Medicon Engineering Themes
Volume 8 Issue 2 February 2025
Article Type: Research Article
ISSN: 2834-7218

Φshing You Understanding Phishing Susceptibility through Personality, Age, Education Level, and Gender

Alia El Bolock[1]* and Saifeldin Madany[2]

[1] *Computer Science and Engineering, The American University in Cairo, Egypt*

[2] *Information Security, German International University, Egypt*

***Corresponding Author:** Alia El Bolock, The American University in Cairo, New Cairo, Cairo, Egypt.

Received: January 28, 2025; **Published:** February 04, 2025

DOI: 10.55162/MCET.08.263

Abstract

This research investigates the relationship between character (personality traits and background) and susceptibility to phishing attacks in social engineering contexts. Our study uses a practical experimental design with controlled scenarios to measure susceptibility to phishing in a real simulated attack. Ethical safeguards, such as informed consent, anonymized data handling, and a comprehensive participant debriefing, were integral to the research. The findings indicate that high extroversion and low neuroticism greatly increase the probability of falling for a phishing attack. However, the age range was also a significant influencer of susceptibility, while educational background and gender had no effect. These results highlight the need to consider personality and demographic factors in cybersecurity defenses. This paper offers nuanced insights into personality-driven vulnerabilities and supports the value of ethical, realistic experimental designs in social engineering research.

Introduction

Phishing attacks remain one of the most prevalent and effective forms of cybercrime, exploiting human vulnerabilities rather than technical flaws to deceive individuals into revealing sensitive information. With the rapid expansion of the digital world, understanding the psychological and behavioral factors that influence phishing susceptibility has become increasingly critical. Personality traits, such as openness, conscientiousness, extroversion, agreeableness, and neuroticism, play a significant role in individual behavior and decision-making, making them key predictors of susceptibility to phishing attacks.

Research has shown that certain personality traits correlate with cybersecurity behaviors, with extroversion and agreeableness linked to higher susceptibility, while conscientiousness and neuroticism are associated with better adherence to security policies [20]. However, previous studies often consider personality traits in isolation, neglecting their interaction with other stable traits, such as socio-cultural embedding and education, or variable states, such as emotional and cognitive factors [8]. Furthermore, demographic factors, including age, gender, and educational background, have been identified as significant predictors of phishing susceptibility. For instance, older individuals tend to exhibit greater caution, while younger participants are more prone to impulsive behaviors [17].

Despite growing interest in this area, most studies are limited by the use of artificial experiments and static data collection rather than realistic attack scenarios. This reduces the practical applicability of their findings. Moreover, many studies fail to address ethical concerns related to participant data and informed consent, further limiting their scope and generalizability.

This study addresses these gaps by implementing *Φshing*, a controlled simulation of a phishing attack designed to identify the characteristics of individuals most vulnerable to phishing. The study evaluates the relationships between personality traits, age, socio-economic status, educational level, and gender to determine their impact on susceptibility. To achieve this, five hypotheses are tested:

- ***H1***: Age is a significant predictor of susceptibility.
- ***H2***: High extroversion and agreeableness increase susceptibility.
- ***H3***: Low neuroticism increases susceptibility.
- ***H4***: Educational level significantly predicts susceptibility.
- ***H5***: Gender significantly predicts susceptibility.

This study offers four main contributions. First, it establishes the relationships between personality traits and phishing susceptibility, identifying extroversion and neuroticism as key predictors. Second, it examines the influence of age and gender on susceptibility, challenging the assumption that personality is the sole determinant. Third, it employs an ethically sound experimental design, incorporating informed consent, anonymized data handling, and comprehensive debriefing. Finally, it provides actionable recommendations for designing cybersecurity training and awareness programs tailored to individual personality profiles and demographic characteristics.

By integrating behavioral insights, demographic analysis, and ethical considerations, this research contributes to a more holistic understanding of phishing susceptibility and offers practical solutions for mitigating risks in real-world scenarios.

Related Work

The relationship between personality traits, cognitive processes, and susceptibility to social engineering attacks, particularly phishing, has been extensively studied. This section synthesizes recent findings on how psychological, demographic, and situational factors influence cybersecurity behaviors.

Personality Traits and Phishing Susceptibility

The Big Five Personality Model has been widely used to examine individual differences in susceptibility to phishing attacks. The found correlations include:

- ***Agreeableness***: Trusting individuals are more prone to persuasion tactics that exploit social validation [12, 9]. However, some studies suggest they may exhibit better deception detection skills under specific conditions [23].
- ***Extraversion***: Sociable and outgoing individuals are at greater risk due to their tendency to engage in social proof scenarios [7, 3].
- ***Conscientiousness***: Generally linked to cautious behavior, this trait may reduce susceptibility, though convenience-prioritizing individuals remain vulnerable [12, 7].
- ***Neuroticism***: High neuroticism correlates with heightened anxiety, often leading to impulsivity and susceptibility [9]. Conversely, internet anxiety may reduce vulnerability to spear-phishing [22].
- ***Openness***: Curious and exploratory individuals may fall victim to phishing attempts exploiting novelty and innovation [25, 14].

[15] challenged the predictive power of personality traits, finding minimal cultural differences and suggesting that situational and cognitive factors play more significant roles in phishing susceptibility.

Cognitive Processes and Decision-Making Heuristics

Cognitive biases and processing styles significantly influence phishing vulnerability. Individuals relying on quick judgments are more susceptible to phishing attempts. Analytical processing, often associated with conscientiousness, reduces this risk [24, 13]. High cognitive engagement correlates with reduced susceptibility, particularly in individuals with high openness and conscientiousness [25].

Research by Lin et al. [14] emphasized the role of emotional states like loneliness and social isolation in increasing susceptibility, particularly among older adults. Studies also highlight how specific phishing tactics exploit psychological vulnerabilities, such as fear and urgency, to influence decision-making [13].

Demographic Factors and Cultural Influences

Demographics, including age, gender, and education level, impact phishing susceptibility. Younger individuals often exhibit impulsive behaviors, increasing their risk, while older adults demonstrate greater caution due to experience [20]. Alhaddad et al. [2] emphasized the interplay between personality traits and demographics in predicting susceptibility.

Cultural influences on phishing susceptibility were explored by Raian Ali et al. [15], who found no significant differences between UK and Arab samples. This suggests that universal behavioral patterns, rather than cultural differences, may drive vulnerability to social engineering attacks.

Technical Vulnerabilities and Attack Techniques

Phishing attacks leverage both psychological and technical vulnerabilities. Techniques such as URL manipulation and JavaScript-based fraud are common [19]. Cyber Situational Awareness (CyberSA) frameworks, as proposed by Dutt et al. [5], aim to mitigate these risks through real-time threat detection and behavioral analysis.

Economic losses from phishing attacks remain substantial, with billions lost annually. Ghazi-Tehrani and Ali [11] emphasized the need for holistic approaches combining technical solutions with user education to mitigate these losses.

Training and Awareness Programs

Targeted training programs are essential for improving phishing detection. Lawson et al. [13] advocated for tailored interventions addressing personality-specific vulnerabilities, such as promoting skepticism among agreeable users. Awareness campaigns that expose users to repeated phishing scenarios have been shown to enhance detection rates [1, 4].

Studies like Georgiadou et al. [10] focused on insider threats, linking personality traits like openness and extroversion to risky behaviors. These findings highlight the importance of continuous training to foster a culture of cybersecurity awareness.

The interplay between personality traits, cognitive processes, and demographic factors underscores the complexity of phishing susceptibility. While personality traits provide insights, their predictive power is limited. Recent studies, e.g., [15], emphasize the need to integrate situational and environmental factors into training and awareness programs. Future research should focus on holistic strategies that combine technical, psychological, and educational measures to mitigate social engineering risks.

Experiment Design and *Φshing* Approach

This study investigates how personality traits and demographic factors influence susceptibility to phishing attacks. A phased experimental design was adopted to simulate real-world phishing scenario, *Φshing*, and analyze participant behavior in a controlled environment. The methodology integrates surveys for trait measurement with phishing simulations to link individual characteristics to susceptibility metrics. Ethical safeguards were incorporated at every stage to ensure compliance with institutional guidelines and maintain participant trust.

Participant Recruitment and Ethics

Participants were recruited via online platforms, university mailing lists, and social media advertisements. Recruitment targeted a diverse demographic to ensure generalizability, including individuals across age ranges, educational levels, and socio-economic backgrounds. Eligibility criteria required participants to:

- Be over 18 years old.
- Use email or WhatsApp regularly.
- Have no prior involvement in phishing or cybersecurity studies.

Informed consent was obtained digitally and participants were provided with information on the purpose of the study, confidentiality measures, and the right to withdraw at any time. Ethical approval was granted and all procedures adhered to ethical guidelines and GDPR regulations. Ethical concerns related to deception were addressed by acquiring initial consent, anonymizing all collected data, not collecting any sensitive information, and conducting comprehensive debriefing sessions at the study's conclusion.

Survey Design

The survey consisted of 20 items, taking an average of 5 minutes to fill. The survey collected the following information from the participants after asking for their informed consent:

- ***BFI-10***: A 10-item Big Five Inventory based on the Five Factor Model of Personality validated for reliability and brevity [16].
- ***Age***: grouped into ranges.
- ***Educational background***: highest qualification achieved.
- ***Socio-economic status***: self-reported on a 5-point scale.
- ***Cybersecurity awareness***: questions about prior exposure to phishing and similar attacks.

Attention checks were included to ensure high-quality responses with internal validity.

Experiment Overview

The experiment aimed at evaluating the responses of the participants to simulated phishing scenarios. Phishing messages were tailored to test hypotheses about personality traits, specifically extroversion, agreeableness, and neuroticism. Two experimental conditions were created:

- ***Experimental Group***: Received phishing messages designed to exploit personality traits.
- ***Control Group***: Received neutral messages without deceptive intent. The experiment was structured to assess both direct (e.g., clicking links) and indirect (e.g., response time) measures of susceptibility.

Data Collection and Analysis

Behavioral data from the phishing simulation (e.g., link clicks, data sharing) were logged anonymously and securely. Survey responses were encrypted and stored on institutional servers. Data analysis included statistical methods and machine learning. Regression and correlation analysis were used to identify trait susceptibility relationships. kNN was used to predict the susceptibility and kmeans clustering grouped participants based on their behavior patterns in reaction to the phishing attacks. Both methods were validated using cross-validation. [inline]Figure 1 provides an overview of the research design, illustrating the integration of survey data and phishing simulations across the study phases.

[inline]Figure 2 experimental workflow

Φshing Design

The phishing attack was designed to simulate real-world scenarios and test hypotheses about personality-driven susceptibility. Participants were exposed to messages via email and WhatsApp, reflecting common phishing tactics. The attack aimed to measure both immediate reactions (e.g., link clicks) and broader behavior patterns (e.g., data shared). Realism was prioritized by including personalized elements in phishing messages.

Phases and Stages of the Φshing Attack

The implementation and delivery of the *Φshing* attack consisted of three phases and distinguished between three stages of attack success. Figure 1 shows the entire process used to link a person's traits with their susceptibility to get attacked or not.

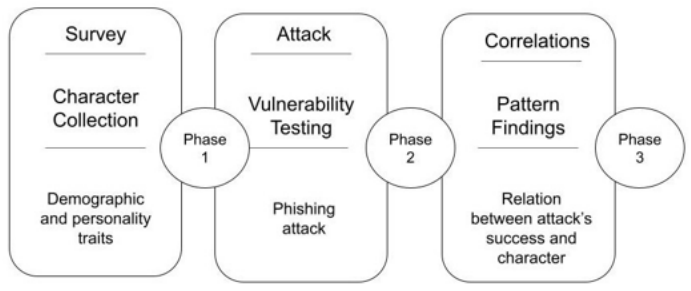


Figure 1: Overview of the 3 main phases of the implementation.

Phase 1 Pre-Attack Preparation The study began with the distribution of surveys, designed to collect personality traits and demographic data, as well as to set up the pretext for the phishing attack. The survey was created using Google Forms, ensuring familiarity and ease of use for participants. It included the BFI-10 personality test and demographic questions about age, gender, and education. The survey also captured participant email addresses for validation and future communication.

Once the survey was completed, participants were informed that they would receive detailed results of their personality analysis. This served as the ”bait” for the phishing attack, creating a realistic and credible pretext.

To prepare the attack, phishing materials were designed to resemble legitimate communications. The phishing link was a replica of a Google login page, created using Kali Linux tools. The URL was masked and secured with HTTPS to increase trustworthiness and bypass browser security warnings. Each link was unique and refreshed every four hours to ensure individual tracking and to prevent group sharing of information.

Ethical safeguards were implemented to protect participants, including anonymizing data, encrypting collected information, and ensuring that no real credentials were stored. All passwords entered were immediately encrypted and discarded after use, in compliance with ”White Hat Hacking” principles.

Phase 2 Attack Simulation The phishing attack was carried out over two weeks, targeting participants individually to prevent cross-contamination of results. Participants were sent personalized phishing links via WhatsApp, as it allowed for real-time delivery and monitoring of interactions. The attack flow is shown in Figure 2, illustrating how each participant progressed through the attack stages.

Each phishing message included a personalized introduction referencing the survey and the promise of personality analysis results. When participants clicked the link, they were redirected to a fake Google sign-in page, which logged their IP addresses (Stage 1). If they entered their credentials, the system captured their email addresses (Stage 2).

To avoid suspicion, participants who clicked the link received an automated response stating, ”There seems to be a bug; your results have already been sent to your inbox.” This reassured participants and prevented them from suspecting the simulated nature of the attack. The results are forwarded to the participants inbox as reassurance and for increased realism.

The following metrics were recorded:

1. ***Link Click Rate***: The percentage of participants who clicked on the phishing link.
2. ***Data Disclosure Rate***: The percentage of participants who entered their credentials.
3. ***Response Time***: The time participants took to click on the link or enter their credentials.

Phase 3 Post-Attack Evaluation Following the attack, participants were debriefed and informed about the simulated nature of the phishing attempt. They were provided with their personality analysis results, along with educational materials on identifying and avoiding phishing attacks.

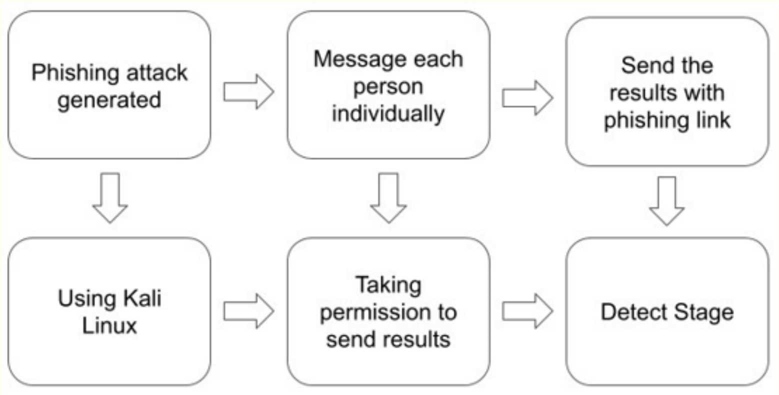

Phishing attack generated
Message each person individually
Send the results with phishing link
Using Kali Linux
Taking permission to send results
Detect Stage

Figure 2: Attack flow showing the different steps of the Φshing simulation.

A follow-up survey assessed participants' awareness of phishing risks and their reactions to the scenarios. Metrics collected during the attack were correlated with survey responses to analyze the relationship between personality traits, demographics, and phishing susceptibility.

Φshing Attack Stages The success of the attack was represented through three levels mapping to three stages of *Φshing* progression. This staging effectively demonstrates the varying degrees of success in phishing attacks. These stages allowed for precise classification of participant behavior, enabling a detailed analysis of susceptibility patterns.

- ***Φshing Stage 0***: The participant did not click the phishing link, i.e., not susceptible to phishing.
- ***Φshing Stage 1***: The participant clicked the link but did not enter their credentials. At this stage, only their IP address is captured via the listening port.
- ***Φshing Stage 2***: The attack is fully successful, as the participant clicked the link and enters their credentials on the phishing page.

Technical Implementation of Φshing

The phishing infrastructure was developed using Kali Linux tools to create a realistic yet ethically compliant simulation environment. Key components and methodologies included:

Phishing links were distributed via WhatsApp instead of email, as it allowed for real-time tracking and ensured participants would interact with the link individually. Each phishing message referenced the earlier survey, offering participants their personality analysis results to establish credibility and reduce suspicion. Personalized links were generated for each participant and refreshed every four hours to prevent sharing or reuse. Automated responses reassured participants by stating, ”This is just a bug; your results have already been sent to your inbox.”

The phishing pages were exact replicas of the Google login page, designed to appear authentic and trustworthy. Masked URLs were used to incorporate HTTPS, bypassing browser warnings from Chrome, Firefox, and Safari. This ensured participants did not encounter alerts that might have deterred interaction. Dynamic elements, such as personalized greetings, further enhanced the realism of the phishing pages.

Behavioral responses were monitored in real time using a backdoor listener hosted on the same server:

- ***Φshing Stage 0***: No information is captured.
- ***Φshing Stage 1***: IP addresses captured when participants clicked the phishing link.
- ***Φshing Stage 2***: Email addresses entered by participants attempting to log in are captured.

No real credentials were stored; dummy credentials were pre-generated and encrypted to ensure compliance with ethical guidelines. The phishing links redirected participants to the legitimate Google Apps page after their interaction to maintain the illusion of authenticity.

Servers were fully isolated from public networks, minimizing risks to participant privacy. Masked URLs and HTTPS were used to avoid browser security warnings and ensure participants interacted with the phishing pages without suspicion. All collected data were anonymized and stored on institutional servers encrypted according to GDPR standards. Participants' real credentials were not stored. Instead, encrypted placeholders were generated to ensure no sensitive data were retained.

To make the phishing attack seamless and undetectable, links were dynamically created with HTTPS to build user trust. The phishing page used optical illusions to mimic an authentic login process. Participants who clicked the link but did not proceed to log in (Stage 1) triggered a response capturing their IP address. Those who entered their credentials (Stage 2) had their email addresses logged without storing passwords. After interacting with the link, participants received an automated email reinforcing the legitimacy of the process.

Results of *Φshing*

Results are categorized into participant demographics, survey findings, phishing susceptibility metrics, and machine learning analysis. Each hypothesis is evaluated, followed by a discussion of trends, implications, and limitations.

Participant Demographics and Personality

The study initially targeted 654 participants. 154 participants completed the survey and experiment. 11 participants were excluded due to failing internal validity checks, such as providing identical responses to all Big Five Inventory (BFI) questions or inconsistent answers. The final sample size consisted of 143 participants.

Table 1 summarizes the demographic breakdown of the final participant pool.

The study participants were diverse, with a balanced distribution across age groups, education levels, and socio-economic statuses. Age was grouped into four categories for analysis. Socio-economic status was measured on a 5-point self-reported scale, with a mean of 3.3.

The survey measured personality traits using the Big Five Inventory and collected demographic data. Key results include:

- ***Extroversion***: Higher among younger participants (Mean = 3.9, SD = 0.6 for ages 18-25).
- ***Neuroticism***: Inversely correlated with socio-economic status ($r = -0.3$, $p < 0.05$).

Demographic Attribute	*Percentage*
Age Group (18–25)	35%
Age Group (26–35)	40%
Age Group (36–45)	15%
Age Group (46+)	10%
Educational Level (High School)	30%
Educational Level (Undergraduate)	45%
Educational Level (Graduate)	25%
Gender (female)	49%
Gender (male)	51%
Socio-economic Status (Mean, SD)	3.3 (0.7)

Table 1: Participant Demographics.

- ***Agreeableness***: Positively correlated with education level ($r = 0.2$, $p < 0.05$).

Experimental Results: Φshing Susceptibility

Behavioral metrics were analyzed to evaluate participant responses to phishing scenarios, focusing on click rates, data disclosure, and response times. Key findings include:

- ***Click Rates***: 48% of participants clicked on phishing links. Extroverts demonstrated a significantly higher click rate (Mean = 55%, $p < 0.01$), indicating a strong correlation between extroversion and susceptibility.
- ***Data Disclosure***: Participants with low neuroticism disclosed sensitive information at twice the rate of those with high neuroticism (20% vs. 10%, $p < 0.05$), highlighting the impact of emotional stability on risk perception.
- ***Response Time***: Participants in the experimental group responded faster to phishing messages (Mean = 16 seconds) compared to the control group (Mean = 22 seconds), suggesting impulsive behavior as a factor in susceptibility.

The matrix in Figure 3 illustrates the relationships between personality traits, gender, age, and attack outcomes. Extroversion, age, and neuroticism exhibit the strongest correlations with susceptibility, highlighted in distinct colors.

Low neuroticism participants were predominantly categorized in Stage 2, successfully completing the phishing attack by entering their credentials, as shown in Figure 4a.

Participants with high extroversion were more likely to fall victim (Stage 2), while those with low extroversion were mostly categorized in Stage 0, as shown in Figure 4b. Gender distribution was even, confirming its negligible impact on susceptibility.

Figure 4c shows that older participants were primarily categorized in Stage 0, indicating resistance to phishing attempts. Only one individual over 45 reached Stage 1, while younger participants (18-24) dominated Stages 1 and 2.

Machine learning models provided additional insights into phishing susceptibility:

- ***kNN Performance***: The kNN model achieved an accuracy of 83.5%, with precision and recall scores of 81% and 84%, respectively. This result supports the strong predictive power of personality traits and age.
- ***k-Means Clustering***: Clustering identified three distinct participant groups:
  - ***Cluster 1***: High extroversion, high susceptibility (40%).
  - ***Cluster 2***: Moderate traits, moderate susceptibility (35%).
  - ***Cluster 3***: High neuroticism, low susceptibility (25%).

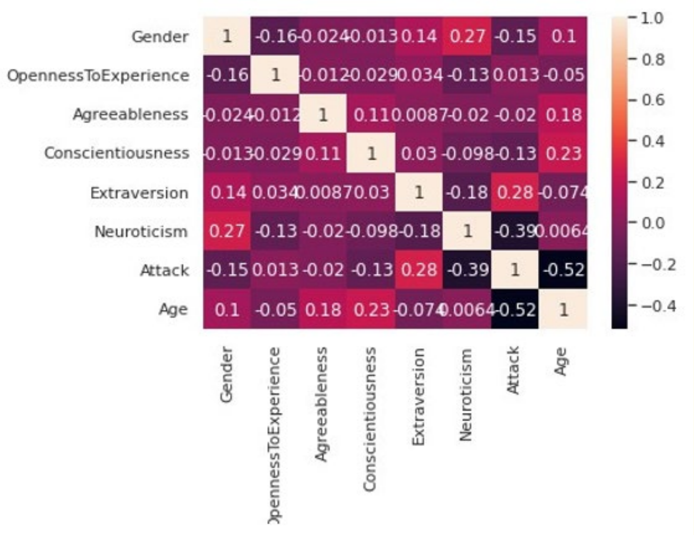
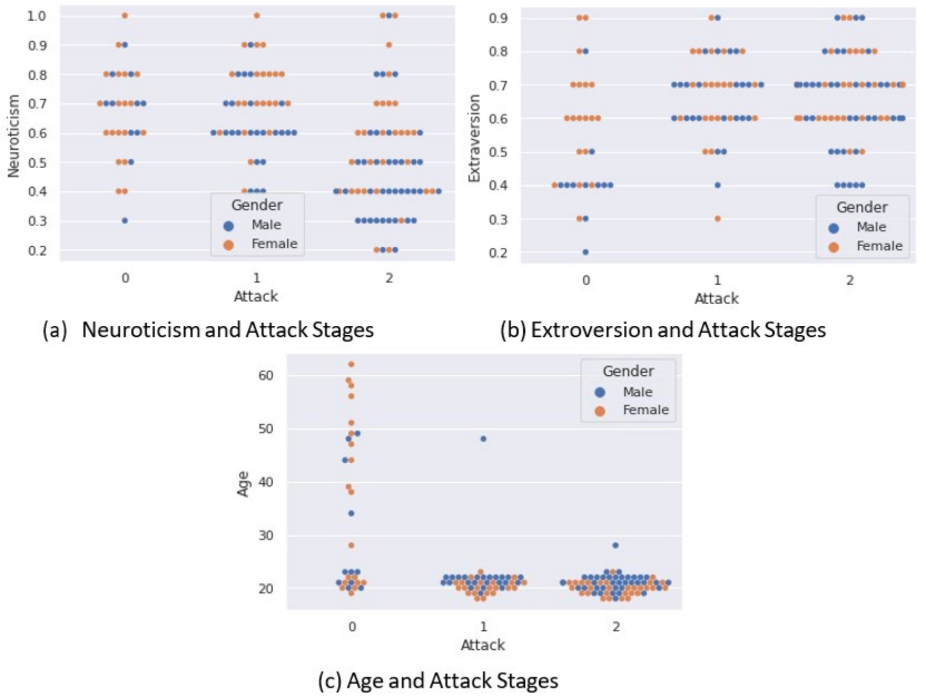


Figure 3: Correlation Matrix.



(a) Neuroticism and Attack Stages

(b) Extroversion and Attack Stages

(c) Age and Attack Stages

Figure 4: Analysis of Personality Traits and Demographics with Respect to Phishing Susceptibility Stages.

Hypothesis Testing

The results were evaluated against the hypotheses of this work:

- ***H1***: Age significantly influences susceptibility. ***Supported***. Younger participants were more susceptible ($r = -0.4$, $p < 0.01$).
- ***H2***: High extroversion and agreeableness increase susceptibility. ***Partially Supported***. Extroversion was significant, but agreeableness showed weaker correlation ($r = 0.2$, $p = 0.07$).
- ***H3***: Low neuroticism increases susceptibility. ***Supported***. Participants with low neuroticism had higher data disclosure rates.
- ***H4***: Educational background significantly impacts susceptibility. ***Not Supported***. Education had no significant effect ($p > 0.1$).
- ***H5***: Gender significantly impacts susceptibility. ***Not Supported***. Although minor differences were observed, they were not statistically significant.

Discussion of Findings

This study provides insights into the correlations between personality traits, demographic factors, and susceptibility to phishing attacks.

The study corroborates the significant role of personality traits in influencing phishing susceptibility. Participants exhibiting higher levels of extraversion were more prone to engaging with phishing attempts. This tendency may stem from their inherent sociability and responsiveness to social cues embedded in phishing messages. Recent research has explored the impact of extraversion on phishing victimization, highlighting the need for further investigation into this relationship [18]. Individuals with lower neuroticism scores demonstrated a higher propensity to disclose sensitive information. Their emotional stability might lead to underestimating potential risks in ambiguous situations. A study examining the correlation between phishing susceptibility and the Big Five personality traits supports this observation, suggesting that certain individuals may be more vulnerable to phishing attacks [6].

The analysis revealed that younger participants were more susceptible to phishing attacks. This finding aligns with reports indicating that younger adults are significantly affected by scams, often due to overconfidence in their digital literacy and a propensity for riskier online behavior [21]. Contrary to initial assumptions, educational attainment did not significantly impact susceptibility. This outcome suggests that general education may not adequately equip individuals to recognize and resist phishing attempts, emphasizing the need for targeted cybersecurity training. In [12], a study linked individual differences, such as demographics and personality traits, to cybersecurity behavior intentions, highlighting the significance of environment-specific research. While their findings emphasized rational decision-making and gender, our study found that extroversion, neuroticism, and age significantly influenced phishing susceptibility, whereas educational background and gender had minimal impact. These results highlight the complex relationship between character traits and cybersecurity behavior and underlines the need for larger sample sizes and considering cultural differences.

Younger individuals with high extraversion levels were particularly susceptible to phishing. The underlying cause could be their extensive social networks and rapid communication styles. This may increase exposure to phishing attempts and also reduce the likelihood of scrutinizing messages thoroughly.

This study highlights the need for personalized cybersecurity interventions. Developing training modules that consider individual personality profiles could enhance effectiveness. For instance, extroverted individuals might benefit from scenarios that emphasize caution in social interactions, while those with low neuroticism could be trained to recognize and appropriately respond to potential risks. Crafting awareness campaigns that are relatable to younger audiences may improve their ability to detect and thus avoid phishing attacks.

There are three main limitations in this study that are being addressed in future research. First, the participant pool, though varied, may not fully represent the broader population. Future studies should aim for larger, more diverse samples to enhance generalizability. Second, phishing strategies continually evolve. Ongoing research is essential to stay abreast of new tactics and develop corresponding countermeasures. Finally, further investigation into a broader range of character traits and states and their interactions with various demographic factors could provide a more detailed understanding of phishing susceptibility.

Conclusion and Future Work

This study investigated the relationship between personality traits, demographic factors, and susceptibility to phishing attacks using a phased experimental design. By integrating survey data and controlled phishing scenarios, the research identified key predictors of phishing vulnerability, including high extraversion, low neuroticism, and younger age groups.

The findings highlight several critical insights:

- Personality traits significantly influence phishing susceptibility, with extraversion and neuroticism emerging as prominent predictors.
- Age was a major determinant, with younger participants demonstrating higher susceptibility, likely due to overconfidence and impulsive online behavior.
- Educational attainment, contrary to expectations, did not significantly affect susceptibility, underscoring the limitations of generalized digital literacy in combating phishing.

These insights underline the importance of tailoring cybersecurity awareness programs to individual characteristics, focusing on personality-driven vulnerabilities and age-specific intervention strategies. This work contributes to the growing body of literature on human factors in cybersecurity by providing actionable insights for enhancing phishing awareness and resistance.

Future studies should involve larger and more diverse participant pools, encompassing different cultural, socio-economic, and occupational backgrounds to improve the generalizability of findings. This study focused on stable personality traits, but variable states such as emotional health, stress levels, and cognitive load could also impact susceptibility. Exploring these dynamic factors may offer a more comprehensive understanding of phishing vulnerability. As phishing tactics evolve, research must adapt to simulate more sophisticated attack methods, such as multi-layered spear-phishing campaigns. Following Character Computing concepts, the research should also be expanded to explore the susceptibility behavior based on different character states and in different situations. This can provide deeper insights into how different character profiles respond to advanced threats. Building on the findings of this study, future work should design and evaluate character-specific cybersecurity training modules. Testing their effectiveness in real-world scenarios can validate their practical applicability. A longitudinal approach could assess how susceptibility evolves over time with changing personal circumstances, exposure to training, and technological developments. Integrating personality and state profiling with behavioral biometrics, such as typing patterns or eye-tracking, may enhance the accuracy of predictive models for phishing susceptibility. Examining how cultural norms and values intersect with personality traits to influence phishing susceptibility can provide globally relevant insights for cybersecurity initiatives. Finally, future research should refine ethical standards for conducting experiments involving deception, ensuring that studies are both impactful and compliant with ethical guidelines.

By addressing these areas, future research can further the understanding of human factors in cybersecurity and enhance the development of targeted interventions to mitigate phishing risks.

References

1. Aldawood H and Skinner G. “Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues”. Future Internet 11.3 (2019): 73.
2. Alhaddad M.e.a. “Study of student personality trait on spear-phishing susceptibility behavior”. International Journal of Advanced Computer Science and Applications (2023).
3. Cristescu I, Ciuperca EM and Cirnu CE. “Exploiting personality traits in social engineering attacks”. Romanian Journal of Information Technology & Automatic Control 32.1 (2022).

4. Dawson J and Thomson R. “The future cybersecurity workforce: going beyond technical skills for successful cyber performance”. Frontiers in psychology 9 (2018): 744.
5. Dutt V and Kaur A. “Cyber security: testing the effects of attack strategy, similarity, and experience on cyber attack detection”. International Journal of Trust Management in Computing and Communications 1.3-4 (2013): 261-273.
6. Eftimie S, Moinescu R and Racuciu C. “Spear-phishing susceptibility stemming from personality traits”. IEEE Access 10 (2022): 81934-81945.
7. Egelman S, Harbach M and Peer E. “Behavior ever follows intention? a validation of the security behavior intentions scale (sebis)”. In: Proceedings of the 2016 CHI conference on human factors in computing systems. (2016): 5257-5261.
8. El Bolock A. “What Is Character Computing?”. Springer International Publishing, Cham (2020): 1-16.
9. Edwin Donald Frauenstein and Stephen Flowerday. “Susceptibility to phishing on social network sites: A personality information processing model”. Computers & Security (2020).
10. Georgiadou A, Mouzakitis S and Askounis D. “Detecting insider threat via a cybersecurity culture framework”. Journal of Computer Information Systems 62.4 (2022): 706-716.
11. Ghazi-Tehrani AK and Pontell HN. “Phishing evolves: Analyzing the enduring cybercrime”. Victims & offenders 16.3 (2021): 316-342.
12. Gratian M., et al. “Correlating human traits and cyber security behavior intentions”. computers & security 73 (2018): 345-358.
13. Lawson PEA. “Interaction of personality and persuasion tactics in email phishing attacks”. Human Factors and Ergonomics Society Annual Meeting (2017).
14. Lin TW., et al. “Susceptibility to spear-phishing emails: Effects of internet user demographics and email content”. ACM Transactions on Computer-Human Interaction 26.5 (2019): 32.
15. Muhanad A., et al. “Do personality traits really impact susceptibility to persuasion in social engineering? a study among uk and arab samples”. preprint (2024).
16. Rammstedt B., et al. “A short scale for assessing the big five dimensions of personality: 10 item big five inventory (bfi-10)”. methods, data, analyses 7.2 (2013): 17.
17. Saini H, Rao YS and Panda TC. “Cyber-crimes and their impacts: A review”. International Journal of Engineering Research and Applications 2.2 (2012): 202-209.
18. Sarno D and Toma CL. “Susceptibility to phishing on social network sites: A personality information processing perspective”. Computers in Human Behavior 110 (2020): 106403.
19. Shahrivari V, Darabi MM and Izadi M. “Phishing detection using machine learning techniques”. arXiv preprint arXiv:2009.11116 (2020).
20. Shropshire J, Warkentin M and Sharma S. “Personality, attitudes, and intentions: Predicting initial adoption of information security behavior”. computers & security 49 (2015): 177-191.
21. Spector N. “There’s a reason even the smartest people fall for scams”. Verywell Mind (2024).
22. Welk A.e.a. “Will the “phisher-men” reel you in?”. International Journal of Cyber Behavior, Psychology and Learning (2015).
23. Whitty M., et al. “Individual differences in cyber security behaviors: an examination of who is sharing passwords”. Cyberpsychology, Behavior, and Social Networking 18.1 (2015): 3-7.
24. Xu T. Analyzing instance representation in cognitive models of phishing decision making (2024).
25. Yang R., et al. “Predicting user susceptibility to phishing based on multidimensional features”. Computational Intelligence and Neuroscience (2022).

Volume 8 Issue 2 February 2025