Behaviour & Information Technology

ISSN: 0144-929X (Print) 1362-3001 (Online) Journal homepage: www.tandfonline.com/journals/tbit20

Forest or trees? Evidence for global processing via an information board study into cues utilised in phishing identification

Daniel Conway, Kun Yu, Marcus Butavicius, Fang Chen & Anna Hepworth

To cite this article: Daniel Conway, Kun Yu, Marcus Butavicius, Fang Chen & Anna Hepworth (14 Jul 2025): Forest or trees? Evidence for global processing via an information board study into cues utilised in phishing identification, Behaviour & Information Technology, DOI: 10.1080/0144929X.2025.2530012

To link to this article: https://doi.org/10.1080/0144929X.2025.2530012

Published online: 14 Jul 2025.

BEHAVIOUR & INFORMATION TECHNOLOGY
https://doi.org/10.1080/0144929X.2025.2530012

Taylor & Francis
Taylor & Francis Group

Forest or trees? Evidence for global processing via an information board study into cues utilised in phishing identification

Daniel Conway [a], Kun Yu [a], Marcus Butavicius [b], Fang Chen [a] and Anna Hepworth[c]

[a]Data Science Institute, University of Technology Sydney, Sydney, Australia; [b]Defence Science and Technology Group, Department of Defence, Adelaide, Australia; [c]Media, Creative Arts and Social Enquiry, Curtin University, Perth, Australia

ABSTRACT

We examined the patterns of cues people utilised as they attempted to classify emails as legitimate or phishing via a novel approach – an information board study. In this paradigm, participants had to click on email elements to examine them, revealing which cues are utilised in the decision-making process as well as viewing duration. An online email classification task (87 Ps) was presented, including a between-subjects' manipulation of cognitive load. This revealed consistent patterns of behaviour associated with identification of legitimate emails such as more time spent looking at signoffs aiding in identification, whereas more time spent looking at logo and greetings was associated with worse performance. We also found no-load condition participants with lower intuitive decision-making style scores identified more phishing emails correctly suggesting elaborative processing as an important determinant of good decision-making. However, none of; cyber security experience, impulsivity, and checking the sender's address corresponded to higher rates of phishing email identification. Furthermore, we found no behavioural, cue-based patterns associated with correct decisions for phishing emails. We speculate that this decision-making process may be based on a global, holistic interpretation of the stimuli. This has important implications for awareness campaigns suggesting a more holistic approach to email evaluation.

ARTICLE HISTORY
Received 1 September 2024
Accepted 30 June 2025

KEYWORDS
Phishing; decision-making; dual process; cue utilisation; behaviour; cyber security

1. Introduction

Phishing emails remain the most common method of attack in a cyber-attacker's arsenal with, globally, an estimated 29 billion spam emails being sent every day (Osman 2013). In Australia, 74% of cyber-attacks are estimated to be email based and phishing is rated as the most common type of cyber-attack by the Australian Competition and Consumer Commission (Bayl-Smith, Sturman, and Wiggins 2020).

For the purposes of this work we define phishing emails as generically constructed, mass–distributed emails with either an attachment containing malicious code, or a link to an external website designed to trick the reader into divulging information such as authorisation credentials (Akbar 2014). These emails are constructed to appear as legitimate requests for information or a call to action. Users are therefore almost universally faced with the ongoing task of detecting these malicious attacks during day-to-day use of their email systems (Parsons et al. 2019).

Phishing victimisation has been increasingly widely studied since the phenomenon first came to light in 1996 (Akbar 2014). It has been subjected to a wide variety of investigative lenses, each with a different set of a priori, assumptions and methods and each delivering a range of insights of varying utility. In this paper we applied a cue utilisation framework via an experimental design derived from information board studies. We also aimed to examine the contribution of elaborative processing to a phishing identification task via the deployment of a secondary task in a between-participants manipulation. This work is novel in that it explicitly examines which cues are attended to and for how long during the decision-making process as well as examining individual differences as antecedents of the decision-making processes. We then connect our findings to the global processing literature as pioneered by Navon (1977) with his seminal paper that included the phrase 'Forest Before Trees' in the title.

By understanding which cues people attend to when they evaluate the veracity of emails and the reliance on elaborative thought in doing so means that we will be able to better mitigate risk by adapting our electronic systems to the fundamental architectures, constraints and foibles of human cognition.

CONTACT Daniel Conway daniel.conway@uts.edu.au Data Science Institute, University of Technology Sydney, Sydney 2007, Australia

2. Background

2.1. Information board studies

Information board studies, themselves a subset of process tracing methods, aim to reveal aspects of the otherwise invisible processes of decision-making. Originally these were developed to investigate, and make visible, aspects of multi-attribute decision-making. In these early experiments (Payne 1976; Svenson 1979) participants were asked to choose between multiple options of an item – each of which had different values for common attributes. As an example, participants would be asked to choose a washing machine from three available options and have access to several attributes for each option such as price, energy efficiency and load size. However, the values of these attributes would initially be hidden, so that participants would be required to turn over pieces of paper arranged on an 'information board' to reveal the value of an attribute of one option – but only ever one at a time. Dependent variables were then which pieces of information were interrogated, in which order, and then the final decision. Schulte-Mecklenbeck et al. (2017) defined process tracing as: 'time-dependent, pre-decisional observations used to inform predictions regarding the psychological mechanisms assumed to operate concurrently with the choice-generating process'. It should be noted that this method is not normative and does not assume an ideal process – but instead seeks to reveal which attributes of a stimuli are used to make a decision (Harte and Koele 2002). In this work we will adapt this method to our needs to ascertain (1) which cues are used and (2) which cues are most effective in making veridical decisions, during phishing email detection.

2.2. Elaborative processing

Dual process theories of cognition have been increasingly deployed in the investigation of phishing victimisation. These models suggests that we have two 'systems' in our mind that can both contribute to a decision (De Neys, Cromheeke, and Osman 2011; Kahneman 2011; Wason and Evans 1974). System 1 is characterised as a collection of intuitive, fast, sub-conscious and automatic heuristics, while System 2 thought (referred to hereafter as elaborative thought) consists of effortful, rational, analytic processing of information (Evans and Stanovich 2013). In relation to phishing emails, it has been suggested that people engaging in elaborative processing while evaluating incoming emails are more likely to identify the malicious nature of the message and therefore, when applied, improve phishing email detection (Jones, Towse, and Race 2015; Musuva, Getao, and Chepken 2019; Vishwanath 2015).

An important phenomenon observed within the dual process literature, and one that is again relevant to the experimental designs that follow, is the dependence of elaborative thought on working memory (De Neys 2006; Whitney, Rinehart, and Hinson 2008; Zu et al. 2020). While our 'instinctive' System 1 processes run automatically, often unconsciously, and without any perceived effort or capacity bottlenecks, System 2 thinking relies on working memory and this processing can be engaged along a continuum ranging from less to more.

This dependence of elaborative thought (but not System 1) on working memory has been extensively explored within dual process experiments (Bago and De Neys 2017; Johnson, Tubau, and De Neys 2014; Miyake et al. 2001; Purcell, Wastell, and Sweller 2021; Whitney, Rinehart, and Hinson 2008). Here it is common for researchers to experimentally manipulate the ability of elaborative thought to contribute to a given decision-making process by loading working memory with extraneous load via a secondary task (often referred to as 'cognitive constraint') such as a dot-memorisation task, span task or finger tapping a given rhythm while carrying out the primary task (Whitney, Rinehart, and Hinson 2008). These secondary tasks consume the processing power available to working memory, impacting how much working memory is available for the primary task. When confronted with a high extraneous load, elaborative, System 2 processing capacity is diminished. However, since System 1 processing is independent of working memory, its outputs are unaffected, resulting in System 1 contributions more likely to 'win' the race to respond (Bago and De Neys 2017). Experimentally therefore, this technique allows us to bias the decision-making process towards System 1 outputs thereby illuminating the automatic, instinctive contributions to the decision-making processes.

2.3. Phishing as conflict problem

Central to many of the experimental paradigms around dual process theories is the concept of 'conflict'. If we accept that there exist two systems within our minds, each of which is capable of providing an answer to a problem, then it follows that in some conditions, the answers provided by the two systems may not agree with one another (Stanovich 2018). This is the essence of a conflict problem.

A central tenet of this paper is that phishing emails can be viewed as conflict problems. These messages usually include persuasive techniques, described in the social engineering literature, such as scarcity, urgency and social proof (Cialdini 1993; Ferreira, Coventry, and Lenzini 2015). These tactics are designed very

specifically to illicit a powerful System 1 type response and thereby influence the decision-making process in favour of completing the attacker's call to action within the email (Lawson et al. 2020; Musuva, Getao, and Chepken 2019). Since Chaiken (1980) posits that the two systems compete in a 'race' to arrive at some form of sufficiency threshold, the fact that they are deliberately provoking System 1 heuristics means that they are biasing the decision-making process against the likelihood of System 2 contributing to the process (Xu and Zhang 2012). Thus, a dual process interpretation of encountering a phishing email would suggest that while the content of an email is deliberately provoking a powerful intuitive response of 'click here' or 'download this file', System 2 processes, if engaged, are likely to be saying 'hold on – something is not right here'. By this formulation phishing emails can very specifically be seen to be 'conflict problems' where the behavioural outcome that the attacker desires are the result of System 1 winning the race to our sufficiency threshold, whereas System 2 thought should result in elaboration on the nature of the message and therefore a higher likelihood of correct identification of the malicious nature of the message. The experiment that follows deploys a between-participant manipulation of cognitive constraint via a secondary task to establish whether elaborative processing is implicated in phishing email identification.

2.4. Cue utilisation

Phishing emails provide a challenge to research from a cognitive psychology standpoint because they are such feature-rich stimuli. Within every email there are multiple elements that contain information varying along dimensions such as font, size and colour, relating to the content, the sender, the recipient, and the nature of the connection between the two – all of which can be used to attempt to ascertain the veracity of the message. Subtle and difficult to quantify attributes such as the image quality of a logo, or variances in layout result in an intractably large problem space that people evaluate, consciously or not, as they view an email.

A prominent method of trying to grapple with this variation is via the framework of 'cues' where a cue is considered to be a feature that has been associated in the mind of the participant with outcomes or events from previous experience (Bayl-Smith, Sturman, and Wiggins 2020). This allows us to narrow down the exceedingly large number of possible combinations of perceptual signals into ones that are recognised by the participant as having informational value. Thus, individual elements of an email such as logos, greetings, text, and sender's address can be considered cues in that participants will have previously encountered these stimuli and have some association with previously encountered information as well as onwards journeys and outcomes, all stored in long term memory. A corollary to this lens of analysis that is important to our work is that frequent exposure to a given stimulus and its associated outcome will result in expertise and therefore faster and less effortful processing of the cue, its implications and stored, associated memories.

There has been some work previously into the relationship between cues present in phishing emails and participant's responses to them. Instances of this approach come from both Blythe, Petrie, and Clark (2011) and E. J. Williams and Polage (2019). Blythe found that typographical errors were often considered a cue, but were not present in all phishing emails, and Williams that people were often deceived by the presence of a logo in the email. More generally, researchers have investigated cues as 'credibility' signals in both websites and phishing emails. Wogalter and Mayhorn (2008) found that more experienced internet users were more trusting of such signals, Vishwanath (2022) incorporates credibility heuristics into his Vishwas triad of trust framework and suggests that the effect of multiple signals are cumulative, and Shan et al. (2016) applied the concept of source credibility within a Dual Process framework (The Heuristic Systemic Model).

The sender's address in emails is a cue that has received much attention from both research and industry training efforts where it is often held up as an important cue to evaluate (Parsons et al. 2016) because of its high diagnostic value. Attributes of senders' addresses that are taught as predicting malicious intent are: letter substitution (e.g.: noreply@mazon.com), unusual domain names (e.g.: mailer.srvvscust-yaoelauzwb9446325@mntapjwaku.com), and domains that do not match the content of the email (Burita, Klaban, and Racil 2022; Jakobsson 2007; Parsons et al. 2016; Xiong et al. 2017). Jakobsson (2007) found that people were good at recognising dubious senders' addresses, however, Parsons et al. (2016) found that while the sender's address was rated by experts as an important cue to evaluate an email's legitimacy, naïve users did not rate the cue as important.

Hamilton, Shih, and Mohammed (2016) contributed an important aspect to the conversation around cues with the application of the concept of 'leakage cues' as an extension of Ekman and Friesen's original formulation of deceptive cues in non-verbal communications (Ekman and Friesen 1969). In this interpretation, cues may inadvertently reveal their malicious intent, with this framework thereby centring the deceptive nature of phishing emails. Kim and Kim (2013) found that phishing emails contained cues relating to rational,

emotional, or motivational appeals. Blythe, Petrie, and Clark (2011) carried out an extensive analysis of phishing emails and noted that spelling mistakes were not ubiquitous in malicious emails and that many used convincing company logos to increase credibility. E. J. Williams and Polage (2019) also found that the presence of a logo increased ratings of trustworthiness. This observation is echoed by Vishwanath (2022), who suggested that cues that are familiar to people, (referred to as 'credibility signals') trigger heuristic responses.

These two assertions fit neatly within a dual process interpretation of phishing victimisation where certain cues, when familiar or trusted, trigger heuristic processing and thereby increase the likelihood of victimisation by decreasing the likelihood of elaborative processing. Elaborative processing, on the other hand, is seen as protective against victimisation since subjects are then likely to engage in a more thorough analysis of the message, content and contexts, and thereby more likely to uncover the deceptive elements present in leakage cues. However what cues are actually attended to and which ones influence decisions are unresolved questions, which we will attempt to answer in this work.

A promising, more recent lens of analysis has been the measurement of a specific individual differences, namely the tendency to glean information from cues, referred to as 'cue utilisation'. A catalogue of recent findings is beyond the scope of this work, but overall it suggests that some people are better at utilising existing cues to extract meaningful information and that this skill is associated with improved phishing email identification (Ackerley et al. 2022; Bayl-Smith, Sturman, and Wiggins 2020; E. J. Williams and Polage 2019; R. Sturman et al. 2023; Valenzuela 2021; Williams et al. 2024). Many of these studies, while including analysis of the number of cues utilised by participants in phishing identification tasks, often either have not analysed which cues are actually used in this task (Bayl-Smith, Sturman, and Wiggins 2020; R. Sturman et al. 2023; Williams et al. 2024) or more intriguingly, when they have looked, have failed to find systematic patterns of cues utilised by participants (Ackerley et al. 2022).

Specifically, Ackerley et al. (2022) found no differences in which cues were examined between high and low cue utilising groups. They noted this as an important open question and in their conclusion called for an investigation of which cues were utilised in decision-making. Greene et al. (2018) also found that there was no particular pattern of cues examined or considered in the phishing/non-phishing decision, and cues did not vary across people who clicked or did not click. Evidence from a different but related approach to this problem, derived from eye-tracking studies, also supports this view. McAlaney and Hills (2020) found that there was no significant relationship between the amount of time spent viewing cues commonly associated with phishing email detection and the trust-worthiness ratings of emails.

Thus, a number of authors have been puzzled by these initial findings and have suggested that which cues are actually attended to and which ones influence decisions be a focus of future research. We therefore present this work in an attempt to answer this important open question and hope to contribute to our understanding of which specific cues people utilise in the task of detecting of phishing emails.

2.5. Individual differences

A large number of individual differences have been suggested to impact phishing victimisation (Canfield, Fischhoff, and Davis 2016; Jeong et al. 2019; Lawson et al. 2020; Montañez, Golob, and Xu 2020; Oliveira et al. 2017). We sought to measure some of the most commonly discussed individual differences in order to assess how patterns of cue utilisation varied in association with these variables.

Variables related to knowledge, such as prior experience of phishing victimisation, training and computer literacy have been a central thrust of the 'awareness' teams within industry for some time now (R. Wright, Johnson, and Kitchens 2023) and are thought to be important determinants of improved detection of phishing emails. Harrison, Vishwanath, and Rao (2016) found that both subjective confidence around email practices and objective knowledge of on-line attacks were predictors of increased elaboration in response to suspicious emails. Zielinska et al. (2015) found that there were significant differences in mental models between expert and naïve users. However, while not directly related to phishing, Stephanou (2008) carried out a pre-test, post-test experiment into security behaviours more generally (such as having strong passwords), and found that while information and training resulted in better understanding of security in the experimental group rather than the control, it did not reliably lead to better practices. We were therefore interested in measuring cyber security experience.

Meta-cognitive variables such as impulsivity (Parsons et al. 2019) have also been investigated as possible indicators of increased likelihood of victimisation. Butavicius et al. (2016) showed that low impulsivity participants were more likely to judge a fraudulent email unsafe but impulsivity had no effect on genuine emails. This is in marked contrast with much of the commercial phishing defence industry that relies almost exclusively

on 'education' in the hope that more information alone will arm people against email-based attacks.

Finally, since we were interested in the effect of elaborative / system 2 thought on the email evaluation process, we noted that there has been evidence of individual differences in people's tendency towards analytical thought (Stanovich 2018). This variable is often referred to as cognitive 'style'. Within the context of phishing victimisation, Wang et al. (2012) has shown that attention to 'visceral' (superficial / heuristic) aspects of a phishing email reduced cognitive processing and increased victimisation. Divergent processing styles have also been shown to be evident in the way people analyse phishing emails (Neupane 2015). However, in contrast, Vishwanath et al. (2011) showed that peripheral cues in some cases increase elaborative processing – but at the expense of processing of message content – leading to increased victimisation. This picture is still far from clear.

3. The present study

We sought to understand which cues people attended to when evaluating emails, which cues aided in correct identification, and how these might vary according to commonly discussed individual differences implicated in phishing victimisation (i.e. impulsivity, cyber security experience and decision-making style).

As such we presented an email classification study presented via a novel approach – an information board protocol – where participants were required to click on each cue present in the email to make it legible. Only one cue could be legible at a time, and we recorded which cues were clicked on and the duration the cues were legible for before participants made their final decision.

Since elaborative processing has often been cited as being protective against phishing victimisation, we deployed two, between participant, conditions. A no load condition, and a load condition in which extraneous cognitive load was applied to participants via a visual matrix secondary task that they were required to carry out concurrently with the (primary) email classification task.

Finally, we gathered data on participants' individual differences (intuitive decision-making style, impulsivity and cyber security experience) via three surveys at the conclusion of the experiment.

3.1. Hypotheses

3.1.1. Elaborative processing

1a) Participants in the no load condition will identify more phishing emails correctly than those in the load condition.
1b) This effect would be less for legitimate emails.

3.1.2. Individual differences

2a) Participants with higher intuitive decision-making style scores will identify fewer phishing emails correctly than those with lower intuitive scores.

2b) Participants with higher impulsivity scores will identify fewer phishing emails correctly than those with more lower impulsivity scores.

2c) Participants with higher cyber security experience scores would correctly identify more phishing emails correctly than those with lower cyber security experience scores.

3.1.3. Behaviour

We thought people who engage more with the stimuli would correctly identify more phishing emails than those who do less so. Specifically, we hypothesised:

3a) Participants who spend more time on each trial will correctly identify more phishing emails than those who spend less time doing so.

3b) Participants who click on more cues in each trial will correctly identify more phishing emails than those who click on less cues.

We thought that participants who utilise the sender's address more in their decision-making would identify more phishing emails correctly than those who do so less. Therefore, we hypothesised:

4a) Participants who spend more time looking at the sender's address will correctly identify more phishing emails than those who spend less time doing so.

4b) Participants who click more often on the sender's address will correctly identify more phishing emails than those who do so less.

4c) Participants who viewed the senders address at all will identify more phishing emails correctly than those who did not.

4d) Participants who viewed the sender's address first will identify more phishing emails correctly than those who did not.

4. Method

4.1. Participants

100 participants were recruited via the 'Prolific' online platform (www.prolific.co). After removing incomplete responses and two responses for having Cook's D values of more than 1 in order to escape the undue influence of those points (Stevens 1984), a total of 87 participant data files remained (women: 45, men: 40, non-binary/gender diverse: 2), age: (Min = 18, Max = 72, $M = 35.4$, $SD = 12.6$). Participants were from Australia (46), The United

States (10), United Kingdom (10), New Zealand (18) and unknown (3). Pre-requisites for completion were: fluent in English, not affected by drugs or alcohol, and presentation of the experiment on a full-screen monitor (not mobile device). Median experiment duration was 17 min, 22 s.

4.2. Design

A between-participants manipulation of cognitive load was deployed where half the participants (randomly selected) were presented with a visual matrix task to complete concurrently with making each email classification decision. This is referred to as the load condition.

4.3. Materials

4.3.1. Information board style phishing identification task

The email stimuli presented were screen captures of real emails, both phishing and legitimate, with sender's address visible and presented as if in the standard preview panel of major commercial web-email applications (Gmail, Outlook360). A small collection was made of phishing emails received by the author and colleagues in the two years months before the experiment was carried out. This corpus was analysed as to characteristics noted by other authors as indicative of phishing emails. We then selected emails that were most representative of these characteristics namely; typographical errors 2% by word count (Nasser et al. 2020) Spelling errors 0% by word-count (Harrison, Vishwanath, and Rao 2016), grammatical errors 8% by word-count (Wang et al. 2012), no personalisation (recipient name etc …) as according to 84% of the phishing email corpus (Karakasiliotis, Furnell, and Papadaki 2006) and incongruent sender's email address and domain name (83% of the corpus) (Bayl-Smith, Sturman, and Wiggins 2020). As such we believe that the phishing emails presented were broadly representative of phishing emails in circulation at the time of writing. The legitimate emails presented were selected to be similar in format to the phishing emails in that they were not personal communications and contained a call to action.

The 20 emails selected as stimuli for this experiment, while likely to represent many of the types of emails currently in circulation, therefore also included considerable variation of style and content. We considered this would add noise to our final analyses where we may be comparing responses to emails with and without the presence of different cues. For example: some emails contained company logos, a greeting in the text, signoffs, and so on; some did not. To reduce this variance while still maintaining a wide variety of emails presented, we selected 14 emails (seven legitimate and seven phishing) that all had the same cues present and we classified these as being 'cue-consistent stimuli'. Removing the emails that did not have this consistent set of cues meant that all of the remaining seven legitimate emails and the seven phishing emails contained all the elements of: subject, sender's address, task irrelevant interface objects (such as navigation or social media buttons), logo, link, greeting, text, and signoff. All analysis that follows concerns only this subset of 14 stimuli with consistent cues and the remaining stimuli (which did not have all cues present) can be considered distractors (Table 1) .

Table 1. Email cues.

Cue number	Cue
1	Subject line
2	Sender's address
3	Task irrelevant interface objects (buttons, social media icons etc …)
4	Logo
5	Link
6	Greeting (including personalisation or generic)
7	Text
8	Sign-off

Email stimuli were prepared by blurring the original image to the point where the position of cues could be identified but would not be legible (Gaussian blur; radius 7.2 pixels). Cue labels were then added on to the blurred images so that participants could identify the nature of each cue before clicking as seen in Figure 1.

4.3.2. Visual matrix secondary task

In the load condition extraneous cognitive load was applied via a concurrent secondary task. We chose the visual matrix task since it has been used in a number of seminal dual process papers manipulating System 2 capacity (Bago and De Neys 2017; De Neys 2006; Johnson, Tubau, and De Neys 2014). In the load condition then, participants were shown a visual matrix consisting of 12 cells in a 4×3 arrangement at the beginning of each trial. Four randomly selected cells within the matrix were shaded blue. This matrix was presented for two seconds and participants were required to memorise the pattern of shaded cells and maintain this pattern in their working memory while they completed the primary task. At the completion of each trial, and after they had entered their email classification response, they were then presented with a blank matrix and were required to re-create the pattern of coloured cells presented at the outset of the trial by clicking in the cells to colour them blue. See Figure 2 for a user flow of the load condition.

Figure 1. A screenshot of a trial in its initial state: the email blurred but all cues labelled. Cue labels in experiment were purple to provide visual contrast with email image.

4.4. Apparatus

The experiment was coded in PsychoPy, an open source, open science experiment presentation platform that features a high degree of visual stimuli and timing precision (Peirce et al. 2019). The experiment was presented online and once begun, it automatically ran in full-screen mode and accepted input from keyboard and mouse.

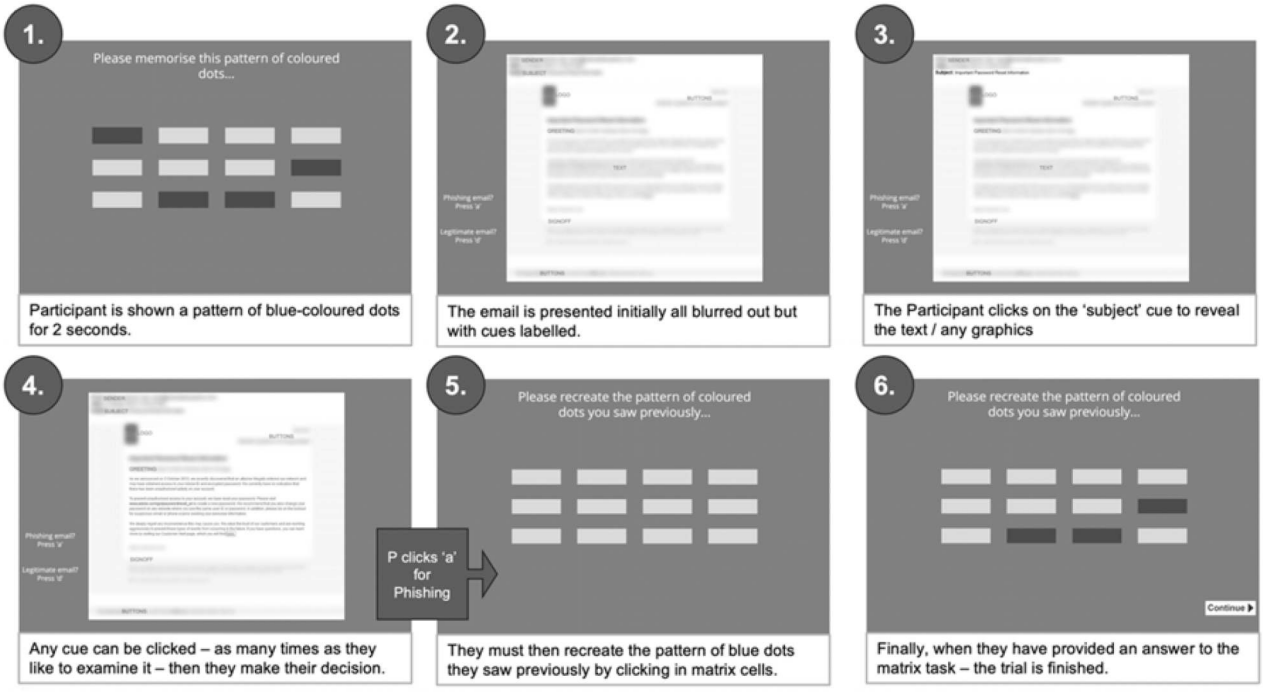

Figure 2. A user flow of an entire trial in the load condition, including secondary visual matrix task.

4.5. Procedure

Participants were randomly assigned to either the no load or load condition. After consent was gathered, ethics information displayed, and detailed instructions provided (including animated gifs of clicking cue names to reveal the unblurred cue beneath) participants then carried out the phishing task followed by three short surveys.

Two practice trials of the phishing task were presented and then 20 trials of the phishing classification task itself. 10 of these were blurred and labelled screenshots of legitimate emails, and 10 were the same of phishing emails, presented in random order. When emails were initially presented – they were entirely blurred (see Figure 1). Participants could click on a cue label – or anywhere within the bounding box of the cue – and this would render that particular cue unblurred and fully legible (see Figure 3). This cue would then remain legible until another cue was clicked or the participant made their final decision by hitting the 'a' key (for phishing emails) or 'd' key (for legitimate emails) on their computer keyboard.

4.6. Measures

For each trial of the phishing classification task we recorded which cues were clicked on to view them, the total number of cues examined, the accumulated duration for which each cue was legible (potentially over multiple clicks), total trial response time (RT) and then the participants' final decision of whether the stimuli presented was a phishing or legitimate email. We also gathered basic demographic information (age, gender) at the outset of the experiment and finally measured a small number of individual differences via a questionnaire at the conclusion (cyber security experience, impulsivity and decision-making style). For each participant we also calculated a score of the proportion of trials in which the sender's address was clicked on at all, and a similar score for the proportion of trials in which the sender's address was clicked on first, before any other cue.

4.6.1. Cyber security experience

Since there appears to be a dearth of published instruments that assess a person's level of cyber security training and experience we utilised the same instrument that we developed previously (Conway et al. 2023). This consisted of seven questions measured via five-point Likert scale resulting in scores from 7 to 35. All items were presented as statements and participants selected how much they agreed with each statement, with responses gathered via anchors labelled ('*Strongly disagree', 'Disagree', 'Neutral', 'Agree', 'Strongly agree*'). See Table 2 for the text of all the questions. We should note that this scale has not been validated and can therefore not provide reliability data.

4.6.2. Hamilton's intuitive decision-making style scale

To quantify participants' tendency towards an intuitive decision-making style, we deployed the intuitive scale items from Hamilton's decision-making style instrument (Hamilton, Shih, and Mohammed 2016). This scale was reported as having $r^2 = .79$ test/retest reliability. All questions were presented as statements and participants would select how much they agreed with each statement, with responses gathered via a five-point Likert scale with all anchors labelled: (*'Strongly disagree', 'Disagree', 'Neutral', 'Agree', 'Strongly agree'*). Final scores were from 5 to 25 with higher scores indicating a more intuitive decision-making style. See Table 3 for the text of all the questions.

4.6.3. Barrett's impulsivity score, brief scale (BIS8)

To assess participant's impulsivity we presented the brief, sex question version of the Barratt's impulsivity

Figure 3. When a user clicks on a cue name, or within the bounding box surrounding the whole cue, the cue becomes legible.

Table 2. Cyber security experience questionnaire items.

Question Number	Item
1	I have read about or heard about how to identify phishing emails.
2	I have had one or more training sessions on how to identify phishing emails at work.
3	I have had one or more training sessions on how to identify phishing emails elsewhere (not at work).
4	My company regularly sends out phishing drills / emails.
5	I know how to identify phishing emails.
6	I have fallen victim to one or more phishing emails in the past.
7	I teach others how to identify phishing emails.

Table 3. Hamilton's intuitive decision-making scale items.

Question Number	Item
1	I weigh feelings more than analysis in making decisions.
2	When making decisions, I rely mainly on my gut feelings.
3	My first thought about decisions is generally what I follow.
4	I make decisions based on intuition.
5	I rely on my first impressions when making decisions.

scale (Steinberg et al. 2013) with a reported Cronbach's $\alpha = .73$. All items were presented as a statement with responses gathered via a 4 point Likert scale with anchors labelled: '*Rarely/never*', '*Occasionally*', '*Often*', '*Almost always/always*'. Items 1, 3 and 4 were reverse scored resulting in a value from 6 to 24 with higher scores indicating a higher level of impulsivity. See Table 4 for the text of all the questions.

5. Results

5.1. Data preparation

Of the total 1780 trials, those with a total trial response time of more than three times the IQR (68 s) were excluded based on examination of the response sets. This is double the commonly used value and represents a deliberately liberal approach to data cleaning since only those with extremely long response times showed evidence of a lack of attention. This exclusion criterion removed 28 trials. Analysis of responses times (RT) (min = 2.04s) revealed that an RT 2σ less than the mean (Ratcliff 1993) was −5.82 owing to the skewed shape of the distribution. Further analysis showed that responses 1σ less than the mean exhibited a proportion of correct responses of .9 suggesting that faster responses were not at chance and therefore not spurious but rather the result of fast, accurate decision-making. These responses were therefore left in the data for analysis.

Table 4. Barrett's impulsivity scale items.

Question Number	Item
1	I plan tasks carefully. *
2	I do things without thinking.
3	I am self-controlled. *
4	I am a careful thinker. *
5	I say things without thinking.
6	I act in the moment.

Note: Items with an asterisk are reverse scored.

Those trials where participants made their decision without looking at any cues were also removed (100 trials).

Additionally, two participants' data files were excluded from the regression model as having Cook's D values of more than .1 and having undue influence on the model, leaving the analysis presented below based on 87 participants.

It should be noted that because of the removal of these trials the total response tallies reported in this work are often not full multiples of the number of participants x trials and calculations based on proportions are often used to overcome this problem. We also examined primary task performance as a function of matrix task performance and found there was little evidence of trade-offs so we did not pursue this avenue of analysis.

The dataset was then finally reduced to include only those email stimuli which had an identical set of cues. This meant that we could avoid the increased noise in the response set resulting from, for example, some emails having a logo and some not. This left us with seven legitimate emails and seven phishing emails – from the original 20 stimuli, leaving us with 1117 trials from 87 participants. These trials were then analysed and formatted into a by-participant table which included tallies of events for each participant such as proportion of phishing emails answered correctly, accumulated time spent looking at cue one to eight, number of clicks to view cue one to eight and so forth over all trials. These by-participant records were the basis of the regression models presented below.

5.2. Descriptive statistics

As a manipulation check, and to test the relative difficulty of identifying the phishing and legitimate emails, a two-sample test for equality of proportions was carried out for correct and incorrect answers of phishing trials and legitimate email trials. There was no significant effect for email type, χ^2 (1) = .06, $p = .799$, with the mean proportion of legitimate emails answered correctly being .8 and the mean proportion of phishing emails answered correctly being .81. The proportion of correct answers for the 14 'consistent stimuli' are displayed in Figure 4. Light coloured columns are the six distractor stimuli which did not have consistent cues present and were therefore omitted from analysis.

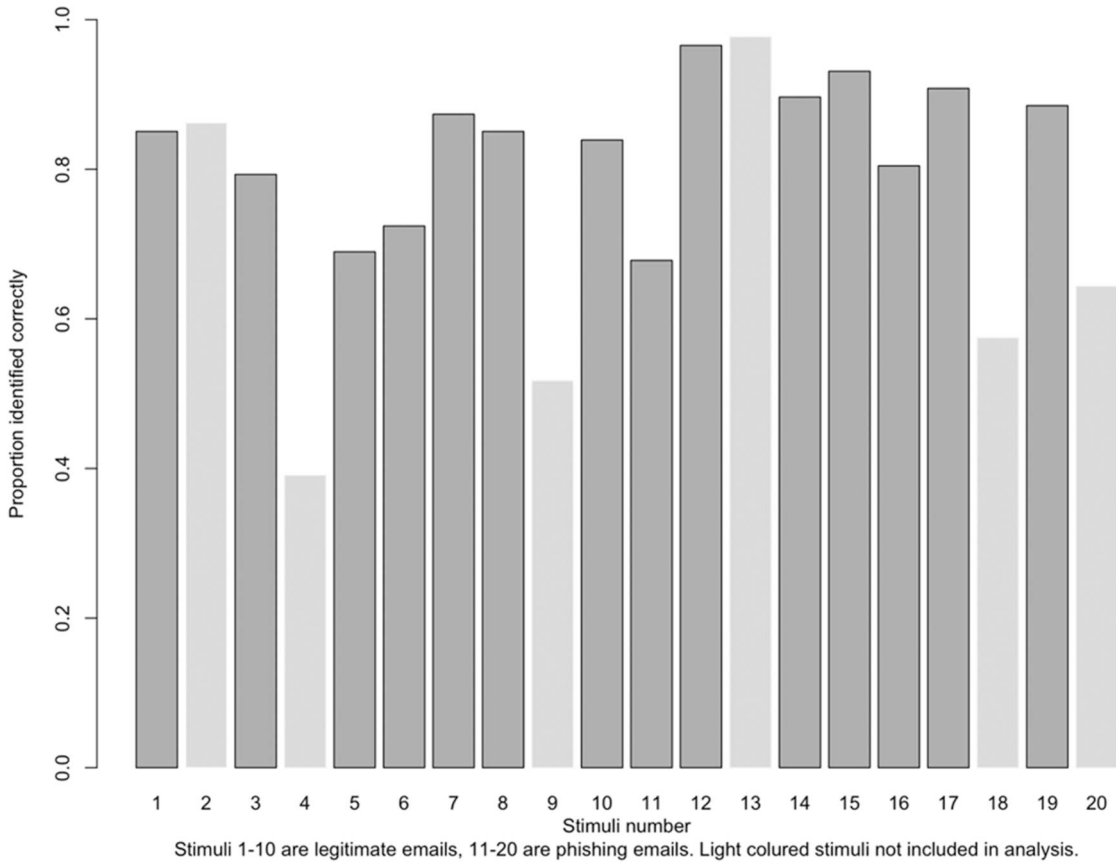

Figure 4. The proportion of participants who answered correctly by email stimuli.

In order to understand which cues participants utilised in making their decisions we recorded the number of times participants clicked on each cue before making their decision and the accumulated amount of time spent examining each cue. Overall, the pattern of mean times each participant spent looking at each cue in each trial can be seen in Figure 5 and the total number of clicks on each cue for the 14 stimuli can be seen in Figure 6.

5.3. Regression models

Initially a regression model was built using the simultaneous method, therefore including all parameters and run with the dependent variable being the proportion of correct email identification scores for all trials ($p < .001$, adjusted $R^2 = .36$). Since we were also interested specifically in participants' responses to phishing emails, we then reran the model with the proportion correct of phishing email trials as the dependent variable ($p = .054$, adjusted $R^2 = .05$). Since these two models proved so different for the different types of trials, and in order to isolate those parameters that explained the most variation in the data we therefore then built two models – one for phishing emails ($p = .003$, adjusted $R^2 = .11$) and one for legitimate emails ($p < .001$, adjusted $R^2 = .39$) using forward stepwise entry method and with the overall model fit as the criterion for predictor inclusion. Interaction terms between various parameters were added but then abandoned if they did not improve model fit. A backward elimination process was also carried out to confirm the inclusion of parameters. These two models, one for phishing emails and one for legitimate emails, are reported in Table 5. This table includes rows for all the terms that we attempted to include in the model in order to illustrate what was and was not predictive. However, statistics are reported only for parameters included in the final models – and as mentioned above – some of these parameters were not significant predictors but were included because they improved model fit.

For regression model 1, where the proportion of correct identification of only legitimate emails was the dependent variable, the model was significant at $p < .001$ and the overall model fit was 39% (adjusted R^2). Condition was significant where participants under load were more likely to make correct decisions ($\beta = 0.09$, $p = .008$). Clicking on the greeting more often was associated with more correct identification

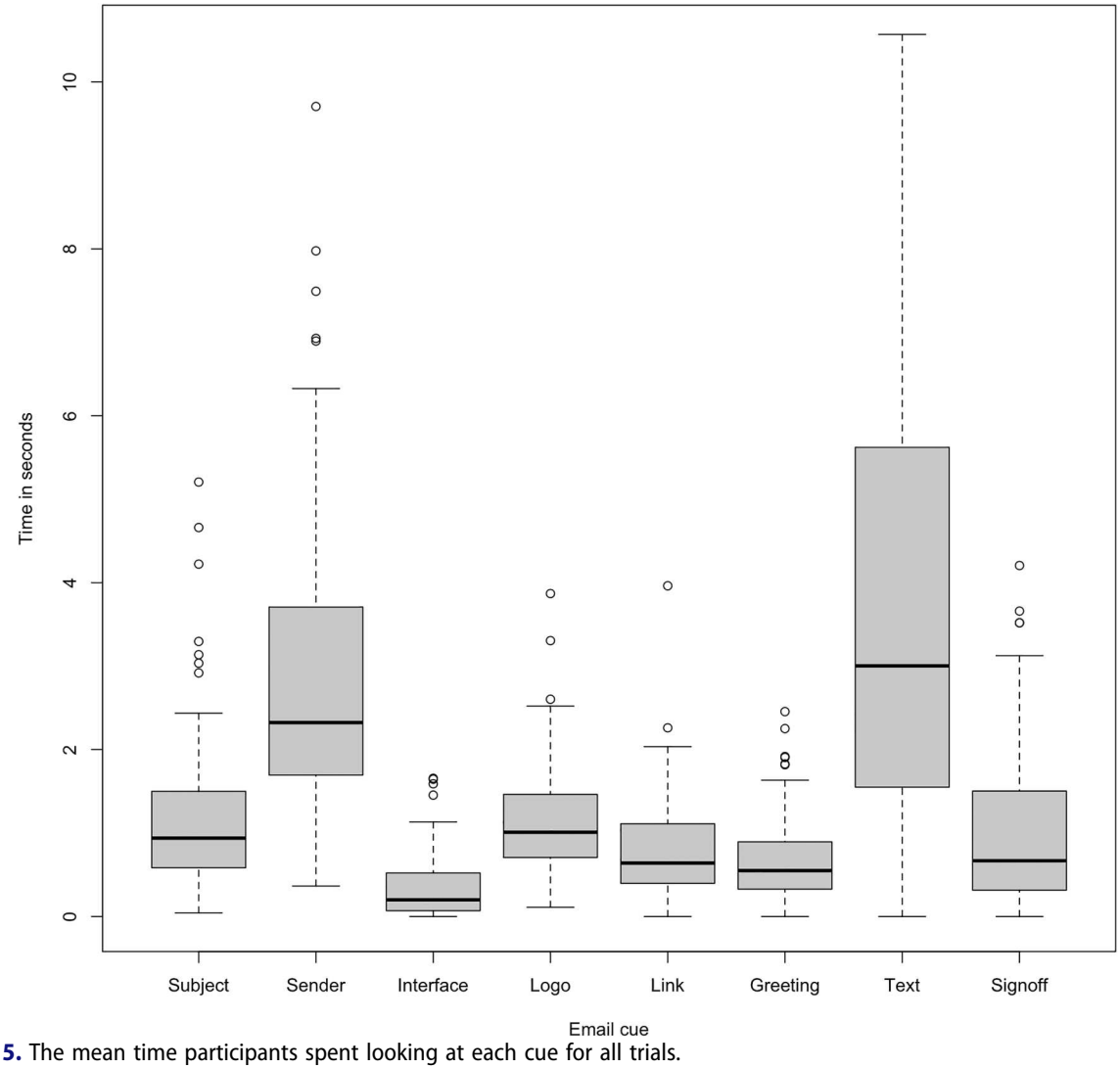

Figure 5. The mean time participants spent looking at each cue for all trials.

($\beta = 0.01$, $p = .04$) and looking at the sign-off more often was associated with less correct identification ($\beta = -0.04$, $p < .001$). Spending more time looking at the logo ($\beta = -0.16$, $p < .001$) and greeting ($\beta = -0.24$, $p < .001$) was associated with less correct identification while spending more time looking at the signoff was associated with more correct identification ($\beta = 0.16$, $p < .001$). The interaction term of cyber security experience and mean trial response time was significant ($\beta = -0.001$, $p < .033$) indicating a cross-over interaction between response times and cyber security experience scores, but the estimate was so small as to not be meaningful.

Regression model 2, where the proportion of correct identification of phishing emails was the dependent variable, the model was also significant at $p = .003$ and the overall model fit was 11% (adjusted R^2). Condition was significant where participants in the load condition were less likely to make correct decisions ($\beta = -0.07$, $p < .044$) and intuitive scale scores were significant where higher participant scores were associated with less correct identification ($\beta = -0.02$, $p < .003$).

5.4. Hypothesis testing

5.4.1. Elaborative processing

Hypothesis 1 stated that elaborative processing would aid in correct identification of phishing emails (with a corollary of this effect would be of less magnitude for legitimate emails). This hypothesis was supported where condition (load vs no load) was significantly, negatively associated with correct identification in model 2 (phishing emails: $\beta = -0.07$, $p < .044$) but positively associated with more correct identification of emails in model 1 (legitimate emails: $\beta = 0.09$, $p = .008$).

5.4.2. Individual differences

Hypothesis 2a stated that people with higher intuitive decision-making scores would identify fewer phishing emails correctly than those with lower intuitive scores.

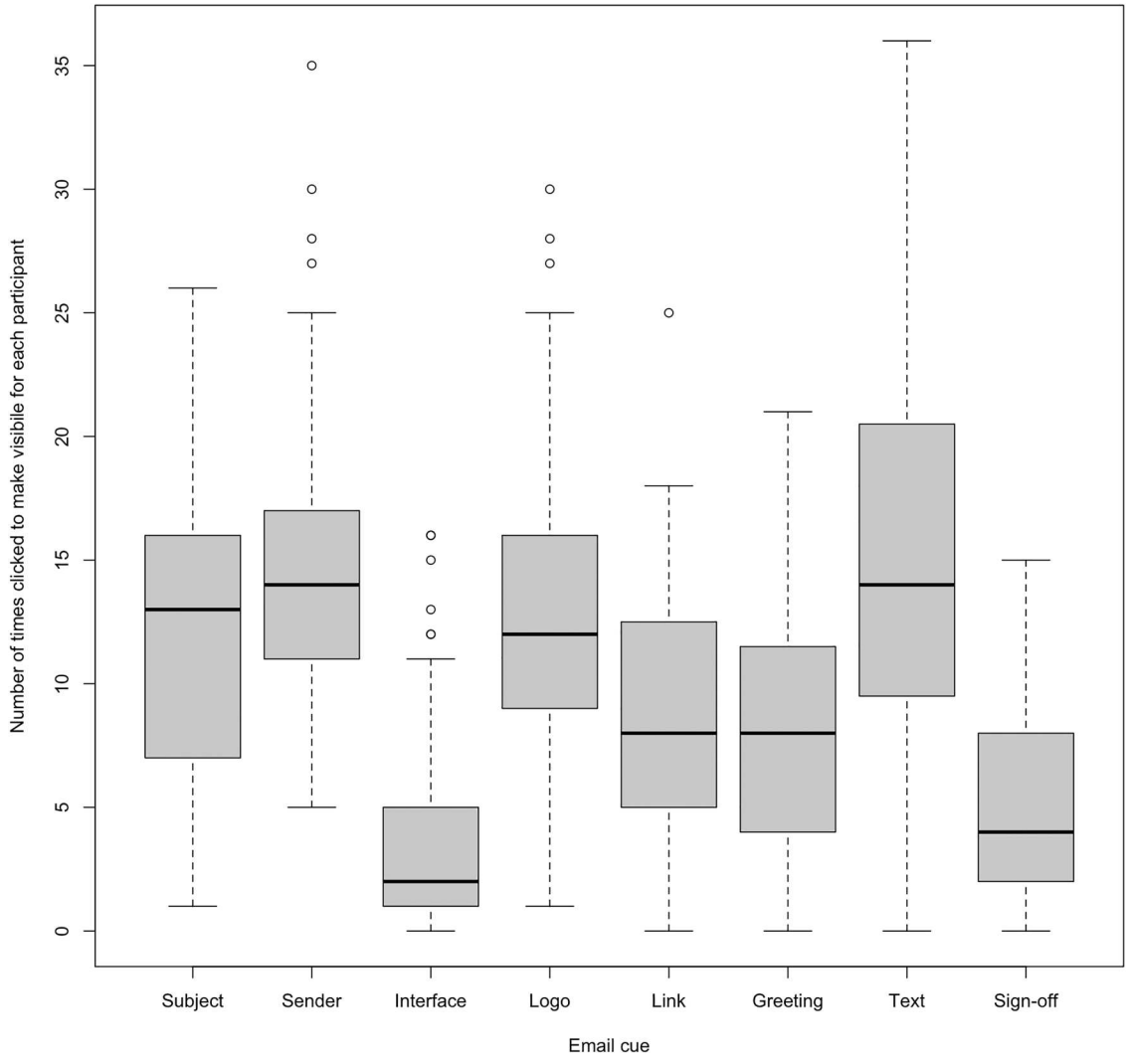

Figure 6. Cue examination tallies for each participant for all trials.

This hypothesis was supported in that for phishing emails higher intuitive scores were significantly associated with lower correct identification scores ($\beta = -0.02$, $p < .003$).

Hypothesis 2b stated that people with higher impulsivity scores would identify fewer phishing emails correctly than those with lower impulsivity scores. This hypothesis was not supported since BIS scores were not found to be a significant predictor for model 2 (phishing emails).

Hypothesis 2c stated that people with higher cyber security experience scores would correctly identify more phishing emails. This hypothesis was not supported since cyber security experience scores were not found to be a significant predictor for model 2 (phishing emails).

5.4.3. Behaviour

Hypothesis 3a stated that participants who spent longer on decisions (total trial response time) would be more likely to correctly identify phishing emails. This hypothesis was also not supported since response times were not found to be a significant predictor for model 2 (phishing emails).

We were also interested in whether there were differences more generally in response times between correct and incorrect responses. We therefore calculated the mean RT for all correct decisions and also incorrect decisions for each participant, this time for all trials (both phishing and legitimate) as seen in Figure 7. A t-test of this response set showed that correct decision RTs ($M = 18.24$s, $SD = 8.39$) were significantly shorter, $t(138.96) = -2.6$, $p = 0.01$, than the RTs for incorrect decisions ($M = 22.48$s, $SD = 12.15$).

Hypothesis 3b stated that participants who clicked on more cues would be more likely to correctly identify phishing emails. This hypothesis was not supported since the mean number of cues examined per trial for each participant was not found to be a predictive factor for model 2 (phishing emails).

Table 5. Regression models.

	Model 1 – Legitimate emails				Model 2 – Phishing emails			
Parameter	Estimate	Std error	*t*-value	*p*	Estimate	Std error	*t*-value	*p*
(Intercept)	1.13	0.165	6.851	**<.001*** **	1.062	0.077	13.846	**<.001*** **
Misc. behavioural								
Condition (load)	0.094	0.034	2.750	**.008****	−0.073	0.035	−2.049	**.044***
Mean number of cues examined								
Looked at sender's address at all score								
Looked at sender's address first score	0.003	0.006	0.510	.612				
Mean RT	−0.006	0.007	−0.858	.394				
Frequency of clicks on cues								
1 – Subject line								
2 – Sender's address	0.008	0.005	1.626	.108				
3 – Interface objects	0.019	0.011	1.716	.09.				
4 – Logo								
5 – Link								
6 – Greeting	0.014	0.006	2.087	**.04***				
7 – Text								
8 – Signoff	−0.044	0.012	−3.751	**<.001*** **				
Time spent looking at cues								
1 – Subject line								
2 – Sender's address								
3 – Interface objects	−0.108	0.1	−1.080	.284				
4 – Logo	−0.158	0.045	−3.502	**<.001*** **				
5 – Link								
6 – Greeting	−0.241	0.065	−3.720	**<.001*** **				
7 – Text								
8 – Signoff	0.164	0.045	3.654	**<.001*** **				
Individual differences								
Cyber security experience score	−0.015	0.008	−1.895	.062				
BIS impulsivity score	−0.001	0.006	−1.759	.083				
Hamilton's intuitive scale score					−0.015	0.005	−3.060	**.003****
Interaction terms								
Mean RT * Cyber security experience score	0.001	0.000	2.173	**.033***				
Model fit:								
Adjusted R^2	0.39				0.11			
p =	**<.001*** **				**.003****			

Notes: All variables tested for inclusion in the models are presented here. Only predictors included in the final models have statistics reported. *$p < .05$, **$p < .01$, ***$p < .001$.

Again, we were interested in whether this differed more generally between correct and incorrect responses. We therefore calculated the mean number of cues clicked on for correct decisions for each participant, and then for incorrect decisions, but for all trials (both phishing and legitimate) as seen in Figure 8. A t-test of these two sets of scores showed that the mean number of cues clicked on for correct decisions ($M = 5.74$, $SD = 2.37$) was significantly higher, $t(152.96) = -3.39$, $p < .001$, than for incorrect decisions ($M = 7.23$, $SD = 3.35$).

Hypothesis 4a stated that participants who spent more time looking at the sender's address would be more likely to correctly identify phishing emails. This hypothesis was not supported since participant's time spent looking at the sender's address cue was not found to be a significant predictor for model 2 (phishing emails).

Hypothesis 4b stated that participants who clicked more often on the sender's address would be more likely to correctly identify phishing emails. This hypothesis was not supported since participant's frequency of clicking on the sender's address cue was not found to be a significant predictor for model 2 (phishing emails).

Hypotheses 4c stated that participants who looked at the sender's address at all would be more likely to identify phishing emails correctly than those who did not. This hypothesis was not supported in our regression model since the 'Looked at sender's at all score' was not found to be a significant predictor for model 2 (phishing emails).

To examine this result more closely, we calculated a score for each participant, of how many phishing trials where they accessed the sender's address and answered correctly, as a proportion of all the phishing email trials where they accessed this cue. We calculated a similar proportion correct score for trials where they did not access the sender's address at all. A two-tailed, two-sample t-test showed that, for trials where participants examined the sender's address, the mean proportion of correct decisions ($M = .75$, $SD = .23$) was lower than those trials where they did not examine the sender's address ($M = .97$, $SD = .09$), $t(124.64) = -7.8759$, $p = < .001$.

We also tallied the number of trials, for each participant, where they accessed the sender's address, as well as the number of trials, by participant, where they did not access this cue. A two-tailed t-test showed that the

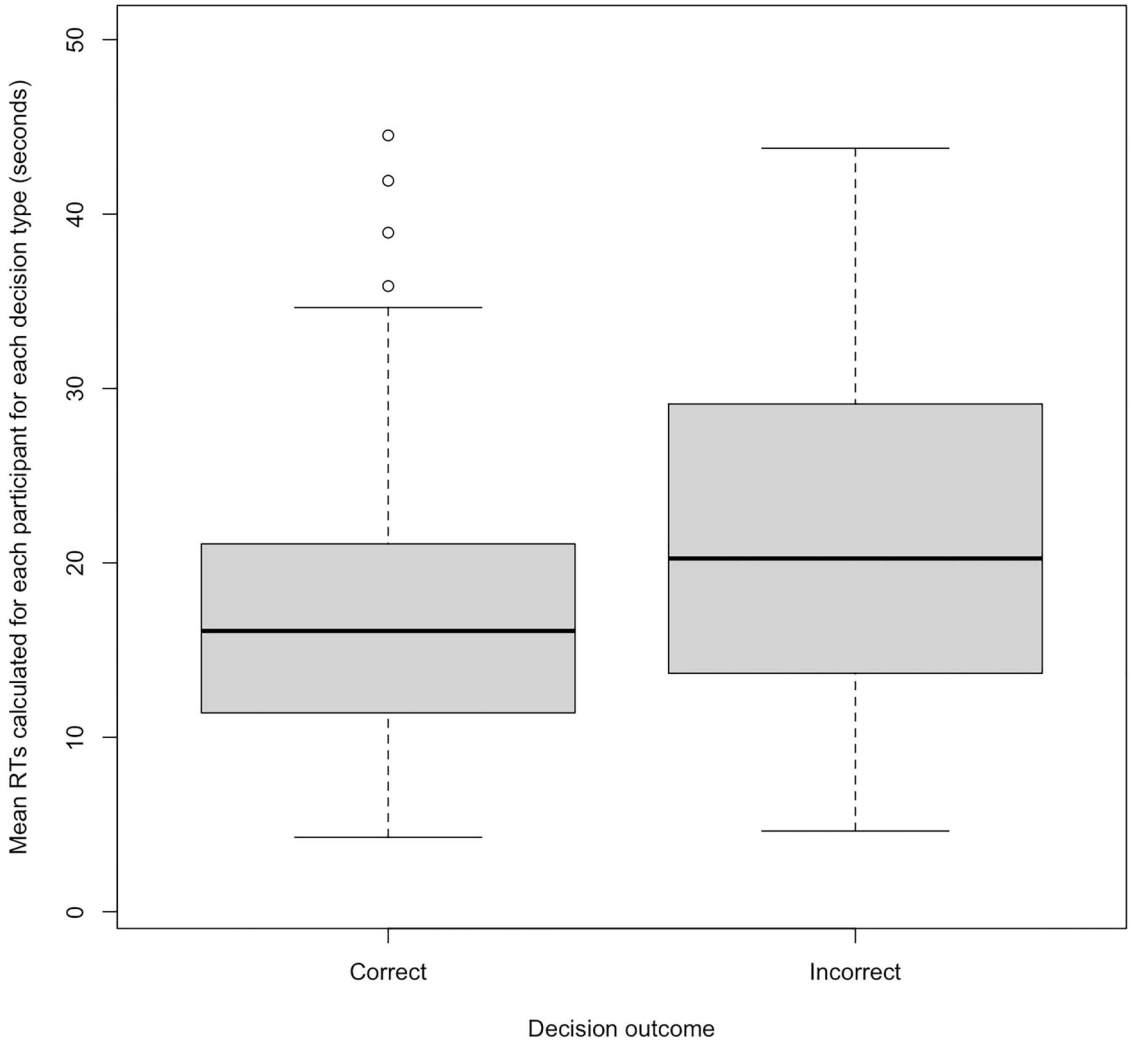

Figure 7. Mean (by participant) RTs for correct and incorrect decisions.

number of trials where participants accessed this cue (M = 4.68, SD = 1.46) was higher than the tally of trials where participants did not access it (M = 1.46, SD = 1.36), $t(171.44) = 15.129$, $p < .001$. See Figure 9 for a related plot of the relative proportions of correct and incorrect responses of all individual phishing trials where the participant did or did not examine the sender's address.

Hypotheses 4d stated that participants who looked at the sender's address first would be more likely to identify phishing emails correctly than those who did not. This hypothesis was not supported in our regression model since the 'looked at sender's first score' was not found to be a significant predictor for model 2 (phishing emails).

To examine this result more closely, we calculated a score for each participant, of how many phishing trials where they accessed the sender's address first and answered correctly, as a proportion of all the phishing email trials where they accessed this cue first. We calculated a similar proportion correct score for trials where they did not access the sender's address first. A two-tailed, two-sample t-test showed that, for trials where participants examined the sender's address first, the mean proportion of correct decisions (M = .65, SD = .04) was lower than those trials where they did not examine the sender's address (M = .87, SD = .02), $t(119.77) = -4.618$, $p = < .001$.

We also tallied the number of trials, for each participant, where they access the sender's address first, as well as the number of trials, by participant, where they did not access this cue first. A two-tailed t-test showed that the number of trials where participants accessed this cue first (M = 1.98, SD = 1.14) was higher than the tally of trials where participants did not access it (M = 4.16, SD = 1.71), $t(149.86) = -9.905$, $p < .001$. See Figure 10 for a related plot of the relative proportions of correct and incorrect phishing trials of all individual trials where the participants did or did not examine the sender's address first.

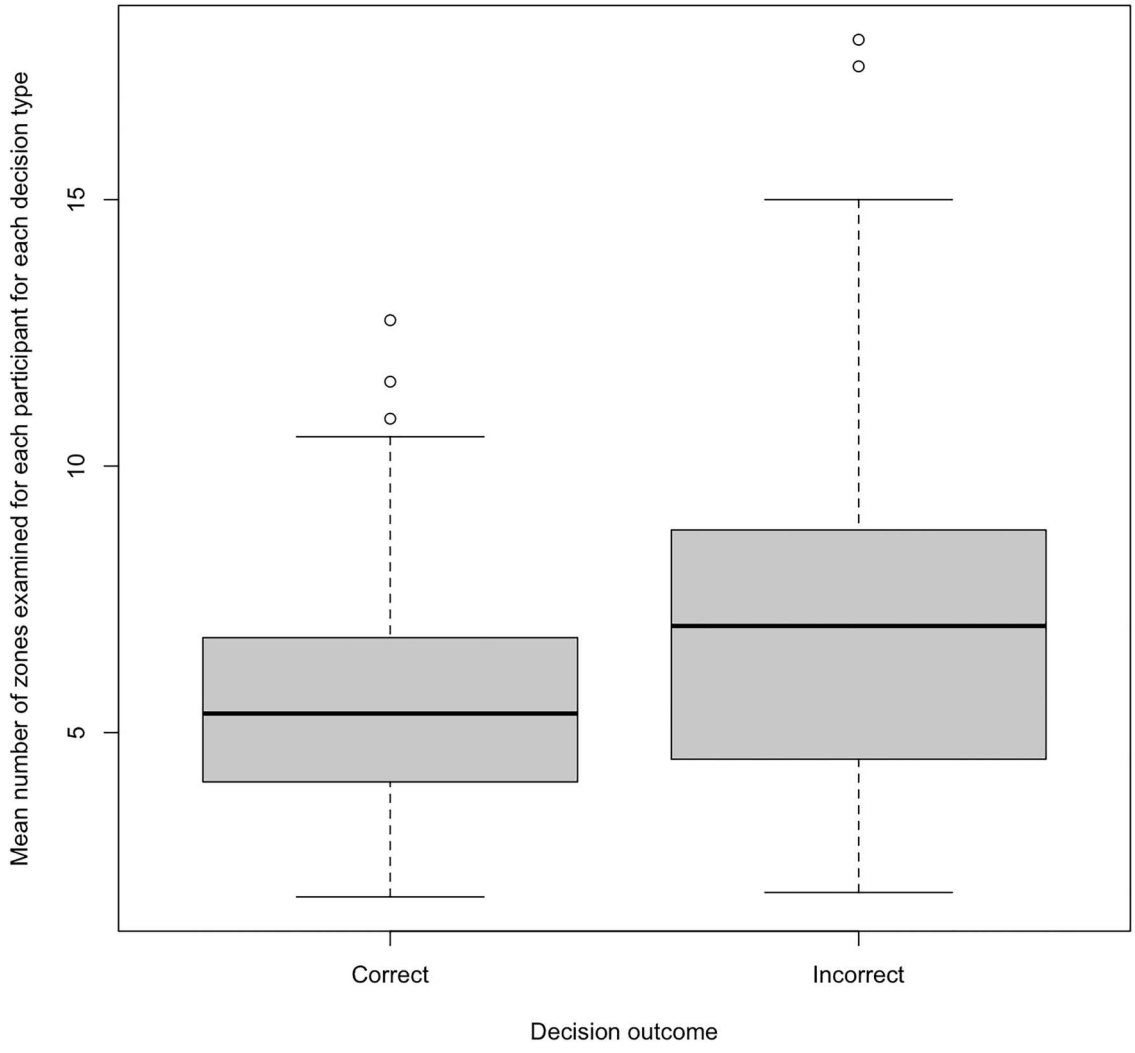

Figure 8. Mean (by participant) number of cues examined for correct and incorrect decisions.

6. Discussion

We sought to understand which cues, present in emails, people used in making judgements about email veracity. We also investigated if patterns of cue usage differed between individuals according to three measured individual differences, and we wanted to gauge the involvement of elaborative processing in this task. We did this via a novel method – that of an information board/process tracing study – where stimuli were originally presented to participant in a blurred-out state (but with each cue labelled) and participants could then click on one cue at a time to examine it. We then recorded which cues were examined and for how long up until participants made their final phishing / legitimate decision.

6.1. The role of elaborative thought and phishing as dual process problem

We sought to understand whether the task of identifying phishing emails is subject to dual process dynamics and specifically tested whether elaborative, System 2 thought was a protective factor in correctly identifying possible email threats. By doing so we formulated phishing emails as conflict problems within the dual process framework since attackers include cues that strongly trigger System 1 responses in the hope of hindering or overcoming System 2 processing, thereby setting these two systems in conflict. We found that under external cognitive load, and therefore with less access to elaborative processing, participants were worse at correctly identifying phishing emails, supporting our hypothesis and contributing evidence to the argument that phishing emails are conflict problems. Additionally, we found that participants under load were better at identifying legitimate emails. While we had hypothesised that load would have less effect on legitimate emails, the increased performance seen in this condition was surprising. However, there are some important clues from the literature that may go some way in explaining this result. Firstly Nasser et al. (2020) found that

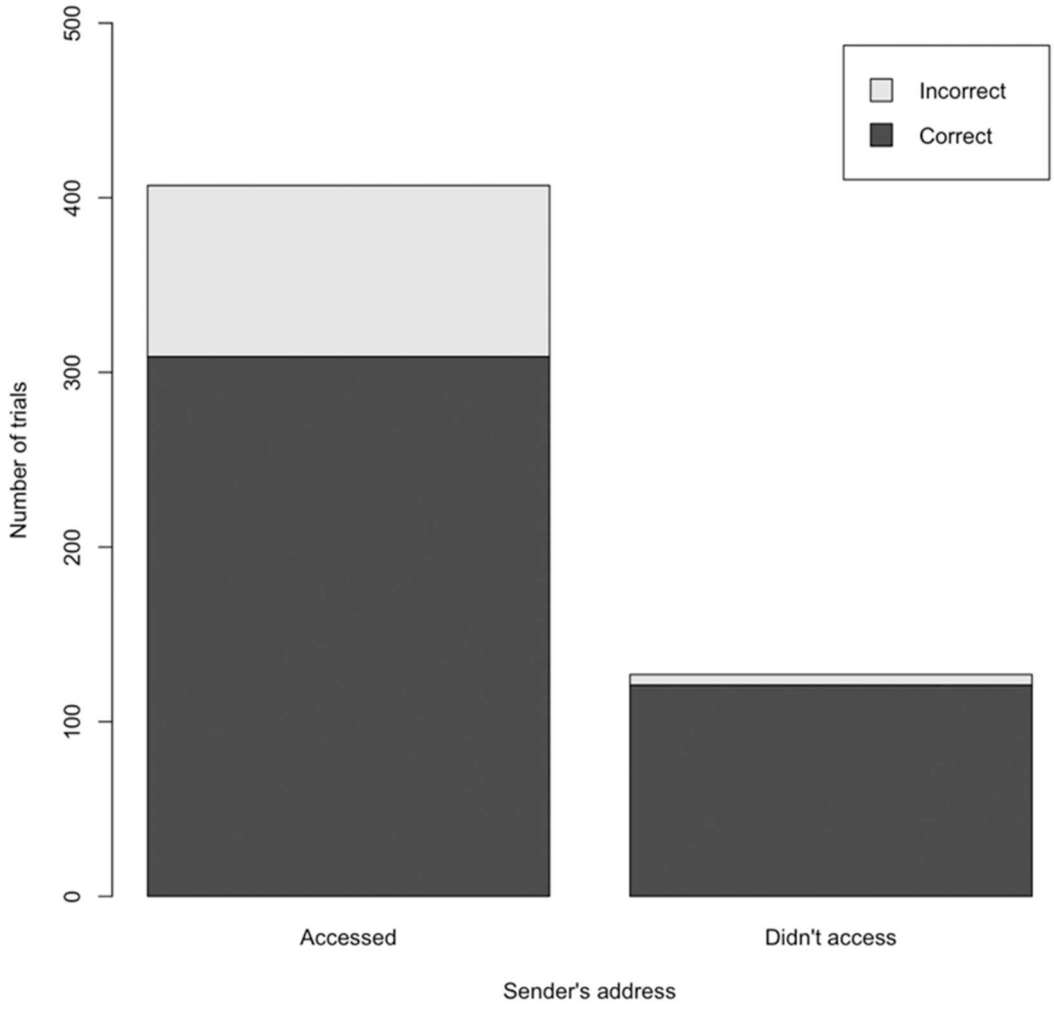

Figure 9. Total number of trials by whether the participant accessed the sender's address or not and decision outcome.

inducing external cognitive load had no effect on their primary phishing detection task. Furthermore, they noted a non-significant trend of improved performance on the primary task under higher levels of load. Bago and De Neys (2019) also found that participants were able to complete a logic problem (the bat and ball task) while carrying out a simultaneous visual matrix task.

In addition, some studies have also noted that additional task difficulty can actually facilitate mental processing in that participants meet increased task demands by devoting more mental capacities to the tasks – resulting in improved performance on the primary task (Hegarty, Shah, and Miyake 2000; Washburn and Putney 2001). Given the increased performance under load for legitimate emails, it is possible that this phenomenon is also present in our conflict task, and we could speculate that without this facilitating effect, our results for phishing emails would be stronger still. If this were the case, then this would provide more evidence of the importance of elaborative processing in correctly identifying phishing emails.

Encouragingly, industry at large seems to be on the verge of recognising the important role than elaborative thought plays in Phishing email identification – albeit in the form of the recent discussions around 'mindfulness'. Some researchers have begun to utilise this term to refer to increased mental processing in response to complicated or ambiguous mental situations, and the construct appears to closely resemble System 2 thought (Chou, Chen, and Lo 2021; Jari 2022; Thatcher et al. 2018). Numerous grey-literature sources and industry pundits are also now espousing this as an important factor in user training (Carpenter 2023; Collard 2023; Warner 2022), and hopefully, the cyber security industry and 'awareness' teams within organisations will subsequently begin to adapt their training and mitigation efforts to focus on this important new approach.

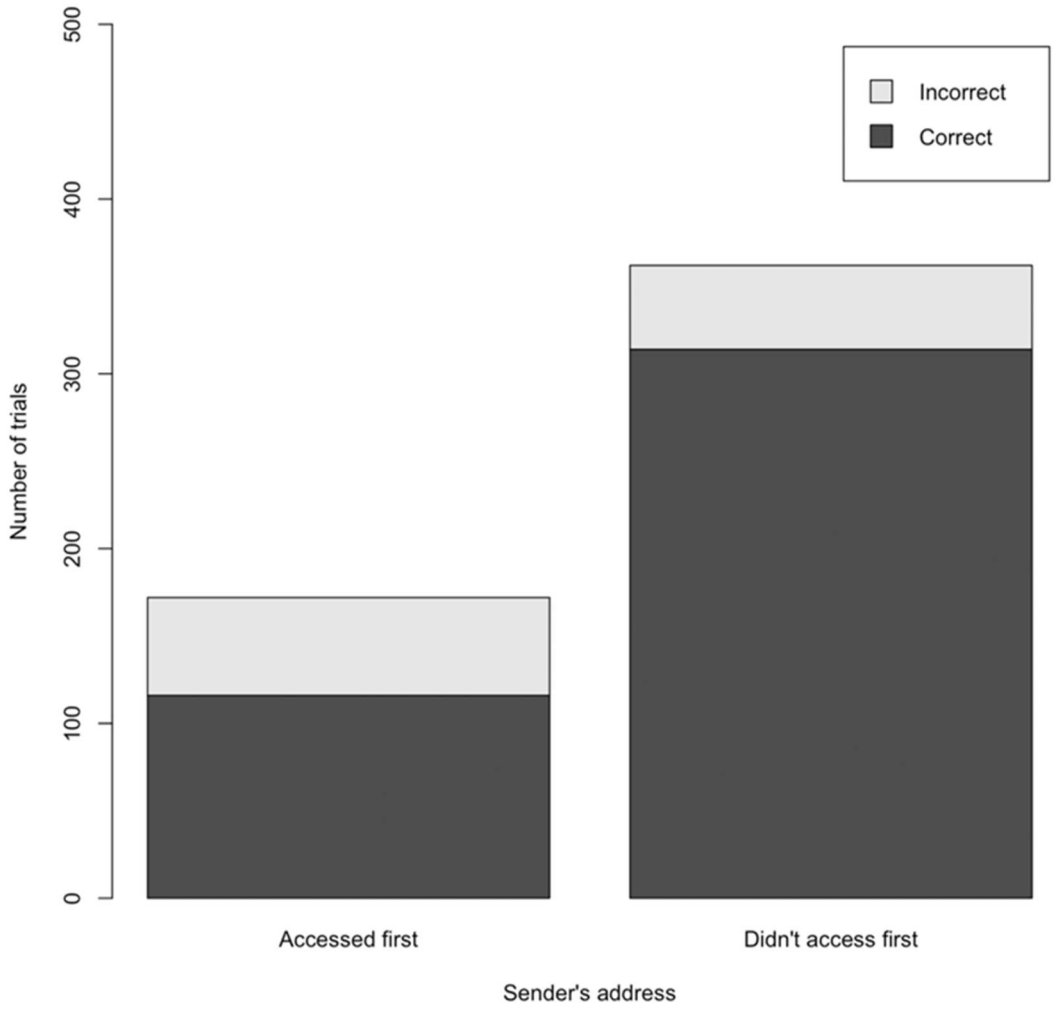

Figure 10. Total number of trials by whether the participant accessed the sender's address first or not and decision outcome.

6.2. Cue utilisation

We should note, before discussing patterns of behaviour for individual cues, that two unexpected factors complicated the conclusions we could draw from our analysis of cue utilisation.

(1) For results based on response times we originally expected to see (hypothesis 3a) that more time spent viewing a cue indicated more engagement with that cue and therefore would be associated with better decision-making for those cues with diagnostic qualities. However, we saw the opposite effect where longer response times were associated with more incorrect decisions (see section 5.4 Behaviour). This finding is in line with similar work from eyetracking (Pfeffel, Ulsamer, and Müller 2019; Zhuo et al. 2024). In our original thinking, we had not considered that people with better decision-making practices, or higher decision confidence, may require less time to glean important information from a cue than those with less efficient practices or lower confidence. Hence our time results need to be viewed within the lens of being modulated by expertise.

(2) For results based on the number of clicks on cues we again encountered a similar unexpected dynamic. We had expected (hypothesis 3b) the number of clicks on cues to be a proxy for interest and attention and more clicks on diagnostic cues (such as the sender's address) to be associated with better decisions. However, we found overall that people who clicked more often were more likely to make incorrect decisions (see section 5.4 Behaviour), suggesting again that expertise confounds what was expected to be a simple relationship. Presumably participants who were uncertain hoped to glean more information that might help them make their decision and clicked more often than those who were more confident in their

decisions. Again – this means that the discussion of results based on these measures must accommodate this phenomenon.

6.3. Time

Hypothesis 3a stated that participants who spent longer on decisions were more likely to correctly identify phishing emails. Similarly, this hypothesis was neither supported for phishing emails (predictor not significant therefore not included in model) nor for legitimate emails ($\beta = -0.006$, $p = .39$). As discussed above, this appears to be because participants who were more unsure took longer to make decisions. However, this observation is important in itself from a methodological standpoint since response time has occasionally been used in other experiments (Bayl-Smith, Sturman, and Wiggins 2020) as a proxy for elaborative processing. We suggest that this approach is therefore dubious, and likely to be contaminated by the relationship between expertise and response time.

This is borne out in McAlaney's (McAlaney and Hills 2020) study where they found that when emails contained 'phishing indicators' this did not increase response times – regardless of correct identification, and they suggested that subjects required little additional processing time to recognise these elements. Further evidence for this observation comes from Pfeffel, Ulsamer, and Müller (2019), who also observed that phishing detecting 'experts' were better at detecting phishing emails, but required less time for it. However, they also noted that for those who had less expertise, spending more time assessing emails increased their accuracy.

6.4. Cue utilisation – legitimate emails

Overall, our results for the behaviour that participants exhibited in identifying legitimate emails provided a number of findings that align well with and extend the current literature around phishing email detection.

6.4.1. Signoff

We found that participants who clicked to view email signoffs more often were less likely to make accurate assessments of email veracity. This finding should be evaluated in the context of our other observation that spending more time examining the signoff resulted in a significantly higher rate of correct decisions. It should also be noted that the error state specifically in this instance is a legitimate email being mis-categorised as a phishing email. We observed that the signoffs in our selection of emails were often quite lengthy and contained a lot of information about the sender, the purpose of the emails, and information about the information channel itself (such as unsubscribe options). We therefore consider this particular cue as highly diagnostic in relation to email legitimacy in that malicious emails will contain more leakage cues in this type of information. As such we interpret this finding to suggest that people are generally aware that this information is important and for those who make correct decisions, if they view the cue, they are able to quickly identify leakage cues present. However, for those who are uncertain, they are attempting to ascertain email veracity by multiple clicks – but seemingly do not have the information or relevant cue associations to be able to identify the leakage cues present. This observation has important implications for phishing mitigation programmes in that people should be directed to examine sign-offs closely as a cue with diagnostic value. However, our findings also suggest that when people are trying to evaluate this cue, they frequently do not know what to look for, which again suggests that education programmes need to better equip people better with knowledge around the leakage cues present in this email element.

6.4.2. Logos and greeting

We found that participants spending more time spent looking at the logo and the greeting were both associated with less correct identification of legitimate emails. However, we also found that clicking on the greeting cue more often was associated better identification. Again, it is important to note that the failure state in these cases is mistaking legitimate emails for phishing emails. If we assume that the finding of clicking more often on the cue is the result of uncertainty, as discussed above, then the other findings relating to time spent examining these cues can nonetheless be taken as a proxy for attention. Given this, these observations then tie in well with the existing literature and widely adopted theoretical frameworks.

Bullee et al. (2017) found that spear phishing emails with a personalised greeting were 1.7 times more likely to induce a response compared with emails with generic greetings and Marett and Wright (2009) showed that personalisation leads to increased victimisation. Blythe, Petrie, and Clark (2011) showed that emails with logos were more convincing than those without and R. T. Wright and Marett (2010) showed that emails with logos avoided arousing suspicion.

In short, across various theoretical frameworks, and backed up by a variety of evidence, we can assert that these particular cues contain little diagnostic information and are highly effective at triggering shallow, System 1 heuristic processing and are therefore cues

that people should pay attention to least when evaluating an email's veracity.

6.5. Cue utilisation – phishing emails

In contrast to our findings regarding cue utilisation for legitimate emails, when we ran our regression model with the proportion of phishing emails correctly identified as the dependent variable, we saw notably different results. The behavioural variables we attempted to include in the model included the number of clicks on each type of cue, the time spent looking at each type of cue, the overall trial response time as well as a score of whether people looked at the sender's address at all in each trial, or looked at the sender's address first in each trial. None of these were found to be a significant predictor of correct phishing email identification.

This suggests that there were effectively no behavioural correlates for correctly identifying phishing emails. This surprising result implies that while there are clear patterns of what people do, and are trained to do, to attempt to identify suspicious emails – and that these are effective for helping people make decisions about legitimate emails, these patterns are not the strategies used in the process of correctly identifying malicious emails.

In order to contextualise this finding, it may help to examine other work in the same area. While other authors have not explicitly sought out the relationship between decision-making and individual cues, we note that there have been instances of results pointing in the same direction as our findings, in particular within the growing body of work investigating the individual difference of cue utilisation as a predictor of phishing victimisation. Again, we note that McAlaney and Hills (2020), in an eye-tracking study, found no relationship between the time spent examining cues commonly implicated in phishing victimisation and ratings of email trustworthiness. They go on to say: 'the relationship between the presence of features related to phishing emails and how trustworthy that email is seen to be is more complex than expected'. Greene et al. (2018), after finding no differences in patterns of cue utilisation between people who did and did not click on phishing emails said: 'There seemed to be an accumulation of cues that contributed to their click/non-click decisions in each exercise'. Finally, Vishwanath (2022) suggested that the process was enormously complicated and that simple cue to outcome relationships were unlikely to be found and R. Williams et al. (2024) support this view saying we need 'a more wholistic, sociotechnical systems approach to cyber interventions'.

The findings presented here are therefore both novel and important in that they confirm a number of preliminary or indicative findings from a wide range of studies and have a number of implications from both theoretical and practical standpoints.

These findings suggest that the processing of conflict email stimuli in such a classification task (and possibly more broadly) happens on a more global rather than local level. This resembles a particular style of information processing that has been observed in many other domains. Navon (1977) first observed these differences in local vs global processing styles using geometric figures with a paper that included the phrase 'Forest Before Trees' in the title, this term then becoming associated with findings to do with the interaction between global and local processing in perception. Since then, (Beukeboom and Semin 2005, 2006) observed similar differences in recalling autobiographical events and Isbell (2004) observed similar global vs local processing differences in social judgements. But this is the first time, we believe, that such a processing style has been identified in phishing email identification. How this particular model of information processing, in particular top-down vs bottom up processing (Stokes and Matthen 2015), may be resolved with a dual process account remain an open question.

From a practical standpoint, and which has important ramifications for industry mitigation and training efforts, this suggests that education efforts are failing to equip people to utilise cues in a manner that decreases their chances at victimisation. Furthermore, considering the complexity mentioned above, it would suggest that there is no 'silver bullet' of cue-based email identification strategies that will consistently decrease victimisation.

6.6. Cue utilisation – sender's address

An important cue that we investigated was the sender's email address. We focussed specifically on this particular cue because it is regarded as highly diagnostic since it is likely to contain numerous leakage cues potentially revealing the deceptive nature of the sender. As a specific cue it is rated by experts (Nasser et al. 2020; Parsons et al. 2016) as highly important to attend to in an evaluation process and is central to many industry training programmes (Burita, Klaban, and Racil 2022; Liu et al. 2023).

Our hypotheses (4a, 4b) about spending more time examining and clicking more often on the sender's resulting in a higher rate of correct decisions were not supported, as discussed previously. Here, people who made incorrect decisions spent longer looking at, and clicked on the cue more often, than those who made correct decisions, presumably because of uncertainty about their decision.

Our regression model also suggested that looking at the sender's address had no effect on correct identification. However, when we also looked at this relationship in a different way we found that correct responses were lower for trials where participants clicked on this cue than where they did not. We also noted that, by participant, the mean number of trials where this cue was accessed (4.68 trials) was significantly higher than the mean number of trials where the cue was not accessed (1.46 trials). This implies that people appear to be aware this is an important cue – but are failing to be able to extract the necessary information from it to make good decisions. This is also borne out in our plot of cue examination tallies (see Figure 6) where this particular cue has the highest median number of clicks over 14 trials (14.7 clicks) and in our mean time participant plot (see Figure 5) where it has the second highest median viewing time (3.07s).

This finding runs counter to much prevailing theory that the sender's address contains many opportunities for leakage cues and that examining it should result in improved discrimination between legitimate and phishing emails. In fact, the sender's addresses included in our experiment contained many of the much-discussed leakage cues discussed in the literature – e.g.: letter substitutions (Burita, Klaban, and Racil 2022), unusual domain names (Jakobsson 2007) and domains that did not match the content of the email (Parsons et al. 2016). However, in some tangentially supportive evidence Zhuo et al. (2024) noted that, in an eye-tracking study, victimisation rates did not vary between participants who looked at the URL of a phishing site and those who did not. The presence of these leakage cues in an explicit email classification task and the fact that participants could not capitalise on them suggests that participants are failing to recognise these cues – even when they are present.

Since examining the sender's address is often heavily emphasised in cyber security training programmes, we suspected that those with expertise might look at this cue first in the making their decision (hypothesis 4d). However, when we looked at this variable in isolation, we again found the proportion of correct responses was lower for those who looked at the sender's address first. This finding also contradicts much accepted wisdom around the value of checking the sender's address in that even for participants who prioritised evaluation of this cue and looked at it first – there was no improvement in phishing email detection.

Altogether these findings are worrisome in that they suggest that education programmes are not sufficiently equipping people with the necessary knowledge to evaluate the most diagnostic cue present in phishing emails and further, that even when attempting to utilise this cue, people are not capable of recognising the leakage cues present.

6.7. Individual differences

6.7.1. Intuitive decision-making style

Since it has been noted that people vary in their tendency to rely more on System 1 or System 2 thought, we were interested in how this tendency, as an individual difference, impacted on phishing identification performance generally. We deployed the 'intuitive thinking' scale by Hamilton, Shih, and Mohammed (2016) to measure participant's tendency towards shallow, System 1 processing. This was the only individual difference we found to impact on correct identification scores, and only for phishing emails, where it was found that higher intuitive decision-making scores were associated with fewer correct judgements about phishing emails (hypothesis 2a).

This again underscores the importance of elaborative thought when attempting to identify the malicious intent of incoming emails. Furthermore, the fact that this variable was a significant predictor for phishing emails, but not legitimate emails is additional evidence for the conflict nature of phishing emails. This implies that legitimate emails are not 'conflict' stimuli in that in these cases both System 1 and System 2 are suggesting the same decision, and therefore a tendency to not devote System 2 processing to a problem will regardless result in the same decision.

6.7.2. Impulsivity

Previous work (Butavicius et al. 2016; Parsons et al. 2019) has suggested that people with higher levels of impulsivity are more likely to fall victim to phishing emails (hypothesis 2a). We found little evidence of this in our experiment where this score was only marginally associated with correct identification of legitimate emails – and not at all for phishing emails. This perhaps can be attributed to the fact that our experiment was effectively a lab experiment and therefore was, in some important ways, quite different to the processes that people go through when sorting their in-box and responding to emails 'in real life'. In our experiment, the concept of phishing emails is already cued and likely highly present in people's thoughts as they complete the task. Since this precept is unlikely to be as much cued and present in the minds of people as they process their inbox in a real-world scenario – perhaps this construct is more of a determinant in this context – and is implicated in responding to emails before a more elaborative evaluation of an email's veracity takes place.

6.7.3. Cyber security experience

We had hypothesised that participants with more cyber security experience would correctly identify more phishing emails than those with lower levels of experience (hypothesis 2c). However, our regression model showed that, for phishing emails, cyber security was not a significant predictor of task performance. The same regression model, when run with performance on identifying legitimate emails as the dependent variable, also failed to show experience as a significant coefficient and in fact showed a marginal negative trend in this regard. This is a surprising result. However, we must acknowledge that the instrument we developed to measure experience is novel and is therefore not a psychometrically validated tool.

The result presented here then, supported by other emerging evidence from the field, has far-reaching implications for 'awareness' efforts by industry. It would suggest that current user awareness pedagogies are either failing to impart the appropriate knowledge that help users make better decisions, or, that while this knowledge may be a necessary antecedent to identifying phishing emails, it is not enough to ensure consistently hygienic user behaviour.

7. Limitations and future work

As with most lab-based studies, and in particular those involving web recruitment, it is difficult to ascertain that our sample is truly representative of any given population. We acknowledge this and are cognisant of the fact that this might skew the results presented here in unpredictable ways. We therefore suggest that further work that deploys this paradigm should involve larger sample sizes, and also focus more on individual populations (such as the elderly, or by geographic location), and potentially with a more controlled sample of trained vs untrained users.

We also acknowledge that a regression model such as the one used here can reveal overall patterns in data, but may not be particularly sensitive to a high level of individual variance. As such we suggest that further research using analysis methods of this or similar data that focusses on individual differences in response to this paradigm might be highly revealing. We must also acknowledge that the r^2 for our regression model for phishing emails is not particularly large (.11), but this again supports our argument that there do not appear to be reliable, simple cue to outcome relationships for people evaluating phishing emails.

We used duration of cue visibility as a key independent variable in our analysis. We acknowledge that this is only a proxy for attention and there is no way of knowing that participants paid close attention to each cue the entire time it was visible. We can however, say that participants did not examine the cues for longer than the period captured. Our results confirming prior literature such as the stimuli examined in legitimate emails and their corresponding effect on task performance, help us to believe – while all proxies for attention are imperfect – this method is of value. Future experiments may also benefit from excluding the cue labels from the stimuli in order to avoid the possibility of participant being prompted to examine cues that they may not have without the presence of such labels.

This experiment pertains to and can aid in our understanding of a particular subset of the overall problem of phishing victimisation, namely those who have recognised that an email might be a phishing email and are trying to decide if valid or not. It is possible that it would have little bearing on those people who are not initially suspicious in some way. This is a common problem with lab-based phishing studies, and while we maintain that these approaches are a useful and important lens of enquiry – it should be acknowledged that studies with a higher level of ecological validity are also important. Further work in this direction might therefore attempt to capture these dynamics in more 'real-life' situations – where participants are dealing with their email inboxes during the course of their normal lives – although the technical and logistic challenges of mounting this an experimental paradigm in such a context are considerable.

Overall though, this finding suggests confirmation by further study. We suggest that the replication of this experimental design and variants thereof will cast more light on this result. We also suggest that the information board format presented is likely to be useful for a range of investigations – including individual differences in cue utilisation. Eye-tracking studies also hold promise as worthwhile methods to confirm these results.

8. Conclusions

A number of recent studies in the field of cue utilisation have pointed towards the idea that there are no particular patterns of individual cues used in phishing email detection. This work shows that these initial intimations were, in fact, correct. Decision-making about phishing emails cannot be characterised as a mechanistic relationship between examining individual cues and making better decisions – but rather this process is more likely to involve a complicated integration of a host of informational sources present in an email. Since there are no behavioural correlates of correctly

identifying phishing emails, it would appear that this decision-making takes place at a higher level than previously imagined. One possible explanation for this this finding is that people are making their decisions based on some form of global processing of cues or via an emergent 'gestalt' based on the entirety of information present in the email – presumably also including their context and individual knowledge about the world.

Although the results presented here are novel, we are encouraged to believe their veracity since (1) they reflect a number of other preliminary findings pointing in the same direction (2) the same method applied to legitimate emails showed a number of phenomena noted in other literature, overall suggesting that the experimental paradigm is itself sound.

This suggests that there is no 'silver bullet' as to what behaviour leads to either victimisation or escape from it. No matter how much logging of behaviour that institutions do – they are unlikely to find guaranteed predictors of victimisation, in the form of a 'cue-present to outcome' relationship. This has important implications for industry training efforts. While most current training is focussed on providing information about individual cues present that may be evaluated for leakage of malicious intent, the apparent holistic processing of such stimuli suggests additional approaches. In this case, it would appear necessary to encourage a wider, and deeper engagement of the problem space, effectively increasing users' meta-cognition about their own thought processes. Future training efforts then may begin to emphasise sensitivity to overall impressions of emails such as 'feeling off' as an important criterion for decision-making. While a rigorous and pedagogically sound educational campaign is beyond the scope of this work, we hope to see both confirming evidence of these findings in the future and then educational campaigns adapt these insights into their approaches.

On the other hand, we have provided more evidence here in support of the argument that elaborative processing aids in phishing email identification. This suggests that the current move towards user mitigation approaches based on 'mindfulness' is likely to decrease victimisation. We would therefore encourage awareness teams and others involved in protecting people and systems to emphasise this approach in their training.

We therefore suggest that this is an important factor in why existing education campaigns may be reaching the point of diminishing returns. Information and education are important but not enough. What the final aspects are remains an open question – but elaborative processing and a tendency towards it is clearly an important factor – and indicators point towards other higher level, non-specific-cue-based processing abilities.

Author contributions

CRediT: **Anna Hepworth:** Methodology.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by Australian Government.

ORCID

Daniel Conway http://orcid.org/0009-0007-9963-9611
Kun Yu http://orcid.org/0000-0001-5138-6749
Marcus Butavicius http://orcid.org/0000-0003-0722-3912
Fang Chen http://orcid.org/0000-0003-4971-8729

References

Ackerley, M., B. W. Morrison, K. Ingrey, M. W. Wiggins, P. Bayl-Smith, and N. M. V. Morrison. 2022. "Errors, Irregularities, and Misdirection: Cue Utilisation and Cognitive Reflection in the Diagnosis of Phishing Emails." *Australasian Journal of Information Systems* 26. https://doi.org/10.3127/AJIS.V26I0.3615.

Akbar, N. 2014. "Analysing Persuasion Principles in Phishing Emails." Master thesis, University of Twente. http://essay.utwente.nl/66177/.

Bago, B., and W. De Neys. 2017. "Fast Logic?: Examining the Time Course Assumption of Dual Process Theory." *Cognition* 158:90–109. https://doi.org/10.1016/j.cognition.2016.10.014.

Bago, B., and W. De Neys. 2019. "The Smart System 1: Evidence for the Intuitive Nature of Correct Responding on the Bat-and-Ball Problem." *Thinking & Reasoning* 25 (3): 257–299. https://doi.org/10.1080/13546783.2018.1507949.

Bayl-Smith, P., D. Sturman, and M. Wiggins. 2020. "Cue Utilization, Phishing Feature and Phishing Email Detection." In *Financial Cryptography and Data Security*, edited by M. Bernhard, A. Bracciali, L. J. Camp, S. Matsuo, A. Maurushat, P. B. Rønne, and M. Sala, 56–70. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-54455-3_5.

Beukeboom, C. J., and G. R. Semin. 2005. "Mood and Representations of Behaviour: The How and Why." *Cognition and Emotion* 19 (8): 1242–1251. https://doi.org/10.1080/02699930500203369.

Beukeboom, C. J., and G. R. Semin. 2006. "How Mood Turns on Language." *Journal of Experimental Social Psychology* 42 (5): 553–566. https://doi.org/10.1016/j.jesp.2005.09.005.

Blythe, M., H. Petrie, and J. Clark. 2011. "F for Fake: Four Studies on How We Fall for Phish." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 3469–

3478. Vancouver: Association for Computing Machinery. https://doi.org/10.1145/1978942.1979459.

Bullee, J.-W., L. Montoya, M. Junger, and P. Hartel. 2017. "Spear Phishing in Organisations Explained." *Information & Computer Security* 25 (5): 593–613. https://doi.org/10.1108/ICS-03-2017-0009.

Burita, L., I. Klaban, and T. Racil. 2022. "Education and Training against Threat of Phishing Emails." *International Conference on Cyber Warfare and Security* 17 (1): Article 1. https://doi.org/10.34190/iccws.17.1.28.

Butavicius, M., K. Parsons, M. Pattinson, and A. McCormac. 2016. "Breaching the Human Firewall: Social Engineering in Phishing and Spear-Phishing Emails." *arXiv:1606.00887 [Cs]*. http://arxiv.org/abs/1606.00887.

Canfield, C. I., B. Fischhoff, and A. Davis. 2016. "Quantifying Phishing Susceptibility for Detection and Behavior Decisions." *Human Factors* 58 (8): 1158–1172. https://doi.org/10.1177/0018720816665025.

Carpenter, Perry. 2023. *Cyber Mindfulness: How to Face Cyber Risks and Human Error*. https://www.forbes.com/sites/forbesbusinesscouncil/2023/06/26/cyber-mindfulness-How-to-face-cyber-risks-and-human-error/.

Chaiken, S. 1980. "Heuristic versus Systematic Information Processing and the Use of Source versus Message Cues in Persuasion." *Journal of Personality and Social Psychology* 39 (5): 752–766. https://doi.org/10.1037/0022-3514.39.5.752.

Chou, F. K.-Y., A. P.-S. Chen, and V. C.-L. Lo. 2021. "Mindless Response or Mindful Interpretation: Examining the Effect of Message Influence on Phishing Susceptibility." *Sustainability* 13 (4): Article 4. https://doi.org/10.3390/su13041651.

Cialdini, R. B. 1993. *The Psychology of Persuasion*. New York: HaperCollins.

Collard, A. 2023. "Mindfulness in Cybersecurity Culture." AnnaCollard, February 20. https://www.annacollard.com/post/mindfulness-in-cybersecurity-culture.

Conway, D., M. Butavicius, K. Yu, and F. Chen. 2023. "Are People with Cyber Security Training Worse at Checking Phishing Email Addresses? Testing the Automaticity of Verifying the Sender's Address." In *Human Aspects of Information Security and Assurance*, edited by S. Furnell and N. Clarke, 310–323. Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-38530-8_25.

De Neys, W. 2006. "Automatic–Heuristic and Executive–Analytic Processing during Reasoning: Chronometric and Dual-Task Considerations." *Quarterly Journal of Experimental Psychology* 59 (6): 1070–1100. https://doi.org/10.1080/02724980543000123.

De Neys, W., S. Cromheeke, and M. Osman. 2011. "Biased but in Doubt: Conflict and Decision Confidence." *PLoS One* 6 (1): e15954. https://doi.org/10.1371/journal.pone.0015954.

Ekman, P., and W. V. Friesen. 1969. "Nonverbal Leakage and Clues to Deception." *Psychiatry: Journal for the Study of Interpersonal Processes* 32 (1): 88–106. https://doi.org/10.1080/00332747.1969.11023575.

Evans, J. St. B. T., and K. E. Stanovich. 2013. "Dual-Process Theories of Higher Cognition: Advancing the Debate." *Perspectives on Psychological Science* 8 (3): 223–241. https://doi.org/10.1177/1745691612460685.

Ferreira, A., L. Coventry, and G. Lenzini. 2015. "Principles of Persuasion in Social Engineering and Their Use in Phishing." In *Human Aspects of Information Security, Privacy, and Trust*, edited by T. Tryfonas and I. Askoxylakis, 36–47. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-20376-8_4.

Greene, K., M. Steves, M. Theofanos, and J. Kostick. 2018. "User Context: An Explanatory Variable in Phishing Susceptibility." Workshop on Usable Security (USEC) 2018; February 18–21; San Diego, CA. https://csrc.nist.gov/Pubs/conference/2018/02/18/user-context-an-explanatory-variable-in-phishing-s/Final.

Hamilton, K., S.-I. Shih, and S. Mohammed. 2016. "The Development and Validation of the Rational and Intuitive Decision Styles Scale." *Journal of Personality Assessment* 98 (5): 523–535. https://doi.org/10.1080/00223891.2015.1132426.

Harrison, B., A. Vishwanath, and R. Rao. 2016. "A User-Centered Approach to Phishing Susceptibility: The Role of a Suspicious Personality in Protecting against Phishing." In *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, 5628–5634. https://doi.org/10.1109/HICSS.2016.696.

Harte, J. M., and P. Koele. 2002. "Psychometric and Methodological Aspects of Process Tracing Research." In *Decision Making*, edited by R. Crozier, R. Ranyard, and O. Svenson, 35–48. Routledge.

Hegarty, M., P. Shah, and A. Miyake. 2000. "Constraints on Using the Dual-Task Methodology to Specify the Degree of Central Executive Involvement in Cognitive Tasks." *Memory & Cognition* 28 (3): 376–385. https://doi.org/10.3758/BF03198553.

Isbell, L. M. 2004. "Not All Happy People Are Lazy or Stupid: Evidence of Systematic Processing in Happy Moods." *Journal of Experimental Social Psychology* 40 (3): 341–349. https://doi.org/10.1016/j.jesp.2003.06.003.

Jakobsson, M. 2007. "The Human Factor in Phishing." *Privacy & Security of Consumer Information* 7 (1): 1–19.

Jari, M. 2022. "An Overview of Phishing Victimization: Human Factors, Training and the Role of Emotions." arXiv.Org. https://doi.org/10.5121/csit.2022.121319.

Jeong, J., J. Mihelcic, G. Oliver, and C. Rudolph. 2019. "Towards an Improved Understanding of Human Factors in Cybersecurity." In *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, Los Angeles, CA, 338–345. https://doi.org/10.1109/CIC48465.2019.00047.

Johnson, E. D., E. Tubau, and W. De Neys. 2014. "The Unbearable Burden of Executive Load on Cognitive Reflection: A Validation of Dual Process Theory." *Proceedings of the Annual Meeting of the Cognitive Science Society* 36 (36): 2441–2446. https://escholarship.org/uc/item/01x9w1hw.

Jones, H. S., J. N. Towse, and N. Race. 2015. "Susceptibility to Email Fraud: A Review of Psychological Perspectives, Data-Collection Methods, and Ethical Considerations." *International Journal of Cyber Behavior, Psychology and Learning (IJCBPL)* 5 (3): 13–29. https://doi.org/10.4018/IJCBPL.2015070102.

Kahneman, D. 2011. *Thinking, Fast and Slow*, 499. Farrar, Straus and Giroux.

Karakasiliotis, A., S. Furnell, and M. Papadaki. 2006. "Assessing End-User Awareness of Social Engineering and Phishing." In *Australian Information Warfare and*

Security Conference, Perth, Western Australia. https://doi.org/10.4225/75/57a80e47aa0cb.

Kim, D., and J. Kim. 2013. "Understanding Persuasive Elements in Phishing e-Mails a Categorical Content and Semantic Network Analysis." *Online Information Review* 37 (6): 835–850. https://doi.org/10.1108/OIR-03-2012-0037.

Lawson, P., C. J. Pearson, A. Crowson, and C. B. Mayhorn. 2020. "Email Phishing and Signal Detection: How Persuasion Principles and Personality Influence Response Patterns and Accuracy." *Applied Ergonomics* 86:103084. https://doi.org/10.1016/j.apergo.2020.103084.

Liu, E., L. Sun, A. Bellon, G. Ho, G. M. Voelker, S. Savage, and I. N. S. Munyaka. 2023. *Understanding the Viability of Gmail's Origin Indicator for Identifying the Sender*, 77–95. https://www.usenix.org/conference/soups2023/presentation/liu.

Marett, K., and R. Wright. 2009. "The Effectiveness of Deceptive Tactics in Phishing." *AMCIS 2009 Proceedings*. https://aisel.aisnet.org/amcis2009/340.

McAlaney, J., and P. J. Hills. 2020. "Understanding Phishing Email Processing and Perceived Trustworthiness through Eye Tracking." *Frontiers in Psychology* 11. https://doi.org/10.3389/fpsyg.2020.01756.

Miyake, A., N. P. Friedman, D. A. Rettinger, P. Shah, and M. Hegarty. 2001. "How Are Visuospatial Working Memory, Executive Functioning, and Spatial Abilities Related? A Latent-Variable Analysis." *Journal of Experimental Psychology: General* 130 (4): 621–640. https://doi.org/10.1037/0096-3445.130.4.621.

Montañez, R., E. Golob, and S. Xu. 2020. "Human Cognition through the Lens of Social Engineering Cyberattacks." *Frontiers in Psychology* 11. https://doi.org/10.3389/fpsyg.2020.01755.

Musuva, P. M. W., K. W. Getao, and C. K. Chepken. 2019. "A New Approach to Modelling the Effects of Cognitive Processing and Threat Detection on Phishing Susceptibility." *Computers in Human Behavior* 94:154–175. https://doi.org/10.1016/j.chb.2018.12.036.

Nasser, G., B. W. Morrison, P. Bayl-Smith, R. Taib, M. Gayed, and M. W. Wiggins. 2020. "The Role of Cue Utilization and Cognitive Load in the Recognition of Phishing Emails." *Frontiers in Big Data* 3: 37–55. https://doi.org/10.3389/fdata.2020.546860.

Navon, D. 1977. "Forest before Trees: The Precedence of Global Features in Visual Perception." *Cognitive Psychology* 9 (3): 353–383. https://doi.org/10.1016/0010-0285(77)90012-3.

Neupane, A. 2015. "A Multi-modal Neuro-Physiological Study of Phishing Detection and Malware Warnings." In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 479–491. Denver, CO: Association for Computing Machinery. https://doi.org/10.1145/2810103.2813660.

Oliveira, D., H. Rocha, H. Yang, D. Ellis, S. Dommaraju, M. Muradoglu, D. Weir, A. Soliman, T. Lin, and N. Ebner. 2017. "Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing." In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 6412–6424. Denver, CO: Association for Computing Machinery. https://doi.org/10.1145/3025453.3025831.

Osman, M. 2013. "A Case Study: Dual-Process Theories of Higher Cognition – Commentary on Evans & Stanovich (2013)." *Perspectives on Psychological Science* 8 (3): 248–252. https://doi.org/10.1177/1745691613483475.

Parsons, K., M. Butavicius, P. Delfabbro, and M. Lillie. 2019. "Predicting Susceptibility to Social Influence in Phishing Emails." *International Journal of Human-Computer Studies* 128:17–26. https://doi.org/10.1016/j.ijhcs.2019.02.007.

Parsons, K., M. Butavicius, M. Pattinson, D. Calic, A. Mccormac, and C. Jerram. 2016. "Do Users Focus on the Correct Cues to Differentiate Between Phishing and Genuine Emails?" (arXiv:1605.04717). arXiv. https://doi.org/10.48550/arXiv.1605.04717.

Payne, J. W. 1976. "Task Complexity and Contingent Processing in Decision Making: An Information Search and Protocol Analysis." *Organizational Behavior and Human Performance* 16 (2): 366–387. https://doi.org/10.1016/0030-5073(76)90022-2.

Peirce, J., J. R. Gray, S. Simpson, M. MacAskill, R. Höchenberger, H. Sogo, E. Kastman, and J. K. Lindeløv. 2019. "PsychoPy2: Experiments in Behavior Made Easy." *Behavior Research Methods* 51 (1): 195–203. https://doi.org/10.3758/s13428-018-01193-y.

Pfeffel, K., P. Ulsamer, and N. H. Müller. 2019. "Where the User Does Look When Reading Phishing Mails – an Eye-Tracking Study." In *Learning and Collaboration Technologies. Designing Learning Experiences*, edited by P. Zaphiris and A. Ioannou, 277–287. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-21814-0_21.

Purcell, Z. A., C. A. Wastell, and N. Sweller. 2021. "Domain-Specific Experience and Dual-Process Thinking." *Thinking & Reasoning* 27 (2): 239–267. https://doi.org/10.1080/13546783.2020.1793813.

Ratcliff, R. 1993. "Methods for Dealing with Reaction Time Outliers." *Psychological Bulletin* 114 (3): 510–532. https://doi.org/10.1037/0033-2909.114.3.510.

Schulte-Mecklenbeck, M., J. G. Johnson, U. Böckenholt, D. G. Goldstein, J. E. Russo, N. J. Sullivan, and M. C. Willemsen. 2017. "Process-Tracing Methods in Decision Making: On Growing up in the 70s." *Current Directions in Psychological Science* 26 (5): 442–450. https://doi.org/10.1177/0963721417708229.

Shan, T. L., G. N. Samy, B. Shanmugam, S. Azam, K. C. Yeo, and K. Kannoorpatti. 2016. "Heuristic Systematic Model Based Guidelines for Phishing Victims." In *2016 IEEE Annual India Conference (INDICON)*, 1–6, Bangalore. https://doi.org/10.1109/INDICON.2016.7839123.

Stanovich, K. E. 2018. "Miserliness in Human Cognition: The Interaction of Detection, Override and Mindware." *Thinking & Reasoning* 24 (4): 423–444. https://doi.org/10.1080/13546783.2018.1459314.

Steinberg, L., C. Sharp, M. S. Stanford, and A. T. Tharp. 2013. "New Tricks for an Old Measure: The Development of the Barratt Impulsiveness Scale–Brief (BIS-Brief)." *Psychological Assessment* 25 (1): 216–226. https://doi.org/10.1037/a0030550.

Stephanou, A. 2008. "The Impact of Information Security Awareness Training on Information Security Behaviour."

Stevens, J. P. 1984. "Outliers and Influential Data Points in Regression Analysis." *Psychological Bulletin* 95 (2): 334–344. https://doi.org/10.1037/0033-2909.95.2.334.

Stokes, D., and M. Matthen. 2015. *Perception and Its Modalities*. Oxford University Press.

Sturman, D., C. Valenzuela, O. Plate, T. Tanvir, J. C. Auton, P. Bayl-Smith, and M. W. Wiggins. 2023. "The Role of Cue Utilization in the Detection of Phishing Emails." *Applied Ergonomics* 106:103887. https://doi.org/10.1016/j.apergo.2022.103887.

Svenson, O. 1979. "Process Descriptions of Decision Making." *Organizational Behavior and Human Performance* 23 (1): 86–112. https://doi.org/10.1016/0030-5073(79)90048-5.

Thatcher, J. B., R. T. Wright, H. Sun, T. J. Zagenczyk, and R. Klein. 2018. "Mindfulness in Information Technology Use: Definitions, Distinctions, and a New Measure." *MIS Quarterly* 42 (3): 831–848. https://doi.org/10.25300/MISQ/2018/11881.

Valenzuela, C. 2021. "The Individual Differences in Cue Utilisation, Decision Making, and Time Pressure on Phishing Susceptibility." Thesis. https://digital.library.adelaide.edu.au/dspace/handle/2440/133959.

Vishwanath, A. 2015. "Examining the Distinct Antecedents of E-Mail Habits and Its Influence on the Outcomes of a Phishing Attack." *Journal of Computer-Mediated Communication* 20 (5): 570–584. https://doi.org/10.1111/jcc4.12126.

Vishwanath, A. 2022. *The Weakest Link: How to Diagnose, Detect, and Defend Users from Phishing*. The MIT Press.

Vishwanath, A., T. Herath, R. Chen, J. Wang, and H. R. Rao. 2011. "Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model." *Decision Support Systems* 51 (3): 576–586. https://doi.org/10.1016/j.dss.2011.03.002.

Wang, J., T. Herath, R. Chen, A. Vishwanath, and H. R. Rao. 2012. "Research Article Phishing Susceptibility: An Investigation into the Processing of a Targeted Spear Phishing Email." *IEEE Transactions on Professional Communication* 55 (4): 345–362. https://doi.org/10.1109/TPC.2012.2208392.

Warner, L. 2022. "3 Mindfulness Techniques Your Team Can Use to Prevent Phishing." *AMP Creative*, February 25. https://ampcreative.com/the-human-firewall-3-mindfulness-techniques-Your-team-Can-use-to-prevent-phishing/.

Washburn, D. A., and R. T. Putney. 2001. "Attention and Task Difficulty: When Is Performance Facilitated?" *Learning and Motivation* 32 (1): 36–47. https://doi.org/10.1006/lmot.2000.1065.

Wason, P. C., and J. S. B. Evans. 1974. "Dual Processes in Reasoning?" *Cognition* 3 (2): 141–154. https://doi.org/10.1016/0010-0277(74)90017-1.

Whitney, P., C. A. Rinehart, and J. M. Hinson. 2008. "Framing Effects under Cognitive Load: The Role of Working Memory in Risky Decisions." *Psychonomic Bulletin & Review* 15 (6): 1179–1184. https://doi.org/10.3758/PBR.15.6.1179.

Williams, R., B. W. Morrison, M. W. Wiggins, and P. Bayl-Smith. 2024. "The Role of Conscientiousness and Cue Utilisation in the Detection of Phishing Emails in Controlled and Naturalistic Settings." *Behaviour & Information Technology* 43 (9): 1842–1858. https://doi.org/10.1080/0144929X.2023.2230307.

Williams, E. J., and D. Polage. 2019. "How Persuasive Is Phishing Email? The Role of Authentic Design, Influence and Current Events in Email Judgements." *Behaviour & Information Technology* 38 (2): 184–197. https://doi.org/10.1080/0144929X.2018.1519599.

Wogalter, M. S., and C. B. Mayhorn. 2008. "Trusting the Internet: Cues Affecting Perceived Credibility." *International Journal of Technology and Human Interaction (IJTHI)* 4 (1): 75–93. https://doi.org/10.4018/jthi.2008010105.

Wright, R., S. Johnson, and B. Kitchens. 2023. "Phishing Susceptibility in Context: A Multilevel Information Processing Perspective on Deception Detection." *Management Information Systems Quarterly* 47 (2): 803–832. https://doi.org/10.25300/MISQ/2022/16625.

Wright, R. T., and K. Marett. 2010. "The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived." *Journal of Management Information Systems* 27 (1): 273–303. https://doi.org/10.2753/MIS0742-1222270111.

Xiong, A., R. W. Proctor, W. Yang, and N. Li. 2017. "Is Domain Highlighting Actually Helpful in Identifying Phishing Web Pages?" *Human Factors* 59 (4): 640–660. https://doi.org/10.1177/0018720816684064.

Xu, Z., and W. Zhang. 2012. "Victimized by Phishing: A Heuristic-Systematic Perspective." *Journal of Internet Banking and Commerce* 17 (3): 1–16.

Zhuo, S., R. Biddle, J. Daniel Recomendable, G. Russello, and D. Lottridge. 2024. "Eyes on the Phish(er): Towards Understanding Users' Email Processing Pattern and Mental Models in Phishing Detection." In *Proceedings of the 2024 European Symposium on Usable Security*, 15–29. Karlstad: Association for Computing Machinery. https://doi.org/10.1145/3688459.3688465.

Zielinska, O. A., A. K. Welk, C. B. Mayhorn, and E. Murphy-Hill. 2015. "Exploring Expert and Novice Mental Models of Phishing." *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 59 (1): 1132–1136. https://doi.org/10.1177/1541931215591165.

Zu, T., J. Hutson, L. C. Loschky, and N. S. Rebello. 2020. "Using Eye Movements to Measure Intrinsic, Extraneous, and Germane Load in a Multimedia Learning Environment." *Journal of Educational Psychology* 112 (7): 1338–1352. https://doi.org/10.1037/edu0000441.

Appendix. Combined regression model of correct responses to both phishing and legitimate emails

Table A1. Regression model: both legitimate and phishing emails.

Parameter	Estimate	Std error	*t*-value	*p*
(Intercept)	1.089	0.157	6.948	**<.001*** **
Misc. behavioural				
Condition (load)	0.004	0.03	0.146	.88
Mean number of cues examined	0.041	0.03	1.342	.185
Looked at sender's address at all score	−0.017	0.01	−1.642	.106
Looked at sender's address first score	0.003	0.006	0.407	.685
Mean RT	−0.003	0.009	−0.27	.788
Frequency of clicks on cues				
1 – Subject line	0.005	0.006	0.955	.343
2 – Sender's address	0.009	0.006	1.386	.171
3 – Interface objects	0.009	0.009	0.917	.363
4 – Logo	0.001	0.007	0.197	.844
5 – Link	−0.002	0.001	−0.164	.87
6 – Greeting	0.005	0.006	0.937	.353
7 – Text	−0.009	0.005	−1.997	**.05**
8 – Signoff	−0.033	0.01	−3.283	**.002****
Time spent looking at cues				
1 – Subject line	−0.044	0.033	−1.358	.18
2 – Sender's address	−0.014	0.022	−0.668	.507
3 – Interface objects	−0.126	0.086	−1.473	.146
4 – Logo	−0.108	0.044	−2.434	**.018***
5 – Link	0.09	0.058	1.556	.125
6 – Greeting	−0.172	0.064	−2.707	**.009****
7 – Text	0.009	0.012	0.719	.475
8 – Signoff	0.087	0.036	2.442	**.018***
Individual differences				
Cyber security experience score	−0.01	0.006	−1.753	.085.
BIS impulsivity score	−0.001	0.005	−0.398	.692
Hamilton's intuitive scale score	−0.006	0.004	−1.564	.123
Interaction terms				
Mean RT * Cyber security experience score	0.001	0.000	2.009	**.049***
Model fit:				
Adjusted r^2	0.36			
p =	**<.001*****			

***$p < 0.01$; **$p < 0.05$.