American Journal of Education and Technology (AJET)

ISSN: 2832-9481 (ONLINE)

VOLUME 4 ISSUE 3 (2025)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Education and Technology (AJET)

Volume 4 Issue 3, Year 2025
ISSN: 2832-9481 (Online)
DOI: https://doi.org/10.54536/ajet.v4i3.4773
https://journals.e-palli.com/home/index.php/ajet

Academic Trust Betrayed: Unravelling the Factors Behind Lecturers' Vulnerability to Social Engineering Attacks

Samuel Adu-Gyimah[1] , Oliver Kufour Boansi[1], George Asante[1*], Prince Clement Addo[1]

Article Information

Received: April 07, 2025
Accepted: May 03, 2025
Published: August 28, 2025

Keywords

Cybersecurity, Phishing, Pretexting, Susceptibility, Social Engineering Attacks

ABSTRACT

Social engineering (SE) attacks are the most treacherous cyber-attacks, which are not rooted in the manipulation of code or exploitation of system vulnerabilities but target the human factor, which has historically been the weakest link in the security chain. The school settings that promote collaboration among students and lecturers alike, the openness of sharing information among students and lecturers and the trust built over time in this communities make them vulnerable to SE attacks. This study then seeks to investigate how effective cybersecurity education and training intervention has in reducing the susceptibility of SE attacks among the staff of higher education. 292 participants were exposed to four types of SE attacks (Pretexting, phishing, baiting and quid pro quo), before and after the intervention. The results of the study show high reduction in susceptibility to all four attacks with the largest reduction observed in quid pro quo attacks. The intervention shows effective among younger age groups and certain faculties. Therefore, showing the need for tailored educational strategies on cybersecurity. The results also show the importance of comprehensive and targeted cybersecurity education in reducing SE threats. The study then recommends that future study should explore the long-term effects of such interventions and their potential in diverse contexts.

INTRODUCTION

This current era has seen digital transformation in every sector, including education, bringing with it an array of opportunities for innovation, growth and efficiency. These advancements also come with challenges, as the security of information Systems has become a critical issue of Concern. Among the potential threats, one of the most treacherous is not rooted in the manipulation of code or exploiting the vulnerabilities of systems, but rather it targets the users (human) of a system, who happen to be the weakest Link in the security chain (Adu-Gyimah et al, 2022). This threat is SE attack. SE attack is a cyberattack that employs manipulation techniques by attackers to trick their victims into divulging important information or performing actions that would compromise the integrity of a system (Birthriya *et al.,* 2024). SE attacks include baiting (Singh, 2025), phishing (Schmitt & Flechais, 2024), pretexting (Femi-Oyewole *et al.,* 2024), quid pro quo (Hussain & Abbas, 2025), tailgating (Cochran, 2024), etc. each design with some capabilities to psychological trigger to exploit the vulnerabilities of human.

SE attacks hinge on the trust victims place in their attackers, their quest to be helpful, their weakness to persuasion, their inclination towards fear, and so on. All these make humans easy targets for SE attacks (Gururaj *et al.,* 2024). Attacks on humans render even the most advanced security technological systems or advanced protocols ineffective if the human at the center is successfully compromised.

A study conducted by Riahi & Islam (2024) has shown that users have diverse views and practices concerning information security, all of which can impact their susceptibility to social engineering attacks. (Hadan *et al.,* 2024) study provides qualitative data on users' perceptions of security risks and their responses, underscoring the need for cybersecurity education and training interventions to be tailored to address users' specific needs and contexts. Therefore, this study contributes to the body of knowledge by implementing and evaluating an intervention on cybersecurity education in a higher education setting.

The human weakness in SE attacks has led to an increase in the frequency and intensity of SE attacks on several sectors, of which the education sector has not been spared. The nature of this sector, such as the openness of information sharing, the collaborative nature of work, and the trust inherent within its communities, makes it vulnerable to SE attacks. There is, therefore, a need to investigate this problem more thoroughly within the school setting and devise effective strategies to counter it. Our reliance on modern technological advancements, coupled with the openness and trust within the school settings, makes the educational sector a prime target for SE attacks (Mudi, 2024). Among the potential targets within the school settings, lecturers stand out as the most to be targeted due to these factors:

First of all, they have access to sensitive information ranging from students' academic data to valuable intellectual properties. Also, the role they play demands a high level of collaboration and interaction among both

[1] Department of Information Technology Education, Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development, Ghana
[*] Corresponding author's e-mail: gasante@aamusted.edu.gh

students and other staff, which can expose them to an increased risk of SE tactics such as phishing, pretexting, quid pro quo, and baiting (Creese *et al.,* 2021).

Secondly, digital competence among lecturers may vary. A lack of cybersecurity awareness and training can make them vulnerable to SE attacks (Aslan *et al.,* 2023). The constant pursuit of academic glories and the pressure to stay well-informed academically may divert their focus from understanding the evolving landscape of information security threats, therefore increasing their susceptibility to SE attacks.

Studies into the effectiveness of interventions designed to reduce vulnerability to SE attacks in school settings remain limited (Jeong *et al.,* 2019). Therefore, this study seeks to address this research gap by investigating the effectiveness of a cybersecurity education and training intervention among university lecturers.

The whole idea of the intervention is to improve awareness and prevention of four types of SE attacks: quid pro quo, phishing, baiting, and pretexting.

The key hypothesis of the study (H1) is that cybersecurity education and training will largely reduce vulnerability to SE attacks among university lecturers. Moreover, this study aims to explore the differential impact of the intervention across different demographic groups and faculties (H2). It is hypothesized that the decrease in vulnerability will be greater for certain types of attacks compared to others after the intervention (H3). Furthermore, the study expects that the rate of change in vulnerability (from pre- to post-intervention) will be greater for age groups who are younger as compared to older age groups, therefore suggesting that younger individuals are more responsive to cybersecurity education and training (H4).

These hypotheses fall in line with a previous study suggesting the efficacy of cybersecurity education in reducing susceptibility to cyberattacks (Shillair *et al.,* n.d.). This study contributes to the growing body of evidence on the efficacy of cybersecurity education and training in reducing SE attacks and extends it by examining the impact of such interventions in a school setting. The findings of the study have important implications for the design of cybersecurity education and training programs in universities and potentially other similar institutions. By establishing which demographic groups and faculties are most responsive to the intervention and which types of attacks are most effectively reduced, the intervention can be further tailored to maximize its effectiveness.

LITERATURE REVIEW

Social Engineering Attacks

Social engineering attacks have become a critical concern in the field of cybersecurity (Almutairi *et al.,* 2022). These attacks rely on human interaction to manipulate individuals into breaking standard security practices, thus allowing unauthorized access to systems or data (Aslan *et al.,* 2023). SE attacks comes in many forms, and a range of tactics from phishing to baiting, pretexting, quid pro quo, tailgating, dustbin diving, shoulder surfing, etc. (Gururaj *et al.,* 2024).

This section reviews literature around the four types of SE attacks used in the study. They are phishing, pretexting, quid pro quo, and baiting. The study simulates these attacks.

Recently much attention has been drawn to the distractive nature of SE attacks and the tactics used in these attacks, just to create awareness. This attention is partly due to an understanding that while technological defenses are essential, they are insufficient in the face of attacks that primarily exploit human psychology (Marble *et al.,* 2015). This has led to a growing interest in the role of cybersecurity education and training as a crucial line of defense (Aslan *et al.,* 2023; Mudi, 2024).

Phishing Attack

The most widely studied form of SE attack is Phishing attack (51 Must-Know Phishing Statistics for 2023, n.d.; Burita *et al.,* 2021). It is characterized by attempts to trick individuals into giving sensitive information, often through receiving deceptive emails that poses as from legitimate entities (Kirda *et al.,* n.d.). This attack has evolved into several sub-forms like 'vishing' (voice phishing) (Jones *et al.,* 2020), 'smishing' (SMS phishing) (Soykan & Energies, 2020), and 'spear phishing' (targeted phishing) (Al-Hamar *et al.,* n.d.; Burns *et al.,* 2019), each using unique tactics for deception.

Pretexting Attack

A pretexting attack involves creating a fictitious scenario (the pretext) to trick an individual into providing access to information. A pretexting attack relies on building trust with the victim. It uses complex SE manipulation techniques (Mouton, Leenen, & Security, 2016)

Quid Pro Quo Attack

Quid pro quo attacks, that is, 'something for something' attacks, involve an attacker offering some kind of services or giving some forms of benefits in exchange for information or access to a system with fictitious intent. The attacker impersonates a technical support agent and then offers help in exchange for the victim's login details or other sensitive information (Hussain & Abbas, 2025).

Baiting Attack

Baiting attack looks similar to quid pro quo attacks, but involves the giving of something just to use as a 'bait' to lure the victim. These things could be an offer of free software downloads, a USB stick left in a public place, or any other interesting thing that could lure someone into falling for the trap (Singh, 2025).

This study aims to examine the effectiveness of cybersecurity education and training in reducing vulnerability to these different types of SE attacks, thereby contributing to the growing body of research in this area. It is through this context that the study's hypotheses have been formulated.

Social Engineering Attack in the Educational Sector

SE attacks have become a major concern in higher educational institutions worldwide. Schools are also attractive targets for cybercriminals due to the openness in their operations and of academic networks that are established among stakeholders, the type of data they hold, and the population they serve (young, technologically adept individuals who may not yet have developed a strong sense of cybersecurity awareness). Some empirical evidence supports this claim. A study by the EDUCAUSE Center for Analysis and Research (2021) reported that higher education institutions are among the top three sectors targeted by phishing attacks, making up 6% of all phishing campaigns worldwide (Karthikeyan, n.d.; Kendall, 2022). Similarly, research by Proofpoint (2019) highlighted that educational institutions are 4.5 times more likely to suffer from email fraud as compared to other sectors (Alawida *et al.,* 2022).

Also, Lallie *et al.* (2025) in their study analyzed the susceptibility of universities to SE attacks, finding that university employees, including lecturers, are often easy targets for these attacks due to their limited awareness of such threats. Their study demonstrated the efficacy of using simulated SE attacks as a training tool, aligning with the approach taken in our study.

Furthermore, Mouton, Venter, and Rabe (2016) surveyed university students. They found that while students had a general understanding of SE threats, they were deficient in knowledge about specific SE attack tactics, therefore potentially vulnerable to such attacks.

These, therefore, underpin the importance of the extensive cybersecurity education and training intervention implemented in our study.

The Gap in the Literature

Even though a considerable number of studies have been done on SE and cybersecurity education, some gaps persist in the existing literature. Largely, the academic context has been under studied. Though numerous studies have researched into the susceptibility of corporations and institutions to SE attacks, few have focused specifically on the school settings, mostly on university lecturers (Arachchilage & behavior, 2014). Given the role of university lecturers in managing sensitive academic records, it is important to understand their vulnerability to SE attacks and the effectiveness of interventions in reducing this susceptibility. Also, there is no study investigating the relative effectiveness of cybersecurity education across diverse types of SE attacks. While some studies have evaluated the impact of such interventions, very few have made comparisons across various SE attack types like pretexting, phishing, baiting, and quid pro quo (Pfleeger & Caputo, 2012).

This research aims to bridge this gap by assessing and comparing the effectiveness of the intervention across these four SE attack types. Additionally, there are insufficient studies that look into the role of demographic factors in SE attack vulnerability and intervention effectiveness. This research seeks to address this gap by examining the intervention's effectiveness across different age groups, genders, and faculty departments. By so doing, it will offer a more comprehensive understanding of who is most vulnerable to these SE attacks and how interventions can be best custom-made to different demographic groups.

MATERIALS AND METHODS

Participants

The participant sample for this study consists of lecturers from the Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development - AAMUSTED. An experimental research design was adopted using Primary Experimental Data collection, where the participants were informed of the general nature and purpose of the research without going into specifics. This ethical deception was employed to prevent participants from altering their natural behaviour during the course of a study. All participants gave their consent to participate before the commencement of the simulations. Based on the American Psychological Association (APA) guidelines (American Psychological Association Guidelines 7th Edition - Google Search, n.d.), the informed consent procedure was designed to ensure that participants are given as much information as necessary to decide whether to participate. No actual sensitive data was collected. Most of the data collected included dichotomous values (Yes, No; victim, not victim; bait successful, bait fail; Active, inactive). A total of 292 participants signed up for the initial experiment with a demographic distribution across age, gender, years of teaching experience, and area of specialization.

Baseline Assessment: A pre-intervention social engineering attack simulation (phishing, pretexting, quid pro quo, and baiting) was conducted on the participant sample to establish a baseline of their vulnerability to these types of attacks.

Simulation Design and Execution

To assess the effectiveness of our cybersecurity education and training intervention, we needed to accurately measure the participants' susceptibility to social engineering attacks both before and after the intervention. Drawing from the work of Kruger and Kearney (2006), who developed a model for assessing information security awareness, we designed a simulation exercise that emulated different types of social engineering attacks (Kruger & Kearney, 2006). This approach allowed us to not only measure the initial level of susceptibility but also to track any changes in susceptibility over time, thereby providing a clear indication of the intervention's effectiveness.

The study involved designing four social engineering attack simulations, each representing one of the following tactics: phishing, pretexting, quid pro quo, and baiting. Phishing and pretexting remain one of the top SE attack methods, and the reason they were selected. Quid pro quo and baiting are less seen in SE literature, which makes them less known, and so are those that can be easily used on unsuspecting victims (Langlois, 2020).

Each simulation was meticulously designed to replicate real-world social engineering scenarios, and they were executed in a controlled and ethical manner, ensuring the participants' data security and privacy. Phishing was geared towards exploiting trust and authority, pretexting by building credible but fake stories, and quid pro quo using the principle of reciprocity, while our baiting leverages curiosity and greed. This is done to diversify the simulation methods.

Phishing Simulation

The phishing simulation involved a simulated email appearing to come from a trusted source within the university, asking the lecturers to click on a link to enter their login credentials for a seemingly legitimate purpose. They were also instructed to click on a similar link for system updates. A self-developed website with a URL very similar to the university's legitimate examination portal was sent through a mirrored university email.

Pretexting Simulation

In the pretexting simulation, a researcher posing as a member of the university IT unit contacted the lecturers via phone, stating that they needed to confirm their identity for a system update and asked for sensitive information including IP address, username, password, password recovery email, date of birth and providing emails to receive links for system updates among others.

Quid Pro Quo Simulation

The quid pro quo simulation involved offering a service, including free software, promising research funding in exchange for information, and access to academic resources for article downloading in exchange for login credentials or other sensitive information. The offer was made through an email appearing to be from a reputable external organization.

Baiting Simulation

The baiting simulation involved leaving a USB drive labelled with an enticing label "Confidential", "Exam Questions", "UN scholarship and funding", "Annual budget", "presidential award 2025", etc., in a place frequented by lecturers. The drive contained a harmless file that, when opened, sent a notification to the researchers, indicating that the bait had been taken. In all simulations, no actual sensitive information was collected or stored; the goal was merely to ascertain whether the lecturer would take the bait. After each simulation, debriefing sessions were held to explain the purpose of the simulation and educate participants about the social engineering tactic used.

Data Collection

Data was collected based on whether the participants responded to the deceptive prompts in the simulations. In the case of the phishing, pretexting, and quid pro quo simulations, a response was counted if the participant entered any information into the deceptive form or provided (begin to provide) it over the phone. For the baiting simulation, data was collected when the file inside the USB drive was accessed. The participants were randomly assigned so each person can only participate in two of the simulations to deal with carry-over effects at the post-intervention stage.

Intervention and Education

After each simulation, participants were debriefed. The participants were taken through a day cybersecurity education and training program aimed at improving awareness and prevention of social engineering attacks This educational component was a critical part of the process, aimed not only to enhance the understanding of the participants but also to increase general awareness about social engineering threats within the university. In designing our cybersecurity education and training intervention, we drew inspiration from practical and engaging approaches employed in previous research. A notable example is the work of Kumaraguru *et al.* (2007), who designed and evaluated a training email system aimed at protecting individuals from phishing attacks (Kumaraguru *et al.,* 2007). Such practical, contextually relevant interventions have proven to be effective in enhancing individuals' cybersecurity awareness and skills. In our case, we developed a series of tailored training modules that encompassed the most common types of social engineering attacks, including phishing, pretexting, quid pro quo, and baiting.

Dealing with Carry-Over Effects

The study employed several techniques to deal with carry-over effects. First, the participants were randomly exposed to only two out of the four SE attack simulations at the pre-intervention stage. The participants are then exposed to all four simulations at the post-intervention stage to determine if they will be susceptible to all or some of the SE attacks. Next, the study allowed a 7-week washout period between the pre- and post-intervention simulations. During this period, participants are not exposed to any conditions of the experiment. The goal is to allow any effects from the previous condition to 'wear off' before the next condition is introduced. Finally, we introduced a counterbalance to be certain that any observed effects are due to the simulations themselves, rather than their order of presentation.

Post-Intervention

After the 7-week washout period, the post-intervention stage commenced. This stage aimed to assess the effectiveness of the cybersecurity education and training program in improving participants' awareness and their ability to identify and prevent the four types of social engineering attacks.

Simulation Re-run

The same four SE attack simulations (phishing,

pretexting, quid pro quo, and baiting) were run again with all participants. Unlike the pre-intervention stage, each participant was exposed to all four simulations this time. The order of the simulations was counterbalanced to control for order effects.

Data Collection

As in the pre-intervention stage, the same response criteria were used. The data used were collected based on the participants' responses to the deceptive prompts in the simulations.

Debriefing

Participants were debriefed following the post-intervention simulations. The debriefing helped to reinforce the key takeaways from the cybersecurity education and training program, addressing any concerns, and also, providing more advice on the protection against SE attacks.

Data Analysis

The data from both pre- and post-intervention stages were compared to assess the efficacy of the intervention. The rate of vulnerability to each type of SE attack before and after the intervention was analyzed. Moreover, the overall vulnerability rate to any form of the SE attacks was evaluated to determine the general efficacy of the intervention across all the SE attack types

RESULTS AND DISCUSSION

The pre- and post-simulation results are presented in this section. In line with Kruger and Kearney's (2006) model for assessing information security awareness, we conducted a comparative analysis of the pre-and post-intervention susceptibility rates.

This involves analyzing the vulnerability rate to each type of SE attack before and after the intervention. The findings were compared to assess the overall efficacy of the intervention across all the four SE attack types. The approach helped us to measure the change in information security awareness over time, then providing a vigorous assessment of the intervention's impact. The results are organized by the type of SE attack, with comparisons made between the pre-and post-intervention stages.

Descriptive Statistics

Table 1 provides an overview of the proportion of participants who fell for each type of the SE attacks at the pre-intervention and post-intervention stages. The participants are of a total of 292.

Table 1: Proportion of Participants Falling for Each Attack Type

Attack Type	Pre-Intervention (N=292)	Post-Intervention (N=292)
Phishing	186 (63.70%)	92 (31.51%)
Pretexting	137 (46.92%)	44 (15.07%)
Quid Pro Quo	206 (70.55%)	87 (29.79%)
Baiting	97 (33.22%)	25 (8.56%)

N=292

Inferential Statistics

An analysis of the data reveals significant reductions in susceptibility to all types of social engineering attacks from the pre- to post-intervention stages. There was a significant decrease in susceptibility in all cases with a 32.19 percentage points reduction in phishing attacks from 63.70% to 31.51%. Pretexting dropped from 46.92% to 15.07% (31.85 percentage points reduction). Similarly, quid pro quo attacks and baiting showed a decrease in susceptibility with 40.76 and 24.66 percentage points decrease respectively. The largest decrease was observed in the case of Quid Pro Quo attacks, which dropped from 70.55% pre-intervention to 29.79% post-intervention.

Table 2 is the result of a paired-sample t-test performed to compare the susceptibility rates, at the pre-and post-intervention stages.

There has been a statistically significant decrease

Table 2: Paired-Sample T-test

Attack Type	t-value	df	p-value
Phishing	8.65	291	<0.001
Pretexting	8.12	291	<0.001
Quid Pro Quo	10.32	291	<0.001
Baiting	7.49	291	<0.001

in the susceptibility rates from the pre- to post-intervention stages as shown in the p-values which are all less than 0.001. The t-values indicate the change in the susceptibility rates between the pre and post-intervention stages. Higher t-values are an indication of a larger rate of change between the two stages. The results indicate that Quid Pro Quo attacks (t-value = 10.32) saw the highest difference, followed by Phishing (t-value = 8.65), Pretexting (t-value = 8.12), and Baiting (t-value = 7.49). These results indicate that the intervention was highly

effective in reducing susceptibility to all four types of social engineering attacks among the participants.

Comparing the results in Table 3 to Cohen's benchmarks (Cohen, 1988), the effect sizes for all four types of attacks are within the medium to large range, suggesting that the cybersecurity education and training program had a considerable practical significance in reducing susceptibility to these social engineering attacks.

We conducted ANOVA to compare the effectiveness of the intervention across the four SE attacks followed by a post-hoc comparisons test to investigate which pairs of means are significantly different.

Table 3: Effect Sizes for Pre- and Post-Intervention Comparisons

Attack Type	M1	SD1	M2	SD2	SDpooled=sqrt [(SD1^2+SD2^2)/2]	Cohen's d = (M2-M1) / SDpooled
Phishing	0.6370	0.52	0.3151	0.47	0.495	-0.65
Pretexting	0.4692	0.50	0.1507	0.36	0.43	-0.74
Quid Pro Quo	0.7055	0.48	0.2979	0.46	0.47	-0.87
Baiting	0.3322	0.47	0.0856	0.28	0.375	-0.66

Table 4: ANOVA

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	20.25	3	6.75	6.53	0.00032	2.60
Within Groups	123.50	48	2.57			
Total	143.75	51				

The F-value of 6.53 is greater than the critical F-value of 2.60, and the p-value is less than 0.05. Hence, we reject the null hypothesis that there's no difference in the means and conclude that there's a significant difference in the susceptibility rates among the different attack types at the 0.05 level of significance.

The susceptibility rate to Phishing and Baiting is significantly different ($p<0.05$), as well as between Quid Pro Quo and Baiting, and Pretexting and Quid Pro Quo. The cybersecurity education and training intervention

Table 5: Post-Hoc Pairwise Comparisons

Attack Type (I)	Attack Type (J)	Mean Difference (I-J)	Std. Error	Sig.
Phishing	Pretexting	0.176	0.101	0.073
Phishing	Quid Pro Quo	-0.068	0.101	0.499
Phishing	Baiting	0.304	0.101	0.001
Pretexting	Quid Pro Quo	-0.244	0.101	0.017
Pretexting	Baiting	0.128	0.101	0.202
Quid Pro Quo	Baiting	0.372	0.101	0.000

Table 6: Intervention Efficacy by Demographic Group

Demographic Group	Categories	Pre-Intervention Susceptibility (%)	Post-Intervention Susceptibility (%)	Change (%)
Gender	Male	65	28	-37
	Female	62	32	-30
Age Group	Below 35	68	30	-38
	35-44	66	28	-38
	45-54	62	34	-28
	55 and above	60	36	-24
Faculties	Technical Education	67	31	-36
	Applied Sciences and Mathematics	65	24	-41
	Vocational Education	63	33	-30
	Business Education	64	32	-32
	Education and Com. Sciences	61	35	-26

N=292

significantly reduced susceptibility to social engineering attacks across all demographic groups and faculties. Males demonstrated a slightly larger decrease in susceptibility rates than females, with reductions of 37 and 30 percentage points, respectively. The intervention was most effective among younger age groups ("Below 35" and "35-44"), with a decrease of 38 percentage points, while the "45-54" and "55 and above" groups saw reductions of 28 and 24 percentage points, respectively. Among faculties, the largest decrease was observed in the "Applied Sciences and Mathematics" faculty (41 percentage point decrease), and the smallest in the "Education and Communication Sciences" faculty (26 percentage point decrease).

Interpretation of Results

Our findings indicate a significant decrease in susceptibility to social engineering attacks after the intervention, across all attack types. The t-tests demonstrated significant decreases in susceptibility rates for phishing, pretexting, quid pro quo, and baiting attacks. Moreover, the effect size calculations showed large effects for all types of attacks, suggesting that the intervention had a considerable impact. The ANOVA and posthoc tests further revealed significant differences between the pre- and post-intervention susceptibility rates, strengthening the evidence for the effectiveness of the intervention. Lastly, the demographic group analysis showed that all groups experienced a decrease in susceptibility, although there were variations across different demographics and faculties. These findings align with previous research on the impact of cybersecurity awareness and training on reducing vulnerability to social engineering attacks (Campbell, 2020; Hadlington, 2017).

Discussion

The findings from our study provide strong empirical support for all the proposed hypotheses, thus adding to the growing body of literature on the importance of cybersecurity education and training in mitigating SE attacks. As predicted in Hypothesis 1, our intervention significantly reduced susceptibility to all types of SE attacks examined in this study: phishing, pretexting, quid pro quo, and baiting. This fall in line with previous studies that highlighted the efficacy of cybersecurity education in reducing susceptibility to cyberattacks (Vishwanath, 2015; Weimann, 2015).

Hypothesis 2 recommended variation in the efficacy of the intervention across different demographic groups and faculties. Our results showed that the decrease in vulnerability is more noticeable among males, those under the age of 35 years, and those from the Applied Sciences and Mathematics and Technical Education faculties. This then recommends the need for custom-made cybersecurity education and training to the precise needs and characteristics of different demographic groups and faculties.

Corresponding to Hypothesis 3, we found that the vulnerability reduction is greater for certain types of SE attacks compared to others after the intervention. Precisely, vulnerability to phishing and pretexting was decreased more than that to quid pro quo and baiting. This shows that while our intervention is effective across all the SE attack types, its efficacy is more noticeable for phishing and pretexting. As hypothesized in Hypothesis 5, the rate of change in vulnerability to SE attacks was better for younger age groups compared to older ones. This suggests that younger individuals are more responsive to cybersecurity education and training, highlighting the importance of early intervention in this area.

The substantial decrease in vulnerability to phishing attacks observed in our study aligns with findings from earlier research. As Kumaraguru *et al.* (2007) demonstrated the effectiveness of an embedded training email system in protecting individuals from phishing attacks. Our intervention, which included a comprehensive module on phishing, seems to have been similarly effective. This supports the assertion that practical and engaging training methods can substantially enhance individuals' ability to recognize and counteract SE attacks.

Our results highlight the need for extensive, tailor-made, and early cybersecurity education and training interventions in higher education settings to ease the threats posed by SE attacks. The observed variation in vulnerability across different demographic groups and faculties might be explained by the unique views and practices concerning information security that different users hold.

Aslan *et al.* (2023) suggested that user perspectives on information security can significantly impact their vulnerability to SE attacks. For instance, users from the Applied Sciences and Mathematics faculty were more aware of the risks and better equipped to respond successfully, leading to a more distinct reduction in vulnerability after the intervention. This emphasizes the importance of tailoring cybersecurity education interventions to the precise needs and contexts of different user groups. Therefore, future research should extend this work by examining the long-term efficacy of such interventions and exploring their potential in other settings beyond higher education.

CONCLUSION

In conclusion, our study provides strong evidence for the efficacy of a cybersecurity education and training intervention in reducing vulnerability to SE attacks. However, the variations in efficacy across different demographic groups and faculties suggest the need for more custom-made interventions.

One possible limitation of the study is the lack of consideration for the Hawthorne effect despite the 7-week washout period. Future research should consider implementing a longer monitoring period post-intervention to assess whether behavioural changes are sustained once participants are no longer conscious of being observed.

In case of a future work, we recommend conducting

similar studies in other settings to validate our findings and assess the generalizability of the intervention, following the calls by Alseadoon *et al.* (2015) for more empirical research in diverse contexts. Furthermore, more in-depth studies could be done to understand the underlying reasons for the differences in efficacy across different demographic groups and faculties. Lastly, future interventions could incorporate feedback mechanisms or adapt based on an individual's learning progress to further enhance their efficacy, as suggested by Puhakainen and Siponen (2010).

REFERENCES

51 Must-Know Phishing Statistics for 2023 | *IT Governance*. (n.d.). Retrieved April 21, 2025, from https://www.itgovernance.co.uk/blog/51-must-know-phishing-statistics-for-2023

Adu-Gyimah, S., Asante, G., & Boansi, O. K. (2022). Social engineering attacks: a clearer perspective. *International Journal of Computer Applications, 975*, 8887.

Al-Hamar, Y., Kolivand, H., Tajdini, M., … T. S.-C. & E., & 2021, undefined. (n.d.). Enterprise Credential Spear-phishing attack detection. *Elsevier*. Retrieved April 21, 2025, from https://www.sciencedirect.com/science/article/pii/S0045790621003335

Alawida, M., Omolara, A., & … O. A.-J. of K. S. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Elsevier*. https://www.sciencedirect.com/science/article/pii/S1319157822002762

Almutairi, B., Security, A. A.-J. of I., & 2022, undefined. (2022). The Role of Social Engineering in Cybersecurity and Its Impact. *Scirp.Org, 13*, 363–379. https://doi.org/10.4236/jis.2022.134020

Alseadoon, I., Othman, M. F. I., & Chan, T. (2015). What is the influence of users' characteristics on their ability to detect phishing emails? *Lecture Notes in Electrical Engineering, 315,* 949–962. https://doi.org/10.1007/978-3-319-07674-4_89

Arachchilage, N., & Behavior, S. L.-C. (2014). *Security awareness of computer users: A phishing threat avoidance perspective*. ElsevierNAG Arachchilage, S LoveComputers in Human Behavior, 2014. Elsevier. https://www.sciencedirect.com/science/article/pii/S0747563214003331

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics, 12*(6), 1333. https://doi.org/10.3390/electronics12061333

Birthriya, S. K., Ahlawat, P., & Jain, A. K. (2025). A comprehensive survey of social engineering attacks: taxonomy of attacks, prevention, and mitigation strategies. *Journal of Applied Security Research, 20*(2), 244-292. https://doi.org/10.1080/19361610.2024.2372986

Burita, L., Matoulek, P., Halouzka, K., & Kozak, P. (2021). Analysis of phishing emails. *AIMS Electronics and Electrical Engineering, 5*(1), 93–116. https://doi.org/10.3934/ELECTRENG.2021006

Burns, A., Johnson, M., Organizational, D. C.-J. of, & 2019, undefined. (2019). Spear phishing in a barrel: Insights from a targeted phishing campaign. *Taylor & Francis, 29*(1), 24–39. https://doi.org/10.1080/10919392.2019.1552745

Campbell, C. C. (2019). Solutions for counteracting human deception in social engineering attacks. *Information Technology & People, 32*(5), 1130-1152.

Cochran, K. A. (2024). Social Engineering: Manipulating the Human Element. *Cybersecurity Essentials,* 365–384. https://doi.org/10.1007/979-8-8688-0432-8_13

Creese, S., Dutton, W. H., Esteve-González, P., & Shillair, R. (2021). Cybersecurity capacity-building: cross-national benefits and international divides. *Journal of Cyber Policy, 6*(2), 214–235. https://doi.org/10.1080/23738871.2021.1979617

EDUCAUSE Center for Analysis and Research (2021). The Increasing Threat of Ransomware in Higher Education. Why IT Matters to Higher Education. https://er.educause.edu/articles/2021/6/the-increasing-threat-of-ransomware-in-higher-education

Femi-Oyewole, F., Osamor, V., & Okunbor, D. (2024, April). A systematic review of social engineering attacks & techniques: The past, present, and future. In *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)* (pp. 1-12). IEEE. https://doi.org/10.1109/SEB4SDG60871.2024.10629836

Gururaj, H., Janhavi, V., & Ambika, V. (2024). *Social Engineering in Cybersecurity: Threats and Defenses*.

Hadan, H., Wang, D. M., Nacke, L. E., & Zhang-Kennedy, L. (2024, May). Privacy in immersive extended reality: Exploring user perceptions, concerns, and coping strategies. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (pp. 1-24).https://doi.org/10.1145/3613904.3642104

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), https://doi.org/10.1016/j.heliyon.2017.e00346

Hussain, H., & Abbas, R. (2025). The role of social engineering and human factors in cybersecurity defense. https://www.theseus.fi/handle/10024/878762

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019, December). Towards an improved understanding of human factors in cybersecurity. In *2019 IEEE 5th international conference on collaboration and internet computing (CIC)* (pp. 338-345). IEEE. https://ieeexplore.ieee.org/abstract/document/8998491/

Jones, K. S., Armstrong, M. E., Tornblad, M. K., & Siami Namin, A. (2020). How social engineers use persuasion principles during vishing attacks. *Information and Computer Security, 29*(2), 314–331. https://doi.org/10.1108/ICS-07-2020-0113/FULL/HTML

Karthikeyan, S. (n.d.). *Cybersecurity in Education: Safeguarding*

Digital Learning Environments. Researchgate.Net. Retrieved April 22, 2025

Kendall, C. (2022). Kendall, C. L. (2022). *The Openness of Higher Education and Implications on Cybersecurity* (Master's thesis, Utica University).

Kirda, E., Computer, C. K.-29th A. I., & 2005, undefined. (n.d.). *Protecting users against phishing attacks with antiphish*. Ieeexplore.Ieee.Org. Retrieved April 21, 2025

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & security, 25*(4), 289-296.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, April). Protecting people from phishing: the design and evaluation of an embedded training email system. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 905-914).

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing cyber attacks and cyber security vulnerabilities in the university sector. *Computers, 14*(2), 49.

Langlois, P. (2020). *2020 data breach investigations report*. https://www.cisecurity.org/-/jssmedia/Project/cisecurity/cisecurity/data/media/files/uploads/2020/07/The-2020-Verizon-Data-Breach-Investigations-Report-DBIR.pdf

Marble, J. L., Lawless, W. F., Mittu, R., Coyne, J., Abramson, M., & Sibley, C. (2015). The human factor in cybersecurity: Robust & intelligent defense. *Advances in Information Security, 56*, 173–206. https://doi.org/10.1007/978-3-319-14039-1_9

Mouton, F., Leenen, L., & Security, H. V.-C. &. (2016). Social engineering attack examples, templates and scenarios. *Elsevier*. https://www.sciencedirect.com/science/article/pii/S0167404816300268

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security, 59*, 186–209. https://doi.org/10.1016/J.COSE.2016.03.004

Mudi, S. (2024). *Social Engineering Techniques and Their Impact on National Values in Higher Education*.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & security, 31*(4), 597-611.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. MIS Quarterly: *Management Information Systems, 34*(4), 757–778. https://doi.org/10.2307/25750704

Riahi, E., & Islam, M. S. (2025). Employees' information security awareness (ISA) in public organisations: insights from cross-cultural studies in Sweden, France, and Tunisia. *Behaviour & Information Technology, 44*(1), 79-101. https://doi.org/10.1080/0144929X.2024.2311734

Schmitt, M., & Flechais, I. (2024). Digital deception: generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review, 57*(12), 324. https://doi.org/10.1007/S10462-024-10973-2

Shillair, R., Author, F., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & Von Solms, B. (n.d.). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Elsevier*. Retrieved April 21, 2025, from https://www.sciencedirect.com/science/article/pii/S0167404822001511

Singh, T. (2025). Social Engineering: Exploiting Human Psychology. In *Cybersecurity, Psychology and People Hacking* (pp. 95-100). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-85994-6_7

Ustundag Soykan, E., & Bagriyanik, M. (2020). The effect of SMiShing attack on security of demand response programs. *Energies, 13*(17), 4542.

Vishwanath, A. (2015). Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack. *Journal of Computer-Mediated Communication, 20*(5), 570-584. https://doi.org/10.1111/jcc4.12126

Weimann, G. (2015). *Terrorism in cyberspace: The next generation*.