

**Under What Conditions Do Cybersecurity Awareness And Training Programs Effectively
Reduce Users' Susceptibility To Phishing Attacks?**

Reema Chakma

IDS 300W

Dr. Pete Baker

December 10, 2025

Under What Conditions Do Cybersecurity Awareness And Training Programs Effectively Reduce Users' Susceptibility To Phishing Attacks?

In the modern time, technology has become a vital part of our daily lives. It is widely used in pretty much every sector including education, healthcare, retail, and law, across both private and government institutions. As more systems and services transition into digital environments, malicious actors have also shifted their tactics, increasingly targeting these platforms. Among the growing number of cyber threats, phishing remains one of the most common and effective attack techniques. Despite advancements in technological defenses, cyber attacks continue to rise, affecting users and organizations worldwide. To effectively address the rising prevalence of phishing attacks, a comprehensive interdisciplinary approach is much needed. One important solution is to provide users with effective cybersecurity awareness and training programs. However, this alone may not be sufficient, as cyber attacks continue to increase and phishing remains one of the most prevalent methods used by threat actors. This raises a serious question: how effective the cybersecurity awareness and training programs are? Or more specifically, what are the conditions under which the cybersecurity training and awareness programs are most effective in reducing users' susceptibility to phishing attacks? This paper aims to find a comprehensive solution or the answer to this question by using an interdisciplinary approach. The ultimate goal of this paper is to identify and analyze insights from multiple disciplines, and determine common ground in order to address this complex issue of phishing.

As mentioned above, phishing attacks remain one of the most successful tactics used by attackers. Individuals who are not from cybersecurity or IT-related fields may not fully understand what phishing attacks are. In simple terms, phishing is a type of Social Engineering attacks, and a common tactic used by cybercriminals to trick individuals into revealing valuable or sensitive information that they are not supposed to disclose otherwise. This attack has the most success rates because they exploit human vulnerabilities, involving human judgement at multiple levels including, cognitive, social, behavioral and technical. One approach to prevent phishing is providing comprehensive user training and awareness. However, many researchers still struggle to find its effectiveness when addressing phishing. For instance, research suggests that even well-trained users still fall for phishing attempts when they are stressed, distracted, socially pressured, or deceived (Bahari et al., 2025). This complexity makes phishing an inherently interdisciplinary issue, as it involves not only technical mechanisms but also human psychology and behavior. One single discipline alone may not provide the full picture or address this issue completely; therefore, there is a need to incorporate insights from various disciplines including cognitive psychology, sociology, behavioral science, and computer science.

Computer scientists may view successful phishing attacks primarily as a technical issue rather than a human one. They may argue that humans alone, especially without the support of technological tools, cannot effectively help in reducing the growing number of phishing attacks, particularly in an era where technology continues to advance and attackers are increasingly leveraging it for malicious activities. Ho et al.'s findings offer compelling evidence in support of this argument. They evaluated the effectiveness of annual cybersecurity awareness training and embedded anti-phishing exercises by analyzing results from an eight-month randomized controlled experiment involving ten simulated phishing campaigns and thousands of healthcare

employees (Ho et al., 2025). Their findings concluded that currently designed and deployed anti-phishing programs are not very effective and are unlikely to provide any significant value in reducing phishing attacks (Ho et al., 2025). They proposed that because anti-phishing training is relatively cost-effective, organizations with limited resources should prioritize investing in technical countermeasures instead, particularly emphasizing the implementation of multi-factor authentication (MFA) and password managers to store and use strong passwords.

Sociology, behavioral sciences, and psychology share significant common ground when addressing the issue of phishing, as phishing exploits human vulnerabilities. Each discipline may look at the topic from different angles, however their insights overlap to a great extent.

A key common insight from these disciplines is that phishing succeeds by exploiting human cognition and social expectations. For instance, Bahari et al. (2025) show that phishing emails trigger heuristic responses through emotional cues like, trust, urgency or authority. They argue that even when phishing emails use advanced technology to appear professional and legitimate, cybercriminals still are successful by exploiting common human psychological tendencies. By manipulating human emotions such as trust, urgency, or fear, they influence how people think and make decisions, ultimately leading victims to fall for their deceptive schemes (Bahari et al., 2025). Moreover, other research studies show that individual personal traits like openness, conscientiousness, extraversion, agreeableness and neuroticism play a vital role when responding to phishing attacks, suggesting that some individuals are more susceptible to phishing attacks than others (Frauenstein & Flowerday, 2020). One of the research studies included a structural equation modeling (SEM) analysis, which concluded that conscientious users tend to have a negative influence on heuristic processing, making them less susceptible to phishing and further suggesting that heuristic processing increases users' susceptibility to phishing attacks

(Frauenstein & Flowerday, 2020). Furthermore, behavioral science suggests that users often know the right actions to take but still fail to perform it due to time constraints, fatigue, or less attentiveness. Interestingly, these challenges can be addressed by adaptive, data-driven attentive cues by guiding users' focus at the critical moment (Huang et al., 2020). Huang et al. (2020) proposed ADVERT, a human-technical solution that generates adaptive visual aids in real time to prevent users from inadvertently falling victims to phishing attacks, thereby reducing their susceptibility. This approach bridges computer science and behavioral science by suggesting a technical solution that incorporates human emotions and behavior.

Furthermore, according to Jari, practicing mindfulness can be an effective tool for significantly reducing the likelihood of users falling victim to phishing attacks. Jari also highlighted that ineffective training methods are another factor contributing to phishing attacks. While user training is crucial, the approach and methods used also play a critical role in addressing the issue of phishing.

After analyzing insights from multiple disciplines, it can be concluded that user training and awareness programs are essential and play a significant role in reducing phishing attacks. However, their effectiveness depends on a variety of factors, including human behavior, psychological state, personality traits, and technical knowledge. By incorporating these factors into the design and implementation of training programs, organizations can greatly enhance their effectiveness, equipping users with the technical skills and awareness needed to recognize and avoid phishing attempts.

An interdisciplinary approach suggests several key conditions and criteria to enhance the effectiveness of user training and awareness programs, thereby reducing users' susceptibility to phishing attacks. These criteria take into account not only technical measures but also human

factors such as behavior, cognition, and psychological tendencies, emphasizing a holistic strategy that integrates insights from multiple disciplines to optimize training outcomes.

Given below are the conditions or criteria under which cybersecurity training and awareness programs are more effective in reducing users' susceptibility to phishing attacks:

1. Training must explicitly address the management of human psychological states that influence their decision-making during critical situations.

Cybersecurity training must address the common human psychological tendencies that are commonly exploited by the attackers, such as trust, urgency, fear, overconfidence (Bahari et al., 2025). Users need to be trained not only to identify phishing attempts but also to recognize and manage these psychological triggers when they occur. While basic cybersecurity training can teach users how to spot and respond to phishing attacks, it is not sufficient on its own. Research indicates that even well-trained users may still fall victim when their emotional or psychological state is manipulated (Jari, 2022). Therefore, it is crucial for training programs to address vulnerabilities related to human psychology, ensuring users are better prepared to handle real-world phishing scenarios.

Furthermore, behavioral science suggests that practicing mindfulness is one way to address this issue. The technique of mindfulness involves being consciously aware of thoughts, feelings, and surroundings which helps to better understand what is happening around, while also improving individual's ability to regulate emotions and maintain greater control over their behavior (Jari, 2022).

Additionally, Frauenstein and Flowerday also agree that conscientious users tend to have a negative influence on heuristic processing, which makes them less susceptible to phishing.

2. Training must incorporate Technical and Data-Driven Cues

According to Huang et al. (2022), technical tools that provide adaptive, data-driven support can significantly enhance the effectiveness of user training programs. These kinds of systems include attentional cues and are designed to guide users' focus during critical moments such as evaluating email, or clicking a link. These cues tend to work by drawing users' attention to subtle warning signs that they might otherwise overlook.

Huang et al. (2022) emphasize that such tools, like the ADVERT, integrate human behavioral insights with technical automation to help users recognize potential threats in real time. So, by combining human factors with intelligent system design, these cues act as a form of guiding tool which reinforces users' behavior safely during actual phishing attempts, and thereby reducing the likelihood of users engaging with phishing attempts.

3. Training must be adaptive, realistic, and experiential learning

As technology continues to advance, cybersecurity training must also evolve to remain effective against newly emerging threats. Attackers are constantly developing new methods, exploiting vulnerabilities, and refining their tactics, which makes adaptability in training essential. If there are no continuous updates and realistic scenarios, training programs quickly become outdated and lose their effectiveness in preparing users for real-world phishing attacks. Moreover, incorporating experiential learning such as, hands-on simulations, realistic phishing exercises, and interactive scenarios can help

users not only learn phishing concepts but also practice how to respond in real-world scenarios. Ho et al. (2025) show that phishing training that involves learning-by-doing such as simulated phishing attacks, followed with immediate feedback, helps users better understand common phishing tactics, ultimately improving users' ability to identify and avoid phishing attacks.

In conclusion, researchers from multiple disciplines agree that phishing remains a prevalent tactic used by attackers. Even with robust technical defenses, such as firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS), phishing attacks persist because they exploit human vulnerabilities. Therefore, in addition to technical measures, users must receive proper and comprehensive training. However, evidence shows that even trained users can fall victim to phishing, indicating that current cybersecurity training and awareness programs are insufficient and require reevaluation. Therefore, current existing training programs must be revised and reformed to more effectively address the persistent threat of phishing. Interdisciplinary research suggests that training and awareness programs are most effective when they meet specific conditions: they address human psychology, incorporate technical and data-driven cues, and are adaptive, realistic, and experiential in nature.

References:

- Bahari, F. A., Daud, T. A., Arabbi, M. D., Jalah, N. I., Adjid, N. O., Abah, F., Amiddin, S. A. A., Ibno, A. A., Abduhail, A. S., Ajijul, M., Sali, R. M., & Tahlil, S. K. (2025, January 8). *The psychology of phishing: Why users fall victim to deceptive emails*. Zenodo.
<https://zenodo.org/records/14610632>
- Frauenstein, E. D., & Flowerday, S. (2020). *Susceptibility to phishing on social network sites: A personality information processing model*. *Computers & Security*, 94, 101862.
<https://doi.org/10.1016/j.cose.2020.101862>
- Ho, G., Mirian, A., Luo, E., Tong, K., Lee, E., & Liu, L. (2025, June 16). *Understanding the efficacy of phishing training in practice*. IEEE Xplore.
<https://ieeexplore.ieee.org/document/11023357/>
- Huang, L., Jia, S., Balcetis, E., & Zhu, Q. (2022, July 7). *Advert: An adaptive and data-driven attention enhancement mechanism for phishing prevention* | *IEEE Journals & Magazine* | *IEEE Xplore*. IEEE Xplore. <https://ieeexplore.ieee.org/document/9819920/>
- Jari, M. (2022, October 14). *A COMPREHENSIVE SURVEY OF PHISHING ATTACKS AND DEFENCES: HUMAN FACTORS, TRAINING AND THE ROLE OF EMOTIONS*. International Journal of Computer Networks & Communications (IJCNC).
<https://ijcnc.com/2022/10/14/a-comprehensive-survey-of-phishingattacks-and-defences-human-factorstraining-and-the-role-of-emotions/>
- Mouton, F., Leenan, L., & Venter, H. S. (2016, June). *Social engineering attack examples, templates and scenarios*. ScienceDirect.
<https://www.sciencedirect.com/science/article/abs/pii/S0167404816300268>