Phishing Beyond Technology: An Interdisciplinary Analysis of Human Vulnerability

Alexander Walker

Old Dominion University

IDS 300W: Introduction to Interdisciplinary Theory and Concepts

Dr. MaryAnn Kozlowski

11/18/2025

Abstract

Phishing has become one of the most damaging cyber threats, not because attackers rely on advanced technical exploits, but because they manipulate predictable patterns in human psychology and reasoning. Scammers design messages that trigger emotional reactions, push users into fast decision-making, and exploit cognitive shortcuts that normally help people navigate everyday communication. As a result, phishing bypasses even strong technological safeguards by persuading individuals, not machines, to open the door. Understanding why phishing is so effective requires more than technical analysis; it demands an exploration of the emotional, cognitive, and philosophical foundations that shape human decision-making. ***Thesis: Human psychology, emotional instincts, and reasoning patterns make individuals particularly vulnerable to phishing, demonstrating that technology alone can never fully prevent these attacks.***

Interdisciplinary Approach / Method

Phishing is an ideal problem for Repko and Szostak's interdisciplinary research method because it cannot be explained by a single discipline. Step 1 requires defining a complex problem. Phishing is a socio-technical crime because it combines digital delivery with psychological manipulation. Step 2 justifies interdisciplinarity. Understanding phishing requires analyzing human cognition in psychology, technological structure in computer science, and the ways people form belief and take risks in philosophy. Steps 3 through 5, which include identifying disciplines, conducting literature searches, and developing adequacy, support the use

of these three distinct fields. Steps 6 through 9 require analyzing and comparing insights, identifying conflicts such as psychology and philosophy versus computer science interpretations of vulnerability, creating common ground, and synthesizing the insights into one comprehensive explanation. This method helps reveal that phishing succeeds because of the interaction between human behavior and digital environments rather than because of a single point of failure.

Discipline 1: Psychology

Psychology explains phishing by detailing how scammers exploit emotional responses, mental shortcuts, and cognitive overload. Norris et al. (2019) show that successful fraudulent messages "**appeal to specific psychological vulnerabilities**," especially those linked to impulsivity, loneliness, and stress. They emphasize that scammers craft "**time-limited communications designed to enact peripheral rather than central information processing**," meaning the message is meant to force quick, emotional decisions rather than slow, rational thought. Crucially, their review finds that "**almost anyone could become the victim of a scam**," because these vulnerabilities are universal and are not restricted to less educated or technologically inexperienced individuals.

Abroshan et al. (2021) support this view by demonstrating that risk-taking behavior and decision-making styles strongly predict a user's progression through each stage of a phishing attack, from opening an email to entering credentials. They explain that users repeatedly face decision points such as "**to click or not to click**" and later "**to submit personal data or not,**" which are influenced by cognitive shortcuts, emotional triggers, and perceptions of social pressure. For example, users under stress or working quickly are more likely to rely on heuristic reasoning, making them susceptible to messages appearing urgent, authoritative, or beneficial.

Psychology also shows that phishing thrives in environments where cognitive load is high. When individuals are multitasking, emotionally overwhelmed, or fatigued, they are more likely to fall back on impulsive decision patterns. Together, psychological research demonstrates that phishing works by strategically aligning deceptive cues with innate human tendencies, making psychological vulnerability the central mechanism exploited in phishing attacks.

Discipline 2: Computer Science

While psychology explains *why* individuals fall for scams, computer science explains *how* those scams are built and deployed. Alkhalil et al. (2021) define phishing as a "**socio-technical attack**" that blends technological infrastructure with social engineering. Attackers "**exploit human nature… instead of utilizing sophisticated technologies**," meaning that phishing succeeds not through technical novelty but through accurate imitation of legitimate communication. Their proposed anatomy of phishing includes reconnaissance, preparation, delivery, and "**valuables acquisition**" and each stage is designed to exploit the user's trust in digital systems.

Ho et al. (2025) provide one of the most comprehensive real-world evaluations of phishing defenses. In a study of more than 19,500 healthcare employees over eight months, they concluded that "**our model shows no significant association between the time since a user last completed training and their likelihood of failing a phishing simulation**." The authors call the findings "**a sobering picture**" of current training practices, showing that traditional technical training does little to reduce susceptibility. Users clicked phishing emails at similar

rates before and after training, proving that knowledge alone cannot override emotional reaction or cognitive pressure.

Computer science research also shows that no technical protection is flawless. Spam filters, machine-learning detectors, and URL scanners cannot block every phishing attempt because attackers adapt quickly and design realistic messages that bypass automated defenses. Ultimately, computer science concludes that strong digital defenses still depend on human judgment at the moment of decision, which reinforces psychology's finding that human cognition is the primary vulnerability.

Discipline 3: Philosophy

Philosophy addresses a deeper question: *Why do rational, intelligent people knowingly take risks on messages they suspect might be false?* Levy (2025) argues that scams rarely "**induce belief in their victims**"; instead, they work by "**inducing a fantasy that is just plausible enough, and attractive enough, to bring their victims to bet on the scams**." This distinction is important. Victims often *do not fully believe* a phishing message, but they act anyway because the emotional incentive (fear, hope, or curiosity) outweighs the hesitation.

McGlone and Knapp's historical and philosophical study of deception further explains this vulnerability. They note that "**it is in our nature to mislead, but we also generally dislike being misled**," creating a fundamental tension that scammers exploit. Throughout history, deception has been a recognized and even respected tactic; Machiavelli famously advised rulers to "**never attempt to win by force what can be won by deception**." These perspectives

highlight that deception is not a modern digital phenomenon, it is a deeply rooted part of human communication.

Philosophy also explains epistemic vulnerability. Levy argues that humans evolved strong systems of epistemic vigilance—mechanisms that help us detect unreliable information—but these systems can be overridden when emotional incentives are strong. The victim does not accept the message as true; instead, they respond to its *possibility*. This philosophical insight bridges psychology's emotional triggers with computer science's technical mimicry: phishing succeeds when a message is believable enough to encourage risk, even if doubt remains.

Applications and Syntheses

Bringing these perspectives together reveals that phishing succeeds because it is engineered to exploit the intersection of psychological tendencies, technical design, and philosophical reasoning.

Psychology shows that phishing acts in emotional states such as fear, urgency, and curiosity. When scammers design a message implying that an account will be closed in 24 hours, they are intentionally triggering peripheral decision-making concept directly supported by Norris et al. Computer science complements this by demonstrating how these emotional cues are embedded into realistic email formats, spoofed addresses, and convincingly structured websites. The technical framework makes the deception appear authentic, enabling psychological manipulation to take effect.

Philosophy deepens this analysis by showing why psychological manipulation remains effective even when individuals recognize suspicious cues. Levy's notion of "betting on" a belief explains why trained users—people who *know* about phishing—still fall for scams. They act not because they are convinced, but because the fantasy of reward, avoidance of punishment, or emotional pressure is powerful enough to override skepticism. This explains the results of Ho et al., who found that training does not significantly reduce failure rates.

A major interdisciplinary conflict emerges from how the disciplines frame vulnerability. Computer science often discusses phishing in terms of "user error," implying that individuals simply need better training or more caution. Psychology and philosophy challenge this, arguing that vulnerability is inherent, predictable, and rooted in universal cognitive mechanisms, not personal failure. By comparing these perspectives, the interdisciplinary method helps identify the limits of technical solutions and the unrealistic expectation that users can fully overcome cognitive biases.

The synthesis of these fields shows that phishing leverages:

- **Psychological mechanisms** (emotional triggers, heuristics, stress)
- **Technical mimicry** (spoofed systems, realistic digital environments)
- **Philosophical reasoning patterns** (acting on possibilities, fantasies, or emotional incentives)

Together, they create a comprehensive understanding: phishing is powerful because it fits perfectly into the ways humans naturally communicate, decide, and respond to digital

information. The attack is not a breakdown of thought, it is a distortion of normal thought processes designed into the structure of the message.

Conclusion

Phishing persists because it exploits stable features of human behavior rather than weaknesses in technology. Psychological research shows that emotional triggers and cognitive shortcuts make individuals susceptible to deception. Computer science reveals that phishing designs mimic legitimate communication so effectively that technical defenses and training often fail to prevent user clicks. Philosophy clarifies why people act against their better judgment, choosing to take emotional or practical risks on messages they do not fully believe. Together, these perspectives demonstrate that human vulnerability, not system vulnerability, is the core mechanism behind phishing. An interdisciplinary understanding shows that lasting solutions require integrating psychological insight, philosophical reasoning, and user-centered technical design, rather than relying solely on technological improvements.

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). *Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process.* IEEE Access, 9, 44928–44949. https://doi.org/10.1109/access.2021.3066383

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Frontiers in Computer Science, 3, 563060. https://doi.org/10.3389/fcomp.2021.563060

(This is the commonly cited source for the "socio-technical attack" phrasing.)

Ho, G., Mirian, A., Luo, E., Tong, K., Lee, E., Liu, L., Longhurst, C. A., Dameff, C., Savage, S., & Voelker, G. M. (2025). *Understanding the efficacy of phishing training in practice.* 2025 IEEE Symposium on Security and Privacy (SP), 37–54. https://doi.org/10.1109/sp61157.2025.00076

Levy, N. (2025). *Betting on scams.* Social Epistemology, 1–13. https://doi.org/10.1080/02691728.2025.2527768

McGlone, M. S., & Knapp, M. L. (2019). Historical perspectives on the study of lying and deception. In T. Docan-Morgan (Ed.), *The Palgrave handbook of deceptive communication* (pp. 1–26). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-96334-1_1

Morrow, E. (2024). *Scamming higher ed: An analysis of phishing content and trends.* Computers in Human Behavior, 158, 108274. https://doi.org/10.1016/j.chb.2024.108274

Norris, G., Brookes, A., & Dowell, D. (2019). *The psychology of internet fraud victimisation: A systematic review.* Journal of Police and Criminal Psychology, 34(3), 231–245. https://doi.org/10.1007/s11896-019-09334-5