The Effectiveness of Cybersecurity Training In Deterring Phishing Attacks in University Settings

Manuel Morfin, Dr. Jeffrey Zheng
Department of Computer Science, Stephen F. Austin State University

Abstract

Phishing remains one of the most persistent cybersecurity threats in academic settings, where users often lack dedicated cybersecurity training and navigate a wide range of digital platforms. This study examines the effectiveness of scenario-based training in enhancing users' ability to detect phishing attacks at a university.

In the study, 31 participants affiliated with the university completed a pre-test in which they classified nine emails as either phishing, legitimate, or unsure. This was followed by a custom interactive training module and a post-test using nine new yet comparable emails. The results demonstrated an increase in phishing detection accuracy, improving from 47.0% to 57.4%. Additionally, the number of "Unsure" responses decreased from 11.1% to 5.7%. However, the accuracy of identifying legitimate emails dropped from 33.7% to 22.2%, and false positives increased from 3.9% to 9.3%. Overall, this led to a slight decline in total classification accuracy, which decreased from 80.7% to 79.6%.

A one-way ANOVA across eight phishing categories revealed that the type of scenario significantly influenced participant accuracy ($F(7, 557) = 3.83$, $p = 0.00045$). File-sharing and login alert scenarios proved to be particularly challenging. These findings suggest that while brief training can enhance phishing detection and boost user confidence, it may also lead to an increase in cautious misclassifications. This highlights the need for tailored, scenario-specific training interventions as part of university cybersecurity strategies.

Methodology

This study employed a pre-post assessment design measuring participants' phishing identification abilities before and after targeted cybersecurity training. Thirty-one university-affiliated individuals (students, faculty, and staff) completed the Qualtrics-hosted study featuring HTML-formatted email scenarios based on real-world examples.

The procedure consisted of three phases:

(1) A pre-test where participants classified 9 emails (mixture of legitimate and phishing).
(2) An interactive training module featuring common red flags and a "build-your-own" phishing exercise teaching detection through the attacker's perspective.
(3) A post-test where participants classified 9 different but comparable emails.

This approach allowed for direct measurement of how the training intervention affected participants' ability to identify phishing attempts.

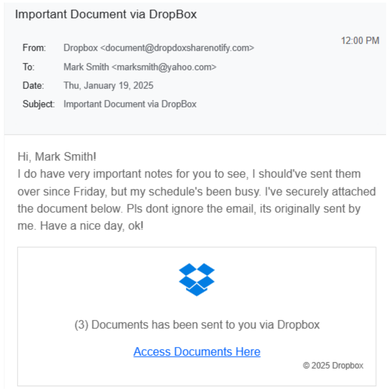

Figure 1. Example Email Template

Figure 2. Training Module

Scenario Examples

The assessment evaluated various phishing tactics common in university settings, including file-sharing notifications (e.g., Dropbox, Google Drive), security alerts (e.g., Facebook, TP-Link), financial messages (e.g., PayPal, Wells Fargo, Chase), professional networking requests (e.g., LinkedIn invitations from spoofed domains), and internal communications (e.g., campus announcements). This approach enabled a comprehensive evaluation of participants' ability to recognize diverse phishing strategies in personal and institutional contexts.

Pre vs Post Classification Distribution

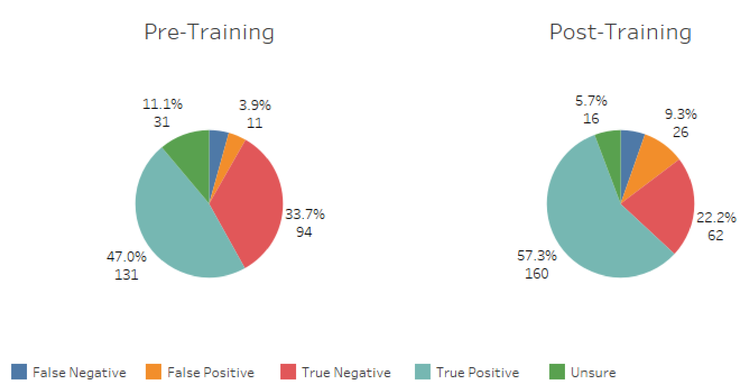

Figure 3. Pre-Training vs. Post-Training Response Distributions

Results

- Phishing detection rate improved: 47.0% to 57.4%
- Legitimate email recognition decreased: 33.7% to 22.2%
- Uncertainty ("Unsure" responses) reduced: 11.1% to 5.7%
- False positive rate increased: 3.9% to 9.3%
- Overall accuracy slightly declined: 80.7% to 79.6%

Statistical Significance:

- One-way ANOVA confirmed significant accuracy differences across scenario types: $F(7, 557) = 3.83$, $p < 0.001$

Most Challenging Scenarios Post-Training:

- File-sharing notifications (Dropbox, colleague-shared work documents)
- Security login alerts (TP-Link, Facebook)

Factor	df_1, df_2	F-statistic	p-value	Interpretation
Prior Training	2, 28	0.36	0.70	Not significant ($p \geq 0.05$)
Comfort Level	3, 27	2.38	0.092	Not significant (trend, $p \approx 0.09$)
Age Group	4, 26	0.09	0.99	Not significant
Gender	2, 28	0.21	0.81	Not significant
User Classification (role)	5, 21	0.80	0.56	Not significant
Scenario Type	7, 557	3.83	0.00045	Significant ($p < 0.001$)

Table 1. Summary of One-Way ANOVA Results (Post-Training % Correct)

Conclusion and Future Work

The study reveals that cybersecurity training improved phishing detection rates and reduced uncertainty, but also increased false positives as participants became more cautious. Sophisticated phishing attempts mimicking trusted services (file sharing, security alerts) remained challenging despite training. These findings demonstrate that interactive training can enhance awareness while highlighting an important security trade-off: improved threat detection versus legitimate email misclassification. The study's limitations including small sample size (n=31), single training session without follow-up, and simulated environment suggest caution in generalizing results to broader populations or real-world settings.

Future work would deploy recurring micro-trainings focused on specific phishing styles (file-sharing, account alerts), incorporate post-training quizzes with real-time feedback, track false positives in parallel with detection accuracy for balanced assessment, and implement tiered difficulty in training materials to avoid user overcorrection. By addressing both detection accuracy and discrimination skills, security programs can better prepare users for the evolving landscape of phishing threats.

Contact

Manuel Morfin
Department of Computer Science
1936 North St.
Nacogdoches, Texas 75965
manuel.morfin@sfasu.edu

Acknowledgements

I extend my deepest gratitude to my late professor, Dr. Cook, whose mentorship inspired my return to postgraduate study. Within the Computer Science Department, I thank Dr. Ivancic for his invaluable support and Dr. Zheng for advising this project.

I am also indebted to Meredith Baily and my ITS Department colleagues for their unwavering encouragement, to Alison Reed for her steadfast friendship, and help in sharing my research, and to Rebekah Raney for exceeding expectations in securing survey compliance.

References

[1] S. Das, C. Nippert-Eng, and L. J. Camp, "Evaluating user susceptibility to phishing attacks," ICS, vol. 30, no. 1, pp. 1–18, Jan. 2022, doi: 10.1108/ICS-12-2020-0204.

[2] A. Ciupe and B. Orza, "Reinforcing Cybersecurity Awareness through Simulated Phishing Attacks: Findings from an HEI Case Study," in *2024 IEEE Global Engineering Education Conference (EDUCON)*, Kos Island, Greece: IEEE, May 2024, pp. 1–4. doi: 10.1109/EDUCON60312.2024.10578700.