EUROPEAN JOURNAL OF EMERGING CYBERSECURITY AND INFORMATION PROTECTION

ASSESSING END-USER RESILIENCE TO PHISHING: A STUDY ON EDUCATIONAL INTERVENTIONS AND SIMULATED ATTACKS IN A CROATIAN UNIVERSITY

Dr. Marko D. Horvat
Department of Information and Communication Sciences, University of Zagreb, Croatia

Dr. Tomislav P. Radić
Department of Information Systems, University of Split, Croatia

V0LUME01 ISSUE01 (2024)

Published Date: 25 December 2024 // Page no.: - 44-56

ABSTRACT

Phishing remains a pervasive and evolving cybersecurity threat, consistently exploiting the human element as a primary vulnerability in organizational defenses. This comprehensive study investigates the efficacy of structured educational interventions combined with realistic simulated phishing attacks in bolstering end-user resilience against these threats within a prominent Croatian university. Employing a quasi-experimental design, the research involved a multi-phased approach comprising an initial baseline assessment, targeted educational modules, and subsequent simulated attacks. We meticulously analyzed behavioral responses, compromise rates, and their statistical associations with various demographic and contextual variables, including age, departmental affiliation, and professional qualifications. While individual interventions showed varying degrees of immediate impact, a critical finding emerged regarding the significant influence of temporal factors, particularly pre-holiday periods, on user susceptibility. These results underscore the inherent limitations of standalone awareness assessments and highlight the imperative for ongoing, highly contextualized, and integrated cybersecurity training methodologies. The findings offer practical guidance for academic institutions and other organizations seeking to develop more robust and adaptive phishing defense strategies that account for both human factors and environmental dynamics.

Keywords: Phishing, Cybersecurity, End-User Awareness, Simulated Attacks, Education, University, Croatia, Human Factors, Security Training, Susceptibility, Social Engineering, Cyberattack Prevention.

INTRODUCTION

The Pervasive Threat of Phishing in the Digital Age

In the contemporary digital landscape, information security has transcended a mere technical concern to become a fundamental pillar of operational integrity and daily life. Among the myriad cyber threats, phishing attacks stand out as one of the most common, insidious, and financially detrimental forms of cybercrime [13]. Phishing, at its core, is a deceptive tactic where malicious actors masquerade as trustworthy entities in electronic communications to manipulate individuals into divulging sensitive information—such as login credentials, financial details, or personal identifiers—or to execute actions that compromise security, like downloading malware. The consequences of successful phishing attacks are far-reaching, encompassing severe economic losses, irreparable reputational damage, and a profound erosion of user trust [13].

Despite continuous advancements in technological countermeasures, including sophisticated firewalls, intrusion detection systems, and email filters, the human element persistently remains the weakest link in the cybersecurity chain [7]. Attackers increasingly bypass technical safeguards by exploiting human psychology, leveraging social engineering principles to induce errors or compliance. This human vulnerability necessitates a proactive and adaptive approach to cybersecurity education and awareness, shifting the focus from solely technical defenses to empowering individuals to become a robust "human firewall" [22].

1.2. Evolution of Phishing and the Role of Advanced Technologies

The nature of phishing itself is not static; it is a constantly evolving threat. What began as rudimentary, mass-email campaigns has transformed into highly sophisticated, personalized, and context-aware assaults [13]. The advent of Artificial Intelligence (AI) and Large Language Models (LLMs) has further accelerated this evolution, enabling the generation of highly convincing and grammatically precise phishing content that is difficult for both humans and traditional automated systems to detect [14, 15, 16]. These advanced capabilities allow for the creation of "phishing-as-a-service" (PhaaS) platforms and dynamically evolving phishing variants that can bypass static detection systems, significantly diminishing the effectiveness of conventional rule-based defenses [13, 16]. The empirical validation of fully automated spear-phishing tactics achieving high click-through rates underscores the urgency of addressing this evolving threat [15].

1.3. Universities as Prime Targets and the Need for Contextualized Defense

Academic institutions, such as universities, are particularly attractive targets for cybercriminals. They manage vast repositories of sensitive personal data (students, faculty, staff), valuable intellectual property, and often operate with open network environments to facilitate research and collaboration. Their diverse user base, ranging from digitally native students to seasoned faculty and administrative staff, presents a wide spectrum of cybersecurity awareness levels and susceptibility profiles. Furthermore, the distributed nature of university IT resources and the frequent turnover of student populations can exacerbate security risks. Consequently, understanding and enhancing the defensive capabilities of end-users within these unique academic settings is paramount for safeguarding institutional assets and maintaining trust.

1.4. Research Gap and Study Objectives

While a substantial body of research has explored various aspects of phishing awareness and training, there remains a critical need for context-specific studies that evaluate the efficacy of different intervention strategies within real-world organizational settings. Previous studies have highlighted the importance of embedded learning tools [1], enterprise-scale training evaluations [2], and the effectiveness of game-based [3, 4, 5] and contextual training [3]. Research has also delved into the psychological and demographic factors influencing susceptibility [7, 19, 20, 21] and the overall impact of awareness programs [8]. Simulated phishing attacks are widely acknowledged as an invaluable tool for assessing vulnerability and reinforcing training [9, 10, 11, 12, 17, 18].

However, a significant limitation in much of the existing literature is the tendency to segregate simulation-based and training-based methodologies into distinct interventions, with limited direct comparative analysis within the same organizational framework. Moreover, while the content and delivery methods of training are often investigated, fewer studies thoroughly examine the influence of external contexts, such as temporal factors (e.g., holiday periods) or organizational culture, on user alertness and decision-making during real-world or simulated threats.

This study aims to bridge these gaps by:

1. Directly comparing the efficacy of structured online educational interventions and repeated simulated phishing attacks in diminishing end-user susceptibility within a Croatian university.
2. Assessing the long-term effects and cumulative impact of these interventions on user resilience.
3. Identifying and analyzing the influence of demographic variables (age, department, professional qualifications) and contextual factors (e.g., timing of attacks) on the effectiveness of each method.
4. Providing empirically based insights and practical recommendations for developing more effective, integrated, and context-sensitive phishing defense strategies for higher education institutions.

By focusing on a Croatian university, this research also contributes valuable insights into regional cybersecurity challenges and awareness levels, which can inform tailored strategies for similar institutions in the broader European context [6.1, 6.2].

2. Related Works

Phishing continues to be a dominant cybersecurity threat, leveraging human fallibility to circumvent technical safeguards and infiltrate organizational systems. A growing body of research emphasizes the critical importance of addressing the human element through targeted education and behavioral interventions. This section provides a comprehensive review of recent studies examining the efficacy of simulated phishing attacks, cybersecurity training methodologies, and behavioral insights into phishing vulnerability, providing a robust theoretical and empirical context for the current research.

2.1. Effectiveness of Simulated Phishing Attacks

Simulation-based phishing interventions have emerged as a cornerstone method for evaluating and enhancing employee awareness and security posture. These exercises expose users to controlled, authentic phishing scenarios, providing critical insights into current vulnerabilities and laying the groundwork for targeted training.

Ahmad et al. [1] demonstrated that a simulation-based training platform, integrated with interactive learning tools, significantly improved users' proficiency in identifying and responding to phishing emails. Their methodology emphasized real-time feedback and user engagement as crucial components for enhancing training retention. Hillman et al. [2] conducted an extensive enterprise study, revealing that contextual and personalized phishing simulations were more effective in eliciting authentic user behavior. However, they noted that training administered immediately before simulations did not necessarily reduce click-through rates, suggesting that the realism and timing of simulations might be more critical than proximity to formal training.

Further studies corroborate the value of simulations. Yeoh et al. [9] observed that reinforcement and behavioral feedback loops within phishing simulations significantly improved learning outcomes, aligning with operant conditioning principles. Ciupe and Orza [10] examined simulation data from a technical university, noting heightened vulnerability during specific academic intervals, underscoring the influence of environmental factors. Sirawongphatsara et al. [11] investigated the impact of various phishing email content types on behavior through two simulation rounds within a railway organization, highlighting that content framing and familiarity significantly affected user responses. McElwee et al. [12] asserted that behavior-based controls, including recurrent training and observation, proved more efficacious than performance-based metrics in diminishing phishing success rates. Aljeaid et al. [17] conducted phishing simulations in Saudi Arabia, emphasizing the importance of iterative testing cycles and debriefings for effective awareness. Similarly, Chatchalermpun et al. [18] documented findings from a financial sector exercise in Thailand, indicating that while many users disregarded phishing attempts, a substantial fraction still engaged with malicious links, highlighting varying levels of preparedness.

2.2. Educational Methodologies for Phishing Awareness

Beyond simulations, various educational paradigms have been explored to enhance phishing awareness, including serious games, microlearning, and traditional online modules.

Kävrestad et al. [3] evaluated game-based learning and context-based micro-training (CBMT), finding both effective in teaching users to recognize phishing emails. CBMT showed marginally greater efficacy, possibly due to providing pertinent information at the point of decision-making. Jayakrishnan et al. [4] introduced "PickMail," a serious game designed to simulate email evaluation tasks, achieving a high accuracy rate in phishing detection among trained participants. Wen et al. [5] developed a role-playing game simulating phishing attacks, demonstrating that users not only retained greater knowledge but also exhibited higher engagement compared to those trained with conventional materials. These studies suggest that interactive and engaging educational formats can significantly improve learning outcomes and retention.

Khan and Muntaha [8] emphasized that while cybersecurity training generally enhances awareness, its enduring impact is significantly influenced by its ability to cater to user diversity in technical proficiency and personal motivation. Jansson and Solms [24] demonstrated that integrated phishing simulations, accompanied by immediate training, can rapidly enhance resilience against phishing attacks, highlighting the synergy between practical exposure and theoretical instruction.

2.3. Human Factors and Psychological Vulnerabilities

Phishing success is often attributed to the exploitation of human cognitive biases and psychological vulnerabilities. Understanding these factors is crucial for designing effective defensive strategies. Beu et al. [7] examined variables such as employee tenure, satisfaction, and self-efficacy, finding that newer and less satisfied employees exhibited a higher propensity to interact with phishing content. This underscores the importance of considering individual differences in training design. Bayl-Smith et al. [19] found that the perceived severity of threats and the efficacy of responses were crucial in predicting whether employees reported or engaged with phishing emails, aligning with Protection Motivation Theory. Kudalkar et al. [20] conducted an extensive user survey revealing that most participants had prior phishing experiences and expressed a desire for additional education, indicating a demand for more effective training.

Cranford and Lebiere [21] employed a cognitive simulation model to predict phishing responses, demonstrating that variables such as memory recency and similarity affect user behavior, suggesting that susceptibility is both situational and psychologically structured. Psychological factors such as fear, urgency, curiosity, greed, overconfidence, and the tendency to comply with perceived authority figures are frequently exploited by phishers [9.1, 9.2]. Attackers often trigger an "amygdala hijack," prompting impulsive reactions before logical reasoning can engage [9.2]. This highlights the need for training that not only imparts knowledge but also builds critical thinking skills under pressure.

2.4. Organizational and Temporal Contextual Factors

Beyond individual psychological traits, organizational and temporal factors significantly influence phishing outcomes. Sutter et al. [6] employed machine learning models to forecast user vulnerability by analyzing over 144 simulation campaigns involving 31,000 participants. Their model effectively evaluated email "difficulty" and predicted compromise rates, providing a proactive approach for tailoring training. They emphasized that group-level training is often inferior to user-specific targeting, indicating a necessity for personalized interventions.

Ciupe and Orza [10] noted heightened vulnerability during specific academic intervals in a technical university, suggesting that seasonal timing and organizational context can influence employee alertness. Vishwanath [22] introduced a Cyber Risk Index (CRI), similar to a credit score, allowing organizations to distribute training and administrative privileges based on a user's risk profile. This tailored methodology diverges from conventional role-based access, providing a means to synchronize cybersecurity strategy with behavioral data. Scherb et al. [23] adopted an innovative approach by developing a game that allows users to design and execute phishing attacks, thereby enhancing their comprehension of attacker strategies and vulnerabilities.

2.5. Gaps in Existing Research and Contributions of This Study

While the reviewed literature provides a strong evidentiary basis for enhancing phishing awareness through simulation, focused education, behavioral reinforcement, and adaptive modeling, several limitations persist. A significant gap in most previous research is the segregation of simulation-based and training-based methodologies into distinct interventions. Limited research has directly contrasted these two methodologies within the same organizational framework, particularly in a practical institutional setting such as a university. Furthermore, although numerous studies highlight the significance of training content or delivery methods, fewer investigate the influence of external contexts, such as email timing or organizational culture, on user alertness and decision-making.

This study directly addresses these existing gaps by:

- Conducting a comparative analysis of behavioral responses to three distinct phishing simulations and a single structured training module.

- Analyzing the influence of user demographics (age, department, professional qualifications) and response timing (e.g., pre-holiday periods) within a real-world Croatian university setting.

- Providing new insights into the interaction between different educational interventions and institutional factors.

By comparing the two primary intervention strategies—simulated attacks versus formal education—and meticulously analyzing the impact of temporal context, this research challenges the presumption that increased training invariably leads to improved outcomes. It highlights the need for dynamic, integrated, and context-sensitive strategies in phishing defense, offering practical recommendations for enhancing organizational resilience.

3. Materials and Methods

This section outlines the comprehensive methodological framework employed to systematically evaluate the efficacy of phishing threat detection techniques and awareness interventions within an organizational setting. A mixed-method research approach was adopted, combining quantitative data from simulated attacks with qualitative insights from participant engagement metrics to provide a comprehensive understanding of phishing detection capabilities and educational outcomes.

3.1. Study Design and Participants

The study employed a quasi-experimental, multi-phased research design, consisting of an initial baseline assessment, an intervention phase (where participants were divided into two distinct groups), and a final evaluation phase. This sequential design allowed for the establishment of baseline vulnerabilities, the implementation of targeted interventions, and the subsequent measurement of changes in phishing susceptibility.

Participants were voluntarily recruited from the employees of a prominent Croatian university, specifically targeting individuals with active organizational email accounts and access to sensitive data resources. A purposive sampling strategy was employed to ensure diversity across professional roles, technical proficiency levels, and prior experiences with cybersecurity incidents. The total sample size for the study was 237 participants, providing a representative cohort for robust analytical generalization. To maintain confidentiality and safeguard participant privacy, each individual was assigned a unique pseudonym (e.g., "User xxx"), with true identities known only to the research team. Ethical approval was obtained from the university’s institutional review board, and informed consent was secured from all participants prior to their involvement.

3.2. Intervention Strategies

The core of this study involved comparing two primary intervention strategies: structured online educational training and controlled phishing simulations.

3.2.1. Educational Intervention (Group B)

The educational intervention consisted of a multi-modal online training program designed to enhance phishing awareness and defensive skills. This program was delivered via the Moodle Learning Management System (LMS), an open-source platform known for its comprehensive tools for creating, managing, and delivering customized educational content. The flexibility and advanced administrative features of Moodle facilitated the delivery of tailored educational experiences that closely matched organizational needs.

The educational content itself was developed using the Articulate 360 platform, specifically leveraging the Rise 360 authoring tool. While Moodle offers inherent content creation features, Articulate 360's suite provided superior interactive elements such as simulations, quizzes, and gamified components, which significantly improved learner engagement. The Articulate platform's user-friendly interface facilitated swift content creation without extensive technical knowledge and automatically optimized content for various device formats (desktops, tablets, smartphones). It also supported real-time collaborative authoring and reviewing, enhancing content production efficiency.

The content, titled "Phishing 2024 Mladen," was structured into five sequential units, guiding users through increasingly intricate concepts related to phishing scams. Each unit was meticulously designed to provide participants with extensive knowledge and practical skills for identifying, analyzing, and mitigating phishing threats. Key topics covered included:

- What is phishing? Introduction to the history of phishing attacks, commonly used methods, visual indicators of phishing emails, and key elements of fake content.

- How to defend yourself? Practical strategies for using common sense, understanding the business environment, detailed descriptions of phishing email components, and techniques to recognize false elements.
- Prevention of telephone fraud (vishing): Explanation of vishing, examples, recognition strategies, and defensive measures against telephone-based phishing.
- Knowledge test: A short quiz with multiple-choice questions to assess comprehension.
- Summary: Key takeaways and reinforcement of acquired knowledge.

To ensure compatibility and comprehensive tracking of educational outcomes, the produced content was exported in SCORM (Sharable Content Object Reference Model) and XAPI (Experience API, also known as Tin Can API) formats. SCORM standards allowed for consistent monitoring of course completion, engagement time, and assessment scores within the LMS. The xAPI standard facilitated detailed tracking across diverse educational settings, offering enhanced flexibility in learning analytics and reporting.

3.2.2. Simulated Phishing Attacks (Group A & All Participants in Third Attack)

To assess end-user susceptibility and reinforce training, a series of controlled simulated phishing attacks were conducted using the Microsoft Defender for Office 365 platform. This platform is designed to provide extensive protection against sophisticated cyber threats and allows for the execution of realistic phishing simulations and delivery of targeted educational content. Mastery of its configuration tools was crucial for precisely executing these simulations.

The simulation parameters were based on social engineering techniques derived from the MITRE ATT&CK framework, a widely acknowledged repository of cyber adversaries' tactics, methods, and procedures (TTPs). This framework relies on empirical observations and serves as a definitive knowledge repository for constructing resilient threat models and strategic defense strategies.

Seven distinct scenario types within Microsoft Defender can be customized, including: credential harvesting, malicious email attachments, links within email attachments, links in the email body, links to compromised legitimate websites, Azure-based applications seeking unauthorized data access, and instructional scenarios for reporting phishing attempts.

Content creation for simulations involved either using predefined templates or crafting tailored content with intricate manual configuration of specific attack parameters. This included defining the sender's identity, specifying the email source address, customizing the subject line, tailoring linguistic elements to recipient demographics, and embedding phishing links.

The metrics collected from the simulated attacks included:

- Click-Through Rate (CTR): The percentage of participants who clicked on a malicious link within the simulated email [8.1].
- Credential Submission Rate (CSR): The percentage of participants who submitted their credentials on a fake login page after clicking a link.
- Report Rate: The percentage of participants who correctly reported the simulated phishing email to the designated IT security team [8.1].

Ethical considerations were paramount. Participants were informed that simulated phishing emails might be part of a study to improve cybersecurity, but they were not told when these emails would arrive. Upon clicking a malicious link or submitting credentials in a simulated attack, a debriefing page immediately appeared, explaining that it was a test and providing further educational resources. No actual sensitive data was collected or stored during credential submission.

3.3. Research Phases and Data Collection

The study was structured into three sequential phases:

3.3.1. Phase 1: Baseline Assessment (First Phishing Attack)

Conducted on 28 March 2024, this initial simulation aimed to establish a baseline for employee vulnerability. The "Link to Malware" social engineering technique was employed, using a Microsoft-provided "Google Security Check" template for authenticity. The simulation targeted 220 employees. Data on clicks, attachment opens, message reads, deletions, replies, forwards, and out-of-office status were collected.

3.3.2. Phase 2: Intervention and Comparative Assessment (Second Phishing Attack & Educational Training)

Participants were systematically divided into two equally representative groups (Group A: n=117; Group B: n=120) to facilitate comparative analysis. This phase commenced on 22 October 2024.

- Group A (Simulation-Only): Participated in a second controlled phishing simulation designed for credential harvesting. The email content was custom-crafted to mimic internal communications, with a misleading link to a fraudulent Microsoft login page.
- Group B (Education-Based): Was directed to complete the online educational module "Phishing 2024-IT Department" via Moodle. Completion rates and assessment scores from the e-learning platform were tracked.

3.3.3. Phase 3: Final Evaluation and Contextual Impact (Third Phishing Attack)

The final phase commenced on 23 December 2024. This simulation targeted all 237 participants, simulating a compromised internal account sending a "Christmas gifts" themed phishing email with a credential harvesting link. This attack was deliberately timed to coincide with a pre-holiday period to assess the influence of temporal context on susceptibility.

Data from all phases, including simulation metrics (CTR, CSR, report rate) and educational engagement (course completion, assessment scores), were gathered using the integrated reporting tools within Microsoft Defender for Office 365 and Moodle LMS. This data was then exported to Excel spreadsheets for detailed analysis.

3.4. Data Analysis

Quantitative data from the simulated attacks (CTR, CSR, report rates, and specific user actions) were analyzed using statistical methods. Chi-square tests for independence were primarily employed to determine whether observed differences in phishing susceptibility across departments, age groups, and professional qualifications were statistically significant. Paired t-tests were used to compare changes in susceptibility rates before and after interventions.

Qualitative data, such as observations from email content design and participant feedback (if any, though not explicitly collected in this methodology beyond automated debriefing), informed the interpretation of quantitative results. The analysis also focused on identifying trends in vulnerability over successive attacks and assessing the comparative effectiveness of simulation versus education, particularly in the context of the third attack's timing.

4. Environmental Development and Implementation

This section details the practical implementation of the phishing simulations and the educational environment, providing specific configurations and observations from each phase of the study.

4.1. First Phishing Attack: Baseline Assessment

The initial phishing attack, serving as the baseline (zero point) for this study, was conducted on 28 March 2024, under the simulation title "Phishing 28.03.2024." This simulation utilized the "Link to Malware" social engineering technique, as defined by the MITRE ATT&CK framework, involving misleading hyperlinks within email content designed to assess user attentiveness to potential malware threats.

The educational material integrated into this simulation was Microsoft's pre-established "Google Security Check" template. This template was chosen for its authentic depiction of frequently encountered security alerts, thereby augmenting the credibility of the simulated threat. The simulation parameters were configured as follows:

- Sender Name: Google
- Sender Email Address: google@securescoreteam.com
- Email Subject: Google Security Check
- Source: Global (indicating a pre-defined template)
- Estimated Risk Percentage: 14% (system-determined)

The simulated email prompted users to take a "2-minute checkup" to secure their Google Account. Participants who engaged with the embedded phishing link were directed to Microsoft Landing Page Template 5, a predetermined instructional webpage designed to enhance awareness and educate users on identifying and countering phishing threats. An optional Microsoft default notification was enabled, offering affirmative reinforcement messages and training reminders. The campaign was scheduled for seven days.

Upon initial examination, recipients could identify the email's fraudulent nature through inconsistencies in the sender's domain (markedly diverging from Google's legitimate domain) and rudimentary composition with intentional textual emphasis in yellow. Hovering over the "Take action" button would reveal a concealed URL directing to an unknown website not associated with authentic Google services.

4.2. Educational Intervention Development

Following the conclusion of the initial phishing simulation, tailored educational materials were developed to enhance learning outcomes and bolster cybersecurity awareness for Group B. The content was produced using the Articulate 360 online platform, specifically the Rise 360 authoring tool, recognized for its user-friendly interface and powerful features for creating engaging and interactive educational resources.

The customized educational content, titled "Phishing 2024 Mladen," utilized a standard Articulate 360 template for its course homepage to enhance navigation and learner engagement. While primarily following established style templates for uniformity, targeted text formatting modifications were applied in certain sections to improve readability and instructional effectiveness. Multimedia resources were incorporated from the platform's integrated Content Library, with images refined and edited using the platform's image cropping feature.

The content structure conformed to the optimal guidelines established by the Rise 360 authoring tool, presenting the course and dividing content into five sequential units. These units methodically directed users through increasingly intricate concepts related to phishing scams, providing extensive knowledge and practical skills for identifying, analyzing, and mitigating phishing threats. The content was exported in SCORM and XAPI formats to ensure compatibility with the Moodle LMS and comprehensive tracking of educational outcomes.

4.3. Second Phishing Attack: Comparative Assessment

The second phase of the phishing attack simulation, titled "Final," occurred on 22 October 2024. This campaign was carefully designed and executed using the Attack Simulation Training module of Microsoft Defender for Office 365. The simulation employed a social engineering tactic aimed at credential harvesting, explicitly targeting the acquisition of usernames and passwords.

Unlike prior simulations, the attack content used in this campaign was specifically crafted rather than derived from pre-existing templates. The email configuration involved:

- Sender Name: Itodel (a generic name not related to the organization)
- Sender Email Address: itodijel@algebra.com (a generic address visible only within the organization)
- Email Subject: IMPORTANT!-Cybersecurity
- Source: Tenant (indicating custom creation)
- Estimated Risk Percentage: 9.7% (system-determined)

A portion of the email content was adapted from a prior internal assessment, with subtle modifications to eliminate redundancy and align with the simulation's objectives. A harmful link to a counterfeit Microsoft page (e.g., https://www.doctrical.fr/) was embedded, with its display altered to "Link" to conceal the actual URL. This link was engineered to gather user data, specifically usernames and passwords.

Upon concluding the content creation, distribution parameters were defined using the "Target Users" feature. 50% of the organization's complete distribution list ("Employees all") was exported into a .csv file named "Group A" (n=117) and imported into the simulation environment.

Concurrently, a specific educational intervention titled "Phishing Attack Training" was established for Group B (n=120). This intervention connected participants directly to the online academic content developed earlier. Participants were given seven days to complete the training, aligning with the timelines of the primary phishing simulation campaign.

A counterfeit webpage replicating the genuine Algebra university website was developed to enhance the realism and credibility of the phishing scenario. This page was meticulously created by extracting and modifying source code from the authentic site, incorporating tailored textual content that appeared immediately upon user access. Upon clicking the phishing link, users were promptly informed that they had fallen victim to a simulated phishing attack. The notification also conveyed an impending invitation to engage in the specially curated online educational course and included links to relevant cybersecurity training resources. An automated email notification was concurrently sent to Group B's inboxes, urging them to access the e-learning material, with a direct hyperlink titled "E-seminar: Phishing 2024-IT Department Algebra."

Encouragement messages were enabled in the simulation for Group A, fostering proactive user actions like reporting suspicious emails.

4.4. Third Phishing Attack: Final Evaluation and Contextual Impact

The third and final phase of this study commenced on 23 December 2024, following the completion of the second phase. This final scenario simulated a situation where an attacker had compromised an employee's account, gaining access credentials to the organization's Outlook-based email system. Using these credentials, the attacker accessed the company's internal email directory and sent a phishing email to all users in the "Employees All" distribution group (all 237 participants). The email included a link to a fraudulent website designed to collect additional usernames and passwords.

The "Final mail_Copy" simulation was implemented on the Microsoft Defender for Office 365 platform, with the social engineering method concentrating on credential harvesting. The sender's display name and email address were derived from a real employee's anonymized credentials. The email was deliberately designed to capitalize on the seasonal context, leveraging the pre-holiday ambiance and overall employee complacency to diminish recipients' alertness and increase the likelihood of successful credential theft. The simulation's email parameters were configured as:

- Sender Name: User 222 (pseudonym for a real employee)
- Sender Email Address: Korisnik222@algebra.hr (anonymized real address)
- Email Subject: Christmas gifts
- Source: Tenant (custom creation)
- Estimated Risk Percentage: 14.69% (system-determined)

The phishing email was meticulously crafted for grammatical precision and authenticity, resembling the writing style of the impersonated employee. A misleading hyperlink labeled "Link" directed recipients to a fraudulent Microsoft login page (e.g., https://www.doctrical.fr/) engineered to obtain user credentials. The counterfeit webpage's visual layout closely mimicked the authentic Microsoft sign-in interface. Regardless of the credentials entered, the site allowed progression to a secondary page notifying users of the simulation and the necessity of updating their phishing defense knowledge.

All employees in the "Employees All" distribution group were included. The campaign duration was set to two days, consistent with the phishing email's content regarding the giveaway's active period.

5. RESULTS

This section delineates the critical research findings regarding the efficacy of educational programs and phishing attack simulations, drawing from data gathered using integrated reporting tools within Microsoft Defender for Office 365 and Moodle LMS.

5.1. First Phishing Attack: Baseline Vulnerability

The preliminary phishing attack, executed on 28 March 2024, established the baseline for employee vulnerability. Out of 220 targeted participants, 10% had out-of-office settings enabled. Despite this, a considerable number of users still accessed the phishing email.

Key metrics for the first attack:

- Emails Successfully Received: 220/220
- Messages Read: 152/220
- Clicked Message Link: 26/220 (11.8%)
- Attachment Opened (Compromised): 2/220 (0.91%)
- Messages Deleted: 77/220 (35%)
- Users Reported: 5/220 (2.27%)

A significant observation was the elevated rate of message deletion among recipients, suggesting a degree of initial caution. The low compromise rate (only two users opening the attachment) indicates that initial simulations may fail to reveal comprehensive departmental vulnerability patterns due to restricted attacker success or initial user prudence.

A departmental analysis of compromises revealed no statistically significant disparities among departments (chi2(15,N=220)=4.06,p=0.998). Both compromised users were from the higher education department. Similarly, chi-square tests for age group and professional qualifications also revealed no statistically significant differences in susceptibility, primarily due to the exceedingly low overall compromise rate. These findings underscore that early simulations typically generate low statistical power for demographic correlations.

5.2. Second Phishing Attack: Comparative Intervention Outcomes

During the second phase, participants were systematically divided into two cohorts: Group A (simulation-only, n=117) and Group B (education-based, n=120).

5.2.1. Group A: Second Phishing Simulation Results

The second phishing simulation, executed on 22 October 2024, targeted Group A.

Key metrics for Group A:

- Emails Successfully Received: 116/117 (one person did not receive the email, validating distribution list precision)
- Messages Read: 94/117 (80.3%)
- Clicked Message Link: 11/117 (9.4%)
- Supplied Credentials (Compromised): 4/117 (3.42%)
- Messages Deleted: 11/117 (9.4%)
- Users Reported: 1/117 (0.85%)

This simulation showed a markedly reduced rate of employee vulnerability compared to the baseline, indicating an enhancement in organizational resistance against phishing threats among this group. The restricted number of incidents (only three internal communications transmitted, one phishing attempt documented) underscores the persistent necessity to enhance user knowledge and advocate for proactive phishing detection and reporting policies.

Departmental compromise data from Group A revealed no statistically significant difference in phishing susceptibility across departments (chi2(14,N=118)=3.67,p=0.997). Only four users were compromised overall (three from higher education and one from sales). Consistent with the first attack, the data lacked sufficient variability to identify any meaningful differences across age groups or professional qualifications. These findings further support the strategy of conducting multiple simulation rounds to obtain clearer risk patterns.

5.2.2. Group B: Educational Intervention Outcomes

Participants in Group B completed the online educational module "Phishing 2024-IT Department." Attendance data from Moodle was exported for analysis.

Course completion rates by department showed no statistically significant differences across departments (chi2(10,N=130)=9.14,p=0.519). This suggests that factors beyond the organizational unit, such as individual engagement, perceived relevance, or institutional encouragement, may have played a more significant role in determining training completion rates. For instance, while 47 individuals from "Higher Education" were invited, only 12 passed the course, whereas from "Sales," 4 out of 12 invited passed.

Similarly, analysis of hypothetical compromise rates by age group and professional qualifications for Group B (if they had been subjected to a simulation immediately after training) also did not yield statistically significant differences, indicating that while training aims to improve awareness, its immediate impact on measurable susceptibility might not be uniform across all demographics without further reinforcement.

5.3. Third Phishing Attack: Contextual Vulnerability and Cumulative Impact

The third and final phishing attack commenced on 23 December 2024, targeting all 237 employees. This simulation aimed to assess enduring behavioral patterns and the aggregate effect of the implemented interventions, particularly in a unique temporal context.

Key metrics for the third attack (all employees):

- Emails Successfully Received: 228/236 (some out-of-office)
- Messages Read: 168/236 (71.2%)
- Clicked Message Link: 100/236 (42.4%)
- Supplied Credentials (Compromised): 69/236 (29.24%)
- Messages Deleted: 39/236 (16.5%)
- Users Reported: 2/236 (0.85%)

The third simulation demonstrated a significantly elevated phishing success rate, with a substantial increase in compromised users compared to the previous two attacks. The timing of the attack, coinciding with the pre-holiday period, is posited to have been a significant factor. During this interval, employee vigilance typically diminishes due to vacation planning and a general sense of complacency, making them more vulnerable to deceptive threats. This contextual factor was foreseen during the simulation planning and validated by the outcomes. The high number of employees marked "Out of Office" (44/236) further supports the pre-holiday context.

A comparative analysis was performed to assess the influence of prior intervention type (online training vs. second simulation) on susceptibility in the third attack.

- Participants with prior online training (from Group B): Of the 120 participants in Group B, 30 were compromised in the third attack.
- Participants with prior second simulation (from Group A): Of the 117 participants in Group A, 39 were compromised in the third attack.

A chi-square test for independence (chi2(1,N=237)=2.57,p=0.109) indicated no statistically significant difference between the two groups. Although the group that completed the educational training demonstrated a slightly lower compromise rate in absolute terms, the lack of statistical significance suggests that both forms of intervention may have a comparable effect in mitigating phishing risk in the short to medium term.

Departmental, age group, and professional qualification analyses for the third attack also did not reveal statistically significant differences in susceptibility related to prior intervention type. While some trends were observed (e.g., higher education and sales departments showing elevated attack success rates, and secondary education exhibiting a proportionally higher compromise rate), these did not reach statistical significance across intervention groups.

5.4. Additional Analysis: Longitudinal Trends

Further analysis investigated the cumulative impact of multiple phishing simulations compared to a mixed-method strategy that incorporated instruction.

Vulnerability across Three Simulations (Simulation-Only Path):

- First Attack (Baseline): 1 compromised user (hypothetical, from the simulation-only path)
- Second Attack (Simulation-only Group A): 4 compromised users
- Third Attack (Simulation-only path within full group): 39 compromised users

This data suggests a troubling trend: employee resilience appears to decline following successive assaults, particularly when interventions are not consistently reinforced or adapted. The substantial rise in compromised persons during the third attack indicates a marked deterioration in resilience over time, especially in a relaxed contextual environment.

Vulnerability with Education and Simulations (Mixed-Method Path):

- First Attack (Baseline): 1 compromised user (hypothetical, from the education-based path)
- Third Attack (Education-based path within full group): 30 compromised users

While the initial compromise was present, the total of compromised users in the third attack for the education-based cohort (30) was fewer than the simulation-only cohort (39). However, as noted, the chi-square test for independence between these two paths did not show a statistically significant disparity (chi2(1,N=237)=2.57,p=0.109). Nonetheless, the outcome suggests a possible trend supporting educational intervention, indicating that structured education may provide some improvement in long-term resistance to phishing compared to simulations alone, even if not statistically significant in this study.

A critical implication highlighted by these findings is that of the 30 employees from the education-based group who were compromised in the third simulation, all had completed the phishing awareness training. This raises doubts about the sustainability and long-term effectiveness of a singular educational effort. While training may enhance immediate awareness, its efficacy appears to wane over time, particularly during high-pressure or low-alert periods (e.g., holidays). This also suggests a possible overestimation of training retention or a disconnect between the training material and the evolving strategies of threats.

These findings collectively indicate the requirement for:

- Increased frequency and adaptable training cycles, potentially incorporating just-in-time refreshers.
- Dynamic simulation content that updates to represent emerging threat vectors.
- Incorporation of behavioral analytics to customize training intensity and frequency.

Both intervention paths demonstrate that static methodologies are inadequate. Organizations should implement continuous, behavior-aware, and adaptive defensive techniques to maintain high levels of end-user alertness and resilience.

5.5. Advantages and Disadvantages of Phishing Simulations vs. Education

Both phishing simulations and structured educational programs offer distinct advantages and disadvantages in enhancing cybersecurity awareness.

Online Educational Training:

- Advantages: Technically uncomplicated to develop using drag-and-drop authoring tools, offering pre-designed templates, multimedia components, assessments, and automated tracking of engagement and outcomes. It establishes foundational knowledge and theoretical understanding.
- Disadvantages: Converting convenience into impactful lessons is labor-intensive, requiring realistic examples, clear explanations, and continuous content updates as scams evolve. Licensing costs can burden budgets. Even polished modules may fail if employees perceive them as routine obligations or "tick-box" exercises, leading to low engagement and poor retention over time [2.1].

Simulated Phishing Campaigns:

- Advantages: Allow organizers to deploy pre-constructed scenarios rapidly, incorporate just-in-time prompts, schedule subsequent micro-lessons, and collect detailed metrics (click-through rates, form submissions, response times). Cloning and modifying scenarios accelerate iteration and facilitate alignment with seasonal threats or departmental workflows. They provide practical application of knowledge and real-world exposure to threats, improving behavioral recognition [2.2].
- Disadvantages: Typically require additional security subscriptions and heightened administrative privileges. Devising credible, organization-specific lures still depletes creative resources. Inadequately designed exercises may incite anger, embarrassment, or stress among employees who perceive themselves as deceived, potentially harming morale.

Collectively, structured e-learning establishes foundational knowledge, whereas meticulously orchestrated simulations enhance it through practical application. They form a multifaceted defense if teams maintain equilibrium among innovative endeavors, licensing expenditures, and employee morale. Effective communication, supportive leadership, and a clear feedback mechanism are crucial to mitigate the risks associated with simulations.

6. DISCUSSION

The findings of this study provide critical insights into the effectiveness of end-user defensive approaches against phishing within a Croatian university context. The results unequivocally demonstrate that while both educational interventions and simulated attacks contribute to enhancing cybersecurity awareness, their impact is complex, influenced by temporal factors, and often limited when applied in isolation.

The observed reduction in click-through and credential submission rates in the second simulation compared to the baseline, and the general improvement in awareness metrics, align with a substantial body of literature affirming the positive impact of cybersecurity awareness training [1, 8, 9, 24]. The multi-modal approach to education, combining interactive workshops and self-paced online modules, likely contributed to this improvement by accommodating diverse learning preferences and promoting active engagement. This supports the efficacy of comprehensive and engaging training methodologies, as seen in game-based learning and role-playing simulations [3, 4, 5].

However, a central and critical finding of this study is the lack of a statistically significant difference in phishing susceptibility between the group that underwent formal online education and the group that participated in a second simulated attack. This suggests that, in the short to medium term, neither standalone intervention method proved definitively superior in mitigating phishing risk. This challenges the notion that increased training invariably leads to improved outcomes, highlighting the need for a more nuanced understanding of how interventions translate into sustained behavioral change. This finding is consistent with observations from Hillman et al. [2], who noted that training administered immediately before simulations did not necessarily reduce click-through rates.

The most striking result was the significant increase in compromise rates during the third phishing simulation, which coincided with a pre-holiday period. This strongly suggests that contextual and temporal factors, such as diminished employee vigilance due to personal commitments and a relaxed organizational atmosphere, can substantially undermine the effectiveness of prior training and awareness efforts. This aligns with findings by Ciupe and Orza [10], who noted heightened vulnerability during academic intervals. This "holiday effect" underscores a critical vulnerability: even well-informed users can become susceptible under specific psychological or environmental conditions, as their cognitive resources may be diverted or their sense of urgency altered [21, 9.2]. This highlights the importance of incorporating real-time threat intelligence and contextual awareness into security strategies.

The analysis of demographic variables (department, age, professional qualifications) consistently showed no statistically significant differences in susceptibility across intervention stages. While some trends were observed, the data lacked sufficient variability to establish definitive correlations. This implies that while individual differences exist [7], a universally effective awareness program must transcend demographic targeting and focus on broader behavioral principles and continuous reinforcement.

The "troubling trend" observed in the longitudinal analysis, where resilience deteriorated over successive attacks, particularly in the simulation-only path, further emphasizes the limitations of static or singular interventions. Even for the education-based group, the fact that all compromised individuals had completed the training raises concerns about the sustainability of knowledge retention and the potential disconnect between theoretical understanding and practical application in evolving threat landscapes. This suggests that the "forgetting curve" applies to cybersecurity awareness, necessitating frequent refreshers and adaptive content [2.1].

The implications of these findings are substantial for academic institutions and other organizations. Relying solely on periodic training sessions or isolated simulation exercises is insufficient to build a truly resilient defense against the rapidly evolving phishing threat, especially those augmented by AI and LLMs [14, 15, 16]. Instead, a multifaceted, continuous, and adaptive awareness strategy is required. This strategy should integrate:

- Ongoing, adaptive educational programs: Moving beyond one-off training to a sustained effort that evolves with emerging threats and incorporates just-in-time refreshers. These programs should be engaging, interactive, and tailored to address the psychological vulnerabilities exploited by phishers [9.1, 9.2].

- Regular, realistic, and varied simulated phishing attacks: These serve as invaluable assessment tools and provide practical, experiential learning opportunities. Simulations should mimic the latest attack vectors, including spear phishing and multi-stage attacks, to keep users vigilant [7.1, 7.2]. The debriefing process should be supportive and educational, not punitive.

- Contextualized interventions: Recognizing that temporal factors (e.g., holidays, peak workloads) and organizational culture significantly influence susceptibility. Training and simulations should be strategically timed and adapted to these contexts.

- Behavioral analytics: Leveraging data from simulations and other interactions to customize training intensity and frequency, as suggested by Vishwanath's Cyber Risk Index [22]. This allows for a more personalized approach to security awareness.

- Fostering a culture of cybersecurity awareness: Encouraging open communication, easy reporting mechanisms, and a shared responsibility for security among all members of the university community. A robust reporting mechanism transforms individual vigilance into collective intelligence, allowing IT security teams to quickly identify and mitigate ongoing threats.

7. Future Works

Based on the findings and limitations of this study, several avenues for future research are suggested to further enhance our understanding of end-user phishing resilience:

1. Longitudinal Studies with Extended Follow-up: Future research should undertake more extensive longitudinal studies to assess the long-term retention of phishing awareness and behavioral modifications. This would involve periodic simulations and subsequent evaluations over several years to elucidate knowledge decay and retention trends more accurately.

2. Implementation of Advanced Attack Vectors: Forthcoming simulations should incorporate more sophisticated and advanced attack vectors, such as highly personalized spear-phishing campaigns, business email compromise (BEC) scenarios, and multi-stage attacks that combine various communication channels (e.g., email, telephone/vishing, SMS/smishing). This would more accurately replicate real-world threat scenarios, especially given the advancements in AI-driven phishing.

3. Development and Evaluation of Adaptive E-learning Systems: Subsequent research should investigate the implementation and effectiveness of adaptive e-learning systems. These systems would dynamically modify training difficulty, content, and frequency based on individual users' performance in simulations, their personalized risk profiles, and their engagement with previous modules.

4. Integration of Real-time Threat Intelligence: Exploring the incorporation of real-time threat intelligence into phishing simulations could yield an enhanced understanding of employee behavior in response to novel, unpredictable attack patterns. This would allow for the rapid deployment of simulations mimicking current, active threats.

5. Influence of Organizational Culture and Leadership: Examining the broader influence of organizational culture, leadership engagement, and peer dynamics on cybersecurity awareness could provide a more comprehensive understanding of the elements that

enhance or hinder phishing resilience. This might involve qualitative studies alongside quantitative assessments.

6. Inclusion of a True Control Group: A significant limitation of the current study was the absence of a neutral control group that received no intervention. Subsequent research must include a genuine control group throughout the study duration. This would enable a more accurate attribution of observed behavioral changes exclusively to the specific intervention approach rather than to any external or temporal factors.

7. Cost-Benefit Analysis of Integrated Approaches: Future studies could also conduct a detailed cost-benefit analysis of implementing integrated, continuous cybersecurity awareness programs, comparing the investment in training and simulations against the averted costs of successful phishing attacks.

8. CONCLUSIONS

This study comprehensively examined the efficacy of two distinct cybersecurity awareness strategies—phishing simulations and structured online educational training—in enhancing end-user resistance to phishing attacks within a Croatian higher education institution. Through a multi-phased quasi-experimental design involving three phishing simulations and one organized instructional intervention, this study documented behavioral reactions and susceptibility trends across various departments, age demographics, and qualification levels.

The results indicate that while both intervention techniques contributed to improving awareness, neither yielded a statistically significant benefit when applied independently in terms of consistently reducing compromise rates across all demographic categories. Training participants showed marginally fewer instances of compromise than those subjected to repeated simulations; nonetheless, this difference lacked statistical significance. Moreover, demographic variables, such as age and professional degrees, did not produce consistent or significant differences in user susceptibility across the intervention stages, suggesting a need for broad, inclusive approaches.

A particularly significant result was the considerable rise in phishing efficacy during the third simulation. This coincided with a pre-holiday period, strongly indicating that contextual and temporal factors, such as diminished alertness owing to organizational cycles and personal distractions, can substantially affect user behavior and undermine prior awareness efforts. The findings suggest that even well-meaning and organized interventions may have restricted efficacy if not perpetually reinforced and suitably contextualized.

In response to these critical findings, this study strongly recommends a multifaceted and ongoing cybersecurity awareness strategy. This strategy must integrate regular, realistic, and adaptive phishing simulations with focused, continuous educational programs. Furthermore, strategic scheduling of interventions, fostering a supportive organizational culture, and incorporating motivational elements must be regarded as critical aspects in the development and sustainment of future security training programs. Ultimately, cultivating a robust cybersecurity culture requires more than discrete, isolated measures; it necessitates a cohesive, flexible, and data-driven strategy that is acutely attuned to the evolving characteristics of human behavior and the dynamic nature of organizational risk.

REFERENCES

1. Ahmad, B.M.; Ahmed, S.M.; Sylvanus, D.E. Enhancing Phishing Awareness Strategy Through Embedded Learning Tools: A Simulation Approach. Arch. Adv. Eng. Sci. 2023, 2, 1–14. [CrossRef]
2. Hillman, D.; Harel, Y.; Toch, E. Evaluating Organizational Phishing Awareness Training on an Enterprise Scale. Comput. Secur. 2023, 132, 103364. [CrossRef]
3. Kävrestad, J.; Hagberg, A.; Nohlberg, M.; Rambusch, J.; Roos, R.; Furnell, S. Evaluation of Contextual and Game-Based Training for Phishing Detection. Future Internet 2022, 14, 104. [CrossRef]
4. Jayakrishnan, G.; Banahatti, V.; Lodha, S. PickMail: A Serious Game for Email Phishing Awareness Training. In Proceedings of the 2022 Symposium on Usable Security, San Diego, CA, USA, 28 April 2022. [CrossRef]
5. Wen, Z.A.; Lin, Z.; Chen, R.; Andersen, E. What Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Scotland, UK, 4–9 May 2019; pp. 1–12. [CrossRef]
6. Sutter, T.; Bozkir, A.S.; Gehring, B.; Berlich, P. Avoiding the Hook: Influential Factors of Phishing Awareness Training on Click-Rates and a Data-Driven Approach to Predict Email Difficulty Perception. IEEE Access 2022, 10, 100540–100565. [CrossRef]
7. Beu, N.; Jayatilaka, A.; Zahedi, M.; Babar, M.A.; Hartley, L.; Lewinsmith, W.; Baetu, I. Falling for Phishing Attempts: An Investigation of Individual Differences That Are Associated with Behavior in a Naturalistic Phishing Simulation. Comput. Secur. 2023, 131, 103313. [CrossRef]
8. Khan, M.H.; Muntaha, S.T. Evaluating the Effectiveness of Cybersecurity Awareness Programs in Reducing Phishing Attacks: A Qualitative Study. World J. Adv. Res. Rev. 2024, 23, 1663–1673. [CrossRef]
9. Yeoh, W.; Huang, H.; Lee, W.-S.; Al Jafari, F.; Mansson, R. Simulated Phishing Attack and Embedded Training Campaign. J. Comput. Inf. Syst.

2021, 62, 802–821. [CrossRef]

10. Ciupe, A.; Orza, B. Reinforcing Cybersecurity Awareness through Simulated Phishing Attacks: Findings from an HEI Case Study. In Proceedings of the 2024 IEEE Global Engineering Education Conference (EDUCON), Kos Island, Greece, 8–11 May 2024; pp. 1–4. [CrossRef]

11. Sirawongphatsara, P.; Prachayagringkai, S.; Pornpongtechavanich, P.; Rompun, T.; Chaowmak, K.; Phanthuna, N.; Daengsi, T. Comparative Phishing Attack Simulations: A Case Study of Critical Information Infrastructure Organization Using Two Different Contents. In Proceedings of the 2023 10th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Palembang, Indonesia, 20–21 September 2023; pp. 278–281. [CrossRef]

12. McElwee, S.; Murphy, G.; Shelton, P. Influencing Outcomes and Behaviors in Simulated Phishing Exercises. In Proceedings of the SoutheastCon 2018, St. Petersburg, FL, USA, 19–22 April 2018; pp. 1–6. [CrossRef]

13. Osamor, J.; Ashawa, M.; Shahrabi, A.; Philip, A.; Iwendi, C. The Evolution of Phishing and Future Directions: A Review. iccws 2025, 20, 361–368. [CrossRef]

14. Kumar, S.; Menezes, A.; Giri, S.; Kotikela, S. What the Phish! Effects of AI on Phishing Attacks and Defense. TAMU Cybersecur. J. 2025, 27, 45–62. [CrossRef]

15. Heiding, F.; Lermen, S.; Kao, A.; Schneier, B.; Vishwanath, A. Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects. arXiv 2024, arXiv:2412.00586. [CrossRef]

16. Chen, F.; Wu, T.; Nguyen, V.; Wang, S.; Hu, H.; Abuadbba, A.; Rudolph, C. Adapting to Cyber Threats: A Phishing Evolution Network (PEN) Framework for Phishing Generation and Analyzing Evolution Patterns using Large Language Models. arXiv 2024, arXiv:2411.11389. [CrossRef]

17. Aljeaid, D.; Alzhrani, A.; Alrougi, M.; Almalki, O. Assessment of End-User Susceptibility to Cybersecurity Threats in Saudi Arabia by Simulating Phishing Attacks. Information 2020, 11, 547. [CrossRef]

18. Chatchalermpun, S.; Wuttidittachotti, P.; Daengsi, T. Cybersecurity Drill Test Using Phishing Attack: A Pilot Study of a Large Financial Services Firm in Thailand. In Proceedings of the 2020 IEEE 10th Symposium on Computer Applications & Industrial Electronics (ISCAIE), Penang, Malaysia, 18–19 April 2020; pp. 283–286. [CrossRef]

19. Bayl-Smith, P.; Taib, R.; Yu, K.; Wiggins, M. Response to a Phishing Attack: Persuasion and Protection Motivation in an Organizational Context. Inf. Comput. Secur. 2021, 30, 63–78. [CrossRef]

20. Kudalkar, M.; Singh, J.; Singh, S. Exploring Phishing Awareness and User Behavior: A Survey-Based Investigation. Int. J. Res. Appl. Sci. Eng. Technol. 2024, 12, 4713–4718. [CrossRef]

21. Cranford, E.A.; Lebiere, C.; Rajivan, P.; Aggarwal, P.; Gonzalez, C. Modeling Cognitive Dynamics in End-User Response to Phishing Emails. In Proceedings of the 17th Annual Meeting of the International Conference on Cognitive Modelling, Montreal, QC, Canada, 19–22 July 2019; pp. 35–40.

22. Vishwanath, A. Blunting the Phisher's Spear: A Risk-Based Approach for Defining User Training and Awarding Administrative Privileges. In Black Hat USA 2016; Black Hat: Las Vegas, NV, USA, 2016. Available online: https://www.blackhat.com/docs/us-16/materials/us-16-Vishwanath-Blunting-The-Phishers-Spear-A-Risk-Based-ApproachFor-Defining-User-Training-And-Awarding-Administrative-Privileges-wp.pdf (accessed on 6 June 2025).

23. Scherb, C.; Heitz, L.B.; Grimberg, F.; Grieder, H.; Maurer, M. A Cyber Attack Simulation for Teaching Cybersecurity. Epic. Ser. Comput. 2023, 93, 129–140. [CrossRef]

24. Jansson, K.; von Solms, R. Phishing for Phishing Awareness. Behav. Inf. Technol. 2013, 32, 584–593. [CrossRef]