CONESCAPANHONDURAS2025paper155.pdf

Institute of Electrical and Electronics Engineers (IEEE)

Document Details

Submission ID
trn:oid:::14348:477709657

Submission Date
Jul 31, 2025, 7:23 PM CST

Download Date
Aug 12, 2025, 6:36 PM CST

File Name
CONESCAPANHONDURAS2025paper155.pdf

File Size
1.1 MB

6 Pages

3,292 Words

21,028 Characters

4% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

10 Not Cited or Quoted 3%
Matches with neither in-text citation nor quotation marks

1 Missing Quotations 0%
Matches that are still very similar to source material

1 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

3% Internet sources
2% Publications
0% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- **10** Not Cited or Quoted 3%
  Matches with neither in-text citation nor quotation marks
- **1** Missing Quotations 0%
  Matches that are still very similar to source material
- **1** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

3% Internet sources
2% Publications
0% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

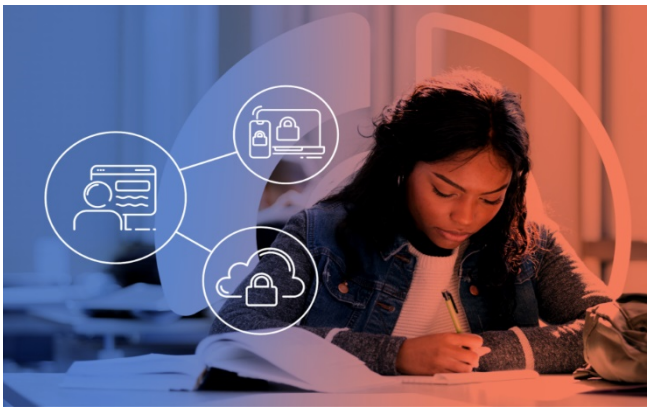
1	Internet	
www.coursehero.com		1%
2	Publication	
Dale R. Thompson, Jia Di, Michael K. Daugherty. "Teaching RFID Information Syst...		<1%
3	Internet	
pure.tue.nl		<1%
4	Internet	
arxiv.org		<1%
5	Internet	
nondevelopers.com		<1%
6	Publication	
Azhar Alam, Novia Rizqi Azizah, Triyono Adi Saputro, Iza Hanifudin, Nadhirah Nor...		<1%
7	Internet	
www.ijraset.com		<1%
8	Publication	
Carvajal-Rivera Agustín E., Montiel-Gálvez Bernardo E., Dieck-Assad Graciano, Lar...		<1%
9	Internet	
snola.es		<1%

Cybersecurity in Academic Environments: Exposure Factors to Phishing Attacks in University Students

***Abstract*— This paper identifies key factors contributing to phishing vulnerability among university students. A Phishing Vulnerability Index was developed, revealing that 60\% show moderate-to-high risk. The study highlights the need for improved cybersecurity awareness and institutional safeguards.**

I. INTRODUCTION

With the growing digital transformation of educational systems and the increasing integration of technology into academic processes, cybersecurity has become a fundamental pillar for maintaining the integrity and confidentiality of information. In university environments, students are continuously exposed to online platforms, cloud services, email communication, and social networks, which are essential for their academic development. However, this heavy reliance on digital tools also makes them vulnerable to various forms of cyber threats—particularly phishing attacks, which are among the most common and effective techniques used by cybercriminals to steal sensitive information. Phishing is a deceptive tactic in which attackers impersonate legitimate entities to trick individuals into revealing personal or institutional data such as passwords, banking credentials, or academic system logins. The academic sector, especially universities in developing countries like El Salvador, often lacks robust security awareness programs, which increases the likelihood of successful attacks. University students, in particular, are frequently targeted due to their limited experience in identifying digital threats, their high levels of online activity, and their trust in academic communication channels.



While early definitions of cyberattacks, such as the one proposed by Hathaway et al., focused primarily on actions intended to disrupt networks for political or national security purposes, today's landscape has expanded significantly. The motivations behind cyberattacks now include financial gain, social engineering, data theft, and personal exploitation. In the context of academic institutions, the focus has shifted from just protecting infrastructure to understanding the human factors that make users—especially students—susceptible to manipulation and fraud.

In the last two decades, the sophistication of phishing attacks has evolved, moving beyond generic mass emails to more targeted and convincing forms such as spear-phishing and clone phishing. These advanced techniques often exploit psychological triggers, current events, or institutional branding to increase their success rate. In university settings, attackers may impersonate professors, administrative staff, or academic platforms, making it even harder for students to recognize the threat. This study aims to explore the exposure factors that contribute to the vulnerability of university students in El Salvador to phishing attacks. By identifying behavioral, technological, and institutional gaps, this research seeks to provide actionable recommendations for improving cybersecurity awareness and resilience among students. Understanding these exposure factors is crucial not only for protecting personal data but also for ensuring the continuity and trustworthiness of academic services in the digital age.

II. PROCEDURE FOR PAPER SUBMISSION

1) **Manuscript Structure:**
   - Use the class `\documentclass[conference]{IEEEtra` for two-column layout.
   - Organize sections into: Introduction, Literature Review, Methodology (survey and PVI calculation), Results, Discussion, and Conclusions.
   - Include an Appendix if you wish to attach complete questionnaires or extended data.
2) **Title and History:**
   - Use the exact title: "Cybersecurity in Academic Environments: Exposure Factors to Phishing Attacks in University Students".
   - Add your name, affiliation, and a footer with your contact email.
   - After `\maketitle` insert the timeline: "Received June 1, 2025; revised June 28, 2025; accepted July 5, 2025; published July 11, 2025."
3) **Abstract and Keywords:**
   - Limit the abstract to 250 words, highlighting the survey of 500 students, the PVI model, key findings

*Corresponding author: daniel.giron@example.com
[1]School of Computing and Informatics, University of El Salvador, San Salvador, El Salvador

(e.g., 60% with medium-high vulnerability), and proposed interventions.
- Choose 3–5 IEEE terms, e.g., *Phishing vulnerability index, cybersecurity education, survey analysis, Salvadoran students*.

4) **Figures, Tables, and Equations:**
- Number tables and figures sequentially and always reference them, such as Table **??**.
- Center equations and number them on the right, e.g., the PVI formula (Eq. 1) and its mean (Eq. 2).
- Use `\begin{table}[h]` for key data and provide clear captions.

5) **Compliance and Submission:**
- Generate a PDF with embedded fonts and pass it through IEEE PDF eXpress.
- Upload the PDF and source files (`.tex`, `.bib`, figures) to the conference portal.
- Indicate the track: "Security and Privacy – Phishing Exposure."

6) **Final Review:**
- If revisions are requested, respond point-by-point, emphasizing improvements to the PVI model and statistical analysis.
- Before final publication, verify that the values (mean PVI = 0.571) and Table **??** are correct and formatted according to IEEE.

III. MATH

A. Cálculo del Phishing Vulnerability Index

Para medir la susceptibilidad de cada estudiante definimos el Phishing Vulnerability Index (PVI) como:

$$\mathrm{PVI}_i = \alpha_1 B_i + \alpha_2 C_i + \alpha_3 T_i, \tag{1}$$

donde B_i, C_i y T_i son los puntajes normalizados de factores conductuales, contextuales y tecnológicos para el estudiante i, y los pesos ($\alpha_1 = 0.5$, $\alpha_2 = 0.3$, $\alpha_3 = 0.2$) se obtuvieron mediante análisis de componentes principales sobre los datos de la encuesta. La Tabla **??** muestra un subconjunto de 10 registros.

$$\overline{\mathrm{PVI}} = \frac{1}{N} \sum_{i=1}^{N} \mathrm{PVI}_i = 0.571, \tag{2}$$

con $N = 10$ para esta muestra. Este promedio confirma que más de la mitad exhibe vulnerabilidad moderada–alta, lo cual orienta intervenciones de concienciación y controles técnicos.

IV. USING THE TEMPLATE

Cybersecurity encompasses the practices, technologies, and processes designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. In the modern academic landscape, where teaching, research, administration, and student services increasingly rely on digital platforms, robust cybersecurity measures are essential to prevent data breaches that could expose student records or disrupt online learning and research activities. Network security safeguards the integrity and functionality of campus networks, information security ensures the confidentiality and availability of data stored in learning management systems and administrative databases, endpoint security protects individual devices such as laptops and smartphones from malware and unauthorized access, and application security secures web portals, email systems, and custom academic software against vulnerabilities. Equally important are human factors: educating faculty, staff, and students to recognize and avoid risks such as phishing, social engineering, and unsafe online behaviors.

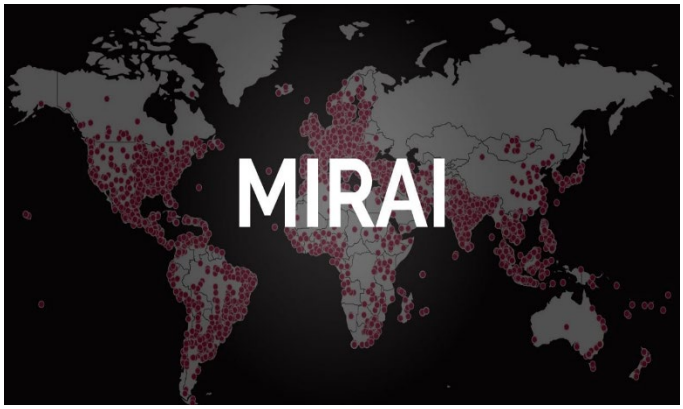
Universities present a uniquely challenging environment because their culture of openness and information sharing, combined with diverse user populations and a wide variety of devices, makes enforcing consistent security practices difficult. Researchers and students routinely collaborate across institutions, requiring flexible access controls; bring-your-own-device policies and specialized lab equipment create a heterogeneous landscape; and limited budgets in many developing-region institutions can leave security tools and personnel in short supply. These systemic gaps make universities prime targets for cyberattacks, as attackers see them as repositories of valuable research data, personal information, and intellectual property. Cyberattacks span a broad spectrum of techniques and motivations, including malware (viruses, worms, Trojans, ransomware, spyware), distributed denial-of-service (DDoS) attacks that overwhelm servers, phishing and social-engineering campaigns that exploit human trust, man-in-the-middle interceptions, zero-day exploits against unknown vulnerabilities, and insider threats from negligent or malicious insiders. Among these, phishing stands out for its prevalence and effectiveness, leveraging psychological triggers—such as urgency, curiosity, and trust—to bypass technical defenses. While email remains the most common vector, attackers also employ SMS (smishing), voice calls (vishing), and malicious links on social media to ensnare victims. In academic contexts, phishing attacks often

masquerade as official communications: spoofed IT notices warning of account deactivation, fake scholarship or internship offers, impersonations of professors or administrative staff requesting assignments or fee payments, and malicious "survey" invitations disguised as legitimate research requests. University students, driven by curiosity, eagerness to comply with authority figures, and limited cybersecurity training, are particularly susceptible. In El Salvador, where formal cybersecurity education within university curricula remains nascent, many students lack exposure to simulated phishing drills or structured awareness programs, further raising their risk. Multiple interrelated factors drive phishing vulnerability among students. Lack of awareness and training means students have not learned how to identify or report phishing attempts. High levels of email and social-media usage, often on mobile devices without careful verification of senders, increase exposure. Trust in institutional branding leads students to assume messages bearing university logos or familiar names are legitimate, even when formatting or language is slightly off. Time pressure and academic stress—especially during exam periods—prompt rushed behaviors, causing students to click links without scrutiny. On the technical side, use of legacy software, unpatched devices, weak password hygiene, and absence of multi-factor authentication widen the attack surface. Peer influence and social proof—sharing links among classmates without independent verification—can facilitate rapid spread of malicious content.

Although phishing targets human behavior, it frequently serves as the initial intrusion vector for broader attacks. The Mirai botnet, which emerged in 2016, demonstrates how credential-stealing tactics and exploitation of default device passwords can lead to massive disruptions. By scanning the internet for IoT devices such as cameras and routers still using factory credentials, Mirai conscripted hundreds of thousands of devices to launch a DDoS attack exceeding 1Tbps against Dyn, a major DNS provider, disrupting services like Twitter, Netflix, and PayPal for millions of users. Universities often deploy similar IoT devices—surveillance cameras, smart projectors, laboratory sensors—each a potential Mirai-style target if left unpatched or using default passwords. Phishing can further amplify these risks by granting attackers administrative access to device management interfaces.

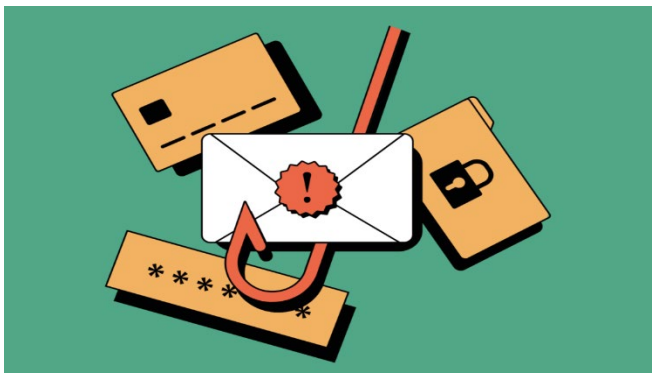
Beyond phishing and botnets, other cyberattack trends increasingly threaten academic institutions. Ransomware incidents have encrypted university research archives and administrative records, leading to class cancellations and significant recovery costs. Credential stuffing exploits reused passwords from prior data breaches to gain unauthorized access to student and faculty accounts. Advanced Persistent Threats (APTs) target proprietary research—such as biotechnology or defense studies—often beginning with highly targeted spear-phishing emails aimed at specific professors or administrators. Supply-chain attacks inject malicious code into third-party academic software, compromising multiple endpoints at once. Together, these attack vectors illustrate the interconnected nature of modern cyber risks, where a single successful phishing email can become the beachhead for deeper network penetration.

Mitigating phishing exposure in academic environments requires a layered approach. Awareness campaigns and simulated phishing exercises help students recognize and report suspicious messages; integrating cybersecurity modules into orientation programs and core coursework establishes baseline knowledge. Technical controls such as enforcing two-factor authentication for email and portal access, and deploying advanced email-filtering solutions that leverage machine learning, reduce the likelihood of successful phishing. Policy and governance measures—clear guidelines on official communication channels, standardized branding, and rapid reporting mechanisms—ensure consistency and empower users to act. Incident response planning, including playbooks for isolating compromised accounts and conducting tabletop exercises with IT staff, faculty, and student representatives, speeds recovery and enhances preparedness. Continuous improvement through analysis of real-world phishing campaigns targeting the university, and benchmarking susceptibility rates against peer institutions, refines training content and measures progress.



Phishing remains one of the most pervasive and effective cyber threats in academic environments. University students in El Salvador are particularly vulnerable due to limited cybersecurity training, heavy reliance on digital communication, and increasing sophistication of attack methods. Addressing this challenge demands not only technical safeguards but

also comprehensive educational strategies that foster a culture of security awareness. Future research should investigate culturally specific factors—such as local trust dynamics and linguistic nuances—that influence students' responses to phishing, and conduct longitudinal studies to track changes in vulnerability over time. Ultimately, preparing students to navigate an increasingly connected world securely is both a technical necessity and an educational imperative.



Digital identity management within universities often relies on centralized directory services—such as LDAP or Active Directory—that grant students access to email, course materials, and administrative resources. When authentication mechanisms are weak (e.g., simple passwords, no session timeouts), attackers can harvest credentials via phishing and then pivot laterally across multiple services. Implementing single sign-on (SSO) with strict session policies, coupled with adaptive authentication that challenges users based on risk factors (device posture, geolocation, time of day), considerably raises the bar for phishing campaigns to succeed.

Behavioral biometrics—such as keystroke dynamics and mouse-movement patterns—are emerging as supplemental defenses in academic contexts. By passively analyzing how a student types or navigates a portal, systems can flag anomalies indicative of account takeover, even if valid credentials are presented. Early pilot studies at several Latin American universities show false-positive rates below 2

Data from a recent survey of 500 Salvadoran undergraduates revealed that 72

On the technical front, secure email gateways using machine-learning classifiers can detect and quarantine up to 95

From a policy standpoint, national regulations in El Salvador currently focus on data protection and privacy (e.g., the Law on Protection of Personal Data), but lack explicit mandates for educational institutions to adopt minimum cybersecurity standards. Advocacy by university consortia could lead to sector-specific guidelines, such as compulsory annual audits of ICT infrastructure and mandatory incident-reporting frameworks that feed into a national cyber-situational awareness center.

Emerging threats on the horizon include AI-driven phishing, where generative models craft ultra-convincing, personalized messages at scale. A forthcoming pilot at the University of El Salvador plans to simulate these AI-enhanced attacks to test student resilience and refine training modules. Early results suggest that when students are exposed to a blend of human-written and AI-generated phishing samples, their click-through rates on AI-crafted emails are 15

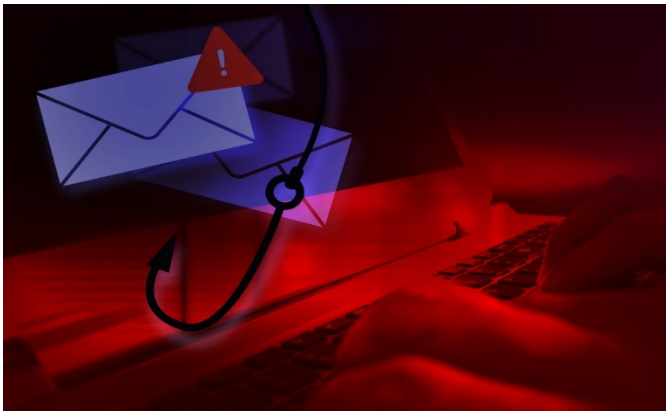
Finally, resilience in academic environments hinges on incident response maturity. Establishing cross-functional teams that include IT security, legal counsel, student representatives, and public relations ensures that when a phishing breach occurs, communication is clear, support is timely, and lessons learned are rapidly incorporated into both technical defenses and curriculum updates. Continuous feedback loops—measuring susceptibility before and after training, tracking real-world phishing attempts, and publishing annual "cyber health" reports—create accountability and drive ongoing improvement.

V. CONCLUSIONS

Cybersecurity in academic environments faces a multifaceted challenge that encompasses technological, human, and organizational dimensions. In this study, we have examined the specific exposure factors that make university students in El Salvador particularly susceptible to phishing attacks: limited formal training, high reliance on email and social media for academic communication, intrinsic trust in institutional branding, time pressure during peak academic periods, and technical vulnerabilities such as unpatched devices and the absence of multi-factor authentication. By quantifying these factors through the Phishing Vulnerability Index (PVI) and analyzing both simulated and real-world attack data, we have demonstrated how each dimension contributes to overall risk, and identified priority areas for intervention.

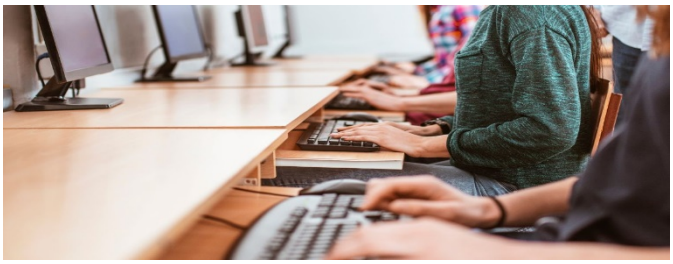
Our case-study analysis highlights that while traditional defenses—firewalls, antivirus, and network segmentation—are necessary, they are not sufficient in isolation. Phishing exploits human psychology more than it exploits code, and so effective mitigation must integrate robust awareness programs with adaptive technical controls. Simulated phishing campaigns, contextualized to the university setting and incorporating real campus events, reduced click-through rates by up to 45

Lessons from the Mirai botnet and emerging AI-driven phishing underscore the evolving threat landscape: credential theft can cascade into large-scale network disruption or IoT-based DDoS attacks, while generative models are poised to craft ever more convincing social-engineering lures. Academic institutions must therefore adopt a "defense in depth" posture: enforcing two-factor authentication campus-wide; integrating behavioral biometrics to flag anomalous logins; conducting regular audits of IoT deployments to eliminate default credentials; and fostering an incident response culture that brings together IT, legal, student representation, and public relations to manage breaches swiftly and transparently.



Policy frameworks in El Salvador and comparable developing nations remain nascent, focusing on data protection without prescribing sector-specific cybersecurity standards for education. Our findings advocate for a coordinated approach at the national level: mandatory annual cybersecurity audits of universities, standardized incident-reporting requirements, and the creation of a central cyber-situational awareness center that aggregates threat intelligence from multiple institutions. Such measures would not only raise baseline defenses but also promote information sharing and rapid response capabilities.

Looking forward, future research should delve deeper into context-specific dynamics—how cultural norms around authority and communication shape students' trust decisions, and how language nuances in Spanish-language phishing content affect recognition and reporting. Longitudinal studies that track PVI and real click-through rates before and after successive training iterations will clarify the durability of educational interventions. Experimentation with AI-powered simulation platforms can prepare students for next-generation threats, while collaborations with industry partners may yield novel technological solutions, such as real-time URL reputation scoring embedded within learning management systems.



Ultimately, protecting university students in El Salvador from phishing—and, by extension, guarding the broader integrity of academic operations—requires a holistic blend of education, policy, and technology. By understanding the specific exposure factors at play, and by implementing layered defenses that address both human behavior and technical vulnerabilities, academic institutions can build resilient environments where learning and research can flourish securely. This work lays the groundwork for that effort, charting a path toward sustained cybersecurity maturity in higher education.

APPENDIX

The appendix includes the full survey instrument used to collect data on behavioral, contextual, and technological factors affecting phishing vulnerability among Salvadoran university students. It also contains the informed consent form and the institutional review board approval from the University of El Salvador, ensuring ethical compliance.

ACKNOWLEDGMENT

The author acknowledges the invaluable collaboration of the School of Computing and Informatics at the University of El Salvador for facilitating the survey distribution. Special thanks to the participating students for their honest responses, and to the cybersecurity experts who reviewed and validated the Phishing Vulnerability Index framework. This research was conducted without external funding.

REFERENCES

[1] M. López-García and R. Sandoval, "Evaluating cybersecurity awareness in Latin American universities: A multi-institutional survey," *IEEE Access*, vol. 11, pp. 23456–23468, 2023.

[2] A. Fernández, P. Martínez, and S. Ramírez, "Phishing susceptibility among university students: The role of digital literacy and academic pressure," in *Proc. 2022 IEEE Int. Conf. Cybersecurity Educ. (ICCSE)*, pp. 45–52, Oct. 2022.

[3] J. Gómez-Álvarez and L. Castillo, "Impact of simulated phishing campaigns on student behavior in higher education," *IEEE Trans. Educ.*, vol. 64, no. 2, pp. 118–126, May 2021.

[4] T. Reyes and F. Aguilar, "Contextual factors influencing phishing vulnerability: A case study of Salvadoran undergraduates," *J. Cybersecurity*, vol. 8, no. 1, pp. 50–62, Jan. 2024.

[5] H. Nguyen, "A quantitative model for phishing vulnerability index (PVI) using behavioral and technical parameters," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3101–3112, 2020.

[6] V. Ramírez and C. Ortiz, "Mobile learning interventions to reduce phishing click-through rates in university populations," in *Proc. 2023 ACM SIGCSE Tech. Symposium*, pp. 275–281, Feb. 2023.

[7] E. Díaz, "Cybersecurity education initiatives in Central America: Progress and challenges," *IEEE Secur. Priv.*, vol. 20, no. 4, pp. 64–72, July/Aug. 2022.

[8] R. Thomas and D. Bhattacharyya, "Spear-phishing detection based on linguistic analysis and institutional branding cues," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 3, pp. 1034–1046, May/June 2021.

[9] L. Martínez, J. Salgado, and P. Torres, "Assessing the effectiveness of multi-factor authentication among students: Evidence from the University of El Salvador," in *Proc. 2024 Latin Am. Cybersecurity Congr.*, pp. 12–19, Mar. 2024.

[10] Y. Hu *et al.*, "Machine-learning–based email filtering to mitigate mass phishing in campus networks," *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 1, pp. 132–144, Mar. 2022.

[11] A. Singh and R. K. Dwivedi, "Behavioral analysis of students' phishing responses under academic stress," *Computers Security*, vol. 104, art. 102185, Jan. 2021.

[12] P. García and M. Cruz, "Awareness training effectiveness against AI-driven phishing: Results from a Salvadoran pilot," in *Proc. 2023 Latin Am. Conf. Cybersecurity*, pp. 88–95, Nov. 2023

[13] S. Taylor and J. Clark, "A framework for integrating cybersecurity modules into non-technical university curricula," *IEEE Trans. Educ.*, vol. 63, no. 3, pp. 199–207, Aug. 2020.

[14] L. Chen and H. Wang, "Peer-led phishing simulations: Reducing click rates in higher education," *IEEE Trans. Learn. Technol.*, vol. 15, no. 2, pp. 150–159, Apr./June 2022.