August 2025

GAMIFICATION-BASED SPEAR PHISHING AWARENESS TRAINING SYSTEM: FOUR NOVEL DESIGN ARTIFACTS

Lina Zhou
UNC Charlotte, lzhou8@charlotte.edu

Abdulrahman Aldkheel
King Saud University, aaldkheel@ksu.edu.sa

Gamification-Based Spear Phishing Awareness Training System: Four Novel Design Artifacts

Emergent Research Forum (ERF) Paper

Lina Zhou
UNC Charlotte
Charlotte, USA
lzhou8@charlotte.edu

Abdulrahman Aldkheel
King Saud University
Riyadh, Saudi Arabia
aaldkheel@ksu.edu.sa

Abstract

Phishing, particularly spear phishing, poses significant threats by exploiting individual and organizational vulnerabilities through deceptive, targeted messages. Despite considerable progress in phishing awareness training, most existing systems target general phishing, with limited focus on specifically addressing spear phishing. Additionally, they also lack personalized feedback and training on phishing behavior. While gamification shows promise for enhancing user engagement, existing phishing awareness training designs often overlook important gamification elements. Building on existing theories, this study introduces several design considerations and proposes novel design artifacts to implement those considerations, including personalized attacks, structured knowledge training, personalized feedback, and competitiveness-driven design. We will evaluate the system's performance in phishing detection and user engagement in phishing awareness training, ultimately promoting a comprehensive cybersecurity education strategy.

Keywords

Spear phishing, training system, gamification, phishing behavior, personalization.

Introduction

In phishing, an attacker uses deception and disguising techniques to gain access to a victim's sensitive information over the internet. As a form of social engineering attack, phishing can be conducted through various channels, including fake emails and fabricated websites. Phishing attacks are often motivated by factors, such as identity theft, financial benefits, defamation, and propagation (Goel & Jain, 2018).

Spear phishing is a targeted form of phishing where the attacker selects specific individuals and tailors the context. Personalization is considered a critical factor in the success of spear phishing emails (Mark Sparshott, 2014). Over the past decade, phishing attacks have grown increasingly sophisticated. Cybercriminals often send phishing emails posing as trusted entities, designing messages to mimic legitimate organizations. These emails typically direct recipients to fake websites via hyperlinks, prompting users to update personal information. Unlike traditional phishing, spear phishing achieves higher success rates by impersonating someone familiar to the victim and incorporating personalized, relevant content, which reduces suspicion (Chiew et al., 2018). Additionally, different user groups may have varying levels of susceptibility to phishing attacks. For example, the elderly and college students may be particularly vulnerable. Therefore, phishing awareness training should not only focus on spear phishing but also ensure it is tailored to the diverse needs of different populations (Sultan, 2019).

Gamification in cybersecurity training, particularly for raising awareness of phishing, has shown significant potential in enhancing user engagement and promoting behavioral changes to prevent phishing attacks. Research has demonstrated that integrating gamification elements can improve the training experience. However, these systems still have limitations, like a lack of focus on spear phishing and personalized feedback and an overlook of phishing behavior training, and the underutilization of some promising gamification elements. This work extends this field by providing a comprehensive system with four design artifacts: personas to simulate attacks, structured knowledge training, phishing behavior classifications, competitiveness-driven gamification elements, and personalized feedback. Instead of surface-level gamification, our proposed system simulates realistic spear-phishing scenarios with user-selected personas. The system will be empirically evaluated after development.

Gamification-based Phishing Awareness Training

Gamification-based phishing awareness training aims to enhance users' ability to identify and avoid phishing attacks by incorporating gamification elements. Game-based training systems turn learning about phishing threats into an engaging experience. While learning how to identify phishing scams, users can also have fun with these interactive games. The interactive and engaging nature of games can contribute to their effectiveness as a tool to improve learning outcomes in the phishing context.

Existing phishing training systems have employed a variety of game mechanics and elements. For example, "Phishy", specifically designed for enterprise users, requires players to hook fish, answer related questions, and avoid obstacles (Cj et al., 2018). During the gameplay, players navigate life-or-death scenarios, which reinforces motivation and self-preservation instincts. In "Anti-Phishing Phil" (Sheng et al., 2007), Phil, a young fish, is required to distinguish between real and phishing URLs disguised as worms while learning and reflecting through story-based content. The game consists of four increasingly challenging rounds, in which Phil must earn points from correct identifications and lose lives from mistakes. "What.Hack" simulates phishing attacks through a role-playing approach, where players assume the role of bank employees who handle emails while being careful not to be attacked by phishing emails (Wen et al., 2019). "PHISHGEM" also educates users on major phishing techniques (Tinubu et al., 2023).

Current gamification-based phishing awareness training systems face several limitations. First, they use general phishing instead of spear phishing, which uses social engineering tactics to tailor messages to the target's specific information. Second, these systems emphasize email classification (phishing or not phishing). They focus on structural behaviors (e.g., fake URLs), neglecting other types of phishing behaviors. Third, their gamification strategies emphasize rewards, like points, while overlooking negative feedback, like penalties, and competitive elements (e.g., leaderboards). Finally, they do not provide personalized feedback to users.

NOPE (No Opportunity for Phishing Exploit)

We propose a gamification-based phishing awareness training system, NOPE (No Opportunity for Phishing Exploit), to address the limitations of existing systems. This section begins by outlining key considerations, then presenting detailed designs of the system’s novel components, and concludes with an overview of the system architecture.

Design Considerations

Our design of the phishing training system is motivated by the limitations of existing systems and informed by multiple theories, such as dual process theory (Stanovich & West, 2000) and protection motivation theory (Rogers, 1975). NOPE has the following key design considerations:

- Personalized attacks in support of spear phishing training: Tailoring phishing emails with relevant information or context specific to target users, thus simulating realistic spear phishing scenarios.
- Structured knowledge training: Helping users gain a systematic understanding of phishing behaviours through the content development of the training system.
- Competitiveness-oriented gamification design: Incorporating elements, such as a leaderboard and well-design reward mechanism to enhance user engagement and performance.
- Personalized feedback: Providing personalized feedback to enable users to focus on and improve their areas of weakness.

Design Artifacts

Personalization via Personas

To create personalized attacks, one approach is to collect personal profiles through online registration. However, privacy concerns may deter users from sharing real information. To balance personalization with privacy, we developed multiple representative personas, each reflecting diverse user profiles to broaden the range of phishing targets. The system will prompt users to select a preferred persona, then generates personalized phishing emails based on that choice.

In the initial design, we created three personas: students, mid-career professionals, and retirees, representing distinct user groups. These personas span various life stages and career phases, each with unique vulnerabilities and phishing recognition experience. The goal is not to cover all demographics but to include a representative cross-section of common phishing targets.

Structured Knowledge Training with Phishing Behavior Classification

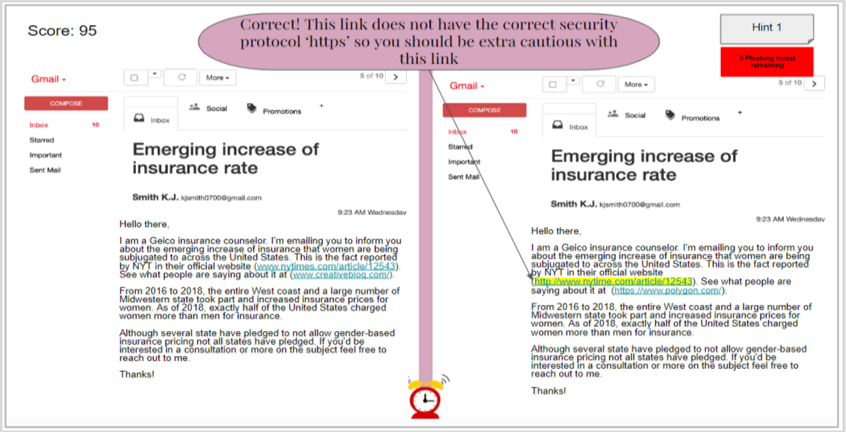
Phishing behaviors refer to the characteristics or patterns in deceptive emails or websites designed to trick users into disclosing their private or confidential information. The first step in detecting phishing emails is to recognizing phishing behaviors or cues. Beyond accurate detection, understanding why an email is phishing is crucial for preventing future attacks. Based on our extensive review of the phishing literature, we categorize phishing behaviors into three categories: structural, lexical, and discourse.

- Structural behaviors concern manipulating the structural elements of an email, such as specious links, fake emails, and time.
- Lexical behaviors involve using specific words, terms, or verbs in a message to enhance the attacker's intention to mislead a target, such as first-person pronouns, interaction requesting words, generalizing terms, and exclusive words.
- Discourse behaviors consider individual parts of an email in relation to other parts of the email, such as mismatched subjects and disguised sentences.

Competitiveness-driven gamification design

NOPE incorporates several gamification artifacts to improve user engagement and experience.

- Role-playing: The main task of the detector role is to identify phishing behaviors through inspection. Drawing on the find-the-difference game, players will learn to thoroughly analyze different elements of an email by comparing two versions of an email side-by-side. As shown in Figure 1, the email on the left is authentic and the version on the right is a phishing attempt, generated by modifying the authentic email). They will allow users to detect subtle inconsistencies, suspicious links, and other phishing cues from the comparison.
- Dynamic leaderboard: The design incorporates a dynamic leaderboard that adds a competitive element by comparing player performance across multiple phishing tasks. This fosters a sense of accomplishment and motivates users to continue engaging with training modules, while simultaneously encouraging improvement in phishing detection skills. Progress and performance are tracked through game history, capturing details like time spent and points earned.
- Penalty mechanic: In contrast to most existing games that focus on positive reinforcement, this system also incorporates penalties. Users will not only earn points as rewards but also lose points.



Correct! This link does not have the correct security protocol 'https' so you should be extra cautious with this link

Emerging increase of insurance rate

Smith K.J. kjsmith0700@gmail.com

9:23 AM Wednesday

Hello there,

I am a Geico insurance counselor. I'm emailing you to inform you about the emerging increase of insurance that women are being subjugated to across the United States. This is the fact reported by NYT in their official website (www.nytimes.com/article/12543). See what people are saying about it at (www.creativeblog.com/).

From 2016 to 2018, the entire West coast and a large number of Midwestern state took part and increased insurance prices for women. As of 2018, exactly half of the United States charged women more than men for insurance.

Although several state have pledged to not allow gender-based insurance pricing not all states have pledged. If you'd be interested in a consultation or more on the subject feel free to reach out to me.

Thanks!

Emerging increase of insurance rate

Smith K.J. kjsmith0700@gmail.com

9:23 AM Wednesday

Hello there,

I am a Geico insurance counselor. I'm emailing you to inform you about the emerging increase of insurance that women are being subjugated to across the United States. This is the fact reported by NYT in their official website (http://www.nytime.com/article/12543). See what people are saying about it at (https://www.polygon.com/).

From 2016 to 2018, the entire West coast and a large number of Midwestern state took part and increased insurance prices for women. As of 2018, exactly half of the United States charged women more than men for insurance.

Although several state have pledged to not allow gender-based insurance pricing not all states have pledged. If you'd be interested in a consultation or more on the subject feel free to reach out to me.

Thanks!

Figure 1. Sample phishing message (right) and authentic message (left).

Personalized Feedback

Phishing training systems are typically one-size-fits-all. Despite existing systems customizing messages based on user data, they fail to provide truly personalized feedback on performance. To address this limitation, NOPE offers tailored reinforcement, allowing users to repeat specific scenarios involving phishing behaviors where they demonstrate vulnerability, receive explanatory guidance contextualized to their particular mistakes, and practice with progressively challenging variants of attacks.

System Architecture

The system consists of three main components: registration, tutorial, and play. During registration, users are asked to create an account by providing some basic demographic information and selecting a persona.

The tutorial module was designed to ensure that all users are equipped with the knowledge necessary to recognize phishing behaviors through systematic and personalized training. The tutorial not only guides users on how to interact with the training system but also educate them on specific phishing behaviors. It includes information about the roles within the gamified environment, the game's rules and the scoring (points awarded for correct choices and deducted for incorrect ones), and time limits. The final score is the total cumulative points earned.

Gamification is a key element in our game design to enhance user engagement. In the training system, users learn to detect phishing by actively analyzing emails and selecting potential phishing behaviors. Positive confirmation reinforces correct identification, while feedback and targeted tips guide users upon incorrect selections, enhancing their understanding of phishing behaviors.

The play mode allows users to actively test their skills acquired from the training on different phishing emails. The main game session mirrors tutorial tasks but incorporates more engaging gamification, informing users about the number of embedded phishing clues in each email. The system tracks user's performance in terms of both accuracy and time for each email, using this data to calculate their scores. Tasks are ordered by increasing difficulty, presenting more and diverse phishing clues. Lastly, users receive feedback on their detection performance.

Discussion

This research addresses the need for more effective cybersecurity training, particularly against spear phishing, through the development of a gamification-based awareness system, NOPE. Our key contribution lies in the introduction of several theoretically novel design artifacts for gamified spear phishing training, including personalized attack simulation using personas, structured knowledge training with phishing behavior classification, competitiveness-driven gamification, and personalized feedback. We have prototyped NOPE and obtained IRB approval for our detailed evaluation methodology. The design and implementation of NOPE are extensible and will incorporate a structured set of spear-phishing characteristics, including diverse personalization features, language styles and tones, various phishing cues, exploitation techniques, and additional realistic scenarios, with plans to add varied narratives and simulated attachments for enhanced realism. Following a pilot study for refinement, we will evaluate NOPE's effectiveness in improving phishing detection training by comparing it against existing anti-phishing training systems (both non-gamified and gamified), as well as a non-gamified version of our system containing only knowledge-based training, across multiple dimensions including usability, educational impact, user engagement, and overall effectiveness.

Acknowledgements

The authors thank Jaewan Lim for the informative discussions in the early stages of prototype design. This work was supported in part by the NSA grant H98230-21-1-0259 and a Truist Business Research and Innovation grant. Any opinions, findings, or recommendations expressed here are those of the authors and are not necessarily those of the sponsors.

REFERENCES

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, *106*, 1–20. https://doi.org/10.1016/j.eswa.2018.03.050

Cj, G., Pandit, S., Vaddepalli, S., Tupsamudre, H., Banahatti, V., & Lodha, S. (2018). PHISHY - A Serious Game to Train Enterprise Users on Phishing Awareness. *Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts*, 169–181. https://doi.org/10.1145/3270316.3273042

Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defense mechanisms: State of art and open research challenges. *Computers & Security*, *73*, 519–544. https://doi.org/10.1016/j.cose.2017.12.006

Mark Sparshott. (2014). *The psychology of phishing*. https://www.helpnetsecurity.com/2014/07/23/the-psychology-of-phishing/

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. *Proceedings of the 3rd Symposium on Usable Privacy and Security*, 88–99. https://doi.org/10.1145/1280680.1280692

Stanovich, K. E., & West, R. F. (2000). Individual differences in reasoning: Implications for the rationality debate? *Behavioral and Brain Sciences*, *23*(5), 645–665. https://doi.org/10.1017/S0140525X00003435

Sultan, A. (2019). Improving cybersecurity awareness in underserved populations. *Center for Long Term Cybersecurity, UC Berkely. Https://Cltc. Berkeley. Edu/Wpcontent/Uploads/2019/04/CLTC_Underserved_Populations. Pdf.*

Tinubu, C. O., Falana, O. J., Oluwumi, E. O., Sodiya, A. S., & Rufai, S. A. (2023). PHISHGEM: A mobile game-based learning for phishing awareness. *Journal of Cyber Security Technology*, *7*(3), 134–153. https://doi.org/10.1080/23742917.2023.2167276

Wen, Z. A., Lin, Z., Chen, R., & Andersen, E. (2019). What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–12. https://doi.org/10.1145/3290605.3300338