



Phishing Susceptibility and Protective Security Behaviors in Higher Education: Evidence for Organizational Cybersecurity Resilience

Chandra Dhimal, Stephanie Schwartz, Michael Douglas

Millersville University

Abstract: Phishing creates organizational risk because a single user action can expose credentials, systems, and institutional information. This study examined event-level responses to a university-wide simulated phishing campaign involving 700 participants, including 600 students and 100 staff members. Outcomes included message reading, link clicking, credential submission, deletion, forwarding, and phishing reporting. The message was read by 296 participants (42.3%), clicked by 35 (5.0%), and followed by credential submission among 21 participants (3.0%). Of the 35 participants who clicked, 21 (60.0%) supplied credentials. Student and staff click rates were similar, at 5.2% and 4.0%, respectively, and the difference was not statistically significant. Credential-submission rates were 3.3% for students and 1.0% for staff, but this difference was also not statistically significant. Staff members were substantially more likely to delete and report the simulated message. These findings indicate that organizational phishing resilience should not be evaluated solely through click avoidance. Initial susceptibility and protective response are distinct dimensions of behavioral risk. Institutions should use multidimensional measures that distinguish clicking, credential disclosure, reporting, and other response behaviors. For managers, the results support role-sensitive interventions, accessible reporting mechanisms, and event-level security governance practices.

Keywords: behavioral risk management, cybersecurity resilience, higher education, organizational security, phishing simulation, reporting behavior

INTRODUCTION

Phishing is frequently described as a technical security problem, but its organizational consequences depend heavily on human behavior. Deceptive messages encourage recipients to click links, disclose credentials, or take other actions that can create operational, reputational, and information risk. Organizations therefore use simulated phishing campaigns to assess user behavior and reinforce security practices.

Higher education provides a useful organizational setting for this analysis. Universities combine large and diverse user populations, decentralized decision making, high dependence on digital communication, and frequent institution-branded messages. Students and employees use common systems but may differ in organizational responsibilities, exposure to security procedures, and expectations regarding incident reporting.

Many phishing assessments emphasize click rates as the principal indicator of failure. That approach can obscure the difference between initial engagement and subsequent behavior. A participant may read a message, click a link, stop before entering credentials,

delete the message, forward it, or report it. Because these actions overlap, organizational resilience cannot be represented fully by a single final outcome.

The present study analyzes event-level records from a university-wide phishing simulation. It compares initial susceptibility and protective response behaviors across student and staff groups and shows how final-activity classifications can understate earlier behaviors. The study therefore treats phishing simulation data as organizational decision support rather than merely a training scorecard.

Research Questions

- RQ1: Do student and staff participants differ in link-clicking and credential-submission rates?
- RQ2: Do student and staff participants differ in message-handling and phishing-reporting behavior?
- RQ3: What do event sequences imply for organizational cybersecurity measurement and risk management?

LITERATURE REVIEW

Phishing Simulations as Organizational Assessment

Controlled phishing simulations provide observed behavioral evidence that complements awareness surveys and self-reported intentions. Díaz Vivas et al. (2024) used a university campaign to assess susceptibility and security weaknesses. Yaro and Mohd (2025) measured staff click and submission behavior alongside awareness measures. Berrou (2026) reported reduced clicking after a brief intervention with university students.

Outcomes across campaigns are not directly interchangeable. Message design, apparent sender, target population, timing, institutional context, security controls, and outcome definitions can influence observed behavior. A final activity category may also omit earlier clicking, credential submission, deletion, or reporting.

Awareness, Behavior, and Reporting

Awareness and secure behavior are related but distinct. Ruzaili et al. (2026) reported that phishing knowledge did not necessarily correspond to preventive behavior. Olaybal and Olaybal (2026) found cybersecurity practices more strongly associated with lower susceptibility than awareness alone. Gwenhure (2025) identified perceived severity, perceived importance, self-efficacy, and cues to action as predictors of reported student security behavior.

Reporting is organizationally important because it can support collective detection and response. Dawkins and Haney (2026) called for meaningful evaluation measures that extend beyond clicking. A user who avoids a link but does not report the threat contributes differently to organizational resilience than a user who alerts the institution.

Training and Behavioral Change

Simulation-based education provides realistic practice, but evidence for durable change is mixed. Berrou (2026) reported improvement after a short intervention, while Lain et al. (2024) found that embedded training may operate partly through reminders and nudges rather than sustained engagement with training content.

This study does not evaluate a training intervention. Its contribution is the separation of initial susceptibility from protective response and the reconstruction of overlapping event sequences for managerial interpretation.

ORGANIZATIONAL CYBERSECURITY RESILIENCE FRAMEWORK

The framework treats phishing response as a behavioral sequence rather than a binary event. Initial susceptibility is represented by clicking and credential submission. Protective response is represented most directly by reporting, while deletion and forwarding are treated as message-handling behaviors whose meaning depends on context.

Risk is reflected not only in whether users avoid harmful actions, but also in whether users contribute to organizational detection and response. Resilience therefore includes both risk reduction and protective contribution. Event-level measures provide a more useful managerial dashboard than a single final-activity label because they preserve the sequence and overlap of user actions.

The simulated message combined authority and urgency cues. It appeared to originate from the university information technology function and warned that recovered messages would be deleted unless the recipient acted. The study did not manipulate these cues independently.

METHOD

Design and Participants

The study used a quantitative field-simulation design. The campaign targeted 700 university participants, including 600 participants classified as students and 100 classified as staff. The simulation email was delivered successfully to all participants. Participant role was reconstructed using the classification embedded in the original analytical workbook. Because that classification was based on institutional email-address conventions rather than independently verified personnel records, subgroup findings should be interpreted cautiously. The analysis used a de-identified workbook. Names, email addresses, and Internet Protocol addresses were removed and replaced with randomized participant identifiers that remained consistent across worksheets.

Simulation Procedure

The campaign was deployed through Microsoft Defender Attack Simulation Training on March 18, 2025. The message imitated an institutional information technology recovery notice and warned that recovered messages older than seven days would be deleted unless action was taken. The embedded link directed participants to a simulated login page.

Measures

Primary outcomes were derived from dedicated event fields rather than the mutually exclusive Last Simulation Activity variable. Binary indicators were constructed for successful delivery, message read, link clicked, credentials supplied, message deleted, message forwarded, and phishing reported. Credential submission and Compromised = Yes identified the same 21 cases. Behavioral categories were not mutually exclusive.

Data Analysis

Counts and within-role percentages were calculated for each behavior. Pearson chi-square tests were used when expected frequencies were adequate. Fisher's exact tests were used for credential submission, reporting, and forwarding because of small expected cell frequencies. Odds ratios and 95% confidence intervals were reported. Cramer's V was used as an effect-size index. All tests were two-tailed.

Ethics and Data Handling

The original thesis reported institutional review approval and stated that participants were at least 18 years of age. The present reanalysis used de-identified records. Exact protocol language, approval number, and consent or waiver procedures should be confirmed before submission.

RESULTS

The simulated email was delivered successfully to all 700 participants. Table 1 reports event-level outcomes by participant role. Outcomes overlap because a participant could complete more than one action.

Table 1: Phishing Simulation Outcomes by Participant Role

Outcome	Students, n = 600 n (%)	Staff, n = 100 n (%)	Total, N = 700 n (%)
Message read	230 (38.3)	66 (66.0)	296 (42.3)
Link clicked	31 (5.2)	4 (4.0)	35 (5.0)
Credentials supplied	20 (3.3)	1 (1.0)	21 (3.0)
Message deleted	57 (9.5)	48 (48.0)	105 (15.0)
Message forwarded	0 (0.0)	6 (6.0)	6 (0.9)
Phishing reported	5 (0.8)	10 (10.0)	15 (2.1)
Marked compromised	20 (3.3)	1 (1.0)	21 (3.0)

Note: Percentages are within role. Outcomes came from dedicated event fields and are not mutually exclusive.

Initial Susceptibility

Thirty-one students (5.2%) and four staff members (4.0%) clicked the simulated link. Role was not significantly associated with clicking, $\chi^2(1, N = 700) = 0.25$, $p = .620$, Cramer's V = .019, OR = 1.31, 95% CI [0.45, 3.79].

Twenty students (3.3%) and one staff member (1.0%) supplied credentials. Fisher's exact test did not identify a significant role difference, $p = .340$, $OR = 3.41$, 95% CI [0.45, 25.73]. Across roles, 21 of 35 clickers supplied credentials, a 60.0% conversion rate among clickers.

Message Handling and Protective Response

A read event occurred for 230 students (38.3%) and 66 staff members (66.0%), $\chi^2(1, N = 700) = 26.88$, $p < .001$, Cramer's $V = .196$, $OR = 0.32$, 95% CI [0.21, 0.50]. Reading indicates exposure rather than security failure. Deletion was recorded for 57 students (9.5%) and 48 staff members (48.0%), $\chi^2(1, N = 700) = 99.65$, $p < .001$, Cramer's $V = .377$, $OR = 0.11$, 95% CI [0.07, 0.18].

Five students (0.8%) and 10 staff members (10.0%) reported the message. Fisher's exact test indicated a significant difference, $p < .001$, $OR = 0.08$, 95% CI [0.03, 0.23]. Staff had approximately 13 times the odds of reporting.

No students forwarded the message, whereas six staff members did. Fisher's exact test was significant, $p < .001$, but the rare event and zero student cell require caution.

DISCUSSION

Initial Susceptibility and Organizational Role

The results do not support a simple conclusion that students were more susceptible than staff. Click rates were similar, and the credential-submission difference was not statistically significant. Role therefore did not adequately explain initial susceptibility in this campaign. Olaybal and Olaybal (2026) likewise found that risk patterns varied across institutional groups. Gwenthure (2025) identified psychological and situational predictors of reported security behavior. The overall click rate was lower than rates in some academic simulations, but direct comparisons require caution. Díaz Vivas et al. (2024) and Yaro and Mohd (2025) used different settings and lures, illustrating the context sensitivity of simulation outcomes.

Post-Click Risk

The 60.0% credential-submission rate among clickers is consequential. Clicking and credential disclosure represent different risk stages. Managers who monitor only click rates may underestimate post-click risk. Event-level reconstruction also corrected the final-activity summaries. The workbook contained 35 click timestamps and 21 credential-submission timestamps, although final-activity classifications listed only eight clickers and ten credential suppliers. Any-occurrence and final-state measures answer different managerial questions.

Protective Contribution and Reporting

The strongest role-related differences concerned reporting and deletion. Staff reported at 10.0%, compared with 0.8% among students, and deleted the message at a much higher rate. The clearest difference involved later response rather than initial clicking.

Reporting supports collective detection and response. Dawkins and Haney (2026) argued that meaningful evaluation should extend beyond clicks. The present findings support viewing reporting as a positive organizational contribution.

Forwarding cannot be classified automatically as protective or unsafe because the recipient and purpose are unknown. Managers should avoid assigning performance meaning to ambiguous event fields without contextual evidence.

Managerial Implications

Organizations should use multidimensional phishing metrics. Click avoidance, credential protection, reporting, deletion, and other response behaviors should be measured separately. A single click rate or final-activity category cannot represent the complete risk sequence. Reporting should be treated as an organizational performance outcome. Managers should ensure that reporting mechanisms are accessible and that users understand how reporting contributes to collective risk reduction. The low student reporting rate identifies an area for intervention, although the data do not establish why reporting was uncommon.

Interventions should be role-sensitive without presuming that one population is uniformly more susceptible. In this campaign, students and staff displayed similar initial click behavior but different reporting and message-handling behavior.

Organizations should preserve event-level simulation data and document outcome definitions. The difference between 35 click events and eight final click classifications demonstrates how data structure can alter managerial conclusions.

Organizational resilience should be defined as both reduction of unsafe actions and presence of protective contributions. Avoiding a click is valuable, but reporting a suspicious message can support wider institutional response.

Implications for Training and Security Culture

The study did not measure awareness or prior training across the full sample, so the differences cannot be attributed to training. Ruzaili et al. (2026) and Olaybal and Olaybal (2026) nevertheless support separating knowledge from behavioral practice. Evidence on embedded training remains mixed. Berrou (2026) reported reduced clicking after a brief intervention, whereas Lain et al. (2024) found that reminders and nudges may explain some effects. Managers should evaluate behavior rather than treating training completion as proof of resilience.

LIMITATIONS

Participant role was reconstructed from the original workbook rather than verified against an authoritative institutional record. The student and staff samples were unequal, and only 21 credential submissions, 15 reports, and six forwarding events were recorded.

The study involved one institution and one phishing scenario. Results may depend on message design, timing, apparent sender, security controls, previous exposure, and institutional culture.

Event data record actions but not motives. They do not establish whether participants recognized the simulation, intentionally tested the link, supplied authentic information, knew how to report, or forwarded for verification.

Behavioral categories overlap. The analysis addressed this issue by using dedicated event fields rather than relying solely on Last Simulation Activity. The original follow-up survey received few responses and was not used as the primary evidentiary basis of this reanalysis.

FUTURE RESEARCH

Future studies should use multiple scenarios varying authority, urgency, topic, and credential request. Participant roles should be independently verified, and future datasets could include nonidentifying measures of previous training, simulation exposure, institutional tenure, technical experience, self-efficacy, and reporting knowledge.

Longitudinal research should measure both risk reduction and protective contribution, including lower clicking and credential submission as well as higher appropriate reporting.

CONCLUSION

The simulation documented a 5.0% link-click rate and a 3.0% credential-submission rate among 700 participants. Student and staff click rates did not differ significantly, and the credential-submission difference was also not significant. Staff were substantially more likely to delete and report the message.

The managerial conclusion is that initial susceptibility and protective response are distinct dimensions of organizational cybersecurity resilience. Organizations should evaluate multiple behavioral stages, preserve event-level evidence, and treat reporting as a central protective contribution alongside click avoidance.

GENERATIVE AI DISCLOSURE

Microsoft Copilot was used to assist with manuscript organization, language revision, literature discovery, and statistical checking. The authors independently reviewed and verified the data, analyses, citations, interpretations, and final text.

REFERENCES

- Berrou, D. (2026). Reducing phishing susceptibility among university students: A pre-post cybersecurity awareness intervention. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 12(2), 38-48. <https://doi.org/10.32628/CSEIT26121325>
- Dawkins, S., & Haney, J. (2026). Beyond the click: Experts weigh in on the phishing training debate. *IEEE Security & Privacy*, 24(4), 51-58. <https://doi.org/10.1109/MSEC.2026.3687644>

- Díaz Vivas, D. E., Gutierrez Pena, W. Y., Cristancho Botero, S. P., & Rojas, A. E. (2024). A controlled phishing attack in a university community: A case study. *Journal of Internet Services and Information Security*, 14(2), 98-110. <https://doi.org/10.58346/JISIS.2024.I2.007>
- Gwenhure, A. K. (2025). University students' security behavior against email phishing attacks: Insights from the health belief model. *Journal of Cybersecurity*, 11(1), tyaf034. <https://doi.org/10.1093/cybsec/tyaf034>
- Lain, D., Jost, T., Matetić, S., Kostianen, K., & Čapkun, S. (2024). Content, nudges and incentives: A study on the effectiveness and perception of embedded phishing training. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security* (pp. 4182-4196). Association for Computing Machinery. <https://doi.org/10.1145/3658644.3690348>
- Olaybal, R. O., & Olaybal, R. A. (2026). Closing the awareness-behavior gap: A role-based phishing training framework for higher education. *Journal of Cybersecurity Education, Research and Practice*, 2026(1), Article 26. <https://digitalcommons.kennesaw.edu/jcerp/vol2026/iss1/26/>
- Ruzaili, H., Katuk, N., Mohd Zaini, K., & Abdullah, W. (2026). Phishing awareness and preventive measures among university students: Knowledge, behaviors, and victimisation perspectives. *Millenium - Journal of Education, Technologies, and Health*, 2(29), e43489. <https://doi.org/10.29352/mill0229.43489>
- Yaro, H. U., & Mohd, M. (2025). Phishing susceptibility metrics in academic environments: Simulation-based analysis at Federal Polytechnic Bali, Nigeria. *Asia-Pacific Journal of Information Technology and Multimedia*, 14(1), 219-239. <https://doi.org/10.17576/apjitm-2025-1401-13>