Project Title

Hooked by the Click: Human Behavior, Cognitive Bias, Phishing Susceptibility, and Cybersecurity Awareness Interventions

Project Objective or Aim

This project aims to investigate why individuals fall victim to phishing attacks and to identify effective strategies for reducing susceptibility. The primary research questions are: (1) What cognitive, behavioral, and contextual factors increase users' likelihood of engaging with phishing emails? and (2) Which educational or design-based interventions most effectively improve users' ability to detect and avoid phishing attempts? This study will focus on college students as a target population, examining how factors such as urgency cues, message framing, and prior cybersecurity knowledge influence decision-making. By analyzing these variables, the project seeks to develop evidence-based recommendations for improving user awareness and strengthening human-centered cybersecurity defenses.

Project Background and Significance

Phishing attacks remain one of the most prevalent and effective forms of cybercrime, largely because they exploit human psychology rather than technical vulnerabilities. Despite advances in automated detection systems and email filtering technologies, attackers continue to succeed by manipulating users through deceptive communication strategies. These attacks often rely on social engineering techniques such as urgency, authority, and fear appeals, which prompt individuals to act quickly without critically evaluating the legitimacy of a message.

This research is important because it focuses on the human side of cybersecurity, which is often seen as the weakest part of any security system. Even though technology plays a big role in protecting systems, it cannot fully reduce risk without also understanding how people behave. Cognitive biases like relying on quick judgments, being overconfident, or trusting authority figures can make people more likely to fall for phishing attacks. For example, when people quickly scan emails instead of carefully reviewing them, they may miss small warning signs that the message is actually a scam.

This study is guided by theoretical frameworks from behavioral psychology and human-computer interaction, including the Dual-Process Theory, which distinguishes between fast, intuitive thinking and slower, analytical reasoning. Phishing attacks typically exploit the intuitive system, encouraging rapid responses without deliberation. Additionally, Protection Motivation Theory (PMT) will be used to examine how perceived threat severity, vulnerability, and self-efficacy influence individuals' motivation to adopt protective behaviors.

Understanding these mechanisms is critical for developing effective interventions. Current cybersecurity training programs often rely on passive information delivery, which may not adequately change behavior. This research seeks to evaluate more interactive and psychologically informed approaches, such as simulated phishing exercises and targeted awareness messaging.

The outcomes of this project will contribute to the growing field of human-centered cybersecurity by providing insights into user vulnerabilities and practical strategies for mitigation. Given the increasing reliance on digital communication in academic and professional environments, improving phishing resilience among college students has broader implications for organizational security and public safety.

Research Methods

This study will employ a mixed-methods approach combining survey data and an experimental phishing simulation to examine user susceptibility and intervention effectiveness. The research will be conducted over the summer semester (May–August) and will focus on undergraduate students.

Phase 1: Survey (May–June)

Participants will complete an online survey assessing demographic information, prior cybersecurity knowledge, and self-reported behaviors related to email use. The survey will also measure psychological constructs such as risk perception, trust, and susceptibility to authority cues. This phase establishes baseline characteristics and identifies potential predictors of phishing vulnerability.

Phase 2: Phishing Simulation (June–July)

Participants will be shown a set of simulated phishing emails that vary in features like urgency, personalization, and how trustworthy the sender appears. Their actions, such as whether they

click on links or report the email, will be tracked. This step is important because it allows the study to capture actual behavior instead of relying only on what participants say they would do.

Phase 3: Intervention (July)

Participants will be randomly assigned to one of two groups: a control group receiving standard cybersecurity tips and an experimental group receiving an interactive training module. The module will include examples of phishing attempts, explanations of common tactics, and immediate feedback on decisions.

Phase 4: Post-Test Evaluation (Late July–August)

A second phishing simulation will be conducted to assess changes in behavior following the intervention. Comparative analysis will determine whether the training improved detection rates and reduced risky actions.

Data Analysis:

Quantitative data will be analyzed using statistical methods such as regression analysis and t-tests to identify significant predictors and intervention effects.

Expected Outcome

The primary deliverables of this project will include a formal research paper suitable for submission to an undergraduate research journal, a poster presentation for a university research symposium, and a summary report that can be shared with campus IT and cybersecurity

awareness programs. Additionally, findings may be adapted into educational materials designed to improve phishing awareness among students.

The expected findings will provide insight into the key psychological and behavioral factors that contribute to phishing susceptibility. It is anticipated that variables such as perceived urgency, message credibility, and lack of cybersecurity knowledge will significantly influence user behavior. The study also expects to demonstrate that interactive and feedback-based training interventions are more effective than passive informational approaches in reducing risky actions.

From a theoretical perspective, this research will contribute to the understanding of how cognitive biases and decision-making processes operate in cybersecurity contexts. It will provide empirical support for applying behavioral theories, such as Dual-Process Theory and Protection Motivation Theory, to real-world digital security challenges.

For the broader field of cybersecurity, the project will offer practical recommendations for designing more effective user-focused defenses. These may include improved training programs, better email interface warnings, and targeted awareness campaigns tailored to specific user vulnerabilities.

Within the university community, the research has direct relevance. College students are frequent targets of phishing attacks due to their heavy reliance on email and online platforms. By identifying common patterns of susceptibility, this project can inform campus-wide cybersecurity initiatives and help reduce the risk of compromised accounts and data breaches.

Ultimately, this research emphasizes that cybersecurity is not solely a technical issue but a human one. By addressing the behavioral component, the project aims to strengthen overall security resilience and promote safer digital practices.

Literature Review

Aleroud, Ahmed, and Lina Zhou. "Phishing environments, techniques, and countermeasures: A survey." *Computers & Security* 68 (2017): 160-196. https://doi.org/10.1016/j.cose.2017.04.006

Dhamija, Rachna, J. Doug Tygar, and Marti Hearst. "Why phishing works." *Proceedings of the SIGCHI conference on Human Factors in computing systems*. 2006. https://doi.org/10.1145/1124772.1124861

Fette, Ian, Norman Sadeh, and Anthony Tomasic. "Learning to detect phishing emails." *Proceedings of the 16th international conference on World Wide Web*. 2007. https://doi.org/10.1145/1242572.1242660

Jagatic, Tom N., et al. "Social phishing." *Communications of the ACM* 50.10 (2007): 94-100. https://doi.org/10.1145/1290958.1290968

Khonji, Mahmoud, Youssef Iraqi, and Andrew Jones. "Phishing detection: a literature survey." *IEEE Communications Surveys & Tutorials* 15.4 (2013): 2091-2121. https://doi.org/10.1109/SURV.2013.032213.00009

Zieni, Rasha, Luisa Massari, and Maria Carla Calzarossa. "Phishing or not phishing? A survey on the detection of phishing websites." *IEEE Access* 11 (2023): 18499-18519. https://doi.org/10.1109/ACCESS.2023.3247135

Preliminary Work and Experience

My academic background in Computer Science has provided me with a strong foundation in both technical and analytical skills relevant to this project. I have also completed coursework in cybersecurity fundamentals, psychology, and research methods, which has equipped me with an understanding of both the technical mechanisms of cyber threats and the human factors that influence user behavior. In particular, my studies have introduced me to concepts such as social engineering, risk perception, and data analysis.

Additionally, I have experience conducting basic research, including designing surveys and analyzing data using statistical tools. Through coursework and independent learning, I have developed familiarity with topics such as phishing attacks, email security, and user awareness strategies. I have also engaged with academic literature on cybersecurity and behavioral science, which has helped me understand current research trends and gaps.

This combination of technical knowledge and research experience positions me well to successfully carry out this project and contribute meaningful insights to the field.

IRB/IACUC Statement

This project requires Institutional Review Board (IRB) approval because it involves human subjects through surveys and behavioral simulations.

Budget

Total Requested: $1,200

Participant incentives ($10 × 60 participants): $600

Survey and data collection tools (e.g., Qualtrics premium features): $200

Software and data analysis tools: $150

Educational intervention materials development: $150

Printing and presentation materials: $100