Information & Computer Security

845

Persuasion under pressure: the influence of persuasion principles and time constraints on phishing email susceptibility

Jaime Claire Auton and Daniel Sturman
Department of Psychology, The University of Adelaide, Adelaide, Australia

Received 22 July 2024
Revised 14 March 2025
29 May 2025
Accepted 30 May 2025

Abstract

Purpose – This study aims to examine how commonly used persuasion principles (authority, scarcity) and less commonly used principles (reciprocity, social proof) influenced users' ability to differentiate between phishing and genuine emails and whether this effect was moderated by time pressure.

Design/methodology/approach – In an online email management study, participants (n = 200) categorised 60 emails (50 genuine, 10 phishing) and assessed the safety of embedded URL links. Time pressure was experimentally manipulated, with participants given either 7 s (greater time pressure) or 15 s (lesser time pressure) to review each email. Emails varied in containing a common, uncommon or no persuasion principle.

Findings – Participants were most skilled at detecting phishing emails and unsafe links when they contained scarcity and social proof principles, indicating that a persuasion principle's ability to deceive users may not rely on its frequency in real-world phishing attacks. While participants demonstrated greater phishing detection and URL safety awareness under lesser time pressure, the effect of persuasion principles was not significantly moderated by time constraints.

Practical implications – Training interventions should focus on helping users recognise persuasion principles and encourage systematic email evaluation, even under time constraints, to mitigate phishing risks.

Keywords Phishing emails, Persuasion principles, Time pressure, Signal detection theory, Cognitive processing, Cybersecurity

Paper type Research paper

Phishing is the fraudulent practice of impersonating legitimate entities to obtain sensitive information from online users (Parsons *et al.*, 2019). These attacks, often executed via email, manipulate users into clicking malicious links, downloading harmful attachments or disclosing confidential data (Williams *et al.*, 2018). Despite advances in cybersecurity measures, there has been a rise in the frequency and sophistication of phishing attacks (Desolda *et al.*, 2022). Globally, phishing was the most common root cause of organisational data breaches in 2023, with each breach costing an average of US$4.45m (IBM Security, 2023). Given that human error contributes to 95% of cyberattacks (IBM Global Technology Services, 2014), understanding the cognitive and psychological mechanisms that influence phishing susceptibility is critical.

Funding: This research was supported by the Australian Research Council (DP230101607).

Information & Computer Security
Vol. 33 No. 5, 2025
pp. 845-859
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-07-2024-0163

Extensive research has explored individual and situational factors that contribute to phishing susceptibility (Wright *et al.*, 2023), including factors relating to the email recipient (e.g. age, gender, personality) and the situation (e.g. email load, workplace environment; Desolda *et al.*, 2022; Sommestad and Karlzén, 2019; Zhuo *et al.*, 2023). More recently, researchers have begun to examine the role of persuasion in phishing attacks, with a growing body of literature examining how psychological persuasion principles are used to manipulate recipients (Zhuo *et al.*, 2023).

Cialdini (2009) identified six key persuasion principles – authority, scarcity, reciprocity, social proof, liking and consistency – that influence decision-making and compliance. Within phishing emails, these principles are strategically embedded to enhance credibility and discourage critical evaluation, increasing the likelihood of successful attacks (Taib *et al.*, 2019). Within the context of phishing emails, authority increases compliance when requests appear to come from figures of power (e.g. CEO, Vice-Chancellor). Scarcity enhances perceived value by emphasising rare or limited offers. Reciprocity leverages the obligation to respond to services or favours received (e.g. request to complete a survey for a loyalty program). Social proof encourages action by implying that others have already complied. Liking increases persuasion when email requests come from familiar or well-liked individuals. Finally, consistency reinforces persuasion by aligning requests with past actions (e.g. donating to a previously supported charity). Prior research has found that the authority and scarcity principles are the most used in everyday phishing emails, while reciprocity and social proof are the least used (Akbar, 2014).

While phishing emails frequently contain persuasion principles, users' cognitive processing of these persuasive elements plays a critical role in their susceptibility to phishing attacks (Vishwanath *et al.*, 2011). According to dual-process models of persuasion, such as the Heuristic-Systematic Model (Chaiken, 1980), individuals evaluate persuasive messages through either heuristic processing (rapid, automatic, intuitive) or systematic processing (slower, deliberate, effortful). Persuasion principles are particularly effective as they are likely to prompt recipients to engage in rapid rather than analytical evaluations of emails (Bayl-Smith *et al.*, 2022). Consequently, recipients are less likely to notice cues signalling a lack of authenticity, such as illegitimate URLs or spelling errors (Parsons *et al.*, 2015).

A small body of research has examined the effectiveness of Cialdini's (2009) persuasion principles within phishing emails; however, findings have been inconsistent. Research conducted within lab-controlled settings (e.g. using an email management study where participants are required to manage a pre-defined set of emails) has found that participants were *least* likely to detect phishing emails containing the authority (Baryshevtsev and McGlynn, 2020; Black and Sarno, 2023; Butavicius *et al.*, 2015), liking (Lawson *et al.*, 2017, 2020) and consistency principles (Parsons *et al.*, 2019). In contrast, participants were *more* likely to detect phishing emails containing the authority (Lawson *et al.*, 2017, 2020), liking (Black and Sarno, 2023), social proof (Baryshevtsev and McGlynn, 2020; Butavicius *et al.*, 2015) and scarcity (Lawson *et al.*, 2017; Parsons *et al.*, 2019) principles.

Studies employing naturalistic methods (e.g. simulated phishing emails sent directly to users' email inboxes) have also garnered inconsistent findings. Phishing emails containing the authority (Alyahya and Weir, 2021; Williams *et al.*, 2018), liking (Wright *et al.*, 2014), social proof (Bayl-Smith *et al.*, 2022; Taib *et al.*, 2019), consistency (Gallo *et al.*, 2024) and scarcity (Lin *et al.*, 2019) principles have resulted in the highest click-through rates. In comparison, phishing emails containing scarcity (Bayl-Smith *et al.*, 2022; Gallo *et al.*, 2024; Taib *et al.*, 2019; Williams *et al.*, 2018), authority (Wright *et al.*, 2014) and social proof (Alyahya and Weir, 2021; Lin *et al.*, 2019) principles have resulted in the lowest click-through rates.

Inconsistent findings regarding the effectiveness of persuasion principles may stem from differences in research methodologies (Black and Sarno, 2023). Naturalistic studies offer higher ecological validity by observing user responses to phishing emails in real-world contexts, where factors such as email load and workplace distractions play a role. In contrast, lab-based studies provide greater experimental control but often lack these contextual constraints, often allowing unlimited time for email evaluation (e.g. Butavicius *et al.*, 2015; Parsons *et al.*, 2019).

Research has consistently shown that time pressure increases phishing susceptibility by impairing users' ability to critically evaluate emails (Butavicius *et al.*, 2022; Jones *et al.*, 2019; Rajagulasingam and Taylor, 2021; Sturman *et al.*, 2023; Wang *et al.*, 2016). Under time constraints, users are more likely to rely on heuristic processing, making them prone to overlooking deception cues such as illegitimate URLs or spelling errors (Wang *et al.*, 2012). To better understand how persuasion principles influence users in real-world settings while maintaining experimental control, studies could incorporate cognitive demands that are typically encountered in everyday email interactions. One approach is to impose time pressure, as users often assess emails under pressure while managing multiple tasks.

The current study

While prior phishing studies have examined persuasion principles and the role of time pressure in email evaluation separately, few have explored their interaction. The only lab-controlled study to do so, conducted by Black and Sarno (2023), found no main effect of time pressure nor an interaction between time pressure and persuasion principles on participants' ability to discriminate phishing from legitimate emails. However, their study implemented set time frames (8 min, 22 min or no limit) to evaluate an entire set of 60 emails, rather than controlling the time allocated to each email. As a result, participants' time spent on individual emails varied depending on the persuasion principle used, potentially obscuring systematic differences in how these principles influence detection under time constraints.

A more controlled approach – where time is standardised for each email – would provide clearer insight into how time pressure affects the processing of different persuasion principles. This is particularly relevant in modern workplaces, where employees manage high email volumes under time constraints, increasing their susceptibility to phishing attacks. Understanding the interplay between persuasion principles and time pressure could inform cybersecurity training and policy development by identifying the conditions under which individuals are most vulnerable.

This study aimed to investigate how commonly and uncommonly used persuasion principles affect phishing susceptibility, and whether this relationship is moderated by time pressure (i.e. time provided to evaluate each email). Participants completed an online Email Management Task, categorising 60 emails (50 genuine, 10 phishing) and assessing the safety of embedded URL links. Each email contained either a common (authority, scarcity), an uncommon (reciprocity, social proof) or no persuasion principle. This classification was based on Akbar (2014), who analysed real-world phishing emails and found authority and scarcity to be the most frequently used persuasion principles, while reciprocity and social proof were the least common. While other persuasion techniques, such as strong affect and distraction, can also influence phishing susceptibility (Ferreira and Teles, 2019), Cialdini's (2009) principles were selected due to their well-documented role in phishing attacks (e.g. Akbar, 2014). Time pressure was experimentally manipulated, where participants were either given seven or 15 s to review each email. Performance was assessed in two ways: discrimination, defined as the ability to correctly differentiate phishing emails from genuine

ones (i.e. correctly identifying phishing emails as fraudulent and genuine emails as legitimate), and safety ratings of URL links within phishing emails.

Development of hypotheses

The role of persuasion principles on discrimination and URL safety ratings

According to inoculation theory (McGuire, 1961), users may more readily detect phishing emails that employ commonly used persuasion principles (authority, scarcity) due to prior exposure in past phishing attempts, resulting in detection rates like emails without persuasion elements. In contrast, less frequently used principles (reciprocity, social proof) may be harder to recognise, reducing users' ability to distinguish phishing emails from genuine ones.

Additionally, persuasion principles can influence how users assess the safety of URLs in phishing emails. When emails use less common persuasion principles, users may be more likely to perceive the links as safer, as they are less likely to recognise deceptive cues compared to emails that employ more familiar principles. Thus, the following hypotheses were proposed:

H1a. Discrimination between phishing and genuine emails will be greater for emails containing no persuasion principles than for those containing uncommon persuasion principles (reciprocity, social proof).

H1b. Discrimination between phishing and genuine emails will not differ between emails containing common persuasion principles (authority, scarcity) and those containing no persuasion principles.

H2a. URL links within phishing emails containing uncommon persuasion principles (reciprocity, social proof) will be rated as safer compared to those containing no persuasion principles.

H2b. There will be no difference in safety ratings for URL links within phishing emails containing common persuasion principles (authority, scarcity) compared to those containing no persuasion principles.

The role of persuasion principles and time pressure on discrimination and URL safety ratings

The effectiveness of persuasion principles may vary based on the time available for email evaluation. According to inoculation theory (McGuire, 1961), users may be more likely to quickly detect phishing emails containing commonly used persuasion principles (authority, scarcity) due to prior exposure. These principles may be recognised rapidly through heuristic processing, meaning additional time is unlikely to significantly improve detection.

In contrast, identifying phishing emails using uncommon principles (reciprocity, social proof) may require systematic processing, which is hindered by time constraints. Under greater time pressure, users may struggle to critically evaluate these less familiar cues, reducing phishing detection accuracy. Thus, phishing emails containing uncommon principles may be more deceptive under time pressure, while those using common principles remain equally detectable regardless of time constraints. Based on this, the following hypotheses were proposed:

H3. The effect of persuasion principles on discrimination between phishing and genuine emails will be moderated by time pressure. Specifically, the difference in discrimination between emails containing no persuasion principles and those containing uncommon persuasion principles (reciprocity, social proof) will be larger

under greater time pressure (7s) than under lesser time pressure (15s). In contrast, there will be no significant interaction between time pressure and discrimination for emails containing common persuasion principles (authority, scarcity) versus no persuasion principles.

H4. Time pressure will moderate the effect of persuasion principles on the safety ratings of URL links in phishing emails. Specifically, under greater time pressure (7s), phishing emails containing uncommon persuasion principles (reciprocity, social proof) will receive higher safety ratings compared to those without persuasion principles, whereas this effect will be weaker under lesser time pressure (15s). In contrast, for phishing emails containing common persuasion principles (authority, scarcity), there will be no difference in safety ratings compared to those without persuasion principles, regardless of time pressure.

Method

Participants

Two hundred participants completed this study. This sample size is consistent with previous studies on phishing susceptibility and persuasion principles, which often employ similar sample sizes to account for variability in individual responses and contextual factors (e.g. Baryshevtsev and McGlynn, 2020; Black and Sarno, 2023; Butavicius *et al.*, 2015; Lawson *et al.*, 2020). Most participants (88.5%) were self-selected undergraduate students from the University of Adelaide who received course credit in exchange for participation. The remaining participants were recruited using convenience sampling via social media and could voluntarily enter a prize-draw to win one of five AU$20 gift cards. Participants were predominantly female (75.5%) and ranged in age from 17 to 56 years (M = 22.44, SD = 7.88). Participants reported receiving an average of 15.08 emails per day (SD = 18.64).

Materials

Email management task. Participants were told to roleplay the personal assistant to "Professor Alex Jones" from the Department of Psychology at the University of Adelaide. To manage Professor Jones' email inbox, participants were required to sort a series of 60 emails into one of 10 different categories (e.g. Urgent, Teaching, Research, Phishing). Participants were provided with descriptions of each category (e.g. *Phishing emails are those that seem fraudulent and malicious*) and completed a practice item before beginning the email Management Task.

Emails were presented to participants in a randomised order to review and sort. Participants were randomly allocated to a time pressure condition, where each email was presented on screen for either seven seconds (*greater* time pressure) or 15 s (*lesser* time pressure). Since the typical email evaluation time is 13.4 s (Erickson, 2019), the seven second condition was designed to induce significant time pressure, encouraging heuristic processing and limiting the ability to carefully evaluate deception cues. The 15 s condition allowed for a more typical, yet still constrained, evaluation. Standardising the time per email ensured experimental control while reflecting real-world conditions where users often assess emails under time pressure.

There was a countdown timer directly above each email, and participants were unable to progress to the next screen before the allocated time had expired. Participants were then presented with a new screen where they were asked to categorise the email into one of the 10 available categories. Participants were then asked to indicate the extent to which they agreed with the statement, "*It is okay to click on the link within this email*" for each email on a scale from 1(*Strongly Disagree*) to 5(*Strongly Agree*).

Email stimuli development. Consistent with the approach adopted by Parsons *et al.* (2019), the 60 emails used in this study were unaltered or modified emails received by the researchers. All emails were selected on the basis that they were legitimate emails (i.e. not phishing emails), consisted of 100 words or less and contained a single URL link. Emails were also selected based on whether they contained one of the four persuasion principles (authority, scarcity, reciprocity, social proof) or did not contain a persuasion principle. Examples of emails from each type of principle are listed in Table 1.

Of the 60 emails, 10 emails were modified to create phishing emails by replacing the original URL links with links sourced from known phishing emails. Five of these phishing emails also included one spelling and one grammatical error in the first line of the email and an illegitimate email senders' address as these are features commonly associated with phishing emails (Parsons *et al.*, 2015). Among the 50 genuine emails, 10 were modified to also contain spelling/grammatical errors or illegitimate senders' addresses. However, these emails were classified as genuine emails as they did not contain malicious links which are a defining characteristic of phishing attempts (Zielinska *et al.*, 2016). The remaining 40 genuine emails went unaltered. Across the 60 emails, 12 emails were intended to represent each of the five persuasion principles. The proportion of phishing to genuine emails was balanced within each persuasion condition, ensuring that each persuasion principle appeared in two phishing emails and 10 genuine emails.

Within all emails, URL links were either displayed as a link within the body of the email or as a HTML button (e.g. "Start Survey"; "Click Here"). Prior to the commencement of the task, participants were told that if the URL links were not visible within the body of the email, they could use the mouse cursor to hover over the HTML buttons to view the URL. Figure 1 shows an example of the URL hover function with a genuine email (left) and phishing email (right).

Table 1. Examples of email type for each persuasion principle

Persuasion principle	Email sender and description	Email topic	Sample text
Authority	Australian Federal Police Australia's national policing agency	Issue of an infringement notice	"You have received this email because you have been issued with an Infringement Notice"
Scarcity	Spotify Digital music, podcast and video streaming service	Spotify subscription payment failure	"You'll lose Premium if we don't have a working payment method for your account within the next 7 days, so update your payment details now!"
Reciprocity	Twitter Free social networking site	Reminder of unread Twitter notifications	"Stay connected, respond to the people who tried to reach out to you"
Social proof	SBS On Demand Free video streaming service available in Australia	Recommendations of popular programs to view	"Join the millions of Australians streaming the latest TV and movies"
No principle	Specsavers Optometrists Australian chain that offers optometry and optician services	Confirmation of an eye appointment	"Your appointment for your eye test at Specsavers Sefton Park is confirmed"

Source(s): Authors' own work

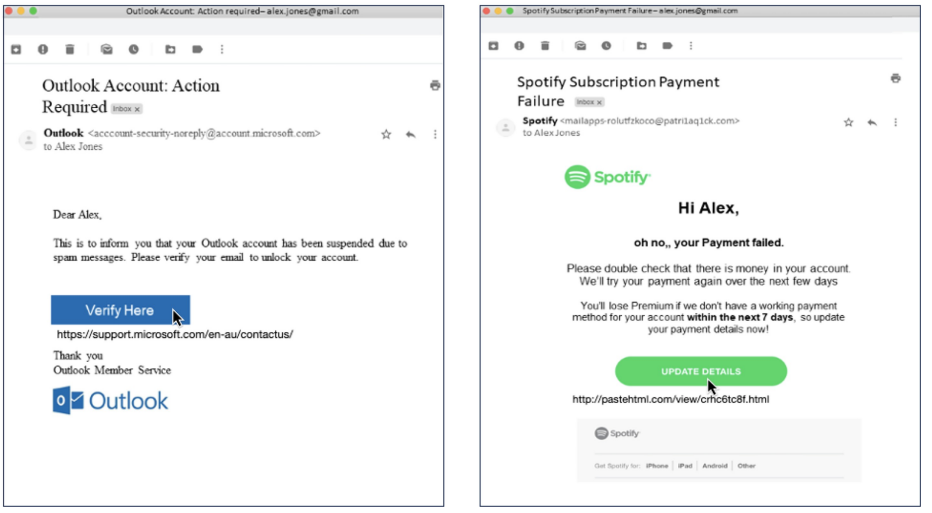

Figure 1. Example of a genuine email (left) and phishing email (right)

Note(s): Emails were presented individually to participants with the countdown timer positioned above the email. Where emails included a HTML button, participants could move their mouse cursor over the button to "reveal" the URL link (as shown in the two examples above). The email on the left is a genuine email containing no persuasion principle; the email on the right is a phishing email containing an illegitimate URL, illegitimate email sender, grammatical errors and the scarcity persuasion principle

Source: Authors' own work

Procedure

This research complied with the American Psychological Association Code of Ethics and was approved by the University of Adelaide's Human Research Ethics Committee (Approval Number 20/39). Participants completed this study online via the Qualtrics online survey platform. After reading the information form and providing informed consent, Qualtrics randomly allocated participants to a time pressure condition. Participants then completed a series of demographic questions and the Email Management Task. Participants were told that the study was investigating user behaviour and emails, and thus, were unaware that the study related to phishing email detection.

Results

Dependent variables

Two dependent variables were included in this study. Firstly, to assess participants' capacity to discriminate phishing from genuine emails, detection sensitivity was calculated using Signal Detection Theory (Stanislaw and Todorov, 1999). For the five groups of 12 emails containing a different persuasion principle, hits and false alarms scores were calculated. Hits were defined as the number of phishing emails that were correctly classified as phishing emails, whereas false alarms were defined as the number of genuine emails that were incorrectly classified as phishing emails. Hits and false alarms were converted to z-scores. A sensitivity score (d') for each group of emails was calculated by subtracting z-scores for false

alarms from z-scores from hits (z[HIT] – z[FA]). For each group of emails containing a different persuasion principle, a higher sensitivity score represented a greater capacity to discriminate between phishing and genuine emails. Sensitivity scores for each persuasion principle across the time pressure conditions are presented in Table 2.

For the second dependent variable, participants were required to respond to the statement "*It is okay to click on the link in this email*" on a five-point Likert scale from 1(*Strongly Disagree*) to 5(*Strongly Agree*) for each of the 10 phishing emails (two containing each persuasion principle). A mean score was computed for each persuasion principle, where higher ratings indicated a stronger safety perception of the URL link. Mean URL safety ratings across the time pressure conditions are presented in Table 3.

Covariates

Pearson's correlations revealed that there was a statistically significant negative correlation between participants' age and one of the dependent variables (URL safety rating for the authority principle), $r(198) = -0.17$, $p = 0.014$. There was also a statistically significant negative correlation between number of emails received and two dependent variables (URL safety rating for the authority principle, $r[197] = -0.16$, $p = 0.028$; and no principle, $r[197] = -0.14$, $p = 0.046$). Consequently, both age and number of emails received were included as covariates in the subsequent analyses. Independent

Table 2. Descriptive statistics for sensitivity (d') scores for each persuasion principle

	Persuasion principle				
	Common		Uncommon		
	Authority	Scarcity	Reciprocity	Social proof	No principle
Time pressure	Mean (SD)	Mean (SD)	Mean (SD)	Mean (SD)	Mean (SD)
Greater (7 s)	0.27 (*1.10*)	1.25 (*1.71*)	−0.39 (*0.97*)	0.34 (*1.52*)	0.76 (*1.58*)
Lesser (15 s)	0.67 (*1.39*)	1.91 (*1.88*)	−0.04 (*1.16*)	1.17 (*1.71*)	1.69 (*1.99*)
Total	0.47 (*1.27*)	1.58 (*1.82*)	−0.22 (*1.08*)	0.75 (*1.66*)	1.22 (*1.85*)

Note(s): A higher sensitivity score represents a greater capacity to discriminate between phishing and genuine emails
Source(s): Authors' own work

Table 3. Descriptive statistics for URL link safety ratings for each persuasion principle

	Persuasion principle				
	Common		Uncommon		
	Authority	Scarcity	Reciprocity	Social proof	No principle
Time pressure	Mean (SD)	Mean (SD)	Mean (SD)	Mean (SD)	Mean (SD)
Greater (7 s)	3.76 (*1.17*)	2.95 (*1.25*)	3.92 (*0.94*)	2.97 (*1.16*)	3.39 (*1.16*)
Lesser (15 s)	3.21 (*1.25*)	2.41 (*1.23*)	3.26 (*1.07*)	2.32 (*1.03*)	2.61 (*1.33*)
Total	3.49 (*1.24*)	2.68 (*1.27*)	3.59 (*1.06*)	2.64 (*1.14*)	3.00 (*1.31*)

Note(s): Ratings were made on a scale from 1(*Strongly Disagree*) to 5(*Strongly Agree*), where higher mean ratings represent a stronger safety perception of URL links within phishing emails
Source(s): Authors' own work

samples *t*-tests revealed no statistically significant differences between males and females for scores on any of the dependent variables ($ps > 0.05$).

Design

For each dependent variable (i.e. sensitivity, URL safety ratings), a 2 × 5 mixed ANOVA was conducted, with Time Pressure (Greater [7s], Lesser [15s]) as the between subjects variable and Persuasion Principle (Authority, Scarcity, Reciprocity, Social Proof, No Principle) as the within subjects variable, with age and number of emails received as the covariates. A Greenhouse-Geisser correction is presented where required.

Analysis 1: Persuasion principle, time pressure and sensitivity

With sensitivity as the dependent variable, there was a significant main effect for time pressure, $F(1,195) = 15.22$, $p < 0.001$, where sensitivity was higher with lesser (15 s) time pressure ($M = 1.07$, $SE = 0.11$), compared to greater (7 s) time pressure ($M = 0.45$, $SE = 0.11$).

There was also a significant main effect for persuasion principle, $F(3.70, 721.93) = 6.63$, $p < 0.001$. To examine *H1a* and *H1b*, four planned pairwise comparisons were conducted, with critical alpha set at $\alpha = 0.0125$ to control for the family-wise error rate. As predicted in *H1a*, the sensitivity scores were significantly lower for the uncommon persuasion principles of Reciprocity ($M = -0.22$, $SD = 1.08$), $p < 0.001$, and Social Proof ($M = 0.75$, $SD = 1.66$), $p < 0.001$, compared to No Principle ($M = 1.22$, $SD = 1.85$). Contrary to the predictions of H1b, the sensitivity score for Scarcity ($M = 1.58$, $SD = 1.82$) was significantly higher than for No Principle ($M = 1.22$, $SD = 1.85$), $p = 0.007$. In contrast, the sensitivity score for Authority ($M = 0.47$, $SD = 1.27$) was significantly lower than for No Principle, ($M = 1.22$, $SD = 1.85$), $p < 0.001$.

There was no statistically significant interaction between persuasion principle and time pressure on sensitivity, $F(3.70, 721.93) = 2.26$, $p = 0.066$ (see Figure 2). As such, there was no support for *H3*.

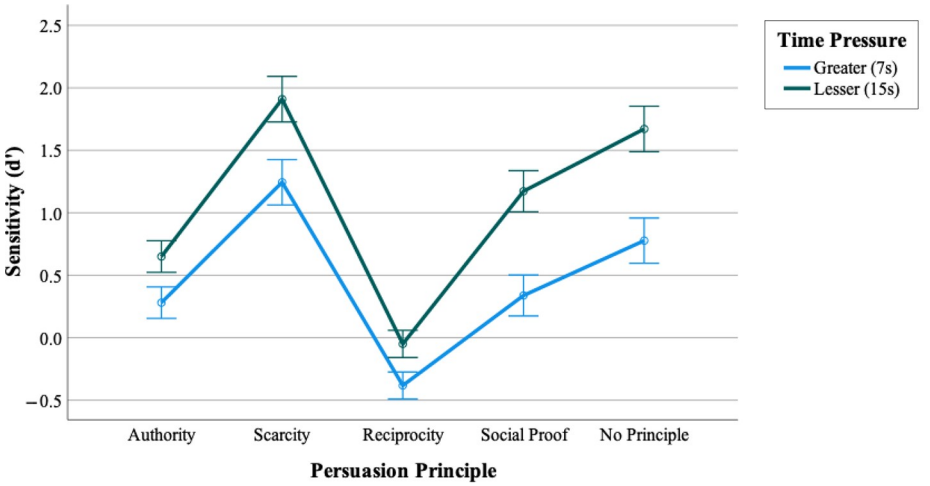

Figure 2. Sensitivity as a function of persuasion principle and time pressure

Note: A higher sensitivity score represents a greater capacity to discriminate phishing from genuine emails. Error bars represent standard errors. Value of covariates: age = 22.46, email frequency = 15.08

Source: Authors' own work

Analysis 2: Persuasion principle, time pressure and URL safety ratings

With URL link safety ratings as the dependent variable, there was a significant main effect for time pressure, $F(1, 195) = 28.07$, $p < 0.001$, where URL links within phishing emails were rated as *less* safe with lesser (15 s) time pressure ($M = 2.74$, $SE = 0.09$), compared to greater (7 s) time pressure ($M = 3.42$, $SE = 0.09$).

A significant main effect of persuasion principle was also observed, $F(3.63, 707.98) = 9.32$, $p < 0.001$. To examine *H2a* and *H2b*, four planned pairwise comparisons were conducted, with critical alpha set at $\alpha = 0.0125$ to control for the family-wise error rate. Partially supporting with *H2a*, URL links within phishing emails were rated as more safe when they contained the uncommon principle of Reciprocity ($M = 3.59$, $SD = 1.06$) compared to No Principle ($M = 3.00$, $SD = 1.31$), $p < 0.001$. However, URL links were rated as less safe when the uncommon principle of Social Proof was used ($M = 2.64$, $SD = 1.14$) compared to No Principle ($M = 3.00$, $SD = 1.31$), $p < 0.001$. Contrary to the predictions of *H2b*, URL links within phishing emails were rated as safer when the common principle of Authority was present ($M = 3.49$, $SD = 1.24$) compared to No Principle ($M = 3.00$, $SD = 1.31$), $p < 0.001$. Conversely, URL links were rated as less safe when the common principle of Scarcity was used ($M = 2.68$, $SD = 1.27$) compared to No Principle ($M = 3.00$, $SD = 1.31$), $p < 0.001$.

There was no statistically significant interaction between persuasion principle and time pressure on URL safety ratings, $F(3.63, 707.98) = 0.61$, $p = 0.637$ (see Figure 3). As such, no support was found for *H4*.

Discussion

The current study had two aims: to investigate how various persuasion principles influenced participants' evaluation of emails, and how this relationship is affected by time pressure. Participants were less able to discriminate between phishing and genuine emails containing the reciprocity (uncommon), authority (common) and social proof (uncommon) principles,

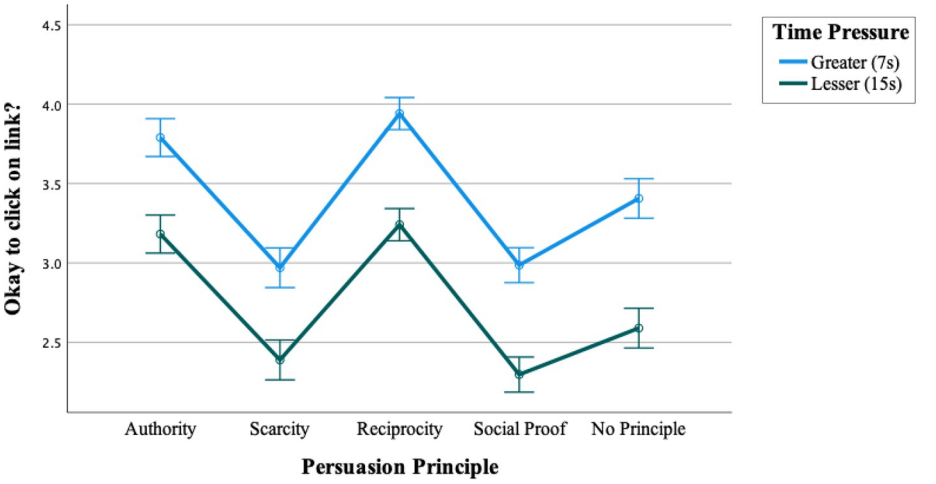

Figure 3. URL safety ratings as a function of persuasion principle and time pressure

Note: A higher mean rating represents a greater perception of safety of URL links within phishing emails. Error bars represent standard errors. Value of covariates: age = 22.46, email frequency = 15.08

Source: Authors' own work

compared to emails containing no persuasion principles. In contrast, participants demonstrated a greater discrimination capacity when emails contained the scarcity (common) principle compared to those containing no persuasion principles. These findings were partially consistent with the proposed hypotheses.

Additionally, URL links within phishing emails containing the reciprocity and authority principles were considered *safer* to click on, while URL links within phishing emails containing the social proof and scarcity principles were considered *less* safe to click on, compared to those with no persuasion principles. These results challenge the predictions of inoculation theory (McGuire, 1961), suggesting that the frequency of persuasion principle use in real-world phishing does not necessarily correlate with its effectiveness. Notably, participants were most skilled at detecting phishing emails and suspicious links containing the scarcity (common) and social proof (uncommon) principles, and least skilled at detecting those with the reciprocity (uncommon) and authority (common) principles.

The second aim of this study investigated the relative efficacy of persuasion principles under different time constraints. While it was hypothesised that greater time pressure would exacerbate the impact of uncommon persuasion principles (reciprocity, social proof), no significant interaction was found between persuasion principles and time pressure. This aligns with Black and Sarno's (2023) findings, suggesting that time pressure does not necessarily alter the relative effectiveness of persuasion principles. However, participants did show reduced discrimination and a higher perception of safety in phishing links under greater time pressure, reinforcing past research indicating that reduced time to evaluate emails increases phishing susceptibility (e.g. Butavicius *et al.*, 2022; Sturman *et al.*, 2023).

Strengths, limitations and future directions

A key strength of this study was the lab-controlled classification task which offers distinct advantages over naturalistic phishing methods. This approach enabled a more comprehensive evaluation of participants' ability to discriminate between phishing and genuine emails, rather than relying solely on click-through rates, which do not capture how users evaluate genuine emails (e.g. Bayl-Smith *et al.*, 2022). Each participant responded to 60 emails across five persuasion conditions, yielding 12,000 total observations. This repeated-measures design enhanced statistical precision by reducing within-subject error variance and enabling the detection of nuanced effects. While some real-world studies involve larger samples (e.g. Bayl-Smith *et al.*, 2022; Taib *et al.*, 2019), they often rely on single binary outcomes (e.g. clicked vs didn't click) and offer limited experimental control. In contrast, the current study generated rich data within a controlled environment, allowing for stronger inferences about the cognitive mechanisms underpinning phishing susceptibility. Finally, although the artificial nature of the lab setting required participants to assess emails outside their typical inbox environment, this trade-off allowed for a high degree of experimental control (Butavicius *et al.*, 2022).

The use of a relatively homogenous sample of undergraduate psychology students, while limiting generalisability, offered important methodological advantages. Specifically, the consistency in participants' age and educational background helped minimise extraneous variability, thereby enabling a clearer interpretation of the effects associated with the experimental manipulations. Nevertheless, this sampling approach may not reflect the diversity of real-world populations targeted by phishing attacks. Future research should aim to include more diverse participant samples from different demographic backgrounds and professional contexts to assess how susceptibility to persuasion principles varies across groups and settings. Such efforts will help validate and extend the current findings to broader populations more representative of real-world phishing targets.

This study contributes to the limited knowledge on persuasion principles and phishing susceptibility. Indeed, the few studies directly examining their relative effectiveness in phishing emails have yielded inconsistent results. While these mixed findings could be accounted for by variations in research methodologies (Black and Sarno, 2023), the persuasiveness of such principles can also vary as a function of individual differences (e.g. Parsons *et al.*, 2019) or other contextual factors (e.g. professional industry characteristics; Tian *et al.*, 2023). As such, further research should investigate additional factors that could influence the effectiveness of Cialdini's (2009) principles in phishing emails. A deeper understanding of these factors will help mitigate phishing risks, especially in populations with specific vulnerabilities.

Practical applications

The outcomes of this study have meaningful implications for phishing education and training. The finding that increased time pressure resulted in greater phishing susceptibility underscores the importance of addressing common workplace stressors, such as deadlines and distractions, in cybersecurity training. Future research should continue exploring how situational factors, such as workload and stress, impact phishing susceptibility.

The findings from this study suggest that instructing email users to adopt a slower, more systematic approach, rather than a quick, intuitive one could potentially decrease the effectiveness of phishing attacks. Recent studies on anti-phishing training campaigns, informed by mindfulness strategies, support this approach. These campaigns prompt users to pause and consider the context in which they receive emails, promoting a more systematic approach to processing email content (Jensen *et al.*, 2017). However, this study also indicates that increasing time spent reviewing emails does not entirely mitigate the influence of persuasion strategies. Therefore, training interventions should focus on helping users recognise key characteristics of phishing emails, including persuasion principles, while promoting strategies for systematic processing.

Theoretical implications

This study extends theoretical understanding of phishing susceptibility by exploring how different persuasion principles, particularly under time pressure, influence decision-making. While previous research has explored individual persuasion principles in phishing, few studies have systematically compared the impact of commonly used principles (e.g. authority, scarcity) with less frequently employed ones (e.g. reciprocity, social proof). This study's findings clarify the varying effectiveness of these principles, particularly when individuals are under time constraints, shedding light on how the speed of decision-making affects the success of phishing attempts.

Conclusion

This study explored how persuasion principles impact participants' evaluation of emails, with a focus on how time pressure influences this relationship. Participants were most skilled at detecting phishing emails and unsafe links containing the scarcity and social proof principles and were least skilled at detecting phishing emails and links containing the reciprocity and authority principles. Greater time pressure reduced participants' ability to distinguish phishing emails and perceive the safety of links, but did not alter the effectiveness of persuasion principles. These findings highlight the importance of incorporating training strategies that promote systematic email review and awareness of persuasive tactics to reduce phishing susceptibility.

References

Akbar, N. (2014), "Analysing persuasion principles in phishing emails", Master's thesis, University of Twente, available at: https://essay.utwente.nl/66177/1/Akbar_MA_EEMCS.pdf

Alyahya, A. and Weir, G.R. (2021), "Understanding responses to phishing in Saudi Arabia via the theory of planned behaviour", Conference session, *National Computing Colleges*, doi: 10.1109/NCCC49330.2021.9428823.

Baryshevtsev, M. and McGlynn, J. (2020), "Persuasive appeals predict credibility judgments of phishing messages", *Cyberpsychology, Behavior, and Social Networking*, Vol. 23 No. 5, pp. 297-302, doi: 10.1089/cyber.2019.0592.

Bayl-Smith, P., Taib, R., Yu, K. and Wiggins, M. (2022), "Response to a phishing attack: persuasion and protection motivation in an organizational context", *Information and Computer Security*, Vol. 30 No. 1, pp. 63-78, doi: 10.1108/ICS-02-2021-0021.

Black, J. and Sarno, D.M. (2023), "The influence of time pressure and persuasion principles on phishing detection", *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 67, pp. 1977-1982, doi: 10.1177/21695067231192442.

Butavicius, M., Taib, R. and Han, S.J. (2022), "Why people keep falling for phishing scams: the effects of time pressure and deception cues on the detection of phishing emails", *Computers and Security*, Vol. 123, p. 102937, doi: 10.1016/j.cose.2022.102937.

Butavicius, M., Parsons, K., Pattinson, M. and McCormac, A. (2015), "Breaching the human firewall: social engineering in phishing and spear-phishing emails", *Proceedings of the 26th Australasian Conference of Information Systems*, available at: https://aisel.aisnet.org/acis2015/98

Chaiken, S. (1980), "Heuristic versus systematic information processing and the use of source versus message cues in persuasion", *Journal of Personality and Social Psychology*, Vol. 39 No. 5, pp. 752-766, doi: 10.1037//0022-3514.39.5.752.

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

Desolda, G., Ferro, L.S., Marrella, A., Catarci, T. and Costabile, M.F. (2022), "Human factors in phishing attacks: a systematic literature review", *ACM Computing Surveys*, Vol. 54 No. 8, pp. 1-35, doi: 10.1145/3469886.

Erickson, D. (2019), "Email reading and dwell times, 2011–2018", available at: https://trends.e-strategyblog.com/2019/06/17/email-reading-times/31795/

Ferreira, A. and Teles, S. (2019), "Persuasion: how phishing emails can influence users and bypass security measures", *International Journal of Human-Computer Studies*, Vol. 125, pp. 19-31, doi: 10.1016/j.ijhcs.2018.12.004.

Gallo, L., Gentile, D., Ruggiero, S., Botta, A. and Ventre, G. (2024), "The human factor in phishing: collecting and analyzing user behavior when reading emails", *Computers and Security*, Vol. 139, p. 103671, doi: 10.1016/j.cose.2023.103671.

IBM Global Technology Services (2014), "IBM security services 2014 cyber security intelligence index: analysis of cyber attack and incident data from IBM's worldwide security operation", available at: https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF

IBM Security (2023), "Cost of a data breach report 2023", available at: www.ibm.com/account/reg/us-en/signup?formid=urx-52258

Jensen, M.L., Dinger, M., Wright, R.T. and Thatcher, J.B. (2017), "Training to mitigate phishing attacks using mindfulness techniques", *Journal of Management Information Systems*, Vol. 34 No. 2, pp. 597-626, doi: 10.1080/07421222.2017.1334499.

Jones, H.S., Towse, J.N., Race, N. and Harrison, T. (2019), "Email fraud: the search for psychological predictors of susceptibility", *Plos One*, Vol. 14 No. 1, pp. 1-15, doi: 10.1371/journal.pone.0209684.

Lawson, P., Pearson, C.J., Crowson, A. and Mayhorn, C.B. (2020), "Email phishing and signal detection: how persuasion principles and personality influence response patterns and accuracy", *Applied Ergonomics*, Vol. 86, p. 103084, doi: 10.1016/j.apergo.2020.103084.

Lawson, P., Zielinska, O., Pearson, C. and Mayhorn, C.B. (2017), "Interaction of personality and persuasion tactics in email phishing attacks", *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 61 No. 1, pp. 1331-1333, doi: 10.1177/1541931213601815

Lin, T., Capecci, D.E., Ellis, D.M., Rocha, H.A., Dommaraju, S., Oliveira, D.S. and Ebner, N.C. (2019), "Susceptibility to spear-phishing emails: effects of internet user demographics and email content", *ACM Transactions on Computer-Human Interaction*, Vol. 26 No. 5, pp. 1-28, doi: 10.1145/3336141.

McGuire, W.J. (1961), "Resistance to persuasion conferred by active and passive prior refutation of the same and alternative counterarguments", *The Journal of Abnormal and Social Psychology*, Vol. 63 No. 2, pp. 326-332, doi: 10.1037/h0048344.

Parsons, K., Butavicius, M., Delfabbro, P. and Lillie, M. (2019), "Predicting susceptibility to social influence in phishing emails", *International Journal of Human-Computer Studies*, Vol. 128, pp. 17-26, doi: 10.1016/j.ijhcs.2019.02.007.

Parsons, K., Butavicius, M., Pattinson, M., McCormac, A. and Jerram, C. (2015), "Do users focus on the correct cues to differentiate between phishing and genuine emails?", Conference paper, *Australasian Conference on Information Systems*, arXiv:1605.04717.

Rajagulasingam, C. and Taylor, J. (2021), "*The roles of self-control, need for cognition, impulsivity and viewing time in deception detection using a realistic e-mail phishing task*", *2021 APWG Symposium on Electronic Crime Research (eCrime), Boston, MA*, doi: 10.1109/eCrime54498.2021.9738794.

Sommestad, T. and Karlzén, H. (2019), "A meta-analysis of field experiments on phishing susceptibility", *2019 APWG symposium on electronic crime research (eCrime), IEEE*, pp. 1-14, doi: 10.1109/eCrime47957.2019.9037502.

Stanislaw, H. and Todorov, N. (1999), "Calculation of signal detection theory measures", *Behavior Research Methods, Instruments, and Computers*, Vol. 31 No. 1, pp. 137-149, doi: 10.3758/bf03207704.

Sturman, D., Valenzuela, C., Plate, O., Tanvir, T., Auton, J.C., Bayl-Smith, P. and Wiggins, M.W. (2023), "The role of cue utilization in the detection of phishing emails", *Applied Ergonomics*, Vol. 106, p. 103887, doi: 10.1016/j.apergo.2022.103887.

Taib, R., Yu, K., Berkovsky, S., Wiggins, M. and Bayl-Smith, P. (2019), "Social engineering and organisational dependencies in phishing attacks (conference paper)", *IFIP Conference on Human-Computer Interaction, Springer International Publishing: Cham*, pp. 564-584, doi: 10.1007/978-3-030-29381-9_35.

Tian, C., Jensen, M.L. and Durcikova, A. (2023), "Phishing susceptibility across industries: the differential impact of influence techniques", *Computers and Security*, Vol. 135, p. 103487, doi: 10.1016/j.cose.2023.103487.

Vishwanath, A., Herath, T., Chen, R., Wang, J. and Rao, H.R. (2011), "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model", *Decision Support Systems*, Vol. 51 No. 3, pp. 576-586, doi: 10.1016/j.dss.2011.03.002.

Wang, J., Li, Y. and Rao, H.R. (2016), "Overconfidence in phishing email detection", *Journal of the Association for Information Systems*, Vol. 17 No. 11, pp. 759-783, doi: 10.17705/1jais.00442.

Wang, J., Herath, T., Chen, R., Vishwanath, A. and Rao, H.R. (2012), "Research article phishing susceptibility: an investigation into the processing of a targeted spear phishing email", *IEEE Transactions on Professional Communication*, Vol. 55 No. 4, pp. 345-362, doi: 10.1109/tpc.2012.2208392.

Williams, E.J., Hinds, J. and Joinson, A.N. (2018), "Exploring susceptibility to phishing in the workplace", *International Journal of Human-Computer Studies*, Vol. 120, pp. 1-13, doi: 10.1016/j.ijhcs.2018.06.004.

Wright, R., Johnson, S. and Kitchens, B. (2023), "Phishing susceptibility in context: a multilevel information processing perspective on deception detection", *MIS Quarterly*, Vol. 47 No. 2, pp. 803-832, doi: 10.25300/misq/2022/16625.

Wright, R.T., Jensen, M.L., Thatcher, J.B., Dinger, M. and Marett, K. (2014), "Influence techniques in phishing attacks: an examination of vulnerability and resistance", *Information Systems Research*, Vol. 25 No. 2, pp. 385-400, doi: 10.1287/isre.2014.0522.

Zhuo, S., Biddle, R., Koh, Y.S., Lottridge, D. and Russello, G. (2023), "SoK: human-centered phishing susceptibility", *ACM Transactions on Privacy and Security*, Vol. 26 No. 3, doi: 10.1145/3575797.

Zielinska, O.A., Welk, A.K., Mayhorn, C.B. and Murphy-Hill, E. (2016), "A temporal analysis of persuasion principles in phishing emails", *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 60 No. 1, pp. 765-769, doi: 10.1177/1541931213601175.

About the authors

Jaime Claire Auton is an organisational psychologist and human factors researcher. Her primary research lies in the assessment and development of expert cognition, particularly with operators working within technical operational environments. Jaime completed her PhD/Master of Organisational Psychology degree at Macquarie University (Sydney, Australia) in 2015 and is currently a Senior Lecturer within the School of Psychology at the University of Adelaide. Jaime Claire Auton is the corresponding author and can be contacted at: jaime.auton@adelaide.edu.au

Daniel Sturman is an organisational psychologist and human factors researcher. His research focuses on performance, decision making and human cognition in high-risk environments, with a focus on applied research, with the goal of developing assessment tools and interventions to assist industry partners in the selection, training and management of experienced personnel. Daniel completed his PhD/Master of Organisational Psychology degree at Macquarie University (Sydney, Australia) in 2020 and is currently a Senior Lecturer within the School of Psychology at the University of Adelaide.