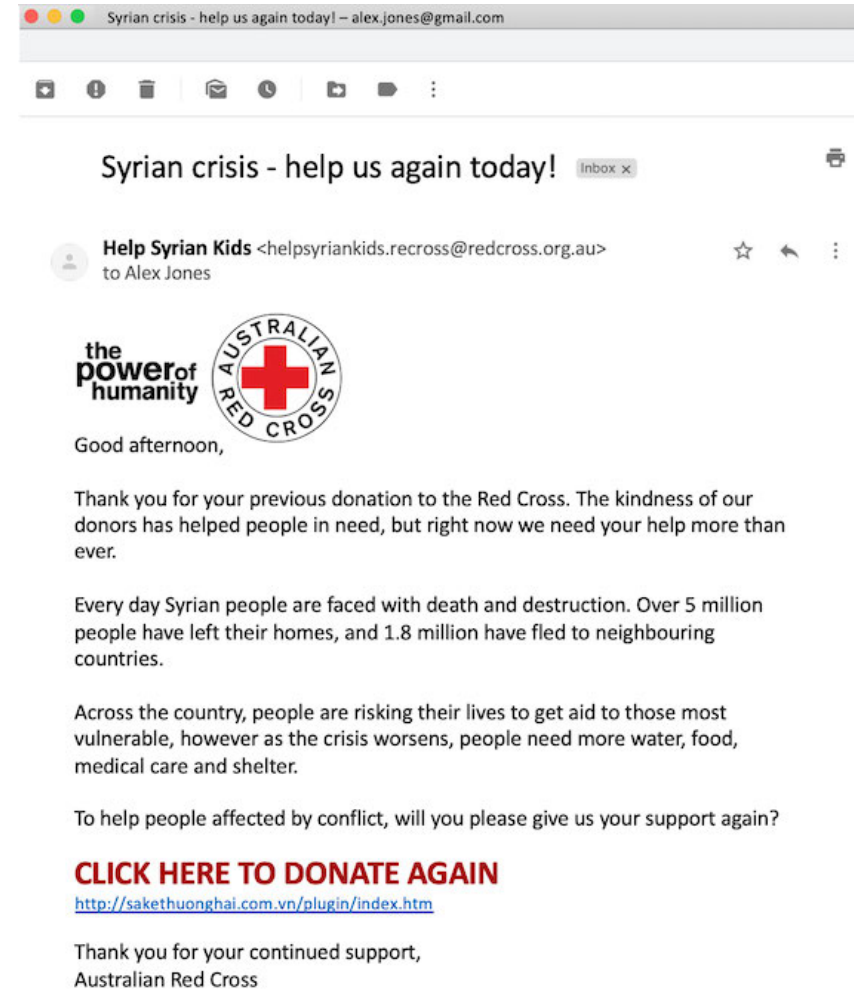
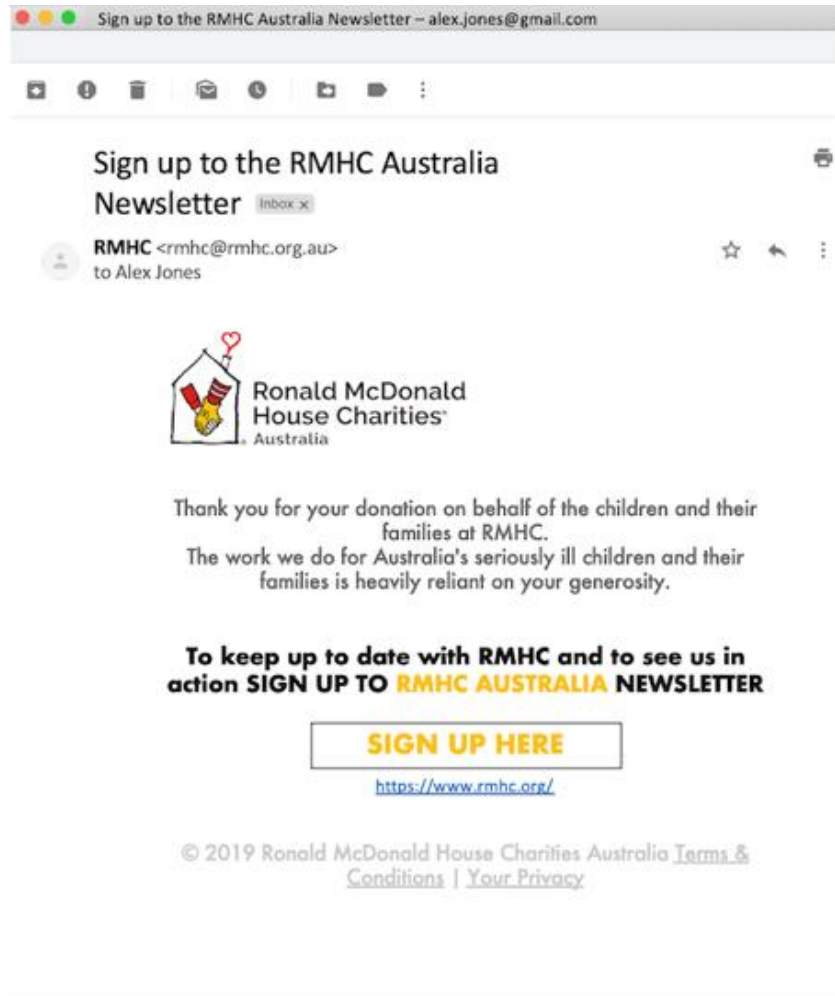
Authority (genuine) and Authority (phishing) Emails



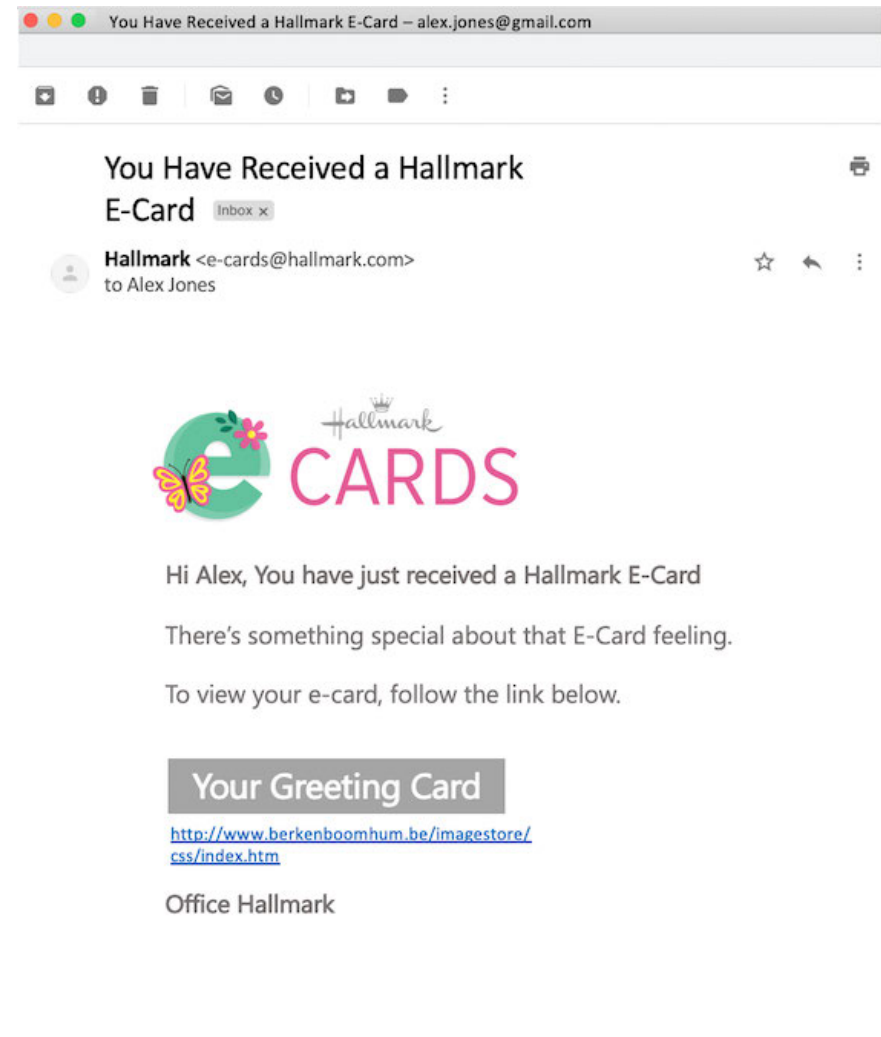
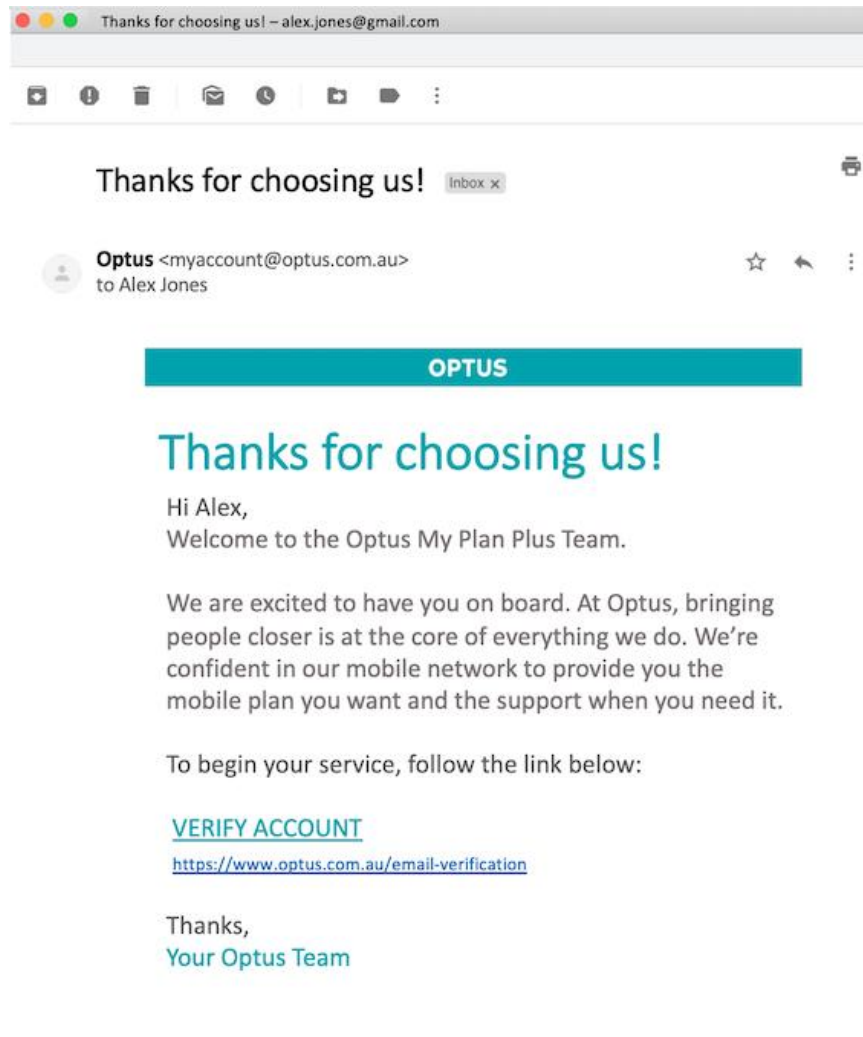
Reciprocity (genuine) and Reciprocity (phishing) Emails



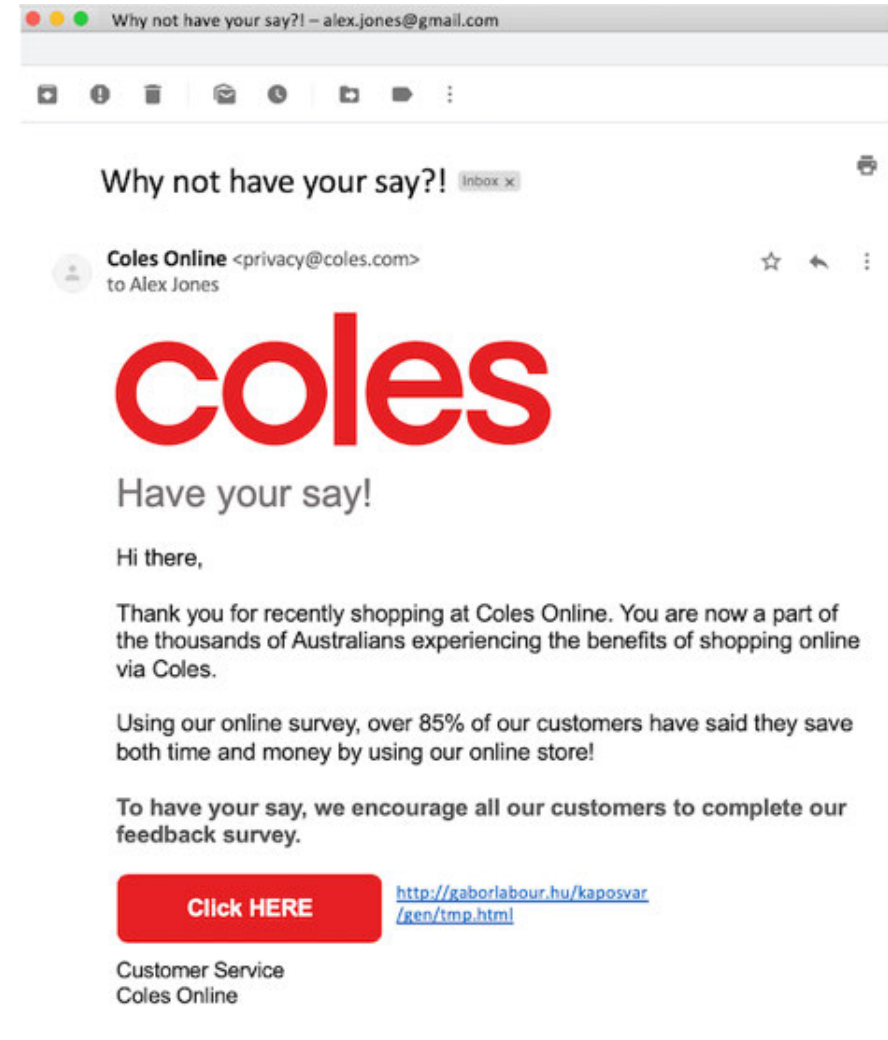
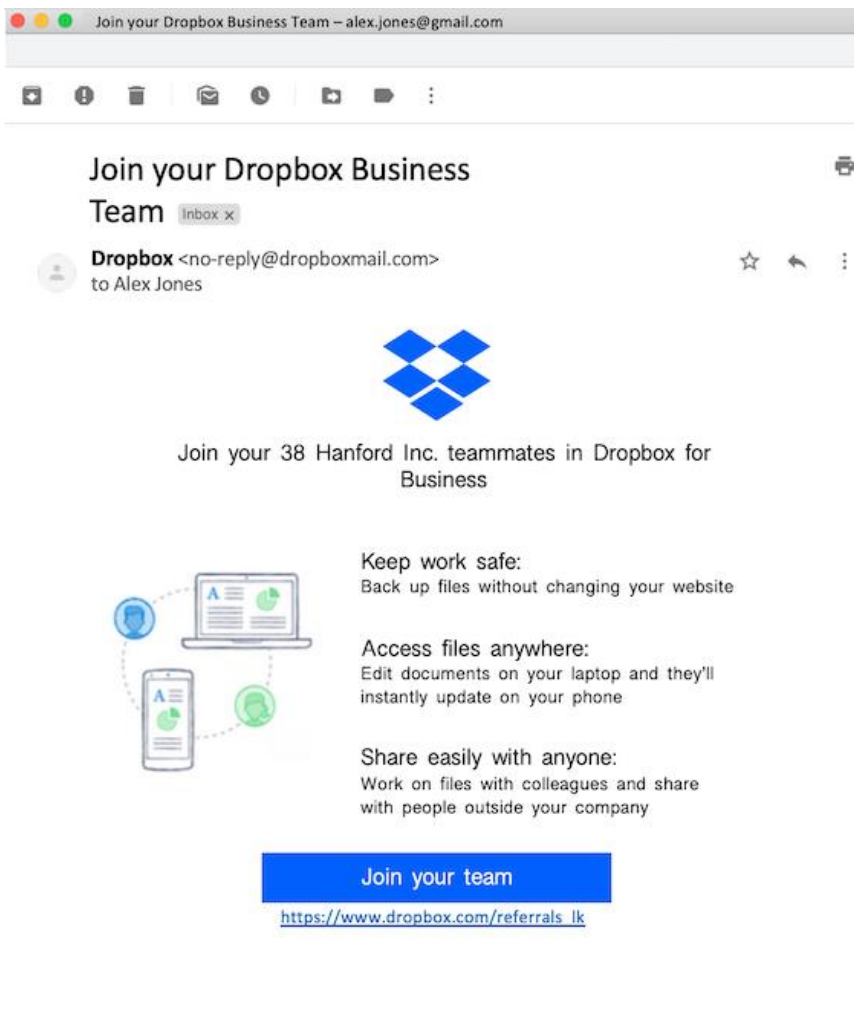
Consistency (genuine) and Consistency (phishing) Emails



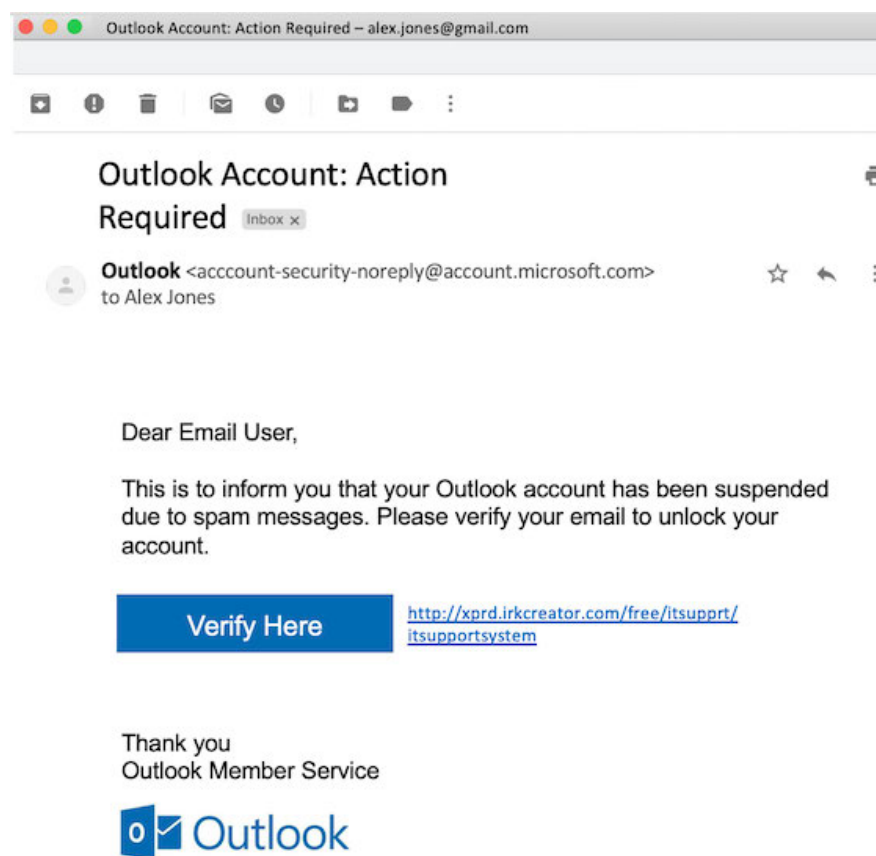
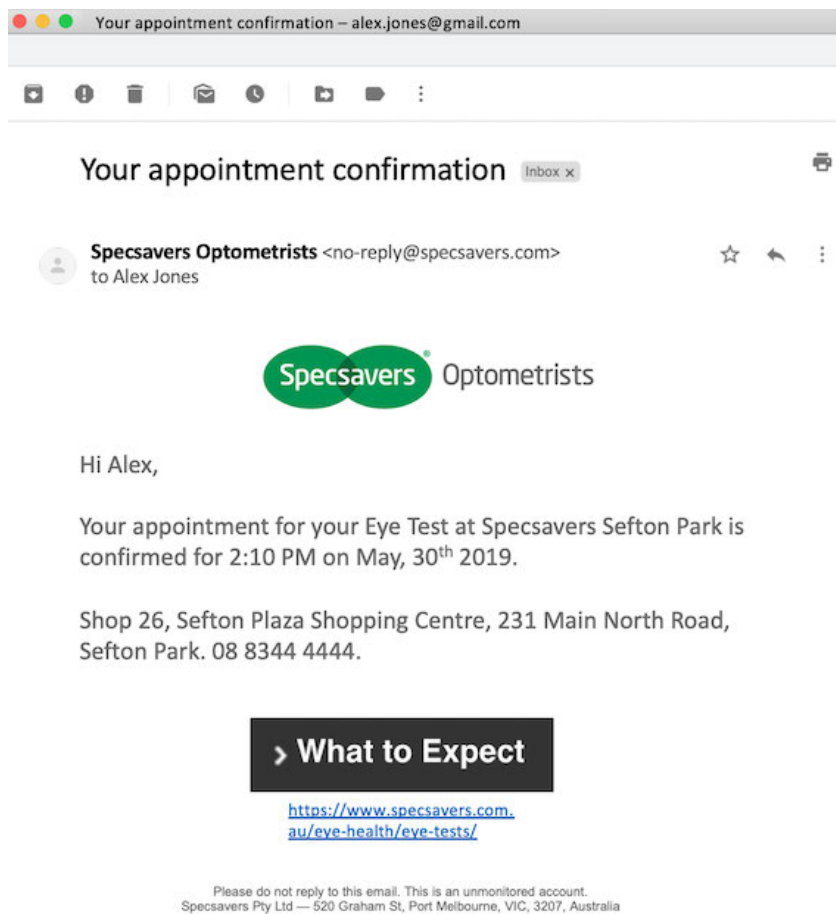
Liking (genuine) and Liking (phishing) Email



Social Proof (genuine) and Social Proof (phishing) Emails



No Principle (genuine) and No Principle (phishing) Email



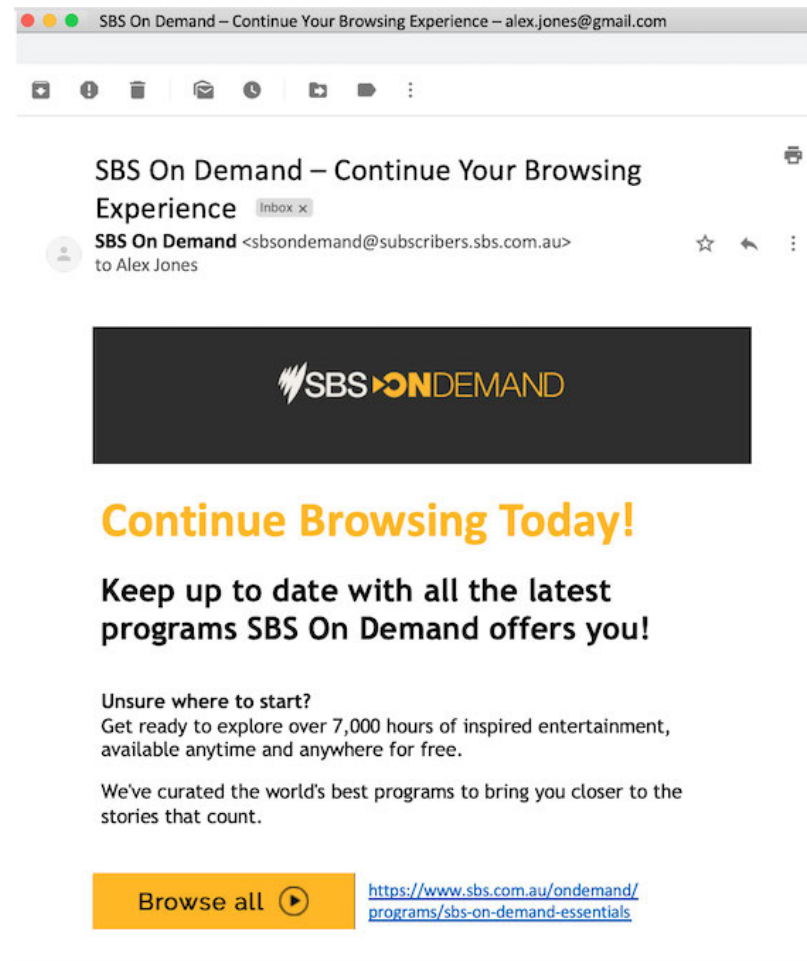
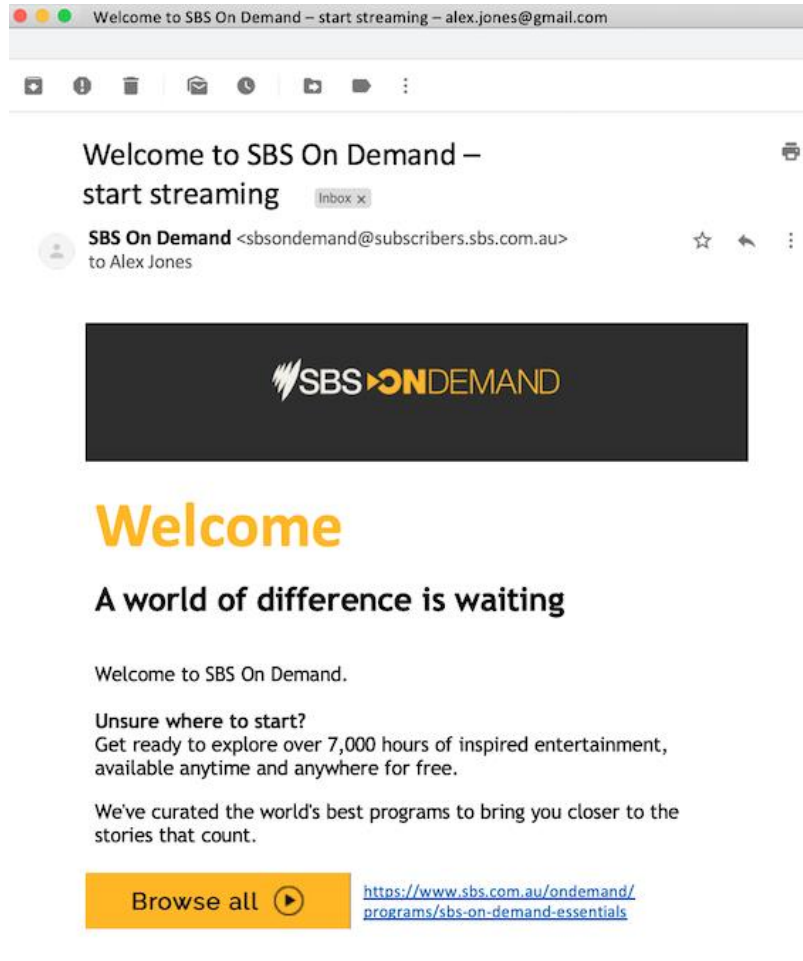
Appendix E: Manipulation Check 1 Results.

Top 3 Ranked Principles for Each Email

Email	Highest Ranked Principle (%)	Second Highest Ranked Principle (%)	Third Highest Ranked Principle (%)
Phishing 1 Scarcity	Scarcity (82%)	No Principle, Authority & Consistency (27%)	No Principle (36%)
Phishing 2 Social Proof	Social Proof (55%)	Social Proof (45%)	No Principle & Liking (36%)
Phishing 3 Authority	Authority (100%)	Scarcity (55%)	No Principle (55%)
Phishing 4 Liking	Liking (73%)	No Principle (64%)	No Principle (82%)
Phishing 5 Reciprocity	Reciprocity (100%)	Consistency (36%)	Liking (36%)
Phishing 6 Consistency	Consistency (73%)	Social Proof (37%)	Liking & Scarcity (27%)
Phishing 7 No Principle*	Authority (64%)	No Principle (45%)	No Principle (73%)
Genuine 1 Scarcity	Scarcity (100%)	Consistency (36%)	No Principle (36%)
Genuine 2 Scarcity	Scarcity (91%)	Consistency (65%)	No Principle (45%)
Genuine 3 Social Proof	Social Proof (64%)	Authority (27%)	No Principle (55%)
Genuine 4 Social Proof	Social Proof (100%)	No Principle & Liking (36%)	No Principle (73%)
Genuine 5 Authority	Authority (64%)	No Principle (36%)	No Principle (55%)
Genuine 6 Authority	Authority (55%)	No Principle (55%)	No Principle (64%)
Genuine 7 Liking*	Consistency (45%)	Reciprocity (64%)	Liking (36%)
Genuine 8 Liking	Liking (55%)	Social Proof (27%)	No Principle (36%)
Genuine 9 Reciprocity	Reciprocity (91%)	Consistency (55%)	No Principle (45%)
Genuine 10 Reciprocity	Reciprocity (36%)	Reciprocity & Consistency (27%)	No Principle (36%)
Genuine 11 Consistency**	Consistency (100%)	No Principle (55%)	No Principle 73%)
Genuine 12 Consistency	Consistency (36%)	Liking (36%)	No Principle (55%)
Genuine 13 No Principle*	Scarcity & Consistency (27%)	No Principle (36%)	No Principle (64%)
Genuine 14 No Principle	No Principle (36%)	No Principle (45%)	No Principle (73%)

Note. * Emails with their intended principle listed as either second or third highest ranked principle, **Results after email was amended due to intended principle not be recognised by participants

Appendix F: Amendment to Consistency Email (Left: Original, Right: Amended)



Appendix G: Manipulation Check 2 Results.

Paired Sample T-Test Between Type of Social Persuasion Principle and Phishing/Genuine Email 'click-ability' ratings

Persuasion Principle	Email Type	<i>M (SD)</i>	Mean Difference (<i>SD</i>)	<i>t</i>	<i>p</i>
Scarcity	Phishing	1.83 (1.40)	-1.96 (1.42)	-4.77	.001
	Genuine	3.79 (0.84)			
Social Proof	Phishing	2.42 (1.16)	-.63 (1.28)	-1.69	.119
	Genuine	3.04 (.99)			
Authority	Phishing	1.42 (.67)	-2.04 (1.01)	-7.00	.000
	Genuine	3.46 (.78)			
Liking	Phishing	2.50 (1.51)	-1.25 (1.63)	-2.66	.022
	Genuine	2.75 (.62)			
Reciprocity	Phishing	1.83 (1.34)	-2.04 (1.53)	-4.62	.001
	Genuine	3.88 (.77)			
Consistency	Phishing	2.33 (1.44)	-1.88 (1.55)	-4.18	.002
	Genuine	4.21 (.86)			
No Principle	Phishing	1.67 (1.15)	-2.25 (1.39)	-5.61	.000
	Genuine	3.92 (.73)			

Appendix H: Paper-and-pencil version of the NASA-TLX

Participant ID: _____

Date: _____

Instructions: Please circle your response to the questions below regarding the task just completed.

How high were the **mental demands** of the task?

E.g., Was the work easy or demanding, simple or complex?

Low *High*

1 2 3 4 5 6 7

How high were the **physical demands** of the task?

E.g., Was the work easy or demanding?

Low *High*

1 2 3 4 5 6 7

How high was the **time pressure** during the task?

E.g., Was the pace slow and leisurely or rapid and frantic?

Low *High*

1 2 3 4 5 6 7

How **hard** did you have to work (mentally and physically) to accomplish your level of performance?

Not very hard *Very hard*

1 2 3 4 5 6 7

How **successful** do you think you were in accomplishing the task?

E.g., How satisfied were you with your performance in accomplishing your work?

Not Successful *Successful*

1 2 3 4 5 6 7

How high was your **level of frustration**?

E.g., How stressed and annoyed versus content and relaxed did you feel?

Low *High*

1 2 3 4 5 6 7

Appendix I: Online Participant Information and Consent Form



User Behaviour and Management of Emails

Participant Information & Consent



User Behaviour and Management of Emails

Dear Participant,

You are invited to participate in the research project described below.

What is the project about?

You are invited to participate in an Honours level thesis study regarding user behaviour and emails. This study aims to investigate how users manage incoming emails from various national or international organisations. This study hopes to empirically measure and identify how students respond to their emails. The implications of this study are to encourage individuals to have a more positive experience with their email accounts.

Who is undertaking the project?

This project is being conducted by Student Researcher Anastasia Falkenberg. This research will form the basis for the degree of Psychology Honours at the University of Adelaide under the supervision of the Principal Investigator Jaime Auton.

Why am I being invited to participate?

You are being invited to participate in this study as you are either a student at the University of Adelaide or a member of the general public who has expressed interest in participating in this project, over the age of 18, and fluent in English/English as your first language.

What am I being invited to do?

You are being invited to participate in a face-to-face lab-based study. The project will begin with a series of online surveys. This will be followed by an online scenario-based task where you will be required to manage incoming emails to the inbox of a fictitious character. You will be required to answer how you would manage the incoming email. A secondary computer-based task will be completed simultaneously where you will be required to re-route rail trains that periodically require diversion. Once completed, using pen and paper you will be given a short survey regarding the overall workload of the task. You will then be asked to complete an online task measuring cue utilisation in the context of user behaviour and email management. All research activities will be located within the assigned computer lab at the University of Adelaide North Terrace Campus. No follow up participation will be requested.

How much time will my involvement in the project take?

You will be required to participate in up to 60 minutes of research. The surveys/questionnaires will take you up to 15 minutes. The performance tasks will take you up to 30 minutes to complete. You will only be required to participate in one research session. If you have signed up to participate via the SONA Research Participation System (RPS), you will be compensated in course credit for your amount of time (ie. 60 minutes = 1 credit).

Are there any risks associated with participating in this project?

There are no foreseeable risks associated with this study. However, you may feel burdened by giving up time to participate or experience some fatigue as the study requires an extended period of cognitive demand. To manage these potential burdens, you have been notified of the time commitment needed to complete the study and will have the option to cease participation at any time throughout.

What are the potential benefits of the research project?

There are no immediate benefits to yourself in this study. However, participating in an Honours Student project is a great way to 'pay it forward' and see how a project at this level is undertaken.

Can I withdraw from the project?

Participation in this project is completely voluntary. If you agree to participate, you can withdraw from the study at any time.

What will happen to my information?

To ensure confidentiality, your name will remain anonymous. The utmost care will be taken to ensure that no personally identifying details are received nor revealed. Information and project records will be stored securely on the University Student's L-Drive. The Principal Investigator will also have secure access to the results. All records will be kept for the duration of the project and be published in the final thesis. A summary of the results can be provided to yourself if requested. You will be asked to provide extended consent for your participation in case the results are used in future research. In accordance to the NHMRC, this warrants the use of the data in future research projects that are an extension of, or closely related to the original project, or in the same general area of research.

If you are a member of the general public, and elect to enter to win 1 of 5 Coles/Myer vouchers valued at \$20, you will be asked to provide your name and email address. These details will only be used for the purpose of the prize draw and will be destroyed after the winners have been notified and rewarded.


Your information will only be used as described in this participant information sheet and it will only be disclosed according to the consent provided, except as required by law.

CONSENT FORM

- I have read the attached Information Sheet and agree to take part in the following research project.
 - I have had the project, so far as it affects me, and the potential risks and burdens fully explained to my satisfaction by the research worker. I have had the opportunity to ask any questions I may have about the project and my participation. My consent is given freely.
 - I have been given the opportunity to have a member of my family or a friend present while the project was explained to me.
 - Although I understand the purpose of the research project, it has also been explained that my involvement may not be of any benefit to me.
 - I agree to participate in the activities outlined in the participant information sheet.
 - I understand that as my participation is anonymous, I can withdraw any time up until submission of the survey/completion of the interview.
 - I have been informed that the information gained in the project will be published in a thesis and may be used in future research projects that are an extension of, or closely related to the original project, or in the same general area of research.
 - I have been informed that in the published materials I will not be identified, and my personal results will not be divulged.
 - I agree to my information being used for future research purposes as follows:
 - Research undertaken by these same researcher(s)
 - Related research undertaken by any researcher(s)
 - Any research undertaken by any researcher(s)
 - I understand my information will only be disclosed according to the consent provided, except where disclosure is required by law.
 - I am aware that I should keep a copy of this Consent Form, when completed, and the attached Information Sheet.
- By clicking this box, I understand the information above and any questions I have asked have been answered to my satisfaction. I agree to participate in this research, knowing that I can withdraw from further participation in the research at any time without consequence.

Start

Appendix J: Instruction page for the PET



My Task Progress 1 2 3 4 5 6

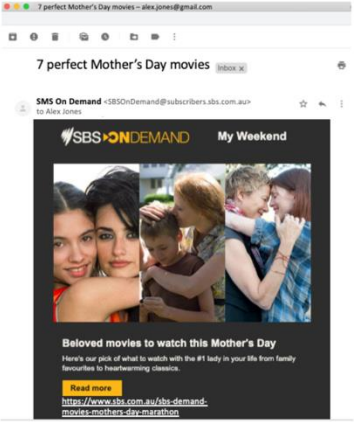
Main Study (PET)_Annie

PET

Instructions:

This task will require you to appraise and respond to 21 incoming emails to the inbox of Alex Jones. All emails are of relevance to Alex Jones.

Each email will contain a prompt button to 'Click Here' for further information relating to the email. For example, in the email below, the prompt button 'Read More' would, hypothetically, take Alex Jones to more information about the Mother's Day movies available on SBS on Demand. In normal email correspondence, Alex could hover over the prompt to see the link associated with the prompt. However, in this exercise, the link associated with the prompt is displayed either below or next to the prompt so you can easily see it. The link in the email below is in white text and is below the prompt 'Read More'.



The screenshot shows an email from 'SBS On Demand' to 'Alex Jones'. The email content includes the SBS On Demand logo, the text 'My Weekend', a photo of a family, and the text 'Beloved movies to watch this Mother's Day'. Below this text is a yellow 'Read more' button and a URL: 'https://www.sbs.com.au/sbs-demand-movies-mothers-day-marathon'.

You will have 30 seconds to read each email and view the link. You are only asked to read the email during this time and not interact with the email in any other way. After 30 seconds, you will automatically be taken to a new page where you will be asked to respond to the following statement: "It is okay to click on the link in this email".

You will indicate the extent to which agree to this statement on a scale of (1) = Strongly Disagree to (5) = Strongly Agree.

The first two emails are practice only. Once you are ready, please click continue.

Continue

Appendix K: Summary of the email click-ability ratings from the PET for anxiety and cue utilisation typologies.

Mean and Standard Deviation for Typologies of State and Trait Anxiety.

Email Condition	Low		Moderate		High	
	State	Trait	State	Trait	State	Trait
Genuine Email	3.89 (.69)	3.97 (.73)	3.62 (.51)	3.62 (.15)	3.21 (.82)	3.34 (.88)
Phishing Email	2.30 (.96)	2.09 (.83)	2.49 (1.06)	2.62 (1.38)	2.20 (.87)	2.46 (.82)

Mean and Standard Deviation for Typologies of Cue Utilisation

Email Condition	Low	High
Genuine Email	3.38 (.85)	3.90 (.71)
Phishing Email	2.18 (.77)	2.45 (.96)