

**Understanding the Human Dimension: The Role of Persuasion and Psychological
Factors in Cyberattack Vulnerability**

Dorien Brinkhof

Faculty of Behavioural, Management and Social Sciences (BMS), University of Twente

PSY-M-23 - Conflict, Risk and Safety (PCRS)

First supervisor: Dr. I. van Sintemaartensdijk

Second supervisor: Dr. Ir. P. W. de Vries

August 30, 2024

Author Note

Correspondence concerning this student paper should be addressed to Dorien Brinkhof, Department of Psychology, University of Twente, Enschede, The Netherlands.

Dedication

Let us remember: One book, one pen, one child, and one teacher can change the world. May our efforts and perseverance pave the way for a more supportive and understanding environment for all studying mothers.

To all the daughters who will pursue their dreams while balancing the demands of motherhood. May you find the strength, support, and equality that every student deserves.

Acknowledgement

This journey's strength, like a family's strength, lies in the unwavering support and loyalty of those who stood by me. I am delighted to present this culmination of my master's degree journey in Psychology. This thesis marks a significant chapter's end, and I am profoundly grateful for the support I received along the way. While I have put significant effort into this project, it would not have been possible without the support of many individuals. Just like success has many fathers, this result also has many contributors deserving my gratitude.

Foremost, I would like to express my sincere gratitude to my adviser, Dr Iris van Sintemaartensdijk, for her continuous support, and guidance. Your knowledge helped me make a contribution to the field of cyberpsychology. You taught me the methodology to carry out this research. Your timely challenges helped elevate the level of my academic contribution. I would also like to thank Dr Peter de Vries, my second supervisor, for giving me insightful and valuable comments. You selflessly sacrificed your spare time for stimulating discussions.

To my loving and wonderful partner, you have demonstrated the utmost patience and understanding over the last six years. Your guidance, and encouragement, made sure I stayed on track. Your support year after year, especially when I was secluded behind my PC, has been invaluable. To my children, you are my inspiration to achieve greatness. I hope the sacrifices you have endured while I pursued this dream will be repaid to you with many opportunities for joy and success in your future. I apologize for being even grumpier than usual while writing this thesis. My heartfelt thanks go to my parents and parents-in-law for their unwavering support and love. Your patience and understanding, even when I became irrational and stubborn, have been deeply appreciated. Thank you for offering care for your grandchildren when I had to 'really work' again.

I would like to thank my friends who kept me sane during the ups and downs of this thesis. You let me share the obstacles I encountered and provided distraction when it was needed the most. The best of luck to you in all of your endeavors.

Last, but not least, the kindness of 53 people who valiantly filled out my online survey. You saved a desperate student from cacao-induced despair!

This academic journey has been transformative, providing profound insights into my identity and fostering personal growth. It takes a village to raise a child, and the same village – plus an exorbitant amount of chocolate – to raise a master's thesis.

Abstract

Phishing represents a significant cybersecurity threat, exploiting human vulnerabilities through deceptive emails. This study investigates how awareness of phishing and knowledge of persuasion techniques influence adults' susceptibility to phishing emails. It examines whether increased awareness and persuasion knowledge correlate with enhanced phishing detection. An online questionnaire collected data from 51 participants, who responded to phishing simulations before and after receiving theory-based instruction on persuasion tactics. The results revealed a moderate improvement in phishing detection skills post-instruction. However, initial awareness and persuasion knowledge varied among participants, influencing their ability to correctly identify phishing emails. Additionally, prior victimization was negatively associated with phishing awareness. These findings highlight the importance of integrating psychological support and robust digital infrastructure into cybersecurity training. Tailored educational approaches that consider diverse learning styles and demographics can significantly enhance cybersecurity resilience. This research underscores the value of combining theoretical insights with practical applications to strengthen individual defenses against phishing attacks.

Keywords: Phishing, Awareness, Persuasion Knowledge Framework (PKF), Cybersecurity, Susceptibility

Understanding the Human Dimension: The Role of Persuasion and Psychological Factors in Cyberattack Vulnerability

In an era dominated by digital connectivity, cyberthreats pose significant challenges to individuals and organizations. As our reliance on technology grows, so does the complexity of cyberattacks, with *phishing* remaining a prevalent form of cybercrime (Griffiths, 2024). Phishing, a form of social engineering, involves the social manipulation of people through psychological tricks to divulge confidential information or perform actions that compromise security (Frauenstein, 2013; Lin et al., 2019; Wang, Zhu, Liu, & Sun, 2021). Attackers leverage human psychology and emotions such as fear, urgency, and trust to manipulate victims into complying with their requests (Alsharnouby et al., 2015; Butavicius et al., 2016; Dhamija et al., 2006; Quinkert et al., 2021). Despite technological advancements, phishing continues to exploit human vulnerabilities through various channels, including emails, texts, and social media (Kumaran & Lugani, 2020). In 2021, over 320,000 internet users fell victim to phishing, leading to significant financial losses averaging \$136 per attack and totaling over \$44 million globally (Griffiths, 2024; Jain & Gupta, 2022). Phishing emails account for 91% of cyberattacks, with the efficacy of these attacks significantly influenced by the content of the message and surrounding circumstances (Bullée & Junger, 2020). This highlights the crucial role of targeted education programs in enhancing users' awareness and detection skills to combat fraudulent schemes effectively (Butavicius et al., 2016; Ferreira & Lenzini, 2015; Ferreira et al., 2015; Rajivan & Gonzalez, 2018).

Understanding and enhancing *awareness* of phishing tactics is critical in combating these attacks. Awareness encompasses the ability to recognize and respond to phishing attempts effectively (Blythe et al., 2011). Traditional cybersecurity efforts focused on technical solutions, such as firewalls, encryption, and antivirus software (Mitnick et al., 2011; Schaab et al., 2016; Tetri & Vuorinen, 2013; Wang, Zhu, Liu, & Sun, 2021). However, it has become increasingly clear that technical measures alone are insufficient without addressing the human element (Mitnick et al., 2011; Schaab et al., 2016; Wang, Zhu, Liu, & Sun, 2021). Effective security awareness training helps individuals recognize and avoid phishing attempts, thus enhancing overall security (Eminağaoğlu et al., 2009). Organizations now prioritize comprehensive training for all internet users due to the prevalence of human error in security breaches, with international standards emphasizing the need for regular awareness campaigns

(Nair & Greeshma, 2023; Scholtz et al., 2006; Wood, 1999). To support this, individuals should receive consistent education on security awareness and utilize various tools and mechanisms to improve security outcomes (Ashenden, 2008; Gehringer, 2002; Lacey, 2009; Williams, 2008).

The concept of *persuasion knowledge* provides a deeper understanding of how phishing attacks manipulate individuals. Persuasion knowledge involves recognizing and understanding the psychological techniques used to influence decision-making (Cialdini, 2009). Techniques such as reciprocity, commitment, social proof, authority, liking, and scarcity are often employed in phishing schemes to exploit cognitive biases and manipulate targets (Cialdini, 2009; Wang, Zhu, Liu, & Sun, 2021). Furthermore, Uebelacker and Quiel's (2014) research elucidates how these psychological principles can be strategically employed in social engineering attacks to exploit human vulnerabilities and achieve the attacker's goals. Increasing individuals' awareness of these persuasive tactics can empower them to better identify and resist deceptive attempts, highlighting the importance of integrating persuasion knowledge into cybersecurity training (Bauer & Bernroider, 2015; Heartfield & Loukas, 2015; Schaab et al., 2016).

This research examines the critical role of persuasion knowledge and awareness of digital phishing in shaping individuals' susceptibility to phishing attacks. Specifically, it addresses the research question: To what extent do awareness of email phishing and knowledge of persuasion influence individuals' susceptibility to phishing emails in private contexts? By investigating this question, the study aims to enhance our understanding of how persuasion knowledge influences the ability to recognize and resist phishing attempts. Furthermore, it seeks to advance the application of the Persuasion Knowledge Framework (PKF) within cybersecurity. This research aspires to bridge the gap between theoretical insights and practical applications, contributing significantly to the development of more effective educational strategies and cybersecurity measures.

Phishing

Information shared via personal computers and handheld devices presents security vulnerabilities that can compromise confidentiality, integrity, and accessibility. Users should actively safeguard their information assets against potential threats.

Social engineering exploits human psychology to manipulate individuals into assisting

attackers, often without their awareness. This technique exploits weaknesses in human reasoning through voice calls, emails, face-to-face interactions, and text messages (Heartfield & Loukas, 2015; Mitnick et al., 2011; Schaab et al., 2016; Tetri & Vuorinen, 2013; Wang, Zhu, & Sun, 2021; Wang, Zhu, Liu, & Sun, 2021). While technical hacking relies on breaching systems through code and software vulnerabilities, social engineering primarily focuses on exploiting human vulnerabilities. It uses psychological concepts equal to cognitive biases and persuasion tactics to manipulate individuals (Dhamija et al., 2006; Frauenstein, 2013) prompting them to inadvertently aid in the attack. Understanding the psychological underpinnings of social engineering can better equip individuals to recognize and resist these manipulative tactics, ultimately enhancing cybersecurity.

Phishing is widely recognized as a prevalent form of social engineering. It leverages deceptive emails to deceive victims into disclosing sensitive information or performing actions that compromise security (Frauenstein, 2013; Lin et al., 2019; Wang, Zhu, Liu, & Sun, 2021). These attacks often exploit cognitive biases, such as confirmation bias and the availability heuristic, leveraging principles such as authority, social proof, similarity, and commitment to manipulate recipients' social norms (Ferreira & Lenzini, 2015; Ferreira et al., 2015; Schaab et al., 2016). For example, an attacker might send an email appearing to come from a trusted source, such as a bank, prompting the recipient to click a link and enter their login details on a spoofed website. Users commonly struggle to differentiate between legitimate and spoofed websites (Dhamija et al., 2006) due to these persuasive techniques. These emails often employ urgent language and familiar professional logos to enhance legitimacy and evoke an immediate emotional response, exploiting the recipient's trust. Phishing attacks illustrate how attackers combine sophisticated technical emails and website designs with persuasive strategies to gain the confidence of their targets, demonstrating the intricate blend of technology and psychology in cybercrime.

Phishing operates on a high volume, low success rate strategy, with an approximate success rate of 36% (Palatty, 2024).

Susceptibility to phishing attacks involves psychological, behavioural, and demographic factors affecting individual's vulnerability to phishing emails. Alsharnouby et al. (2015) explored how awareness of digital phishing, and persuasion knowledge impact phishing susceptibility, defined as the inability to identify phishing emails (e.g.,(Moody et al., 2017;

Ribeiro et al., 2024; Vishwanath et al., 2018). Understanding these factors is crucial for developing effective strategies to combat phishing attacks, as they provide insights into individuals' motivations to trust and respond to deceptive messages. Bridging this understanding with practical applications helps tailor awareness programs more effectively.

Blythe et al. (2011) emphasised the importance of understanding how individuals fall for phishing scams despite educational campaigns, noting that phishing emails are becoming more convincing by using logos and minimising spelling mistakes. Similarly, Köhler et al. (2023) suggested that awareness measures play a crucial role in phishing detection and discuss the impact of previous training on individuals' ability to identify phishing emails. Both emphasize the significance of considering individuals' awareness levels and contextual factors, including language, logos, urgency, and content alignment, in detecting phishing emails effectively. This research underscores the need for individuals to be aware of evolving phishing tactics and focusing on understanding contextual cues that may be missing in phishing attempts. Thus, transitioning from understanding phishing tactics to effectively recognizing and responding to such attacks requires a nuanced comprehension of both technological defenses and human cognitive vulnerabilities.

Recognizing and Responding to Digital Phishing Attacks

Transitioning from understanding phishing tactics to effectively recognizing and responding to such attacks requires a nuanced comprehension of both technological defenses and human cognitive vulnerabilities. Awareness of digital phishing refers to individuals' knowledge of phishing tactics and risks, as well as their ability to recognize suspicious emails (Alsharnouby et al., 2015; Blythe et al., 2011). The core objective of cybersecurity awareness is to empower individuals to respond securely to potential threats. Enhanced awareness serves as a critical defense against phishing attacks, as those well-versed in phishing strategies are more adept at recognizing and avoiding such attempts. (Alkhalil et al., 2021; Alwanain, 2019; Dhamija et al., 2006). This definition of phishing awareness has essential components, and a pivotal role of education in reducing phishing risks.

General security orientation refers to an individual's overall awareness, knowledge, and attitudes towards cybersecurity. According to Knapova et al. (2021), fostering a general security orientation is crucial in promoting secure behaviours, including recognizing phishing attempts. Individuals with a strong general security orientation are more likely to be proactive

about security practices, such as regularly updating settings, being cautious about sharing personal information, and staying informed about common cyberthreats. This proactive stance heightens their awareness of various security threats, including phishing attacks.

Research has shown that a strong security orientation positively impacts phishing detection abilities. A study by Arachchilage and Love (2014) found that users with higher levels of security awareness were better able to identify phishing attempts, with security training improving participants' ability to detect phishing by 40%. Furthermore, Knapova et al. (2021) highlight that individuals who perceive security threats as more severe are more likely to engage in secure behaviours. In the context of phishing, those who understand the potential consequences of falling victim to such attacks (e.g., financial loss, identity theft) are more vigilant and cautious when interacting with suspicious emails or messages. Thus, awareness of the seriousness of security threats enhances individuals' ability to recognize phishing attempts and respond effectively by being alert to the tactics used by cybercriminals, such as urgent requests for personal information and deceptive links.

Threat perception involves an individual's assessment of the risks and potential consequences associated with phishing attacks. Jansen and Van Schaik (2018) demonstrated that higher threat perception was correlated with more protective behaviors against phishing, such as verifying sender identities and scrutinizing URLs. Integrating general security orientation with heightened threat perception fosters a culture where security is a shared responsibility. Individuals with a robust security orientation and strong threat perception are more proactive in identifying and reporting phishing attempts, thus contributing to a collective security posture. Additionally, utilizing feedback from phishing simulations and real incidents to refine training programs ensures that the awareness framework evolves with emerging threats. This continuous improvement loop helps maintain a high level of vigilance among individuals.

Educational initiatives play a crucial role in enhancing phishing awareness. Various anti-phishing training initiatives have been implemented. Some of these initiatives have shown positive outcomes (Dodge et al., 2007; Kumaraguru et al., 2009, 2010; Sheng et al., 2007), demonstrating that education can enhance awareness levels. However, certain interventions have demonstrated limited impact (Caputo et al., 2014; Davinson & Sillence, 2010), and some studies have highlighted potential negative effects of interventions (Junger et al., 2017;

Kearney & Kruger, 2014; Wolff, 2016; Zhang et al., 2014). A critical appraisal revealed that enterprises without awareness training performed 12% better than those with training programs (Ceesay et al., 2018). This mixed evidence underscores the complexity of enhancing awareness and the necessity of refining these strategies. Comprehensive measurement of awareness levels before and after interventions remains a challenge, complicating comparisons and assessments of program effectiveness. Most research focuses on raising awareness through educational programs without adequately assessing the baseline awareness levels of individuals prior to the intervention, making it difficult to compare the effectiveness of these programs accurately.

In conclusion, awareness of digital phishing is fundamental in defending against phishing attacks. Enhanced knowledge of phishing tactics enables individuals to recognize and avoid suspicious emails, thereby reducing vulnerability. Despite the emphasis on awareness in cybersecurity studies, the effectiveness of educational interventions remains inadequately measured, with gaps in understanding baseline awareness levels and specific knowledge impacts. While various training initiatives have shown some success, their mixed results highlight the complexity of improving awareness and the need for more rigorous evaluation. This underscores the necessity of refining these strategies and understanding the factors that contribute to their success, such as incorporating a general security orientation and threat perception, which can significantly enhance an individual's ability to recognize and respond to phishing attempts.

Moreover, understanding how individuals recognize and respond to phishing attempts involves more than just awareness of phishing tactics; it also requires knowledge of the underlying psychological principles that make these tactics effective. This brings us to the concept of persuasion knowledge, which is critical in identifying and countering deceptive messages.

Persuasion Knowledge Framework

Incorporating the Persuasion Knowledge Framework into this exploration of phishing provides a nuanced understanding of the cognitive processes involved in identifying and countering deceptive tactics. Understanding persuasion is crucial in a wide array of human interactions, from marketing to cybersecurity, as it reveals the mechanisms of influence that shape behaviour. In cybersecurity, phishing represents a critical threat that exploits these

persuasive mechanisms to deceive individuals. The *Persuasion Knowledge Framework* (PKF) offers a theoretical lens for understanding how individuals recognize and respond to such persuasive attempts, such as phishing emails. Specifically, the PKF examines the interaction between the target (individual) and the agent (cybercriminal) (Friestad & Wright, 1994), highlighting how awareness of persuasion tactics can empower individuals to identify and resist phishing attempts. This framework highlights how individuals' awareness of persuasion tactics empowers them to recognize and counter misleading claims and emails, while cybercriminal agents strategically exploit these tactics (Ham et al., 2015). By exploring the PKF in the context of phishing, this research seeks to shed light on the psychological strategies used by cybercriminals and the role of persuasion knowledge in enhancing individuals' resilience against such attacks.

Previous studies demonstrated that acquiring persuasion knowledge enables individuals to accurately identify marketers' underlying motives in a persuasion episode (Ham et al., 2015; Nelson & Park, 2014; Xie & Johnson, 2015). This principle extends to recognizing the motives behind phishing emails, where similar psychological techniques are employed to deceive individuals. Persuasion knowledge encompasses three key types of knowledge: topic knowledge, agent knowledge, and persuasion knowledge. Topic knowledge refers to an individual's understanding of the relevant subject, such as financial services or account security. Agent knowledge involves awareness of the characteristics, motives, and tactics of the persuader, in this case, cybercriminal. Persuasion knowledge relates to the general understanding of how persuasion works and the strategies employed in persuasive attempts (Amazeen & Krishna, 2022; Rahmani, 2023). By integrating these types of knowledge, individuals can better evaluate and respond to phishing attempts. Their awareness of cybercriminal tactics, along with their understanding of relevant topics, significantly influences their ability to distinguish phishing attempts from legitimate communications.

Persuasion attempts not only activate but also shape individuals' persuasion knowledge, making persuasive tactics more transparent (Amazeen & Krishna, 2022; Ham et al., 2015). Exposure to phishing incidents updates individual's knowledge about cybercriminals (agent), including the nature of common phishing sources (e.g., whether a bank would send an email in a particular manner) and the deceptive practices used (persuasion knowledge) (Amazeen & Krishna, 2022). Consequently, individuals continuously integrate and

refine all three types of knowledge — persuasion, agent, and topic knowledge — to more effectively evaluate and respond to phishing attempts effectively. Individuals' awareness and persuasion knowledge are not static but continuously evolve through exposure to phishing attempts. This evolving knowledge creates a positive feedback loop, where increased awareness enhances their ability to discriminate between phishing attempts and legitimate communications. As individuals gain renewed insights into account security, financial services, and related topics, their capacity to interpret and differentiate phishing claims improves. For cybercriminals, a persuasion episode involves the attempt to deceive and manipulate their targets. Conversely, for individuals, it involves developing and applying coping behaviours and strategies to recognize and resist these deceptive attempts.

The PKF's versatility spans various contexts including sales (Campbell & Kirmani, 2000), pricing strategies (Das et al., 2020; Hardesty et al., 2007), charity advertising (Germelmann et al., 2020; Hibbert et al., 2007), product placement (Boerman et al., 2017; Wei et al., 2008), digital marketing (Chen & Cheng, 2019), and online misinformation (Amazeen & Krishna, 2022). However, its integration into cybersecurity, particularly in combating phishing, remains underexplored. This underscores the need for research into how persuasion knowledge can be leveraged to mitigate cyberattacks such as phishing.

Researchers have recognized the importance of psychological principles in understanding and combating social engineering attacks such as phishing. Ferreira et al. (2015) synthesized principles from Cialdini (2009), Gragg (2003) and Stajano et al. (2011) into a framework for analyzing social engineering attacks, including phishing emails. Similarly, Van der Heijden and Allodi (2019) use principles introduced by Cialdini to build a classifier that estimates the likelihood of an individual falling for a phishing email, which helps response teams prioritize incoming threats. Additionally, Williams et al. (2018) conducted studies on the effects of urgency and authority in emails, further highlighting the role of psychological triggers in phishing attacks. Schaab et al. (2016) emphasized that current security defense mechanisms often overlook the psychological aspects behind social engineering and user psychology. They stressed the importance of incorporating these principles to enhance defense mechanisms effectively.

Understanding how persuasion works can help individuals defend themselves against deceptive tactics used in cyberattacks. By learning about these psychological principles,

individuals can better recognize and resist attempts to manipulate them online. This approach aligns with Schaap's (2016) focus on addressing the psychological aspects of social engineering to strengthen defense mechanisms and reduce the overall risk posed by such attacks.

Additionally, the Persuasion Knowledge Model highlights individuals' coping behaviours and their ability to choose response tactics from their own repertoire, applicable to phishing emails. Understanding these coping mechanisms, including cognitive and physical actions and their interpretation of an attacker's persuasion behaviour, provides valuable insights into effective strategies for mitigating the impact of phishing attacks (Friestad & Wright, 1994).

The Current Study

The goal of this study is to investigate the influence of awareness and persuasion knowledge on individuals' susceptibility to email phishing in private contexts. Participants will engage in an online questionnaire designed to assess their baseline awareness of digital phishing tactics and their level of persuasion knowledge. Subsequently, participants will engage in a knowledge transfer session focused on phishing and persuasion tactics. Following the intervention, participants will again receive simulated phishing emails to evaluate any changes in their awareness level and ability to differentiate between phishing attempts and legitimate messages.

By conducting these assessments before and after the intervention, this study aims to provide a comprehensive understanding of the actual gain in knowledge resulting from the intervention. This approach will enable a more accurate evaluation of the effectiveness of educational strategies in enhancing cybersecurity awareness and reducing susceptibility to phishing attacks. It takes into account both initial awareness levels and the role of specific knowledge, such as persuasion knowledge. Based on gaps identified in the literature and the theoretical considerations as outlined heretofore, the following hypotheses are formulated:

H1: Participants with a high level of awareness of phishing are expected to exhibit lower susceptibility for phishing.

H2: Participants with high levels of persuasion knowledge are expected to exhibit lower susceptibility for phishing.

H3: Exposure to theory on persuasion techniques will enhance participants' ability to

distinguish phishing emails from legitimate emails.

H4: The effect of exposure to theory on distinguishing phishing emails from legitimate emails will be stronger among participants with initially lower levels of phishing awareness than those with initially higher levels of phishing awareness.

H5: The effect of exposure to theory on distinguishing phishing emails from legitimate emails will be stronger among participants initially possessing lower levels of persuasion knowledge compared to those possessing initially higher levels of persuasion knowledge.

Method

An online questionnaire was utilized to investigate the relationship between persuasion knowledge, awareness, and human vulnerabilities in the context of cybersecurity, particularly in response to phishing emails. The online format enabled efficient data collection and facilitated the inclusion of a diverse participant sample.

Design

The research implemented a pretest - posttest correlational design using the Qualtrics platform. The variables were classified into three broad categories: independent variables (Agent Knowledge, Persuasion Knowledge), according to the Persuasion Knowledge Framework (Friestad & Wright, 1994), the dependent variable (User's susceptibility to phishing email attacks) operationalized as the participants' confidence in identifying phishing emails, and modifying factor (Awareness) regarding cybersecurity threats. User's susceptibility to phishing email attacks measured people's confidence in identifying phishing emails. Both the independent variables (Agent Knowledge, Persuasion Knowledge) and the modifying factors (Awareness) were measured to understand their relationship with the dependent variable.

Participants

Participants were recruited from personal social networks and the University of Twente's Sona-platform, allowing for a diverse sample from various regions. Snowball sampling within personal networks expanded the participant pool. This method may have introduced sampling bias, as participants from similar backgrounds may have been more likely to be recruited, potentially limiting generalisability. Eligibility criteria included being at least

18 years old, having internet access, and understanding English. The required sample size of 26 participants (Button et al., 2013a, 2013b, 2013c; Faul et al., 2009) was calculated based on a power analysis with an effect size of 0.8 and a significance level of 0.05.

A convenience sample of the general population was recruited, comprising 53 participants. Descriptive statistics were conducted to examine the demographic characteristics of the participants. The majority of participants fell within the age range of 18-27 years old ($N = 20$, $M = 34.55$, $SD = 3.17$), with a slightly higher proportion of women ($N = 35$) compared to men ($N = 16$). Regarding educational background, most participants held a Master's degree ($N = 14$). Additionally, out of 51 participants, many reported having good internet access ($N = 25$) and a neutral competence level of cybersecurity knowledge ($N = 25$). The majority of participants reported a (potential) history of cybercrime victimization ($N = 26$) and daily email usage ($N = 28$). Table 1 provides a complete overview of the demographic characteristics of the participants, including ratings of internet access, knowledge of cybersecurity, prior experience with cybercrime, and email usage.

Table 1*Descriptive Statistics for Demographic Variables*

Variable	Category	N	Percentage (%)	Mode
Age	18-27 years old	20	39	18-27 years old
	28-37 years old	9	18	
	38-47 years old	7	14	
	48-57 years old	10	20	
	58-67 years old	2	4	
	68-77 years old	2	4	
	78 or older	1	2	
Gender	Male	16	31	Female
	Female	35	69	
Education	No degree	0	0	Master's degree
	Primary school	0	0	
	High school	12	24	
	Vocational school	2	4	
	University of applied sciences degree	8	16	
	Bachelor's degree	13	25	
	Master's degree	14	27	
Internet Access	PhD degree	2	4	Good
	Terrible	0	0	
	Poor	2	4	
	Average	11	22	
	Good	25	49	
Cybersecurity Knowledge	Excellent	13	25	Neutral
	Extremely incompetent	2	4	
Cybersecurity Knowledge	Somewhat incompetent	7	14	Neutral
	Neutral	25	49	
	Somewhat competent	17	33	
	Extremely competent	2	4	
Cybercrime Victim	No	25	49	No
	Don't know	19	37	
	Yes	7	14	
Email Usage	Never	0	0	Daily
	Biweekly	0	0	
	Weekly	10	20	
	Daily	28	55	
	Hourly	13	25	

Participants recruited via the Sona-platform received 0,25 point for participation. Upon completion of the survey, participants were debriefed.

Materials

Cybercrime Awareness Scale (CAS)

The Cybercrime Awareness Scale (CAS) measured the level of cybercrime awareness with 41 items scored on a five-point Likert-type scale ranging from *strongly disagree* (1) to *strongly agree* (5) (Arpaci & Ateş, 2022). The CAS was designed to measure awareness on a scale from 41 to 205, with higher scores indicating a higher level of cybercrime awareness. Sample items include "I know that engaging in qualified interactive fraud in cyberspace is a crime," "Violating confidentiality of communication between people is a crime", and "It is a crime to use software that violates license agreement in cyberspace".

Summing the scores highlighted the cumulative effect of all items on the scale, representing the overall level of cybercrime awareness for each participant. Since each item contributed equally to the total score, the sum reflected the combined influence of all dimensions of cybercrime awareness, providing a holistic and straightforward view of the participants' understanding. This made the scoring system more intuitive for interpreting overall awareness levels. The overall scale demonstrated excellent reliability (41 items, $\alpha = .91$, $M = 157.35$, $SD = 20.60$), indicating a moderate to high level of cybercrime awareness among the participants.

The CAS was analyzed across various demographic variables. Table 2 presents the summary of CAS scores by *age* group. Notably, the highest mean CAS score was observed in participants aged 78 or older ($M = 200.00$), although this group had only one participant. Table 3 summarizes CAS scores by *gender*, showing that women ($M = 159.00$, $SD = 22.20$) scored slightly higher on average compared to men ($M = 154.00$, $SD = 16.80$). *Educational level*, as summarized in Table 4, indicates that participants with vocational school education had the highest mean CAS score ($M = 173.00$), although this group also had a small sample size. This is an anomaly that might warrant further investigation to understand underlying reasons. Variability in CAS scores is higher in some education categories, like "Master's degree" with a high standard deviation ($M = 151.00$, $SD = 24.8$), suggesting a broader range of scores within that group. Table 5 displays CAS scores by *Internet Access* quality, where participants with *poor* internet access had the highest mean score ($M = 168.00$). In terms of

Cybersecurity knowledge, summarized in Table 6, those who identified as somewhat incompetent had a lower mean CAS score ($M = 149.00$) compared to those who were somewhat competent ($M = 158.00$) and extremely competent ($M = 154.00$). Finally, Table 7 presents the summary of CAS scores by *Cybercrime victim* status. Participants who had been victims of cybercrime had higher mean CAS scores ($M = 166.00$) compared to those who had not ($M = 161.00$). Regarding *Email usage*, Table 8 shows that those who used email daily had the highest mean CAS score ($M = 160.00$).

Table 2

Summary of Cybercrime Awareness Scale Scores by Age

Age	<i>N</i>	<i>M</i>	<i>SD</i>	Min	Max
18-27 years old	20	153	21.20	119	194
28-37 years old	9	165	24.10	122	197
38-47 years old	7	157	20.00	126	184
48-57 years old	10	153	13.30	133	171
58-67 years old	2	165	24.00	148	182
68-77 years old	2	162	20.50	147	176
78 or older	1	200	-	200	200

Table 3

Summary of Cybercrime Awareness Scale Scores by Gender

Gender	<i>N</i>	<i>M</i>	<i>SD</i>	Min	Max
Male	16	154	16.80	126	200
Female	35	159	22.20	119	197

Table 4*Summary of Cybercrime Awareness Scale Scores by Education Level*

Education	<i>N</i>	<i>M</i>	<i>SD</i>	Min	Max
High school	12	160	24.50	121	200
Vocational school	2	173	–	173	173
University of applied sciences degree	8	154	14.10	138	182
Bachelor's degree	13	160	16.10	126	183
Master's degree	14	151	24.80	119	197
PhD degree	2	166	26.20	147	184

Table 5*Summary of Cybercrime Awareness Scale Scores by Internet Access*

Internet Access	<i>N</i>	<i>M</i>	<i>SD</i>	Min	Max
Poor	2	168	10.60	161	176
Average	11	151	25.00	119	194
Good	25	158	19.10	121	200
Excellent	13	159	21.30	128	197

Table 6*Summary of Cybercrime Awareness Scale Scores by Cybersecurity Knowledge*

Cybersecurity Knowledge	<i>N</i>	<i>M</i>	<i>SD</i>	Min	Max
Somewhat incompetent	7	149	27.60	121	185
Neutral	25	159	17.60	119	194
Somewhat competent	17	158	22.40	126	200
Extremely competent	2	154	23.30	138	171

Note. Neutral = Neither competent nor incompetent.

Table 7*Summary of Cybercrime Awareness Scale Scores by Cybercrime Victim Status*

Cybercrime Victim Status	<i>N</i>	<i>M</i>	<i>SD</i>	Min	Max
No	25	161	21.20	126	200
Don't know	19	150	15.50	119	178
Yes	7	166	26.20	121	197

Table 8*Summary of Cybercrime Awareness Scale Scores by Email Usage*

Email Usage	<i>N</i>	<i>M</i>	<i>SD</i>	Min	Max
Daily	30	160	20.00	130	200
Weekly	20	155	18.50	125	190
Monthly	10	150	22.30	120	180
Rarely	5	145	25.00	110	170

Persuasion Knowledge (PK)

Beliefs about persuasion were scored on a 5-point Likert-scale (*strongly disagree - strongly agree*). This custom-made scale contained 11 items like "I know that phishing emails try to trick people into doing certain things, like clicking on harmful links or giving away personal information", "I must be attentive about detecting deceptions by responding to emails", and "I know when a cybercriminal is pressuring me to provide private information."

The Persuasion Knowledge (PK) scale was developed by adapting existing questions (Bearden et al., 2001; Hendriks, 2023; Scott et al., 2013) from previous research to focus on cybercrime and phishing contexts. This adaptation process involved transforming persuasion knowledge questions into items specifically related to phishing. The primary reason for adapting these existing items was the lack of established items specifically targeting persuasion knowledge in the context of phishing. By leveraging validated items from related domains and contextualizing them to cybercrime, the PK scale aims to provide a robust measure of individuals' awareness and detection of phishing and cybercrime tactics. The 11 items were administered both pre-intervention and post-intervention. For the

post-intervention only the prompt was modified slightly so that it was assured participants would answer now with the theory in mind (see Appendix A).

The reliability analysis revealed that items PRE-1-5 and POST-1-5 displayed negative correlations with the first principal component, suggesting the need for their removal. After excluding these items from the dataset, the reliability coefficients for pre- and post-theory PK were recalculated. For pre-theory PK, the alpha coefficient was found to be .87 (10 items, $M = 43.18$, $SD = 5.71$) indicating good internal consistency. Following the updated post-theory reliability analysis, the Cronbach's alpha coefficient for the PK was determined to be .91, indicating excellent internal consistency (10 items, $M = 40.90$, $SD = 11.95$).

Exploratory Factor Analysis (EFA) was conducted on all 11 items of the Persuasion Knowledge scale for both the pre-test and post-test data. This analysis aimed to assess the relationship among the items and identify underlying factors. Since it was uncertain whether the intervention affects the factor structure of Persuasion Knowledge, conducting separate factor analyses for pre-test and post-test data was considered to be insightful into any potential changes or stability in participants' understanding of persuasion knowledge. Although Principal Component Analysis (PCA) could explain the maximum variance, EFA was chosen due to the uncertain theoretical basis for item classification.

For the pre-test, Bartlett's test of sphericity indicated that the correlations between items were sufficiently large for factor analysis, $\chi^2 = 309.29$, $df = 55$, $p < .001$. The Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy was .77, suggesting the sample was adequate for factor analysis. A parallel analysis suggested that three factors should be retained, as three factors had eigenvalues greater than those obtained from randomly generated data. In contrast, a scree plot indicated that two factors had eigenvalues greater than 1 in the factor analysis (5.10 and 1.58), and three factors had eigenvalues greater than 1 in the principal components analysis (5.10, 1.58, and 1.18 respectively). A Principal Axis Factoring factor analysis with Oblimin rotation was performed on the 11-item PK scale. The results revealed a clear factor structure with three factors explaining 55% of the total variance. The communalities ranged from .13 to .77, indicating that the majority of items had substantial common variance. The proportion of variance explained by Factor 1 was 46%, Factor 2 explained 14%, and Factor 3 explained 11% of the variance. These findings suggest that the PK scale primarily measures a multi-dimensional construct with two dominant

factors. One potential interpretation is that the first factor relates to knowledge of various phishing tactics, while the second factor pertains to the ability to detect and respond to these tactics effectively. Understanding these factors provides deeper insight into the components of persuasion knowledge in the context of phishing emails.

For the post-test, Bartlett's test of sphericity was performed to examine the suitability of the data for factor analysis. The test was significant, $\chi^2 = 393.38$, $df = 55$, $p < .001$, indicating that the correlation matrix was not an identity matrix and thus suitable for factor analysis. The Kaiser-Meyer-Olkin (KMO) measure was 0.83, indicating excellent sampling adequacy. A scree plot and parallel analysis were conducted to determine the number of factors to extract. The scree plot suggested that two factors had eigenvalues greater than 1. Parallel analysis indicated that the number of factors to retain was one. Given the theoretical model and the results from the parallel analysis and scree plot, a Principal Axis Factoring (PAF) with Oblimin rotation was performed on PK scale. The communalities ranged from .04 to .86, indicating that the majority of items had substantial common variance. The first two factors had eigenvalues of 5.873 and 1.274, respectively. The two factors explained 53% and 12% of the variance, cumulatively accounting for 65% of the total variance. The post-test factor analysis identified two factors explaining 65% of the variance: practical skills for recognizing and responding to phishing attacks and general phishing knowledge. This shift from a three-factor to a two-factor model suggests that the intervention effectively integrated participants' understanding of phishing. By focusing on practical application and overall awareness, the session likely helped consolidate various aspects of phishing knowledge into a unified framework. This indicates the intervention's success in enhancing both theoretical understanding and practical skills.

The mean PK before the intervention (10 items, $M = 43.18$, $SD = 5.71$) was compared to the mean score after the intervention (10 items, $M = 40.90$, $SD = 11.95$). The mean difference between the post-intervention and pre-intervention scores was -2.35, indicating a slight decrease in scores after the intervention.

Agent Knowledge (AK)

To assess participants' perceptions of cybercriminals' characteristics, skills, and objectives in phishing emails, two scales (Advertiser's Benefits and Advertiser's Investments) of the Inferences of Manipulative Intent (IMI) questionnaire were adapted from Campbell

(1995) (see Appendix B). IMI focuses on the relatively negative aspect of persuasion agents' manipulative intent. Since phishing is always manipulative and negative, it was considered appropriate to use in the present context. The original context was changed from advertisers to cybercriminals and from advertisements to phishing emails. The items were measured on a 5-point Likert scale (*strongly disagree - strongly agree*) and each scale included 5 items.

Cybercriminal's Benefits scale (AKCB) assessed participants' beliefs about what the cybercriminal aims to achieve, such as financial gain or data theft (e.g., "Compared to most emails, the sender has high expectations about the impact this email will have on me"). This scale focused on the perceived outcomes that cybercriminals expect to gain from their phishing attempts. The Cybercriminal's Investments scale (AKCI) evaluated participants' perceptions of the effort and resources the cybercriminal has invested in the phishing attempt (e.g., "The sender seems to have put a lot of time into phishing email."). This scale measured the perceived effort and resources cybercriminals are willing to invest to achieve their objectives. By measuring these distinct aspects - benefits and investments - it was possible to gain a comprehensive understanding of how participants judged the intent behind phishing emails and inferred manipulative intent based on the perceived balance between benefits and investments. This nuanced understanding helped in developing more targeted and effective cybersecurity training and interventions. The individual items within each scale were aggregated to calculate an overall score for that particular scale. Item AKCI4 followed a reversed scoring scheme and hence needed to be reversely coded.

The Cybercriminal's Benefits scale (AKCB) demonstrated a moderate reliability coefficient of .49 ($M = 18.71$, $SD = 2.89$). AKCI, demonstrated a moderate reliability coefficient of = .56 ($M = 15.94$, $SD = 3.20$), though these values are lower than the original scale reliabilities of $\alpha = .71$, and $\alpha = .83$, respectively (Campbell, 1995). The average item correlation for AKCB was .16, and .20 for AKCI. Following this item analysis, AKCB-5 was excluded due to low correlations (-.02) with the respective scale AKCB. After removing this problematic item, the AKCB subscale (4 items) had a Cronbach's alpha of .70 ($M = 16.06$, $SD = 2.74$), and an improved average item correlation of .37. The correlation between the AKCB and AKCI subscales decreased from 0.25 after correction for attenuation to .15, indicating that the scales are less overlapping and more differentiated. This reduction aligns with the theoretical expectation that AKCB and AKCI should measure different aspects or

levels of agent knowledge.

Prior to conducting EFA, the KMO measure of sampling adequacy (10 items, .55) and Bartlett's test of sphericity ($\chi^2 = 115.78$, $df = 45$, $p < .001$) were computed to assess the suitability of data for factor analysis. Results indicated moderate to good sampling adequacy and that the correlation matrix was not an identity matrix and thus suitable for factor analysis. The scree plot suggested a 2-factor solution with eigenvalues of 2.16 and 1.11. According to the parallel analysis, both two factors and three components were suggested by the data. Principal Axis Factoring (PAF) with Oblimin rotation was employed to extract factors from the items. The analysis revealed a clear separation between the AKCB and AKCI scales. It was found that AKCI4 did not load significantly on Factor 1, indicating that it does not contribute strongly to the underlying construct represented by Factor 1. Similarly, AKCB5 did not load significantly on Factor 2, suggesting it does not align well with the underlying construct represented by Factor 2. The fact that AKSI4 and AKSB5 were not loading well in factor analysis and were also problematic in terms of reliability suggests consistency in the findings across different analyses. As a result, their exclusion from both factor analysis and reliability checks supports the decision to potentially remove them from the scales or to interpret them cautiously.

Email Judgment

To assess the ability to distinguish phishing emails from legitimate emails, participants rated their confidence that a presented email was a phishing email (see Appendix C). This was done using 10 email examples (six phishing and four legitimate) with confidence ratings on a 5-point scale, ranging from *not confident at all* (1) to *very confident* (5).

A participant's response of 1 (*Not confident at all*) for a phishing email indicated low confidence in identifying it as a phishing attempt, suggesting potential difficulty in distinguishing phishing emails from legitimate ones. Conversely, a response of 5 (*Very confident*) for a phishing email suggested high confidence in identifying it as phishing, indicating good phishing detection ability.

For legitimate emails, the scoring was interpreted inversely. A response of 1 (*Not confident at all*) for a legitimate email suggested high confidence in recognizing it as legitimate, indicating a strong belief that the email is indeed legitimate. Conversely, a response of 5 (*Very confident*) for a legitimate email suggested difficulties in recognizing it as

legitimate, perhaps being overly cautious or uncertain.

To quantify participants' ability to distinguish between phishing and legitimate emails, correctness scores were computed based on their confidence ratings. Given the distinct nature of phishing and legitimate emails, correctness scores were calculated separately for each category for each participant. Notably, responses for legitimate emails were inverted to align with the interpretation that higher total confidence scores reflect better discrimination ability.

The second time, post-intervention, participants were asked to rate different phishing (six) and legitimate (four) email examples using the same 5-point scale (see Appendix D). The mean pre-intervention correctness score was $M = 32.06$ ($SD = 10.31$), while the mean post-intervention correctness score was $M = 29.9$ ($SD = 10.75$), indicating the effectiveness of the intervention in altering participants' email judgment ability.

HEXACO-60 Personality Test

The 60-item brief HEXACO inventory was utilized to evaluate six aspects of personality (Ashton & Lee, 2009): Honesty-Humility ($\alpha = .67$, $M = 28.11$, $SD = 6.99$), Emotionality ($\alpha = .83$, $M = 30.11$, $SD = 7.50$), Extraversion ($\alpha = .76$, $M = 29.14$, $SD = 7.19$), Agreeableness ($\alpha = .80$, $M = 28.75$, $SD = 7.24$), Conscientiousness ($\alpha = .75$, $M = 29.59$, $SD = 7.48$), and Openness to Experience ($\alpha = .68$, $M = 30.55$, $SD = 7.33$) using a rating scale ranging from 1 to 5 (*strongly disagree - strongly agree*). Some items were reversely coded. Although the HEXACO was initially intended for additional analyses, it ultimately served as an intermission, providing a brief cognitive break before the repetition of persuasion knowledge questions and email judgments. Higher scores represented a greater disposition of a trait.

Procedure

The study has been approved by the Behavioural, management and Social sciences (BMS) Ethics Committee of the University of Twente (request number: 240362). Participants have accessed the survey via a Qualtrics link. After providing informed consent, they have answered questions from the Cybercrime Awareness Scale, demographic questions, Persuasion Knowledge Framework, and Email Judgments. Next, participants have learned the theory (see Appendix E) followed by the HEXACO-60 Personality Test. This intermission has provided a brief delay before repeating persuasion knowledge questions and email judgments. Next, participants have answered the same set of persuasion knowledge questions based on the

theory they had learned. They have reviewed a different set email examples. The survey has concluded with a debriefing statement. The survey took approximately 53.25 minutes to complete. Participants' responses have been securely stored on Qualtrics. Data have been collected within a period of four weeks.

Results

Preliminary Analyses

All data were statistically analysed using the R Statistical software version 2024.04.0 (RStudio Team, 2024). Of the 53 participants in the survey, two participants were excluded for not completing the survey for at least 60%. The remaining 51 participants formed the total convenient sample for the analysis.

Persuasion Knowledge (PK)

To determine the effectiveness of the intervention on participant's *persuasion knowledge* (PK), a paired samples *t*-test was employed. This test was chosen for its ability to compare PK scores before and after the intervention within the same group of participants. By using a paired samples *t*-test, we could control for individual differences and accurately measure changes attributable to the intervention. The paired samples *t*-test results revealed no statistically significant difference between the post-intervention and pre-intervention total scores of the PK scale ($t(50) = -1.343, p = .19$).

Main Analyses

Hypothesis 1. Hypothesis 1 (H1) posited that participants with a higher level of awareness of phishing (as measured by the Cybercrime Awareness Scale, CAS) would be less susceptible to phishing, demonstrated by higher pre-intervention correctness scores.

To test this hypothesis, a linear regression analysis was conducted with the *pre-intervention correctness score* as the dependent variable and the *CAS* score as the independent variable ($\beta = -.034, SE = .03, p = .327$). These findings do not support Hypothesis 1. Despite the expectation that individuals with higher awareness of phishing would be less susceptible to phishing (as indicated by higher correctness scores), the results indicate no significant relationship between the level of phishing awareness and the ability to discern phishing emails from legitimate ones before any intervention. The model explained a significant portion of the variance in the *pre-intervention correctness scores*, $R^2 = .70$, adjusted

$R^2 = .45$, $F(23, 27) = 2.76$, $p = .006$. Several predictors were significant in the model.

The decision to conduct additional analyses beyond testing Hypothesis 1 (H1) was driven by the need to comprehensively explore factors influencing participants' pre-intervention ability to discern phishing emails from legitimate ones. The initial regression analysis focused on *Cybercrime Awareness Scale* (CAS) scores did not support H1, indicating no significant relationship between phishing awareness and *pre-intervention correctness scores*. Subsequently, a multiple regression analysis was performed to examine the collective influence of demographic factors (*age, gender, education*), technological factors (*internet access, cybersecurity knowledge, cybercrime victim status, and email usage*) together with the CAS score on participants' pre-intervention performance. This approach allowed for a more nuanced understanding of the predictors contributing to phishing susceptibility among the study participants. These results are detailed below.

Gender Differences. Women scored significantly higher on *pre-intervention correctness* ($\beta = 4.549$, $SE = 1.56$, $p = .007$) compared to men. The mean *pre-intervention correctness* scores for men was 33.2 ($SD = 5.91$), and for women 33.5 ($SD = 4.51$). *Gender* is a categorical variable in this analysis, where each category represents distinct groups without inherent order. The Type II analysis of variance (ANOVA) revealed a significant effect of *gender* on the ability to distinguish phishing emails from legitimate emails, $F(1,27) = 8.498$, $p = .007$. The effect size, eta squared (η) was .24. Post hoc comparisons using Tukey's HSD test indicated no significant differences among men and women in *pre-intervention correctness* scores ($p = .744$).

Education Differences. Participants with a vocational school education scored significantly lower on *pre-intervention correctness* compared to those with a high school degree ($\beta = -8.718$, $SE = 3.51$, $p = 0.020$). Education levels are ordinal, indicating a ranked order of educational attainment without equal intervals. The Type II analysis of variance (ANOVA) revealed a non-significant effect of education on the ability to distinguish phishing emails from legitimate emails, $F(5, 27) = 2.528$, $p = 0.053$. The effect size, eta squared (η), was 0.32.

Internet Access Differences. Participants with average internet access scored significantly higher on *pre-intervention correctness* ($\beta = 11.18$, $SE = 4.05$, $p = .010$) compared to those with poor access. Participants with good internet access scored significantly higher on *pre-intervention correctness* ($\beta = 15.48$, $SE = 4.36$, $p < .001$)

compared to those with poor access. Participants with excellent internet access scored also significantly higher on *pre-intervention correctness* ($\beta = 17.96$, $SE = 4.63$, $p < .001$) compared to those with poor access. The mean *pre-intervention correctness* scores varied across different levels of internet access: Poor ($M = 28.5$, $SD = 7.78$), Average ($M = 30.8$, $SD = 3.71$), Good ($M = 34$, $SD = 4.78$), and Excellent ($M = 35.2$, $SD = 4.97$). *Internet Access* levels (Terrible, Poor, Average, Good, Excellent) are inherently ordinal and do not represent equal intervals. This approach allows for a more nuanced understanding of how different levels of internet access impact the ability to distinguish phishing emails. The Type II analysis of variance (ANOVA) revealed a significant effect of *Internet Access* on the ability to distinguish phishing emails from legitimate emails, $F(3, 27) = 5.740$, $p = .004$. The effect size, eta squared (η), was .39. Post hoc comparisons using Tukey's HSD test indicated no significant differences among the levels of internet access in *pre-intervention correctness* scores.

Cybercrime victim status. Participants unsure if they were victims of cybercrime scored lower ($\beta = -6.307$, $SE = 1.64$, $p < .001$) compared to those indicating not being a cybercrime victim. Participants who claimed being a victim of cybercrime scored even lower ($\beta = -7.640$, $SE = 2.22$, $p = .002$). The mean *pre-intervention correctness* scores varied across different experiences with cybercrime: No ($M = 34.7$, $SD = 5.12$), Don't know ($M = 32.7$, $SD = 4.43$), and Yes ($M = 30.9$, $SD = 4.85$). *Cybercrime victim status* is a categorical variable with distinct groups. The Type II analysis of variance (ANOVA) revealed a significant effect of being a cybercrime victim on the ability to distinguish phishing emails from legitimate emails, $F(2, 27) = 9.982$, $p = .001$. The effect size, eta squared (η), was .43. Post hoc comparisons using Tukey's HSD test indicated that participants who reported being unsure about their victim status scored significantly lower than those who reported not being victims (mean difference = -3.015 , 95% CI [-5.775 , -0.255], $p = .030$), and those who reported being victims scored significantly lower than those who reported not being victims (mean difference = -4.295 , 95% CI [-8.173 , -0.416], $p = .028$).

CAS, *Age*, *Cybersecurity knowledge*, and *Email usage* were not significant in the multiple regression analysis (see Table 9).

Hypothesis 2. Hypothesis 2 (H2) posited that participants with higher levels of *persuasion knowledge* would be less susceptible to phishing attacks. To test this hypothesis, a multiple regression analysis was conducted with pre-theory email judgment score

Table 9*Multiple Regression Analysis Predicting Pre-Intervention Correctness Scores (N = 51)*

Effect	Estimate	SE	95% CI		p
			LL	UL	
CAS	-.056	.03	-.125	.013	.107
Gender (Female)	4.549	1.56	1.347	7.750	.007**
Education (Vocational school)	-8.718	3.51	-15.927	-1.508	.020*
Education (UAS)	3.885	2.385	-1.008	8.778	.115
Education (Bachelor's degree)	1.3567	1.90	-2.545	5.259	.482
Education (Master's degree)	0.251	1.96	-3.772	4.274	.899
Education (PhD degree)	0.056	4.50	-9.187	9.298	.990
Internet access (Average)	11.182	4.05	2.863	19.501	.010*
Internet access (Good)	15.476	4.36	6.526	24.427	.001**
Internet access (Excellent)	17.958	4.62	8.466	27.450	.001***
Cybercrime victim (Don't know)	-6.307	1.642	-9.676	-2.93	.001***
Cybercrime victim (Yes)	-7.640	2.22	-12.191	-3.090	.002**

Note. CI = confidence interval; LL = lower limit; UL = upper limit; CAS = Cybercrime Awareness Scale; UAS = University of Applied Sciences degree; Neutral = Neither competent nor incompetent.

* $p < .05$, ** $p < .01$, *** $p < .001$

(*pre-intervention correctness*) as the dependent variable, and *agent knowledge* (AKCI and AKCB) and *total pre-theory persuasion knowledge* (PRE-PK) as independent variables.

The coefficients for *Agent knowledge - Cybercriminal's Investment scale* (AKCI), $\beta = -0.166$, $SE = .21$, $p = .429$, *Agent knowledge - Cybercriminal's Benefit scale* (AKCB), $\beta = .093$, $SE = .27$, $p = .732$, and *total pre-theory Persuasion knowledge* (PRE-PK) scale, $\beta = .040$, $SE = .13$, $p = .757$, were all non-significant.

These findings suggest that, contrary to the hypothesis, higher levels of persuasion knowledge, as measured by the scales (PRE-PK, AKCB, and AKCI) used in this study, do not significantly reduce susceptibility to phishing attacks.

Hypothesis 3. Exposure to theory about persuasion techniques will improve individuals' ability to distinguish phishing emails from legitimate emails.

The mean total score for *legitimate emails before theory instruction* was 12.69 ($SD = 4.19$), whereas for phishing emails, it was 20.75 ($SD = 6.91$). After theory instruction, the mean total score for legitimate emails increased to 13.58 ($SD = 3.70$), and for phishing emails, it increased to 21.35 ($SD = 6.04$).

A paired-samples *t*-test was conducted to evaluate the impact of theory instruction on participants' phishing detection abilities. Participants' total scores on phishing detection tasks were compared before and after the theory instruction. The results revealed a statistically significant difference in participants' total scores before ($M = 33.43$, $SD = 4.93$) and after ($M = 34.93$, $SD = 6.18$) the theory instruction; $t(47) = 2.271$, $p = .028$. The mean of the difference in total scores between the two time points was 1.73 (95% CI [0.198, 3.261]), indicating a moderate increase in participants' phishing detection abilities following the theory instruction.

Hypothesis 4. The improvement in distinguishing phishing emails from legitimate emails will be more significant in individuals with initially lower levels of phishing awareness compared to those with higher levels of phishing awareness. The mean *improvement score* for participants was 1.73 ($SD = 5.274$), with a minimum improvement of -9 and a maximum improvement of 14. The mean *Cybercrime Awareness Scale* (CAS) score was 157.35 ($SD = 20.60$). A linear regression analysis was conducted to examine the relationship between improvement scores and CAS scores. The results showed that the CAS score was not statistically significant, $\beta = .020$, $SE = .04$, $p = .582$.

Hypothesis 5. A regression analysis was conducted to examine whether the improvement in distinguishing phishing emails from legitimate emails (measured as the difference in scores between post-intervention and pre-intervention) was associated with participants' initial levels of persuasion knowledge (PK). The model included predictors *agent knowledge* (AKCI and AKCB) and *total pre-theory persuasion knowledge* (PRE-PK).

The overall model was not statistically significant in predicting *improvement scores*, $F(3, 47) = 1.053$, $p = .378$. The model accounted for a negligible amount of variance in *improvement scores*, $R^2 = .063$. None of the individual predictors, *AKCI* ($\beta = .152$, $SE = .24$, $p = .524$), *AKCB* ($\beta = -.336$, $SE = .28$, $p = .237$), or *PRE-PK* ($\beta = .194$, $p = .162$), were

found to be statistically significant in explaining the variance in improvement scores. These results indicate that the initial levels of *persuasion knowledge* did not significantly influence the improvement in participants' ability to distinguish phishing emails from legitimate ones after the intervention.

Although the HEXACO-60 Personality Test data was collected, it was not utilized in the research hypotheses. Initially, it was planned for additional analysis. However, due to the sample size not meeting the required number of participants, it was decided to leave out the HEXACO data. This decision ensures the validity and reliability of the findings reported in the study.

Discussion

To date, most phishing research has focused on Protection Motivation Theory (PMT) and Technology Threat Avoidance Theory (TTAT) (Almansoori et al., 2023; Prümmer et al., 2024), but little to nothing on the Persuasion Knowledge Framework, despite the frequent use of persuasion tactics in phishing. This study investigated experimentally the awareness of cybercrime pre-intervention and knowledge of persuasion pre- and post-intervention among adults in phishing scenarios. Comparing participants' abilities to distinguish between legitimate and phishing emails pre- and post-theory provision allowed assessment of the effectiveness of persuasion theory instruction. Participants showed improved phishing detection abilities after learning about persuasion tactics. Contrary to expectations, previous victimization was negatively associated with awareness levels, challenging the assumption that victimization enhances caution and awareness. The findings also highlighted the complex interplay between awareness, knowledge of persuasion, and phishing susceptibility, suggesting that enhancing educational interventions can be crucial in mitigating phishing risks.

Susceptibility to Phishing Based on Awareness and Knowledge

No significant relationship between cybercrime awareness and the ability to discern phishing emails from legitimate ones before any intervention was found in this research. Many researchers have found the importance of awareness in cybersecurity (Bada et al., 2015; Canfield et al., 2019; Debb, 2021; Mamade & Dabala, 2021). Despite this, the lack of a significant relationship in this study suggests that awareness alone does not translate into actionable skills for phishing detection. This discrepancy can be explained by the nature of phishing attacks, which often exploit cognitive biases and emotional triggers, making them

difficult to detect without specific training. Simply being aware of phishing does not equip individuals with the skills to recognize these subtle cues.

Awareness programs that do not incorporate practical skills training may leave individuals ill-prepared to apply their knowledge in real-world scenarios (Bada et al., 2015; Canfield et al., 2019). Bada et al. (2015) argue that effective awareness campaigns must include clear communication and practical skill training to prevent high-risk behaviour. This perspective is supported by Canfield et al. (2019), who emphasize that awareness needs to be integrated with educational efforts that help individuals develop practical skills and habits.

In a limited number of research studies that have examined the effectiveness of detecting phishing emails versus legitimate emails as distinct entities, Kleitman et al. (2018) discovered a weak yet statistically significant positive relationship between confidence levels and accuracy in identifying both types of emails. The study by Mamade and Dabala (2021) highlighted that many individuals, despite their confidence in identifying phishing attempts, lack the actual knowledge required for effective detection. While individuals may understand phishing conceptually, this awareness does not necessarily equip them with the specific skills needed to identify sophisticated phishing cues in emails. Effective phishing detection requires practical training and experience, as well as an understanding of the evolving tactics used by attackers (Motika, 2022). This disconnect suggests that awareness programs must address both knowledge and practical skills to be effective. Motika (2022) also emphasizes the importance of understanding specific cues in phishing emails, such as grammar and sender addresses, to reduce susceptibility.

The lack of a significant relationship between awareness and phishing detection in this study suggests that theoretical knowledge alone is insufficient. This research focuses on the dissemination of awareness material, and phishing simulations. These approaches aim to enhance individuals' understanding (what) and perhaps as such their skills (how). Nevertheless, akin to the manner in which factual information does not always influence our perspectives, possessing knowledge does not automatically result in changes in behaviour. This might be due to the fact that a crucial element in behaviour modification is the presence of motivation (why) - the reasons behind individuals' actions and decisions. Despite the provision of infinite amounts of knowledge to individuals, without a intrinsic interest in utilizing it, it is money and time thrown out the window.

Impact of Cybercrime Victim Status

Past cybercrime victimization significantly impacts the ability to identify phishing emails negatively. Participants unsure of their victim status scored lower than non-victims, while self-identified victims scored the lowest, indicating that past victimization experiences play a crucial role in phishing susceptibility.

Past cybercrime victimization significantly affects individuals' ability to detect phishing emails. Chen et al. (2020) states that recent phishing encounters can variably influence future susceptibility, with some individuals becoming more cautious while others do not change their behaviour. This view is supported by O'Connor et al. (2021), who found that past victimization impairs phishing detection abilities, and by van 't Hoff - de Goede et al. (2021), who notes that victimization impacts online behaviour and increases susceptibility to future threats. Van 't Hoff - de Goede et al.'s study (2021) indicates that while some may improve their security practices post-victimization, others might remain vulnerable due to psychological effects like anxiety or a sense of inevitability about being victimized again. Hassandoust et al. (2020) further adds that cognitive effects from past victimization can complicate the detection of new phishing attempts, leading to either increased vigilance or heightened susceptibility. These findings collectively suggest that the psychological impact of past victimization often overshadows any improvements in security awareness, highlighting the need for targeted cybersecurity education that addresses both cognitive and behavioural aspects. Contrary, Ribeiro et al. (2024) suggest that past victimization could lead to more cautious behaviour and better security practices.

In conclusion, the evidence indicates that the psychological and cognitive effects of past victimization can sometimes overshadow these improvements in security awareness. This highlights the complexity of the relationship between past victimization and current phishing susceptibility, emphasizing the need for targeted and nuanced approaches in cybersecurity education and support.

Moderating Effects of Initial Awareness and Knowledge Levels

The effectiveness of behavioural interventions on phishing detection is influenced by participants' initial awareness and knowledge levels. Research suggests that individuals with lower initial levels of awareness often benefit more from targeted interventions compared to those with higher levels (Alnajim et al., 2023; Alsharnouby et al., 2015; Canfield et al., 2019;

Köhler et al., 2023; Mamade & Dabala, 2021). This indicates that educational efforts are particularly impactful for those with less prior knowledge, as they have more room to improve their understanding and recognition of phishing threats. Conversely, individuals with higher initial awareness may not experience as significant changes in behaviour, as they are already equipped with the necessary skills to identify and respond to phishing attempts effectively.

On the other hand, Schaab et al. (2016) highlight the importance of designing training programs that enhance both awareness and behaviour, suggesting that interventions can lead to improvements in security practices regardless of initial awareness levels. Similarly, Weickert et al. (2023) emphasize the complexity of changing established behaviours through interventions, particularly when strong habits are present. Their work underscores that interventions targeting behavioural intentions may not be effective for frequently performed behaviours, which complicates the effort to improve phishing detection through training alone.

Despite the general consensus in the literature, the current study's findings reveal that intervention effectiveness was consistent across different levels of initial awareness. This suggests that while initial awareness may influence the degree of improvement, the intervention used in this study was equally effective for participants regardless of their starting level of awareness. This consistency might be attributable to several factors, including the specific content of the intervention, the method of delivery, or the focus of the intervention. For instance, the intervention may have been designed in a way that did not significantly differentiate between varying levels of initial awareness, or it might have lacked the necessary depth to produce differential effects.

Furthermore, it is important to consider that the high level of cybercrime awareness among participants might have been too high for the relatively simple intervention used in this study. Participants may have already possessed a substantial baseline understanding of phishing threats, which could limit the observable impact of the intervention. Additionally, the timing of the phishing attempts may have influenced the results. Participants were exposed to phishing attempts in different rounds, which could have led to improvements in detection skills over time. It is possible that participants became more adept at identifying phishing attempts simply due to increased familiarity and experience with the task across rounds, rather than solely due to the intervention. This effect of time on detection ability warrants further investigation to determine its role in the overall effectiveness of the intervention.

The Role of Persuasion Knowledge in Phishing Detection

The effectiveness of persuasion knowledge in enhancing phishing detection is a nuanced issue, as evidenced by the findings of this research. Contrary to expectations, no significant relationship was found between participants' persuasion knowledge and susceptibility. This lack of correlation suggests that persuasion knowledge alone may not be sufficient to protect against phishing attacks. Previous research has similarly indicated that knowledge-based performance often struggles to translate into practical effectiveness under real-world conditions (Kahneman & Klein, 2009; Klein, 2008). Despite having higher levels of persuasion knowledge, participants did not demonstrate a superior capacity for phishing detection compared to those with lower levels of this knowledge.

The Persuasion Knowledge Framework (PKF) provides a theoretical basis for understanding these results. According to the PKF, individuals utilize various forms of knowledge, including persuasion knowledge, to counteract persuasion attempts effectively (Friestad & Wright, 1994; Ham et al., 2015). Although theory-based instruction led to a statistically significant improvement in phishing detection ability, the size of this improvement was moderate. This suggests that theoretical knowledge alone, without practical application, may not be sufficient for high-level phishing resilience.

Practical training methods, such as simulations and real-time feedback, may offer more substantial benefits in developing phishing detection skills. Research supports that interactive training environments, like those offered by educational games and simulated phishing exercises, can significantly improve individuals' ability to recognize phishing attempts (Alsharnouby et al., 2015; Blythe et al., 2011; Gallo et al., 2024; Montañez et al., 2020; O'Connor et al., 2021). For instance, Alsharnouby et al. (2015) and Gallo et al. (2024) emphasize the effectiveness of interactive platforms such as Anti-Phishing Phil and Spamley, which provide users with hands-on experience in a controlled setting. These methods not only allow for practical application but also offer immediate feedback, reinforcing learning and improving detection skills. Similarly, Montañez et al. (2020) and O'Connor et al. (2021) advocate for simulation-based training, which fosters automatic responses to phishing attempts and enhances resilience against social engineering threats.

In practical situations, the cognitive load and need for quick decision-making may impede the practical utilization of theoretical knowledge. While the original PKF, developed

by Friestad and Wright (1994) in the '80s and '90s, provides valuable insights into how individuals respond to persuasion efforts in offline contexts, its applicability to cybersecurity is limited. The PKF was not designed with online threats in mind and does not fully address the complexities of digital environments. Therefore, while the PKF offers foundational insights into persuasion, it requires adaptation to effectively address the unique challenges posed by online phishing. Integrating elements that account for the emotional and psychological tactics used by cybercriminals could enhance the framework's applicability, making it a more effective tool for understanding and mitigating susceptibility to digital persuasion tactics.

(Sub-)scales

Descriptive statistics revealed high mean score on the Cybercrime Awareness Scale (CAS), indicating that participants generally have a strong understanding of cybercrime awareness. This high mean score suggests that, on average, participants are well-informed about cybercrime.

The intervention aimed at enhancing persuasion knowledge (PK) did not yield significant improvements, as indicated by a slight, non-significant decrease in PK scores from pre- to post-intervention. Several factors may explain this outcome. The content and delivery of the intervention might need reassessment to ensure they are sufficiently engaging and tailored to the specific aspects of PK relevant to phishing. Additionally, the short duration of the intervention and participants' already high baseline PK levels could have constrained the potential for noticeable gains.

Implications and Future Directions

The findings of this study highlight the need to integrate both practical skills and theoretical knowledge into cybersecurity training programs, particularly for phishing detection. While foundational awareness is crucial, its practical application in real-world scenarios is key (Kahneman & Klein, 2009; Klein, 2008).

Future research should explore integrating psychological support mechanisms into cybersecurity training programs to address a range of psychological needs. This includes providing support for individuals who may have been victims of cybercrime as well as those undergoing training. Tailored approaches that consider individual differences in demographics, learning styles, and cognitive abilities can enhance the inclusivity and efficacy of cybersecurity education initiatives (Burke-Smalley & Hutchins, 2007; Grossman & Salas, 2011; Salas &

Cannon-Bowers, 2001). Additionally, ensuring robust digital infrastructure is crucial to support the learning and application of cybersecurity skills effectively. This involves maintaining secure, up-to-date training platforms and simulated environments to enable realistic exercises and ensure that learners can effectively apply their skills in a risk-free setting.

Addressing methodological limitations such as sampling biases and survey-induced awareness remains paramount. Future studies could adopt more controlled experimental designs to mitigate these biases and enhance the authenticity of participants' responses to phishing simulations (Blythe et al., 2011; Kumaraguru et al., 2010). Future research should investigate how psychological factors such as decision-making biases and persuasion knowledge evolve in response to increasingly sophisticated phishing tactics (Sheng et al., 2010). Understanding these dynamics could inform the development of tailored educational interventions and behaviour-focused cybersecurity training programs (Blythe et al., 2011; Kumaraguru et al., 2010).

Furthermore, cyberattackers have improved their methods of attack. Phishing emails are becoming increasingly sophisticated, especially with the rise of personalized spear phishing, making detection of it increasingly challenging (Bullée et al., 2017). Attackers utilize language models like GPT to enhance phishing operations (Heiding et al., 2024). To combat this growing threat, AI-based anti-phishing solutions are being developed that can analyze content in multiple languages (Heiding et al., 2024; Yao et al., 2024). These solutions employ advanced natural language processing (NLP) techniques and machine learning algorithms to detect suspicious patterns, regardless of the language used. However, these AI-based anti-phishing solutions need to be capable of detecting subtle linguistic nuances and cultural context across different languages (Ansari et al., 2022). Languages with limited digital presence or unique scripts may pose additional challenges for AI-based detection systems (Ansari et al., 2022). Future phishing research may focus on evaluating the impact and danger of AI-enabled phishing methods and exploring innovative solutions.

Integrating phishing detection into digital literacy education is crucial. Tools like Anti-Phishing Phil (Sheng et al., 2007) and Samply raise awareness and collect data on user behaviour, helping users recognize phishing threats. Scholars emphasize the importance of information literacy, with higher education institutions incorporating training to combat

phishing (Canfield et al., 2019). Emphasizing self-regulated learning can enhance these trainings and improve metacognitive abilities, thus providing a comprehensive approach to cybersecurity education.

Lastly, expanding the scope of research to encompass global perspectives and diverse cultural contexts is imperative. Cross-cultural studies could illuminate how cultural norms and values influence phishing susceptibility and responses to cybersecurity interventions. Such insights would facilitate the development of culturally sensitive cybersecurity strategies tailored to diverse global audiences (Sheng et al., 2010). Such initiatives would not only enhance learning outcomes but also address the diverse needs and capabilities of learners in different contexts.

Study Limitations

This study acknowledges several limitations that are crucial to consider. Firstly, the use of snowball sampling may have introduced sampling bias, as participants primarily recruited from personal social networks. This method tends to capture individuals who share similar characteristics or affiliations, potentially limiting the diversity of perspectives and backgrounds within the sample. As a result, the findings derived from this sample may not fully represent the broader population. This lack of representativeness can impact the external validity of the study, affecting the ability to generalize the results beyond the specific characteristics of the sample. For instance, if the sample is skewed towards individuals who are more tech-savvy or have higher educational backgrounds, their responses to phishing scenarios might differ systematically from those of a more diverse population. This might affect the generalizability of the results.

Secondly, participants were informing about the study's nature, which might have influenced their responses, potentially introducing awareness biases. This heightened caution among participants could have affected the authenticity of their reactions to phishing emails compared to real-world scenarios.

Thirdly, emails were presented as screenshots without interactive features, such as hover-over links (Downs et al., 2006), which are critical for authenticating email content. This limitation prevented participants from hovering over links to check their authenticity, potentially affecting their ability to accurately assess the emails. Future studies should incorporate more interactive and realistic email formats to better simulate actual phishing

scenarios.

Fourthly, the theoretical framework, which attempted to adapt the Persuasion Knowledge Framework to an email phishing context, faced challenges due to the lack of existing validated questionnaires specifically tailored to this domain. While this framework provided a comprehensive understanding of psychological and contextual factors influencing phishing susceptibility, some mechanisms and vulnerabilities discussed remain theoretical and require further empirical validation.

Lastly, this study provides insights into how awareness and persuasion knowledge affect phishing susceptibility. However, decisions about which items to retain or discard, and how to operationalize and analyze various variables, reflect choices that are not always predetermined. These can influence results. To enhance robustness and replicability, future research should use more stringent, preregistered methods and hypotheses Roettger (2018) and Wicherts et al. (2016). Clearly defined procedures and operational definitions will help isolate intervention effects and improve generalizability.

Conclusion

This study has underscored the critical interplay between awareness and persuasion knowledge in mitigating email phishing susceptibility. While theory-based cybersecurity training improved phishing detection skills, awareness alone proved insufficient, challenging existing assumptions about its direct impact on phishing susceptibility. The research also revealed that prior cybercrime victimization negatively influences phishing detection abilities, adding complexity to our understanding of personal experiences' impact on cybersecurity behaviour. Despite these insights, the study faced limitations, including potential sampling biases and the use of non-interactive email formats, which may affect the generalizability of the findings. The theoretical framework used requires further adaptation to address the complexities of online phishing more effectively. Future research should focus on refining intervention methodologies, leveraging advanced technologies like AI and gamified training, and exploring diverse cultural perspectives to enhance the effectiveness of cybersecurity education. This study underscores the need for a multifaceted approach to phishing prevention, combining practical application with theoretical understanding to address evolving phishing threats comprehensively.

References

- Alkhalil, Z., Hewage, C., Nawaf, L. F., & Khan, I. A. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers of Computer Science*.
- Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Applied Sciences*, *13*, 5700. <https://doi.org/10.3390/app13095700>
- Alnajim, A., Habib, S., Islam, M., Alrawashdeh, H., & Wasim, M. (2023). Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches. *Symmetry*, *15*, 2175. <https://doi.org/10.3390/sym15122175>
- Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *2*. <https://doi.org/10.1016/j.ijhcs.2015.05.005>
- Alwanain, M. (2019). Effects of user-awareness on the detection of phishing emails: A case study. *International Journal of Innovative Technology and Exploring Engineering*, *8*, 480–484.
- Amazeen, M., & Krishna, A. (2022). Processing vaccine misinformation: Recall and effects of source type on claim accuracy via perceived motivations and credibility. *International Journal of Communication*, *17*. <https://ijoc.org/index.php/ijoc/article/view/19795>
- Ansari, M. F., Sharma, P. K., & Dash, B. (2022). Prevention of phishing attacks using ai-based cybersecurity awareness training. *International Journal of Smart Sensor and Adhoc Network*, *3*(6), 61–72. <https://doi.org/10.47893/IJSSAN.2022.1221>
- Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312. <https://doi.org/10.1016/j.chb.2014.05.046>
- Arpaci, I., & Ateş, E. (2022). Development of the cybercrime awareness scale (cas): A validity and reliability study in a turkish sample. *Online Information Review*, *47*. <https://doi.org/10.1108/OIR-01-2022-0023>
- Ashenden, D. (2008). Information security management: A human challenge? *Information Security Technical Report*, *13*(4), 195–201. <https://doi.org/10.1016/j.istr.2008.10.006>

- Ashton, M. C., & Lee, K. (2009). The hexaco-60: A short measure of the major dimensions of personality. *Journal of personality assessment*, *91*(4), 340–5.
<https://doi.org/10.1080/00223890902935878>
- Bada, M., Sasse, A., & Nurse, J. (2015). *Cyber security awareness campaigns: Why do they fail to change behaviour?*
- Bauer, S., & Bernroider, E. (2015). The effects of awareness programs on information security in banks: The roles of protection motivation and monitoring. *International Conference on Human Aspects of Information Security, Privacy, and Trust*, *9190*, 154–164.
https://doi.org/10.1007/978-3-319-20376-8_14
- Bearden, W., Hardesty, D., & Rose, R. (2001). Consumer self-confidence: Refinements in conceptualization and measurement. *Journal of Consumer Research*, *28*, 121–34.
<https://doi.org/10.1086/321951>
- Blythe, M., Petrie, H., & Clark, J. (2011). F for fake: Four studies on how we fall for phish. *Proceedings of the International Conference on Human Factors in Computing Systems*, 3469–3478. <https://doi.org/10.1145/1978942.1979459>
- Boerman, S. C., Willemsen, L. M., & Aa, E. P. V. D. (2017). “this post is sponsored” effects of sponsorship disclosure on persuasion knowledge and electronic word of mouth in the context of facebook. *Journal of Interactive Marketing*, *38*(1), 82–92.
<https://doi.org/10.1016/j.intmar.2016.12.002>
- Bullée, J.-W., & Junger, M. (2020). Social engineering. In T. J. Holt & A. M. Bossler (Eds.), *The palgrave handbook of international cybercrime and cyberdeviance* (pp. 849–875). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_38
- Bullée, J.-W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. *Information and Computer Security*, *25*, 00–00.
<https://doi.org/10.1108/ICS-03-2017-0009>
- Burke-Smalley, L., & Hutchins, H. (2007). Training transfer: An integrative literature review. *Human Resource Development Review*, *6*, 263–296.
<https://doi.org/10.1177/1534484307303035>
- Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. *Proceeding of Australasian Conference on Information Systems*.

- Button, K. S., Ioannidis, J. P. A., Mokrysz, C., Nosek, B. A., Flint, J., Robinson, E. S. J., & Munafò, M. R. (2013a). Confidence and precision increase with high statistical power. *Nature Reviews Neuroscience*, *14*(8), 585–585. <https://doi.org/10.1038/nrn3475-c4>
- Button, K. S., Ioannidis, J. P. A., Mokrysz, C., Nosek, B. A., Flint, J., Robinson, E. S. J., & Munafò, M. R. (2013b). Empirical evidence for low reproducibility indicates low pre-study odds. *Nature Reviews Neuroscience*, *14*(12), 877–877. <https://doi.org/10.1038/nrn3475-c6>
- Button, K. S., Ioannidis, J. P. A., Mokrysz, C., Nosek, B. A., Flint, J., Robinson, E. S. J., & Munafò, M. R. (2013c). Power failure: Why small sample size undermines the reliability of neuroscience. *Nature Reviews Neuroscience*, *14*(5), 365–376. <https://doi.org/10.1038/nrn3475>
- Campbell, M., & Kirmani, A. (2000). Consumers' use of persuasion knowledge: The effects of accessibility and cognitive capacity on perceptions of an influence agent. *Journal of Consumer Research*, *27*, 69–83. <https://doi.org/10.1086/314309>
- Campbell, M. C. (1995). When attention-getting advertising tactics elicit consumer inferences of manipulative intent: The importance of balancing benefits and investments. *Journal of Consumer Psychology*, *4*(3), 225–254. https://doi.org/10.1207/s15327663jcp0403_02
- Canfield, C., Fischhoff, B., & Davis, A. (2019). Better beware: Comparing metacognition for phishing and legitimate emails. *Metacognition and Learning*, *14*. <https://doi.org/10.1007/s11409-019-09197-5>
- Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy*, *12*(1), 28–38. <https://doi.org/10.1109/MSP.2013.106>
- Ceesay, E., Myers, K., & Watters, P. (2018). Human-centered strategies for cyber-physical systems security. *EAI Endorsed Transactions on Security and Safety*, *4*(14). <https://doi.org/10.4108/eai.15-5-2018.154773>
- Chen, R., Gaia, J., & Rao, H. R. (2020). An examination of the effect of recent phishing encounters on phishing susceptibility. *Decision Support Systems*, *133*, 113287. <https://doi.org/10.1016/j.dss.2020.113287>
- Chen, Z. F., & Cheng, Y. (2019). Consumer response to fake news about brands on social media: The effects of self-efficacy, media trust, and persuasion knowledge on brand

- trust. *Journal of Product & Brand Management*.
<https://doi.org/10.1108/JPBM-12-2018-2145>]
- Cialdini, R. B. (2009). *Influence: The psychology of persuasion*. HarperCollins e-books.
<https://books.google.nl/books?id=5dfv0HJ1TEoC>
- Das, G., Roy, R., & Naidoo, V. (2020). When do consumers prefer partitioned prices? the role of mood and pricing tactic persuasion knowledge. *Journal of Business Research*, *116*, 60–67. <https://doi.org/10.1016/j.jbusres.2020.05.013>
- Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior*, *26*(6), 1739–1747.
<https://doi.org/10.1016/j.chb.2010.06.023>
- Debb, S. (2021). Keeping the human in the loop: Awareness and recognition of cybersecurity within cyberpsychology. *Cyberpsychology, Behavior, and Social Networking*, *24*, 581–583. <https://doi.org/10.1089/cyber.2021.29225.sde>
- Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI conference on Human Factors in computing systems*, 581–590.
<https://doi.org/10.1145/1124772.1124861>
- Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security*, *26*(1), 73–80. <https://doi.org/10.1016/j.cose.2006.10.009>
- Downs, J., Lanyon, M., & Cranor, L. (2006). Decision strategies and susceptibility to phishing. *Proceedings of the 2nd Symposium on Usable Privacy and Security, SOUPS 2006, Pittsburgh, Pennsylvania, USA, July 12-14, 2006*, *149*, 79–90.
<https://doi.org/10.1145/1143120.1143131>
- Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies – a case study [Human Factors in Information Security]. *Information Security Technical Report*, *14*(4), 223–229.
<https://doi.org/10.1016/j.istr.2010.05.002>
- Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using g*power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*(4), 1149–1160. <https://doi.org/10.3758/BRM.41.4.1149>
- Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. In T. Tryfonas & I. Askoxylakis (Eds.), *Human aspects of*

- information security, privacy, and trust* (pp. 36–47). Springer International Publishing. https://doi.org/10.1007/978-3-319-20376-8_4
- Ferreira, A., & Lenzini, G. (2015). An analysis of social engineering principles in effective phishing. *2015 Workshop on Socio-Technical Aspects in Security and Trust*, 9–16. <https://doi.org/10.1109/STAST.2015.10>
- Frauenstein, E. (2013, January). *A framework to mitigate phishing threats* [Thesis for Master of Technology]. Nelson Mandela Metropolitan University. <https://www.researchgate.net/publication/267512601>
- Friestad, M., & Wright, P. (1994). The persuasion knowledge model: How people cope with persuasion attempts. *Journal of Consumer Research*, *21*(1), 1–31. <https://doi.org/10.1086/209380>
- Gallo, L., Gentile, D., Ruggiero, S., Botta, A., & Ventre, G. (2024). The human factor in phishing: Collecting and analyzing user behavior when reading emails. *Computers & Security*, *139*, 103671. <https://doi.org/10.1016/j.cose.2023.103671>
- Gehringer, E. F. (2002). Choosing passwords: Security and human factors. *Proceeding for IEEE 2002 International Symposium on Technology and Society (ISTAS'02). Social Implications of Information and Communication Technology. Proceedings (Cat. No. 02CH37293)*, 369–373. <https://doi.org/10.1109/ISTAS.2002.1013839>
- Germelmann, C. C., Herrmann, J.-L., Kacha, M., & Darke, P. R. (2020). Congruence and incongruence in thematic advertisement–medium combinations: Role of awareness, fluency, and persuasion knowledge. *Journal of Advertising*, *49*(2), 141–164. <https://doi.org/10.1080/00913367.2020.1745110>
- Gragg, D. (2003). A multi-level defense against social engineering. *SANS Reading Room*, *13*, 1–21.
- Griffiths, C. (2024). The latest phishing statistics (updated april 2024). <https://aag-it.com/the-latest-phishing-statistics/>
- Grossman, R., & Salas, E. (2011). The transfer of training: What really matters. *International Journal of Training and Development*, *15*. <https://doi.org/10.1111/j.1468-2419.2011.00373.x>

- Ham, C.-D., Nelson, M. R., & Das, S. (2015). How to measure persuasion knowledge [doi: 10.1080/02650487.2014.994730]. *International Journal of Advertising*, 34(1), 17–53. <https://doi.org/10.1080/02650487.2014.994730>
- Hardesty, D. M., Bearden, W. O., & Carlson, J. P. (2007). Persuasion knowledge and consumer reactions to pricing tactics. *Journal of Retailing*, 83(2), 199–210. <https://doi.org/10.1016/j.jretai.2006.06.003>
- Hassandoust, F., Singh, H., & Williams, J. (2020). The role of contextualization in individuals' vulnerability to phishing attempts. *Australasian Journal of Information Systems*, 24. <https://doi.org/10.3127/ajis.v24i0.2693>
- Heartfield, R., & Loukas, G. (2015). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys (CSUR)*, 48(3), 1–39. <https://doi.org/10.1145/2835375>
- Heiding, F., Schneier, B., Vishwanath, A., Bernstein, J., & Park, P. S. (2024). Devising and detecting phishing emails using large language models. *IEEE Access*, 12, 42131–42146. <https://doi.org/10.1109/ACCESS.2024.3375882>
- Hendriks, J. (2023). *The persuasion knowledge model as a determinant of trust in chatbot adoption*. [Thesis].
- Hibbert, S., Smith, A., Davies, A., & Ireland, F. (2007). Guilt appeals: Persuasion knowledge and charitable giving. *Psychology & Marketing*, 24(8), 723–742. <https://doi.org/10.1002/mar.20181>
- Jain, A. K., & Gupta, B. B. (2022). A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*, 16(4), 527–565. <https://doi.org/10.1080/17517575.2021.1896786>
- Jansen, J., & Van Schaik, P. (2018). Persuading end users to act cautiously online: A fear appeals study on phishing. *Information & Computer Security*, 26(3), 264–276.
- Junger, M., Montoya, L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, 66. <https://doi.org/10.1016/j.chb.2016.09.012>
- Kahneman, D., & Klein, G. (2009). Conditions for intuitive expertise: A failure to disagree. *The American psychologist*, 64 6, 515–26. <https://doi.org/10.1037/a0016755>

- Kearney, W., & Kruger, H. (2014). Considering the influence of human trust in practical social engineering exercises. *2014 Information Security for South Africa*, 1–6. <https://doi.org/10.1109/ISSA.2014.6950509>
- Klein, G. (2008). Naturalistic decision making. *Human factors: The Journal of the Human Factors and Ergonomics Society*, 50, 456–60.
- Kleitman, S., Law, M. K. H., & Kay, J. (2018). It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling. *PLoS ONE*, 13. <https://api.semanticscholar.org/CorpusID:53092342>
- Knapova, L., Kruzikova, A., Dedkova, L., & Smahel, D. (2021). Who is smart with their smartphones? determinants of smartphone security behavior. *Cyberpsychology, Behavior, and Social Networking*, 24. <https://doi.org/10.1089/cyber.2020.0599>
- Köhler, D., Pünter, W., & Meinel, C. (2023, October). *Preprint: We have phishing at home: Quantitative study on email phishing susceptibility in private contexts* (Book). <https://doi.org/10.13140/RG.2.2.21865.47201/1>
- Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: A real-world evaluation of anti-phishing training. *Proceedings of the 5th Symposium on Usable Privacy and Security*. <https://doi.org/10.1145/1572532.1572536>
- Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching johnny not to fall for phish. *Association for Computing Machinery Transactions on Internet Technology*, 10(2). <https://doi.org/10.1145/1754393.1754396>
- Kumaran, N., & Lugani, S. (2020). Protecting businesses against cyber threats during covid-19 and beyond. <https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond>
- Lacey, D. (2009). *Managing the human factor in information security: How to win over staff and influence business managers*. John Wiley & Sons.
- Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). Susceptibility to spear-phishing emails: Effects of internet user demographics and email content. *Association for Computing Machinery Transactions on Computer-Human Interaction*, 26(5). <https://doi.org/10.1145/3336141>

- Mamade, B., & Dabala, D. (2021). Exploring the correlation between cyber security awareness, protection measures and the state of victimhood: The case study of ambo university's academic staffs. *Journal of Cyber Security and Mobility, Vol. 10*, 699–724. <https://doi.org/10.13052/jcsm2245-1439.1044>
- Mitnick, K., Simon, W., & Wozniak, S. (2011). *The art of deception: Controlling the human element of security*. Wiley. https://books.google.nl/books?id=OIy4F-8b_uEC
- Montañez, R., Golob, E., & Xu, S. (2020). Human cognition through the lens of social engineering cyberattacks. *Frontiers in Psychology, 11*. <https://doi.org/10.3389/fpsyg.2020.01755>
- Moody, G. D., Galletta, D. F., & Dunn, B. K. (2017). Which phish get caught? an exploratory study of individuals' susceptibility to phishing. *European Journal of Information Systems, 26*(6), 564–584. <https://doi.org/10.1057/s41303-017-0058-x>
- Motika, H. (2022, June). The effects of phishing emails : A meta-analysis. <http://essay.utwente.nl/91936/>
- Nair, A., & Greeshma, M. R. (2023). Mastering information security compliance management. <https://www.oreilly.com/library/view/-/9781803231174/>
- Nelson, M., & Park, J. (2014). Publicity as covert marketing? the role of persuasion knowledge and ethical perceptions on beliefs and credibility in a video news release story. *Journal of Business Ethics, 130*. <https://doi.org/10.1007/s10551-014-2227-3>
- O'Connor, A. M., Judges, R. A., Lee, K., & Evans, A. D. (2021). Can adults discriminate between fraudulent and legitimate e-mails? examining the role of age and prior fraud experience. *Journal of Elder Abuse & Neglect, 33*(3), 181–205. <https://doi.org/10.1080/08946566.2021.1934767>
- Palatty, N. J. (2024). 81 phishing attack statistics 2024: The ultimate insight. <https://www.getastra.com/blog/security-audit/phishing-attack-statistics/>
- Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security, 136*, 103585. <https://doi.org/10.1016/j.cose.2023.103585>
- Quinkert, F., Degeling, M., & Holz, T. (2021). Spotlight on phishing: A longitudinal study on phishing awareness trainings. In L. Bilge, L. Cavallaro, G. Pellegrino, & N. Neves (Eds.), *Detection of intrusions and malware, and vulnerability assessment*

- (pp. 341–360). Springer International Publishing.
https://doi.org/10.1007/978-3-030-80825-9_17
- Rahmani, V. (2023). Persuasion knowledge framework: Toward a comprehensive model of consumers' persuasion knowledge. *Academy of Marketing Science Review*, 13(1), 12–33. <https://doi.org/10.1007/s13162-023-00254-6>
- Rajivan, P., & Gonzalez, C. (2018). Creative persuasion: A study on adversarial behaviors and strategies in phishing attacks. *Frontiers in psychology*, 9, 323697.
<https://doi.org/10.3389/fpsyg.2018.00135>
- Ribeiro, L., Guedes, I. S., & Cardoso, C. S. (2024). Which factors predict susceptibility to phishing? an empirical study. *Computers & Security*, 136, 103558.
<https://doi.org/10.1016/j.cose.2023.103558>
- Roettger, T. (2018). Researcher degrees of freedom in phonetic research.
<https://doi.org/10.31234/osf.io/fp4jr>
- RStudio Team. (2024). Rstudio: Integrated development environment for r.
<http://www.rstudio.com/>
- Salas, E., & Cannon-Bowers, J. (2001). The science of training: A decade of progress. *Annual review of psychology*, 52, 471–99. <https://doi.org/10.1146/annurev.psych.52.1.471>
- Schaab, P., Beckers, K., & Pape, S. (2016). *A systematic gap analysis of social engineering defence mechanisms considering social psychology*.
- Scholtz, T., Byrnes, F., & Heiser, J. (2006). Best practices and common problems for information security programs.
- Scott, M. L., Mende, M., & Bolton, L. E. (2013). Judging the book by its cover? how consumers decode conspicuous consumption cues in buyer-seller relationships. *Journal of Marketing Research*, 50(3), 334–347. <https://doi.org/10.1509/jmr.11.0478>
- Sheng, S., Lanyon, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. *Conference on Human Factors in Computing Systems - Proceedings*, 1, 373–382.
<https://doi.org/10.1145/1753326.1753383>
- Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-phishing phil: The design and evaluation of a game that teaches people

- not to fall for phish. *Proceedings of the 3rd Symposium on Usable Privacy and Security*, 88–99. <https://doi.org/10.1145/1280680.1280692>
- Stajano, F., & Wilson, P. (2011). Understanding scam victims: Seven principles for systems security. *Communication of the Association for Computing Machinery*, 54(3), 70–75. <https://doi.org/10.1145/1897852.1897872>
- Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. *Behaviour & Information Technology*, 32(10), 1014–1023. <https://doi.org/10.1080/0144929X.2013.763860>
- Uebelacker, S., & Quiel, S. (2014). The social engineering personality framework. <https://doi.org/10.1109/STAST.2014.12>
- Van der Heijden, A., & Allodi, L. (2019). Cognitive triaging of phishing attacks. *28th USENIX Security Symposium, August 14–16, 2019 • Santa Clara, CA, USA*, 1309–1326.
- van 't Hoff - de Goede, S., Leukfeldt, E., van der Kleij, R., & van de Weijer, S. (2021, May). The online behaviour and victimization study: The development of an experimental research instrument for measuring and explaining online behaviour and cybercrime victimization. In *Cybercrime in context* (pp. 21–41). https://doi.org/10.1007/978-3-030-60527-8_3
- Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, 45(8), 1146–1166. <https://doi.org/10.1177/0093650215627483>
- Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, 9, 11895–11910. <https://doi.org/10.1109/ACCESS.2021.3051633>
- Wang, Z., Zhu, H., Liu, P., & Sun, L. (2021). Social engineering in cybersecurity: A domain ontology and knowledge graph application examples. *Cybersecurity*, 4, 31.
- Wei, M.-L., Fischer, E., & Main, K. J. (2008). An examination of the effects of activating persuasion knowledge on consumer response to brands engaging in covert marketing. *Journal of Public Policy & Marketing*, 27(1), 34–44. <https://doi.org/10.1509/jppm.27.1.34>
- Weickert, T. D., Joinson, A., & Craggs, B. (2023). Is cybersecurity research missing a trick? Integrating insights from the psychology of habit into research and practice. *Computers Security*, 128, 103130. <https://doi.org/10.1016/j.cose.2023.103130>

- Wicherts, J. M., Veldkamp, C. L. S., Augusteijn, H. E. M., Bakker, M., van Aert, R. C. M., & van Assen, M. A. L. M. (2016). Degrees of freedom in planning, running, analyzing, and reporting psychological studies: A checklist to avoid p-hacking. *Frontiers in Psychology, 7*. <https://doi.org/10.3389/fpsyg.2016.01832>
- Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies, 120*, 1–13. <https://doi.org/10.1016/j.ijhcs.2018.06.004>
- Williams, P. A. (2008). In a ‘trusting’ environment, everyone is responsible for information security. *Information Security Technical Report, 13*(4), 207–215. <https://doi.org/10.1016/j.istr.2008.10.009>
- Wolff, J. (2016). Perverse effects in defense of computer systems: When more is less. *Journal of Management Information Systems, 33*(2), 597–620. <https://doi.org/10.1080/07421222.2016.1205934>
- Wood, C. C. (1999). *Information security policies made easy: Version 7*. PentaSafe Security Technologies.
- Xie, G.-X., & Johnson, J. M. Q. (2015). Examining the third-person effect of baseline omission in numerical comparison: The role of consumer persuasion knowledge. *Psychology & Marketing, 32*(4), 438–449. <https://doi.org/10.1002/mar.20790>
- Yao, Y., Duan, J., Xu, K., Cai, Y., Sun, Z., & Zhang, Y. (2024). A survey on large language model (llm) security and privacy: The good, the bad, and the ugly. *High-Confidence Computing, 4*(2), 100211. <https://doi.org/10.1016/j.hcc.2024.100211>
- Zhang, B., Wu, M., Kang, H., Go, E., & Sundar, S. S. (2014). Effects of security warnings and instant gratification cues on attitudes toward mobile websites. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 111–114. <https://doi.org/10.1145/2556288.2557347>

Appendix A

Persuasion Knowledge

- PK1 I know that phishing emails try to trick people into doing certain things, like clicking on harmful links or giving away personal information.
- PK2 I can spot common tricks used in phishing emails, like making you feel rushed or pretending to be someone trustworthy.
- PK3 I understand that the main aim of phishing emails is to trick people for money or harm.
- PK4 I must be attentive about detecting deceptions by responding to emails.
- PK5 Cybercriminals are constantly trying to trick me.
- PK6 I know when a nasty email is “too good to be true”.
- PK7 I can tell when an email has hidden motives or unexpected requirements.
- PK8 I can easily understand the tricks cybercriminals use to try to get what they want.
- PK9 I know when a cybercriminal is pressuring me to provide private information.
- PK10 I can recognize tricks used to scam me in emails.
- PK11 I can separate fact from fantasy in emails.

Prompt pre-intervention: This section evaluates your understanding of persuasion tactics used in phishing emails. You will be asked about your ability to recognize common tricks. Your responses will provide insights into your awareness of deceptive practices and your capacity to detect and navigate phishing attempts. Please rate the following statements on a scale from 'strongly disagree' to 'strongly agree'. Choose the answer option that best represents your opinion on each statement.

Prompt post-intervention: Now that you have learned some theory about the tactics used in phishing emails, please answer the following questions. We want to understand how this information may have changed your opinions. For each statement, select the option from 'strongly disagree' to 'strongly agree' that best reflects your current views.

Appendix B

Agent Knowledge

A. Cybercriminal's Benefits

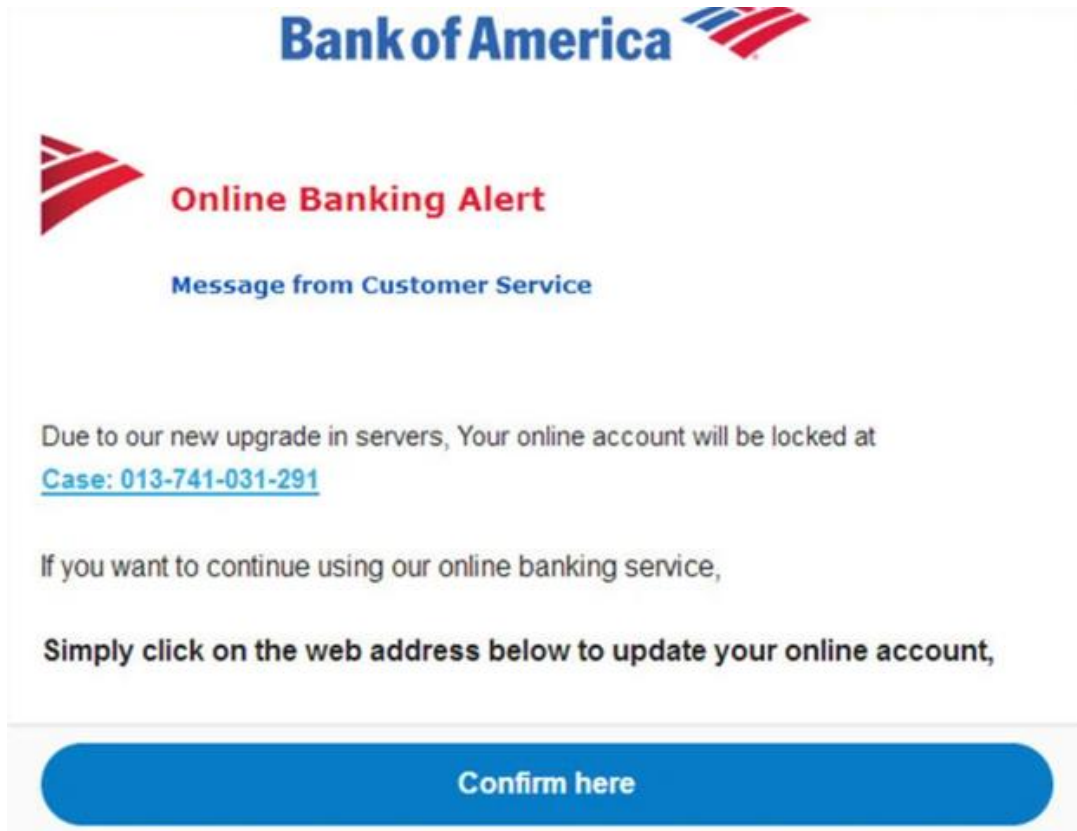
- AK-CB1 Compared to most emails, the sender has high expectations about the impact this email will have on me.
- AK-CB2 The sender's goal for this phishing email is very ambitious.
- AK-CB3 The sender is trying to get a lot from me with this phishing email.
- AK-CB4 The sender has high expectations about what the phishing email will get me to believe.
- AK-CB5 Overall, I don't feel as if the sender of the phishing email is asking that much of me.

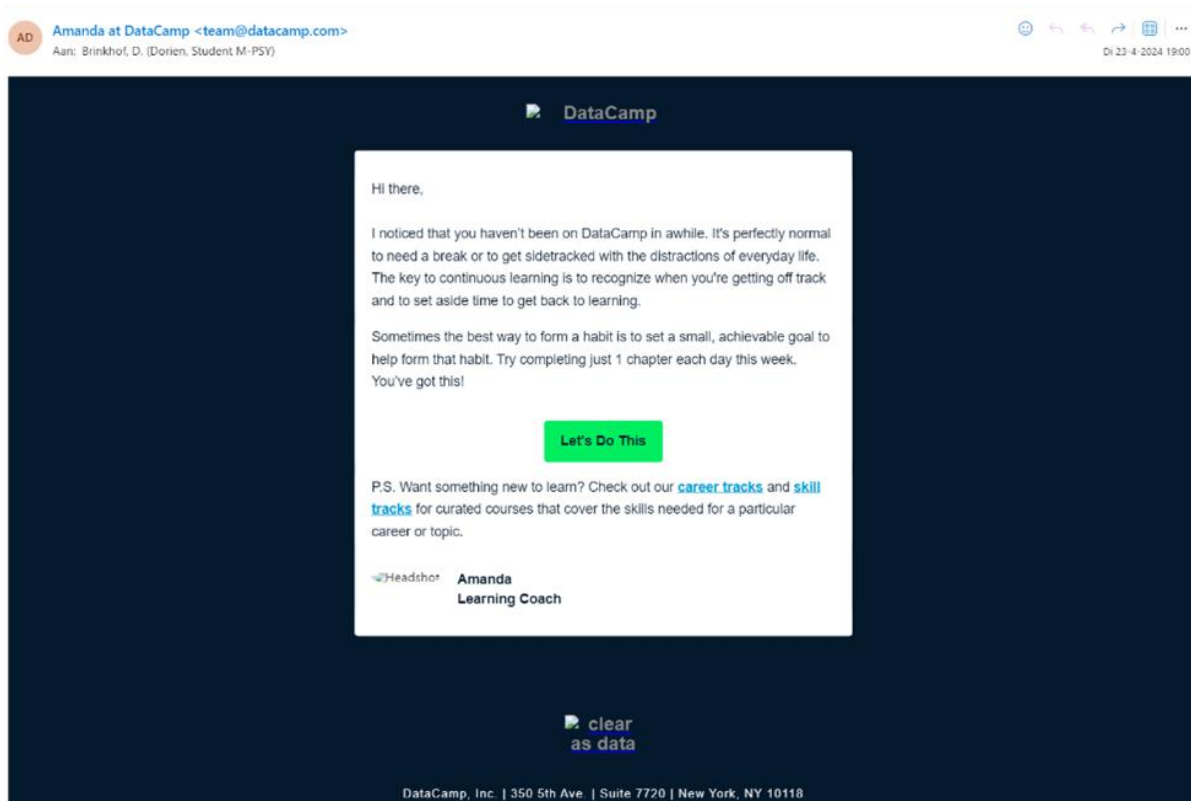
B. Cybercriminal's Investment

- AK-CI1 The sender seems to have put more effort into this email than is usual for non-phishing emails.
- AK-CI2 The sender seems to have put a lot of time into phishing email.
- AK-CI3 The sender deserves credit for the creative effort that went into a phishing email.
- AK-CI4 A phishing email is not expensive to make (r).
- AK-CI5 A phishing email shows a lot of thought and care.

Prompt: The next two sections evaluate your perception of the sender's intentions and efforts in crafting phishing emails in general. You will assess the sender's goals, ambitions, and level of investment in creating phishing emails based on your understanding of such activities. Your responses will provide insights into your perception of the sender's motivations and the effort put into phishing attempts.

Appendix C
PRE-theory emails







Fax Message NoReply [admin] <noreply@efacks.com>
to me ▾


09:17

You have received a 1-page fax at 26/04/2024, 09:17

[Click here to view this fax online](#)



Thank you for using the eFax Service! Please visit www.eFax.com/en/efax/page/help if you have any questions, or believe that you have received this fax in error.
eFax Inc (c) 2024

 **Google** <no-reply@google.support> 09:30
from: Google <no-reply@google.support>
to: Participant <participant@utwente.nl>
date: 26 Apr 2024, 09:30:33
subject: Someone has your password

Someone has your password

Hi,

Someone just used your password to try to sign in to your Google Account.

Information:
Friday, 26 April 2024 at 09:30:33 GMT+02:00
Slatina, Romania
Firefox browser

Google stopped this sign-in attempt. You should change your password immediately

[CHANGE PASSWORD](#)

Best,

The Mail Team

From: Account Support <reza.clalucyankdia6@gmail.com>

Sent: Monday, February 15, 2021 6:41:04 AM

To: [REDACTED]

Subject: Re: Your account has been filtered by our system for authentication.



Dear Customer,

Your account has been filtered by our system for authentication. Please view the possible events listed below for this cause.

Possible events occurred

1. Log in attempts from, Windows 7 - Ontario, Canada.
2. Requesting any operation using unusual pattern.
3. Too many incorrect log in attempts.

For security, all your account features are disabled until a response has been received from you.

Please click "Authenticate now" button below to secure your account.

[Authenticate now](#)

Best regards,

PayPal Inc Help Center

From: accountupdate@google.org.com

To: Your email

Subject: SupremelInvoice: New bill

SupremelInvoice

Here is the new invoice for last week's activities.

Invoice Number	Amount	Click below to connect to the invoice system
36691	1,265.68\$	System Invoice Connect


Thank you for using SupremelInvoice

Academia.edu <premium@academia-mail.com>
Aan: [REDACTED]

Beantwoorden | Allen beantwoorden | Doorsturen | [Grid Icon] | [More Icon]

Wo 10-4-2024 14:31

ACADEMIA





You downloaded the paper,
"Answering Questions about Questions: A Persuasion Knowledge Perspective for Understanding the Effects of Rhetorical Questions"

Bulk Download 37 books in Tourism.


[Bulk Download Now >](#)

580 California St., Suite 400, San Francisco, CA, 94104
Unsubscribe | Privacy Policy | Terms of Service
© 2024 Academia

 **Dropbox** <no-reply@dropboxmail.com>
to me 

09:18

from: Dropbox <no-reply@dropboxmail.com>
to: Participant <participant@utwente.nl>
date: 26 Apr 2024, 09:18:43
subject: Your Dropbox has stopped syncing



Your Dropbox is full and is no longer syncing files. New files added to your Dropbox folder won't be accessible on your other devices and won't be backed up online.

Upgrade your Dropbox today and get 1 TB (1,000 GB) of space and powerful sharing features.

[Upgrade your Dropbox](#)

For other ways to get more space, visit our [Get More Space](#) page.

Happy Dropboxing!

– The Dropbox Team

P.S. If you need the biggest plan we've got, take a look at [Dropbox for Business](#).



NEW! Why You Should Add Disaster Recovery as a Service to Your Portfolio

From: RCPmag.com RCP@1105info.com

To: Participant participant@gmail.com ✓



New Webcast:

Why You Should Add Disaster Recovery as a Service to Your Portfolio >

Monday, July 26th

Monday, July 26th

When you register, you are also signed up for a chance at a \$100 Amazon gift card!*

Hi Participant,

The clock starts ticking the minute a critical business system goes down. As lost revenue piles up and productivity drops, resuming normal operations becomes paramount. The fastest way to recover is to relocate the workload to another server, often at a secondary location. But for most businesses, the redundant hardware, server space and additional Human Resources are far too costly to make this a viable option.

So, in the face of potentially devastating outages, many IT departments simply live with the risk or settle for less expensive backup options for critical workloads.

Join this webinar to learn why you should add disaster recovery as a service to your portfolio.



Sponsored by Carbonite

*One gift card will be awarded based on a random drawing from among all valid entries. All registrations must be received by July 26, 2021. Only valid e-mail addresses will be considered. The prize consists of one gift card in the amount of 100 US dollars towards the purchase of anything in the Amazon.com Store. No substitutions allowed. False and/or deceptive entries or acts shall render entrants ineligible. No purchase is required. Chances of winning depend on the number of respondents. This offer is not valid where prohibited by law.



Your Ink Business Unlimited payment is due on Aug 7

From: Chase no_reply_alerts@chase.com

To: Participant participant@gmail.com



Payment due



Your credit card payment is due on Aug 7

Please review and complete your payment.

Account	Ink Business Unlimited (...1421)
Due date	Aug 7
Minimum payment due	\$63.00
Statement balance as of Jul 28	\$6,355.82

The minimum payment amount above does not include payments, adjustments, or activity since your last statement was generated.

Make a payment

Set up auto-pay

Securely access your accounts with the [Chase Mobile® app](#) or chase.com.

ABOUT THIS MESSAGE

Chase Mobile® app is available for select mobile devices. Message and data rates may apply.

This service email was sent based on your alert settings. Use the Chase Mobile app or visit chase.com/alerts to view or manage your settings.

Chase cannot guarantee the delivery of alerts and notifications. Wireless or internet service provider outages or other circumstances could delay them. You can always check chase.com or the Chase Mobile app for the status of your accounts including your latest account balances and transaction details.

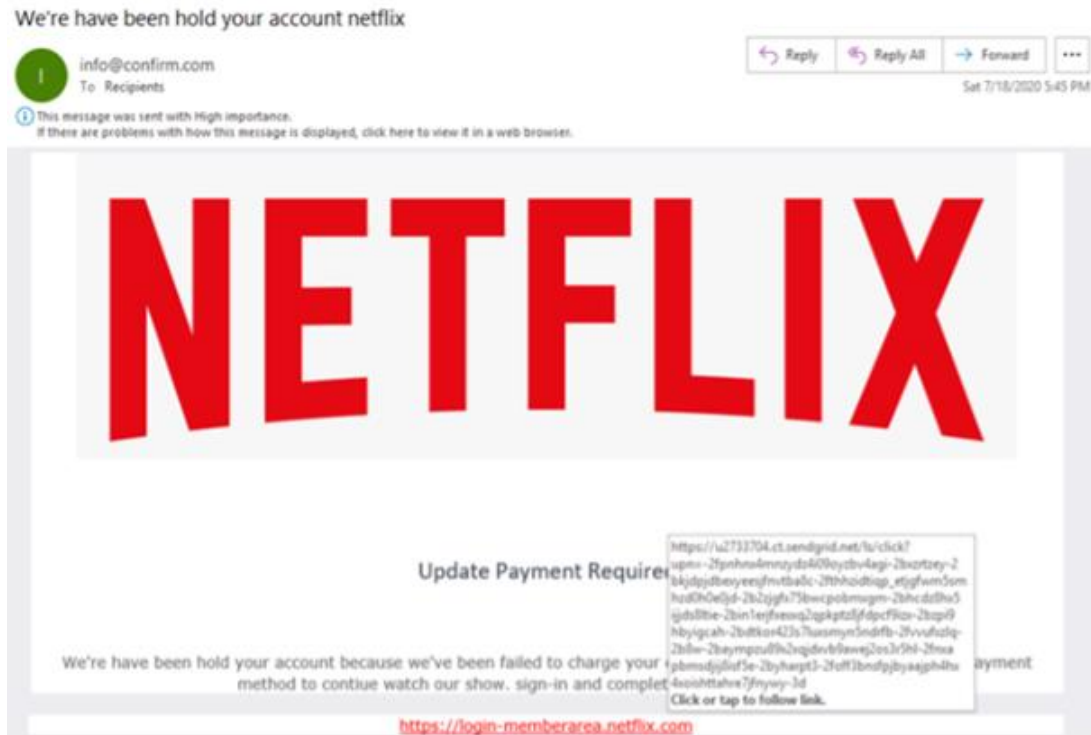
To protect your personal information, please don't reply to this message. Chase won't ask for confidential information in an email.

If you have concerns about the authenticity of this message or have questions about your account visit chase.com/CustomerService for ways to contact us.

Your privacy is important to us. See our online [Security Center](#) to learn how to protect your information.

©2022 JPMorgan Chase & Co.

Appendix D POST-theory emails



From: Bank of America <ba...> ☆
Subject: Security Alert: Unusual Account Activity Detected 7/13/2021, 1:01 AM
To: Value Customer <1...> ☆



Account Suspended

Dear Valued Customer,

We're letting you know that we've detected some unusual activity on your Bank of America account. For your protection, please verify this activity so you can continue making debit/credit card transactions without interruption.

To re-activate your access, Please download and fill the attached file to continue with the validation process to restore your account and continue the use of online banking. We will review and work towards a resolution.

Thank you for being our customer and We sincerely apologize for the inconveniences. Your account security is our top priority.

Note: If you do not verify, certain limitations may be placed on your debit/credit card.

Sincerely,

Thank you for being our customer.



This is a service email from Bank of America. Please note that you may receive service emails in accordance with your Bank of America service agreements, whether or not you elect to receive promotional email.

[Read our Privacy Notice.](#)

Please don't reply directly to this automatically generated email message.

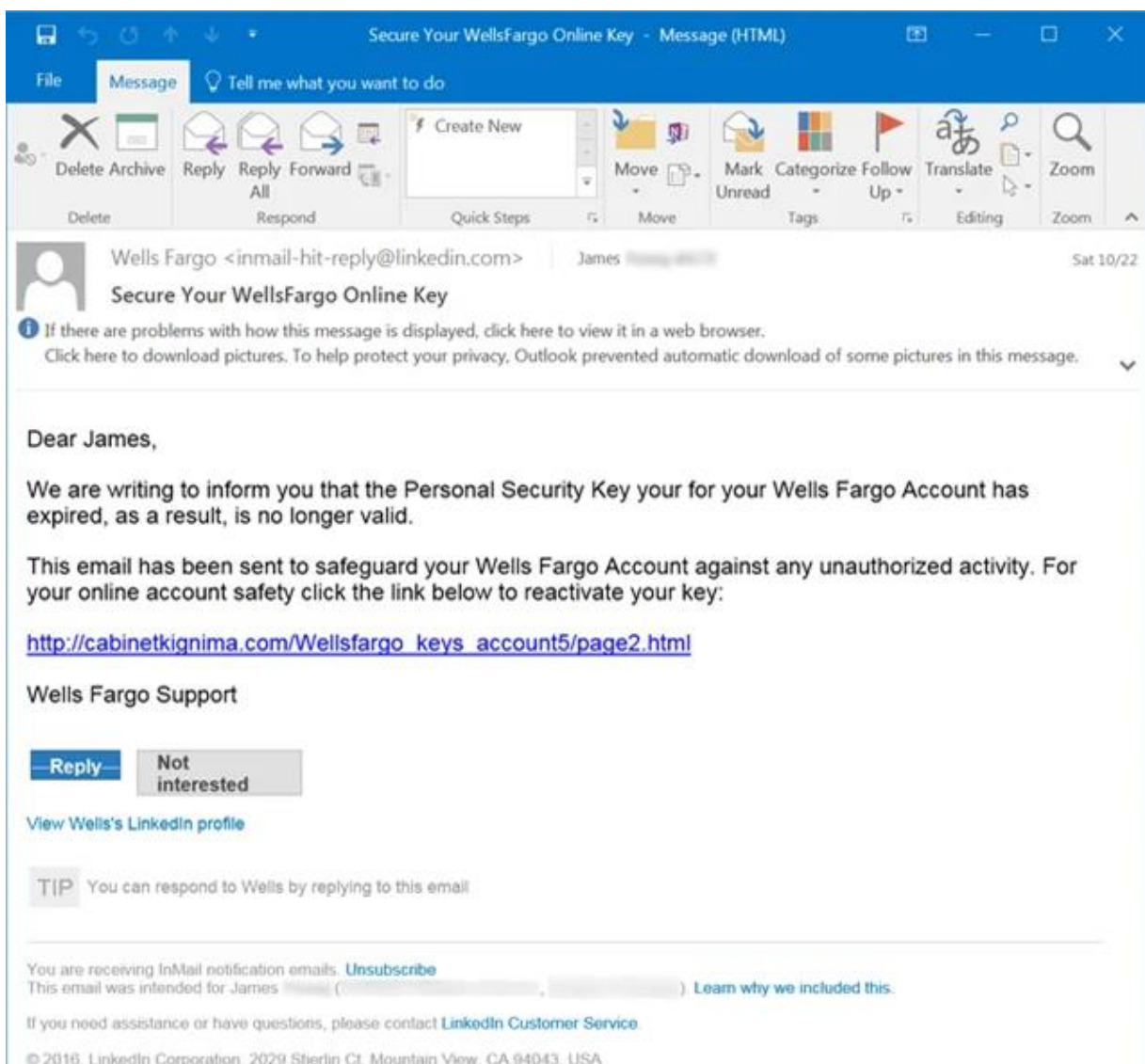
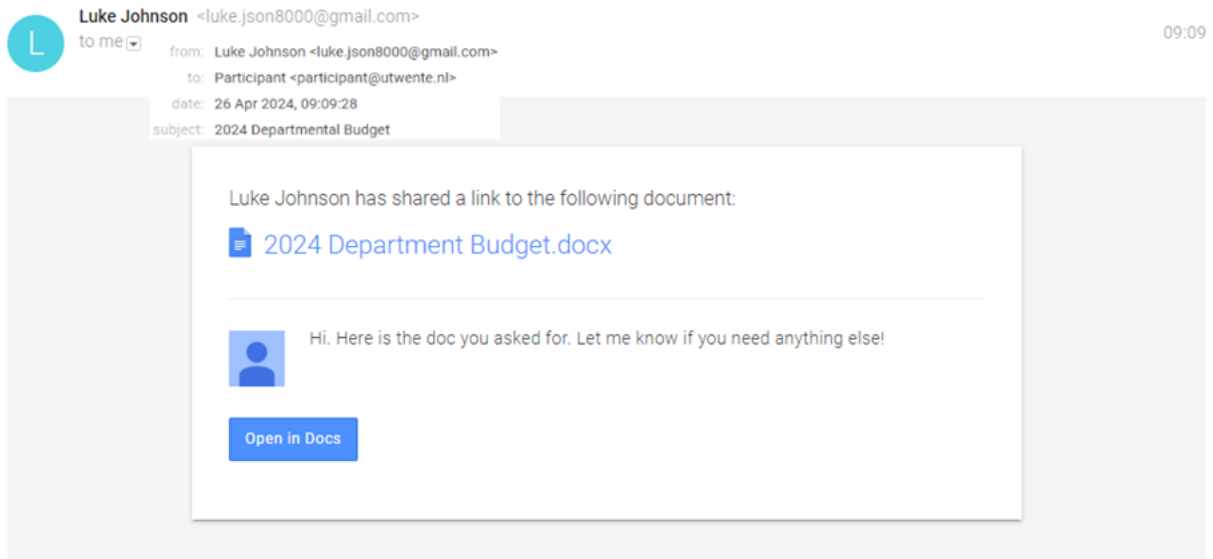
Bank of America Email, NC1-028-09-01, 150 N College St., Charlotte, NC 28255

Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2021 Bank of America Corporation. All rights reserved.


This email was sent to: Valued Customer

1 attachment: Bank of America Account Verification.html 106 KB

Save



Google <no-reply@google.support> 09:34
from: Google <no-reply@google.support>
to: Participant <participant@utwente.nl>
date: 26 Apr 2024, 09:34:17
subject: Someone has your password




Government-backed attackers may be trying to steal your password

There's a chance that this is a false alarm, but we believe that we detected government-backed attackers trying to steal your password. This happens to less than 0.1% of all Gmail users. We can't reveal what tipped us off because the attackers will take note and change their tactics, but if they are successful at some point they could access your data or take other actions using your account. To further improve your security, based on your current settings, we recommend:

[Change password](#)

From: domain@domain-name.com
To: Your email
Subject: Apple Facetime Information Disclosure



National Security Department

A vulnerability has been identified in the Apple Facetime mobile applications that allow an attacker to record calls and videos from your mobile device without your knowledge.

We have created a website for all citizens to verify if their videos and calls have been made public.

To perform the verification, please use the following link:

Facetime Verification

This website will be available for 72 hours.

National Security Department

From: Klarna <noreply-nl@klarna.nl>
Sent: Wednesday, April 24, 2024 11:00:37 PM
To: [REDACTED]
Subject: Information about refund

Klarna.

Vparts

Order#: NL-24-03-18-0002



Hi [REDACTED] We are contacting you regarding a refund for your order from Vparts.

We will refund you €109.50 to your debited bank account. It can take up to seven banking days before you get the money back.

If we only reserved the amount on your bank account we will remove the reservation. In that case you will not receive a refund transfer and you will instead get the reserved amount back.

Refund Amount €109.50

Reference number 4612[REDACTED]0140

[Open in App](#)

FAQ

Your refund will be processed within 5-7 business days. Once the store has registered your return or cancellation, you will receive your refund according to the store's refund policy.

[Click here for more questions](#)

This email has been sent out automatically and cannot be answered.

K.

f @ t in

Klarna Bank AB (publ)
Sveavägen 46
111 34 Stockholm, Sweden
Org. nr: SE556737-0431

Postadres:
Klarna BV
Weesperstraat 61
1018 VN Amsterdam, Nederland
KvK: 50315250
klarna.com

AA Anjali - ProjectPro Advisor <anjali@projectpro.io>
 Aan: [REDACTED]



Hi,

It's been a while since we last connected, but we're excited to reach out to you once again with a fantastic offer! We're reaching out to you today with an exciting opportunity to revisit [ProjectPro](#) and experience all it has to offer once again. Here is an exclusive invitation to you for a [7-day FREE trial of ProjectPro](#). This is your chance to experience firsthand how ProjectPro can help you grow your data skills.

[Sign Up for 7 Day FREE Trial](#)

During your 7-day FREE trial, you'll have the opportunity to explore our vast library of 270+ reusable project templates covering a wide range of topics like [LLM & Generative AI](#), [MLOps](#), [Machine Learning](#), [Computer Vision](#), [NLP](#), Data Science, [AWS](#), [Azure](#), [GCP](#), and many more. Our reusable project templates not only simplify the learning process but also improve productivity, enabling you to focus on delivering results. Take this opportunity to revisit the platform and experience all the latest projects and features we've added since you last used it.

[Get Access Now](#)

Why ProjectPro?

- **Unrestricted Access:** 270+ Enterprise-Grade projects to choose from. Access to any 15 premium projects of your choice covering diverse domains like AI, Machine Learning, Data Engineering, Data Science, Big Data and Cloud Computing.
- **Advanced Personalised Learning Paths:** Master advanced skills with curated learning paths personalised to your career goals and aspirations. [Check Out ProjectPro's Most Trending Learning Paths](#).
- **Hands-On Exercises:** Project-Based Exercises for Concept Understanding
- **Build a Portfolio based on Real-World Projects.**
- **Personalization options across various domains**
- **Unlimited learning opportunities to enhance your skills and expertise**

Should you wish to understand how these projects can accelerate your career, or have any queries, reply to this email.

Best Regards,

Anjali from ProjectPro

Helping Every Developer Become a 10x Developer



ProjectPro


Copyright © 2024 Binnydezyre. All rights reserved.

Just a friendly reminder: You're receiving this email because you signed up for ProjectPro. If you have any questions or concerns, feel free to reach out to us anytime!



Verify Email


From: Doodle no-reply@doodle.com
To: Participant participant@gmail.com



Confirm your email address

Please confirm your account by navigating to the link provided below:

[Verify email](#)



Doodle AG, Werdstrasse 21, 8021 Zürich



Bill 22427 from Steven Murphy Electrical Contractors Pty Ltd is due

From: invoicereinders@post.xero.com
To: Participant participant@gmail.com

[View Invoice](#) 433.00 due 14 Jul
22427

Hi Participant,

Thank you for your business. Your bill for \$433.00 was due on 14 Jul.

If you've already paid it, please ignore this email. If you've not done so, please pay immediately.

To view your bill visit:
<https://in.xero.com/oY8zP3TUYDgSwb296zotAwydQXL3UJhdxKmDvEzM>.

If you've got any questions, or want to arrange alternative payment don't hesitate to get in touch.

Regards
Bob Smith
Accounts Manager
Steven Murphy Electrical Contractors Pty Ltd

Appendix E

Theory

Theory about Understanding Phishing Emails

We often hear about protecting ourselves from phishing emails by checking for spelling errors or strange requests. But did you know that these emails also use tactics like deception and persuasion to trick us? Let's explore these tactics to stay ahead of scammers:

Phishing emails...

- ...pretend to be from trusted sources (bank or government) to trick you into giving away personal information or clicking on harmful links. They may create a sense of urgency, pushing you to act quickly. Always verify the sender's email address and take your time to assess the urgency before taking action.
- ...may claim that others are already taking action, pressuring you to do the same. Question anything that seems too good to be true.
- ...may pretend to be from someone you know (friends or colleagues), asking for help or personal information. Verify the sender's identity through other means, such as a phone call or direct message, before responding.
- ...may offer free trials or discounts to lure you into providing personal information to claim the offer. It's tempting to jump at the chance. Better pause and think before accepting any offers and read the fine print.
- ...love to create panic by claiming your account will be blocked unless you act immediately. Take a breath and think logically before reacting.

By understanding these tactics, you can protect yourself from phishing emails. Stay cautious, verify the sender's identity, and report suspicious emails. Together, we can outsmart the scammers and keep our information safe.

Thank you for taking the time to learn about phishing email tactics and how to recognize them. We will use this knowledge in one of the upcoming sections of the survey. Please answer the related questions based on the theory you just read.

- I have taken note of the above-mentioned tactics often used in phishing.