Human Factors in Phishing Attacks: An Assessment of Awareness, Behavior, And Vulnerability

Riddhi Shah[1], Tanvi Rakshe[2], Harshada Dhayagude[3], Guna Dhondwad[4]
doi.org/10.64643/ijirt.208435-459

***Abstract*—Phishing attacks have become one of the most persistent forms of social engineering, exploiting human trust, emotions, habits, and decision-making rather than relying only on technical vulnerabilities. As digital communication continues to expand through email, social media, messaging applications, and online services, attackers are adopting increasingly sophisticated techniques such as impersonation, urgency-based manipulation, spear phishing, smishing, and AI-assisted phishing. This study examines the relationship between phishing attacks and human cybersecurity awareness, with particular emphasis on the factors that influence an individual's susceptibility to modern social engineering attacks.**

The research analyzes existing literature on phishing awareness, user behavior, psychological factors, phishing susceptibility, security awareness training, and social engineering techniques. It focuses on factors such as cybersecurity knowledge, attention, trust, urgency, familiarity, previous experience, demographic characteristics, and decision-making behavior. The study also examines the gap between users' perceived ability to identify phishing attacks and their actual ability to recognize deceptive messages. Furthermore, it evaluates whether conventional security awareness and phishing training are sufficient to produce long-term changes in user behavior. The findings from the reviewed literature indicate that cybersecurity awareness is important but does not necessarily guarantee resistance to phishing. Human decisions are influenced by contextual, psychological, and behavioral factors, while modern phishing messages are increasingly designed to appear legitimate and exploit users' expectations. Therefore, an effective defense strategy should combine user education, realistic phishing simulations, continuous awareness programs, behavioral analysis, technical security controls, and adaptive training approaches. The study highlights the importance of adopting a human-centered cybersecurity approach to reduce phishing susceptibility and improve individual and organizational resilience against evolving social engineering threats.

***Index Terms*—Phishing Attacks, Social Engineering, Human Awareness, Phishing Susceptibility, User Behavior, Cybersecurity Awareness, Security Awareness Training.**

I. INTRODUCTION

Phishing remains a common problem because it does not always require an attacker to break a technical system. Instead, the attacker may try to persuade a person to take an unsafe action. A message may ask the receiver to open a link, provide information, make a payment, or sign in to an account. The success of such an attempt can therefore depend on how the receiver interprets the message and what they decide to do.

Digital communication has made this problem broader than traditional email phishing. People now receive important messages through SMS, social media, messaging applications, educational portals, banking services, and shopping platforms. This gives attackers many opportunities to make a fraudulent message look relevant to the receiver.

A major issue considered in this research is the difference between knowing what phishing looks like and actually behaving safely when a suspicious message is received. A person may know that suspicious links should be checked, but urgency, familiarity, trust, or the expectation of receiving a particular message can still affect the final decision.

This study therefore looks at phishing as a human-behavior problem as well as a cybersecurity problem. It uses a questionnaire and three practical scenarios to examine awareness, confidence, psychological influences, previous training, previous phishing experience, and likely responses to suspicious messages.

Influencing factors	Likely behavioral response	Expected outcome
Awareness, phishing knowledge, training, previous experience	Verify / Ignore / Delete / Report	Lower phishing susceptibility
Trust, urgency, familiarity, suspicion, attention	Click / Reply / Provide information	Higher phishing vulnerability
User context, message relevance, channel, presentation, difficulty	Decision in a realistic scenario	Safer or unsafe behavior

Variable	Category	n	%
Age	18	4	20%
Age	18–20	10	50%
Age	21–25	6	30%
Education	Undergraduate	15	75%
Education	Postgraduate	4	20%
Education	Jr college	1	5%
Usage frequency	Daily	6	30%
Usage frequency	Often	6	30%
Usage frequency	Sometimes	6	30%
Usage frequency	Rarely	2	10%

Measure	Mean (1–5)
Identify common phishing indicators (Q5)	3.85
Know how to check whether a link is legitimate (Q6)	3.60
Know that legitimate organizations generally do not request passwords through unsolicited messages (Q7)	3.90
Confidence in identifying phishing (Q8)	3.65
Distinguish legitimate and convincing phishing messages (Q9)	3.55
Awareness composite (Q5–Q7)	3.78
Perceived-awareness composite (Q8–Q9)	3.60
Measure	Mean (1–5)
Trust in a message from a known organization (Q10)	3.70
Act quickly when a message creates urgency (Q11)	3.75
Familiar-looking messages reduce suspicion (Q12)	3.65
Pay close attention to sender and link (Q13)	4.00
Psychological-factor composite (Q10–Q12)	3.70

Question	Yes	No	Other
Received cybersecurity/phishing-awareness training	11 (55%)	9 (45%)	—
Previously encountered a suspected phishing attempt	6 (30%)	14 (70%)	—
Among all respondents: experience changed response	4 (20%)	1 (5%)	5 (25%) Not sure; 10 (50%) N/A

Scenario	Safer responses	Less-safe responses	Safer response rate
Urgent account suspension	16	4	80%
SMS package payment	14	6	70%
Educational institution login	12	8	60%

Grouping variable	Mean susceptibility proportion
Received training: Yes (n=11)	0.18
Received training: No (n=9)	0.44
Previous phishing experience: Yes (n=6)	0.17
Previous phishing experience: No (n=14)	0.36

Hypothesis	Current evidence	Status
H1: Awareness associated with lower susceptibility	Awareness–susceptibility correlation $r \approx -0.32$	Preliminary support; not statistically confirmed

H2: Perceived awareness associated with safer behavior	Correlation r ≈ −0.34	Preliminary support; not statistically confirmed
H3: Psychological factors affect susceptibility	Urgency/trust/familiarity means were relatively high; scenario differences observed	Partially supported descriptively
H4: User context affects behavior	Educational scenario had the lowest safer-response rate	Preliminary indication
H5: Training associated with safer behavior	Mean susceptibility 0.18 trained vs 0.44 untrained	Preliminary support
H6: Previous experience associated with improved detection	Mean susceptibility 0.17 experienced vs 0.36 inexperienced	Preliminary support
H7: Urgency associated with susceptibility	Urgency item mean 3.75; one scenario was urgency-based	Cannot be conclusively tested with current data

II. LITERATURE REVIEW

2.1. Human Factors in Phishing

The literature used for this study shows that phishing susceptibility is influenced by more than technical knowledge. People interpret messages using their previous experience, expectations, attention, trust, and the information presented in the message. A human-centered approach is useful because it focuses on why a person makes a particular decision instead of simply describing the person as the weakest part of security.

2.2. Awareness and Actual Behavior

Phishing-awareness programs normally teach users to check senders, links, attachments, requests for confidential information, and unusual payment instructions. These are useful skills, but awareness by itself may not always produce safe behavior. The gap between what a person says they know and what they actually choose in a realistic situation is especially important for this study.

2.3. Trust, Urgency and Familiarity

Several of the sources considered in this research discuss psychological and contextual influences. A message that appears to come from a familiar organization can feel more trustworthy. An urgent request can reduce the amount of time a person spends checking the message. Familiar wording or branding may also lower suspicion. These factors can operate even when a user already knows basic phishing indicators.

2.4. User Context

The situation in which a message is received can change how believable it appears. For example, an academic notification may seem more convincing to a student who is expecting information from a college. A delivery message may seem reasonable to somebody who is waiting for a parcel. This is why phishing assessments should not depend only on generic examples.

2.5. Training and Previous Experience

Training can give users practical ways to recognize and report suspicious communication. Previous exposure to phishing may also make people more cautious. However, the effectiveness of training depends on whether users transfer what they learned to real decisions. This study therefore includes both training history and scenario-based behavior.

2.6. Smishing and New Forms of Social Engineering

Phishing is no longer limited to email. SMS-based scams, social-media impersonation, business email compromise, spear phishing, and AI-assisted messages have increased the range of situations users need to recognize. The survey in this study includes an SMS delivery-payment scenario to reflect this wider environment.

III. RESEARCH GAP

Existing studies have examined awareness, psychological factors, user context, message characteristics, training, and individual differences. The issue is that these factors are often considered

separately. The present study brings several of them together and compares self-reported awareness with responses to practical phishing scenarios.

A second gap addressed by this work is the need to connect the literature with a small, current survey of users. The present survey is exploratory rather than a large-scale population study, but it provides an initial view of how respondents describe their awareness and how they respond to three different suspicious-message situations.

IV. RESEARCH OBJECTIVES

- Measure the level of self-reported cybersecurity and phishing awareness among respondents.
- Observe how respondents say they would react to suspicious digital messages.
- Examine the role of trust, urgency, familiarity, and attention.
- Compare responses according to training and previous phishing experience.
- Look at the difference between perceived awareness and scenario-based behavior.
- Develop practical recommendations for improving phishing resistance.

V. RESEARCH QUESTIONS

- What level of phishing awareness do the respondents report?
- How do respondents react to common phishing situations?
- Which psychological factors appear important in their responses?
- Is greater self-reported awareness associated with safer scenario choices?
- Does the context of a message appear to affect the decision?
- Do respondents with previous training show safer responses?
- Do respondents with previous phishing experience show safer responses?

VI. HYPOTHESES

H1: Higher cybersecurity awareness is associated with lower phishing susceptibility. H2: Higher perceived awareness is associated with safer phishing-related behavior. H3: Trust, urgency, suspicion, and attention are related to phishing susceptibility.

H4: User context is related to how people respond to phishing attempts.

H5: Respondents who have received awareness training show safer behavior.

H6: Previous experience with phishing is associated with better detection behavior. H7: Greater perceived urgency is associated with greater susceptibility.

VII. CONCEPTUAL FRAMEWORK

The framework used in this study treats phishing susceptibility as the result of several interacting influences. Awareness, training, and previous experience may help a person make a safer choice. On the other hand, trust, urgency, familiarity, and message context may make a suspicious message seem more believable.

Factor	Possible response	Expected direction
Awareness, knowledge, training, previous experience	Verify, ignore, delete or report	Lower susceptibility
Trust, urgency, familiarity	Click, reply or provide information	Higher susceptibility
Context and message presentation	Decision based on the situation	May increase or decrease risk

VIII. RESEARCH METHODOLOGY

8.1. Research Design

A quantitative cross-sectional design was used. Data were collected through a Google Forms questionnaire containing Likert-scale statements and scenario questions. The design was chosen because it allowed the study to collect both self-reported opinions and responses to practical situations in the same instrument.

8.2. Participants and Valid Responses

The form received 21 submissions on 21 August 2026. One respondent selected the non-consent option. That response was not included in the analysis. The final dataset used for the results therefore contains 20 consented responses.

8.3. Sampling

Convenience sampling was used. The sample mainly represents young users and students who regularly use digital communication. Because participants were not selected using probability sampling, the results should be viewed as an exploratory snapshot rather than a representation of the entire population.

8.4. Questionnaire

The questionnaire covered consent, age, education, frequency of email or messaging use, cybersecurity awareness, perceived awareness, psychological factors, previous training, previous phishing experience, and three scenario questions. Awareness and psychological statements were rated from 1 to 5.

8.5. Scenario Scoring

For the descriptive analysis, a response was treated as safer when the respondent independently checked an official website or application or chose to delete/report the suspicious communication.

Clicking a provided link, replying to the suspicious message, opening a suspicious link, or paying through the provided link was treated as less safe. The resulting score is an exploratory measure, not a clinically or universally validated phishing-susceptibility scale.

IX. RESULTS

The results below are based on the 20 consented responses. Percentages use 20 as the denominator. Since the sample is small, the results are reported mainly with descriptive statistics.

9.1. Participant Profile

Variable	Category	Responses	Percentage
Age	18	4	20%
Age	18–20	10	50%
Age	21–25	6	30%
Education	Undergraduate	15	75%
Education	Postgraduate	4	20%
Education	Jr college	1	5%
Use frequency	Daily	6	30%
Use frequency	Often	6	30%
Use frequency	Sometimes	6	30%
Use frequency	Rarely	2	10%

9.2. Awareness Results

Measure	Mean / 5
Identify common phishing indicators	3.85
Know how to check a website link	3.60
Know that unsolicited password requests are generally unsafe	3.90
Confidence in identifying phishing	3.65
Distinguish legitimate and convincing phishing messages	3.55

The average of the three awareness questions was 3.78/5. The two perceived-awareness questions averaged 3.60/5.

These scores suggest that respondents generally felt reasonably aware of phishing, but the scenario results show that awareness did not always translate into the safest choice.

9.3. Psychological Factors

Measure	Mean / 5
Trust a message from a known organization	3.70
Act quickly when a message feels urgent	3.75
Familiar-looking messages reduce suspicion	3.65
Pay close attention to sender and link	4.00

Attention to the sender and link had the highest mean at 4.00. At the same time, the means for trust, urgency, and familiarity were also relatively high.

This combination suggests that respondents understand the importance of checking messages but may still recognize that certain situations can influence their judgment.

9.4. Training and Experience

Measure	Yes	No
Received cybersecurity/phishing training	11 (55%)	9 (45%)
Previously encountered suspected phishing	6 (30%)	14 (70%)

A little over half of the respondents had received cybersecurity or phishing-awareness training. Only six respondents reported a previous suspected phishing encounter.

These results provide useful groupings for exploratory comparison, although the sample is too small for strong general conclusions.

9.5. Scenario Results

Scenario	Safer	Less safe	Safer rate
Account suspension	16	4	80%
Package-payment SMS	14	6	70%
Educational login	12	8	60%

The account-suspension scenario produced the highest safer-response rate, at 80%. The package-payment SMS produced a 70% safer-response rate. The educational-login scenario was the most difficult of the three, with only 60% selecting a safer response.

Across the 60 scenario decisions made by the 20 respondents, 36 were classified as safer and 24 as less safe. Thus, 60% of all scenario decisions were safer and 40% were less safe. Ten respondents chose safer actions in all three scenarios, while the remaining respondents had at least one less-safe choice.

9.6. Exploratory Comparisons

Group	Mean susceptibility proportion
Training: Yes (n=11)	0.18
Training: No (n=9)	0.44
Previous experience: Yes (n=6)	0.17
Previous experience: No (n=14)	0.36

The trained group had a lower descriptive susceptibility proportion than the untrained group (0.18 compared with 0.44). The group with previous phishing experience also had a lower proportion than the group without previous experience (0.17 compared with 0.36). These are associations in this sample and should not be interpreted as proof that training or experience caused the difference.

The exploratory correlation between the awareness composite and susceptibility was approximately $r = -0.32$. The correlation between perceived awareness and susceptibility was approximately $r = -0.34$. Both relationships point in the expected negative direction, but the sample is too small to treat them as statistically established findings.

X. DISCUSSION

The survey gives a useful example of the awareness–behavior gap discussed in the literature. Respondents generally rated their awareness positively, yet 24 of the 60 scenario choices were less safe. This means that knowing about phishing indicators did not automatically result in the safest response in every situation.

The educational message was the most difficult scenario for the respondents. One possible explanation is that an academic message can feel personally relevant to students and therefore may receive less suspicion. This interpretation is consistent with the human-context perspective used in the study, but the current data cannot prove that context caused the difference.

Training and previous experience showed encouraging descriptive patterns. The respondents who reported training had a lower average susceptibility proportion than those who did not. A similar pattern appeared for previous phishing experience. The result supports the idea that practical exposure and training may be useful, but a larger sample would be required to test this properly. The psychological questions also matter. Participants reported that urgency, familiarity, and messages appearing to come from known organizations could influence them. At the same time, they reported paying close attention to senders and links. This combination is important because secure behavior depends not only on knowing what to check, but also on consistently applying that knowledge when a message creates pressure or appears familiar.

XI. HYPOTHESIS REVIEW

Hypothesis	Observation from current data	Interpretation
H1	$r \approx -0.32$ between awareness and susceptibility	Direction supports the hypothesis, but not statistically confirmed
H2	$r \approx -0.34$ between perceived awareness and susceptibility	Direction supports the hypothesis, but not statistically confirmed
H3	Psychological-item means were relatively high	Descriptive indication only
H4	Educational scenario had the lowest safer rate	Preliminary indication of context effect
H5	0.18 trained vs 0.44 untrained	Preliminary support
H6	0.17 experienced vs 0.36 inexperienced	Preliminary support
H7	Urgency mean = 3.75	Cannot be conclusively tested with these data

XII. PRACTICAL RECOMMENDATIONS

- Make phishing-awareness training regular rather than a one-time activity.
- Use realistic examples involving email, SMS, academic messages, account alerts, and delivery scams.
- Teach users to pause when a message creates pressure to act immediately.
- Encourage users to open official websites or applications independently instead of following links in unexpected messages.
- Make reporting suspicious messages simple and visible.
- Combine user education with technical protections such as multi-factor authentication, filtering, and malicious-link detection.
- Use scenario-based exercises to check whether training changes decisions, not only whether users can remember definitions.

XIII. LIMITATIONS

- Only 20 consented responses were available for analysis.
- The sample was obtained through convenience sampling and is therefore not representative of the wider population.
- Self-reported answers can be affected by memory or social-desirability bias.
- Scenario questions cannot reproduce every pressure present in an actual phishing incident.
- The exploratory susceptibility score was created for this study and should be validated against established measures.
- The small sample does not support strong inferential or causal conclusions.

XIV. FUTURE SCOPE

A larger study could repeat the same questionnaire with students, employees, and other groups and compare the results. Future work could also test different message designs experimentally, including variations in urgency, personalization, authority, and visual presentation.

Longer-term studies could examine whether training changes behavior over time. It would also be useful to compare email, SMS, social media, and messaging applications. AI-assisted phishing deserves particular attention because generated messages can be highly personalized and may be harder to distinguish from legitimate communication.

XV. CONCLUSION

This study examined phishing from a human-behavior perspective using a small survey of 20 consented respondents. The respondents generally reported moderate to good awareness, but the scenario questions showed that safer behavior was not consistent in every situation. Overall, 60% of scenario choices were classified as safer and 40% as less safe.

The results also showed lower descriptive susceptibility among respondents who reported training or previous phishing experience. The educational-login scenario had the lowest safer-response rate, which suggests that the context of a message may matter. These findings are consistent with the central idea of the research: phishing resistance depends on more than awareness alone. Because the sample is small, these results should be treated as preliminary. Even so, they support the value of combining awareness education with practical scenarios, independent verification habits, reporting mechanisms, and technical security controls. A larger follow-up study would provide stronger evidence for the relationships proposed in this research.

REFERENCES

[1] “SoK: Human-centered phishing susceptibility,” 2023. https://dl.acm.org/doi/10.1145/3575797

[2] “Phishing and the human factor: Insights from a bibliometric analysis,” Information, vol. 15, no. 10, Art. no. 643, 2024. https://www.mdpi.com/2078-2489/15/10/643

[3] “When awareness is not enough: An experimental study on human susceptibility to phishing,” 2026. https://www.scitepress.org/publishedPapers/2026/147243/pdf/index.html

[4] “Profiling user vulnerability to phishing through psychological and behavioral factors,” arXiv preprint arXiv:2605.21246, 2026. https://arxiv.org/abs/2605.21246

[5] “Phishing in an academic community: A study of user susceptibility and behavior,” 2018. https://www.tandfonline.com/doi/abs/10.1080/01

611194.2019.1623343
[6] "Sixteen years of phishing user studies: What have we learned?" arXiv preprint arXiv:2109.04661, 2021. https://arxiv.org/abs/2109.04661
[7] "Why do people get phished? Testing individual differences in phishing vulnerability," 2011. https://www.sciencedirect.com/science/article/pii/S016792361100090X
[8] "Which phish is captured in the net? Understanding phishing susceptibility and individual differences," 2023. https://onlinelibrary.wiley.com/doi/full/10.1002/acp.4075
[9] "The human factor in phishing: Collecting and analyzing user behavior when reading emails," 2024. https://www.sciencedirect.com/science/article/pii/S0167404823005813
[10] "Not all victims are created equal: Investigating differential phishing susceptibility," 2024. https://www.nist.gov/publications/not-all-victims-are-created-equal-investigating-differential-phishing-susceptibility
[11] "User context: An explanatory variable in phishing susceptibility," 2018. https://www.nist.gov/publications/user-context-explanatory-variable-phishing-susceptibility
[12] "Effectiveness of and user preferences for security awareness training methodologies," 2019. https://pubmed.ncbi.nlm.nih.gov/31338464/
[13] "Phishing attacks: A recent comprehensive study and a new anatomy," Frontiers in Computer Science, 2021. https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.563060/full
[14] "Assessing anti-phishing awareness among undergraduate students in India," 2013. https://indianjournals.com/article/ijaritac-4-1-003
[15] "Exploring phishing awareness and user behavior: A survey-based investigation," 2024. https://www.ijraset.com/research-paper/exploring-phishing-awareness-and-user-behavior-a-survey-based-investigation
[16] "Phishing for user security awareness," 2016. https://www.sciencedirect.com/org/science/article/abs/pii/S146845271600041X
[17] "Individual processing of phishing emails," 2016. https://www.sciencedirect.com/org/science/article/abs/pii/S146845271600041X
[18] "The role of cue utilization in the detection of phishing emails," 2023. https://www.sciencedirect.com/science/article/pii/S0003687022002101
[19] "Categorizing human phishing detection difficulty: A phish scale," 2020. https://csrc.nist.gov/pubs/journal/2020/09/categorizing-human-phishing-detection-difficulty-a/final
[20] "A phish scale: Rating human phishing message detection difficulty," 2019. https://csrc.nist.gov/pubs/conference/2019/02/24/rating-human-phishing-message-detection-difficulty/final
[21] "NIST phish scale user guide," 2023. https://csrc.nist.gov/pubs/conference/2019/02/24/rating-human-phishing-message-detection-difficulty/final
[22] "Phishing in organizations: Findings from a large-scale and long-term study," 2022. https://www.nist.gov/publications/nist-phish-scale-user-guide
[23] "Anti-phishing training (still) does not work," arXiv preprint arXiv:2112.07498, 2025. https://arxiv.org/abs/2112.07498
[24] "Suspicion, cognition, and automaticity model of phishing susceptibility," 2018. https://journals.sagepub.com/doi/10.1177/0093650215627483
[25] "Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack," 2015. https://onlinelibrary.wiley.com/doi/10.1111/jcc4.12126
[26] "What you see is not what you get: The role of email presentation in phishing susceptibility," 2023. https://arxiv.org/abs/2304.00664
[27] "Users really do respond to smishing," arXiv preprint arXiv:2212.13312, 2022. https://arxiv.org/abs/2212.13312
[28] "Exploring user risk factors and target groups for phishing victimization in Pakistan," arXiv preprint arXiv:2510.09249, 2025. https://arxiv.org/abs/2510.09249
[29] "Social engineering attacks: A systemisation of knowledge on people against," arXiv preprint, 2026. https://arxiv.org/abs/2601.04215