A Controlled Phishing Attack in a University Community: A Case Study

Diego Esteban Díaz Vivas¹, William Yecid Gutierrez Pena², Sandra Patricia Cristancho Botero³, and Alix E. Rojas^{4*}

¹Universidad Ean, Facultad De Ingeniería, Bogotá, Colombia. ddiazvi29075@universidadean.edu.co, https://orcid.org/0009-0006-4380-6495

²Universidad Ean, Facultad De Ingeniería, Bogotá, Colombia. wgutier59555@universidadean.edu.co, https://orcid.org/0009-0001-1075-3239

³Universidad Ean, Facultad De Ingeniería, Bogotá, Colombia. spcristancho@universidadean.edu.co, https://orcid.org/0000-0002-4555-9065

^{4*}Universidad Ean, Facultad De Ingeniería, Bogotá, Colombia. aerojash@universidadean.edu.co, https://orcid.org/0000-0002-0371-3925

Received: December 21, 2023; Revised: February 09, 2024; Accepted: March 09, 2024; Published: May 30, 2024

Abstract

Nowadays, in the contemporary digital landscape, cybersecurity plays a vital role in safeguarding digital assets and mitigating the risks posed by an interconnected world. Personal, business, and government information is constantly collected and shared online. Data, financial records, intellectual property, and government secrets can be exploited maliciously without proper protection. Cyberattacks come in various forms, and their effectiveness can change over time as attackers develop new techniques and targets. However, phishing attacks have become a pervasive and persistent cybersecurity concern. Their success largely depends on the vulnerability of individuals within an organization.

This case study dwells on the pivotal role of controlled phishing attacks as educational and assessment tools within the cybersecurity paradigm. At its core, we conducted a simulation with the consent of the organization's leadership to emulate a real-world phishing scenario within the university community. This allowed us to measure people's susceptibility, identify security weaknesses, and raise security awareness. With phishing attacks becoming increasingly sophisticated, understanding their impact in an academic setting offers valuable insights into broader cybersecurity. The project aimed to familiarize the university community with the risks of information theft perpetrated through email-based attacks.

Keywords: Phishing, Cybersecurity, Ethical Hacking, Information Security, Social Engineering.

1 Introduction

Cybersecurity encompasses practices intended to protect computer systems, networks, devices, and data from cyber threats, including theft, damage, and unauthorized access. As society evolves into an ever-

Journal of Internet Services and Information Security (JISIS), volume: 14, number: 2 (May), pp. 98-110. DOI: 10.58346/JISIS.2024.12.007

^{*}Corresponding author: Universidad Ean, Facultad De Ingeniería, Bogotá, Colombia.

digital world, cyber threats become increasingly sophisticated, demanding constant adaptation of cybersecurity strategies by organizations and individuals. The above may involve proactive measures, such as implementing recognized standards like ISO 27001 (Fonseca-Herrera et al., 2021) or adopting secure coding practices within organizations, as proposed by (Nivia et al., 2018). Despite advancements in cybersecurity measures, certain attack methods remain highly potent and harmful adversaries. One such attack, phishing, has proven to be particularly successful in exploiting human vulnerabilities, highlighting the need for a deeper understanding of its mechanisms and strategies.

Phishing involves sending deceptive messages to trick individuals into revealing sensitive information. Phishing attacks have evolved in complexity and sophistication over the past decade, presenting significant challenges to cybersecurity professionals and organizations worldwide. Studies have shed light on specific phishing techniques and their implications for security measures; for instance, (Taib et al., 2019) explored the role of social engineering in phishing attacks, emphasizing attackers' manipulation of human psychology to deceive victims. Similarly, (Aslan et al., 2023) investigated the effectiveness of multi-factor authentication in mitigating phishing threats, highlighting the importance of additional security layers. Additionally, (Purkait, 2012; Arora, 2024) examined the persistence of phishing threats in organizational environments, emphasizing the need for robust cybersecurity measures (Caviglione et al., 2021).

One preventive strategy for phishing attacks is ethical hacking, also known as penetration testing or white-hat hacking, where authorized individuals deliberately identify and exploit vulnerabilities in digital assets (Aldawood & Skinner, 2019). Since ethical hacking provides hands-on experience in techniques and tools to carry out computer attacks, the cybersecurity research hotbed at Universidad Ean proposed a project to assess the security posture of the university community by simulating a potential phishing attack. With permission and cooperation from the university's IT department, the project aimed to identify and remediate security weaknesses before malicious actors could exploit them. This proactive approach to cybersecurity provided valuable insights into cyber threats and effective defense strategies (Mahendiren & Kushwaha, 2023).

The subsequent sections show the development and implications of a controlled phishing attack within a specific university community. We begin by reviewing research-related work and contextualizing phishing within the approach of ethical hacking. Next, we outline the methodology behind the controlled phishing attack, detailing its planning, execution, and educational insights. We then present the results of the attack, analyzing and discussing data, trends, and vulnerabilities identified within the university community. Finally, we draw conclusions based on our research, emphasizing the importance of controlled phishing attacks in enhancing cybersecurity awareness and resilience against evolving threats.

2 Related Work

Phishing is a prevalent cyberattack in which attackers use deceptive tactics to trick individuals into divulging sensitive information, such as login credentials, personal details, or financial data (Sreenivasulu, 2024). This type of cyberattack come in various forms, each with a specific approach and goal, continue to evolve in sophistication, exploiting human vulnerabilities and leveraging advanced tactics to deceive individuals and organizations (Hijji & Alam, 2021). Social engineering, a key component of many phishing attacks, plays on psychological triggers to manipulate victims into divulging sensitive information or performing actions that compromise their security. (Syafitri et al., 2022; Gupta et al., 2014; Kashif, 2019) elucidated the role of social engineering in phishing attacks, highlighting how attackers craft convincing narratives and pretext scenarios to deceive victims.

Cybercriminals create a sense of urgency or trust that prompts victims to disclose confidential information or click on malicious links by impersonating trusted entities or exploiting emotional appeals (Veksler et al., 2020; Pinto et al., 2022; Fan et al., 2023).

Email phishing is the most widespread form of phishing and involves cybercriminals sending deceptive emails to a wide audience, impersonating trusted entities such as banks, government agencies, or reputable companies (Mujtaba et al., 2017; Sundararaj & Kul, 2021). These emails are often crafted meticulously, mimicking legitimate organizations' visual design and language. The primary goal of email phishing is to trick recipients into clicking on the provided links, which leads to fake login pages where they are prompted to enter sensitive information, including usernames, passwords, credit card details, or Social Security numbers. As authors indicate (Fette et al., 2007), attackers also commonly use attachments in phishing emails to deliver malware to the victim's device, leading to data theft, ransomware infections, or further compromise of the victim's system.

Vishing, short for "voice phishing," is a form of phishing over phone calls. Attackers impersonate trusted entities, such as banks, government agencies, or IT support, and call individuals, often with a sense of urgency or alarm. The attacker may use caller ID spoofing to make it appear that the call is coming from a legitimate source (Gupta et al., 2016). During the call, the attacker attempts to extract sensitive information, such as Social Security numbers, credit card details, or login credentials, by posing as a trusted authority figure or providing fabricated reasons for needing the information urgently.

Vishing attacks aim to exploit the trust individuals often place in telephone communications, making them particularly effective in convincing victims to divulge sensitive information (Jagatic et al., 2007). Common vishing scenarios include fake IRS agents demanding immediate tax payments, technical support scams claiming computer issues, or financial institutions requesting verification of account details. To protect against vishing, individuals should exercise caution when receiving unsolicited phone calls, especially those requesting sensitive information. Verifying the caller's identity independently and sharing sensitive information over the phone with proper validation is crucial in thwarting vishing attempts. Additionally, (Bubukayr & Almaiah, 2021) warn that organizations can instruct employees about vishing threats and implement call verification procedures to enhance security.

Smishing, or SMS phishing, is a phishing variant that relies on text messages to deceive recipients (Time, 2023). Attackers send fraudulent text messages that appear to be from legitimate sources, such as banks, delivery services, or government agencies (Timko & Rahman, 2023). These messages often contain urgent or enticing information, such as claims of winning a prize, missed package deliveries, or security alerts designed to prompt recipients to take immediate action. Smishing messages may contain links to fake websites or ask recipients to reply with sensitive information.



Figure 1: Popular SMS Phishing attack in Colombia

Due to the prevalence of text messaging and its immediacy, smishing can be highly effective. Recipients who click on the provided links may be directed to counterfeit websites where they are prompted to enter personal or financial data (Anderson & Moore, 2006). In some cases, smishing messages may attempt to install malware on the recipient's device. Protecting against smishing requires individuals to be cautious when receiving unsolicited text messages, especially those that request personal or financial information. Verifying the sender's legitimacy and refraining from clicking on links or providing information through text messages is essential in mitigating smishing risks (Ferreira et al., 2015).



Figure 1 shows a popular attack of this type, which sends the message "Dear customer 472 informs that your package is ready for delivery CO-62823. Pay your tax to receive https://impuesto472.com". Victims clicked the URL and loaded a credible page of the 4-72 website, the official postal company of Colombia. The web form collected credit card data to pay a small amount that supposedly would cover taxes; in dollars, it would be in the range of \$1 to \$4. According to IBM X-Force², hackers in Latin America have increasingly adopted the strategy of accessing legal accounts rather than hacking corporate networks because it presented more favorable prospects. As reported by IBM, Colombia ranked second in the number of cyberattacks among regional countries in 2023.

Furthermore, multi-vector phishing attacks have emerged as a potent threat, combining multiple attack vectors to enhance their effectiveness and evade detection. (Taib et al., 2019) mention the complexities of multi-vector phishing attacks, which may involve a combination of email, SMS, or voice-based communication channels. These attacks leverage a diverse range of tactics, such as domain spoofing, pretexting, and spear-phishing, to tailor messages to specific targets and increase the likelihood of success. Cybercriminals can bypass traditional security defenses and maximize their impact on unsuspecting victims by exploiting multiple entry points and communication channels.

In similar studies, the authors (Desolda et al., 2021) offer empirical evidence regarding the success of malicious strategies in deceiving general users. Through a usability study analyzing various phishing attacks, this research highlights the critical role of user behavior in phishing susceptibility. Notably, the finding that many participants failed to scrutinize browser-based cues, leading to incorrect choices, underscores the importance of security awareness. Another study sheds light on the tactics employed by phishers, a subset of malicious actors engaging in fraudulent activities aimed at acquiring sensitive information (Syafitri et al., 2022). In the survey conducted by Gartner Group provides a glimpse into the success rate of such attacks, revealing that a substantial portion of victims had clicked on phishing links or divulged personal and financial information. Fatima et al., (2019) investigated the effectiveness of anti-phishing measures in mitigating credential harvesting attacks, emphasizing the importance of proactive detection and response strategies. These attacks typically involve the creation of fake login

² The offensive and defensive security services area of IBM Consulting https://exchange.xforce.ibmcloud.com

pages or deceptive forms designed to trick users into entering their usernames and passwords. By masquerading as legitimate websites or services, cybercriminals can harvest a wealth of valuable credentials, enabling unauthorized access to sensitive accounts and data.

3 Methodology

This ethical hacking experiment aimed to conduct good security awareness training to orient community members to the dangers of phishing and other social engineering attacks. The objective of this study was to conduct a controlled phishing attack within a university community, focusing on a pretext related to COVID-19 vaccination, to assess the susceptibility of university community members to phishing attacks, and to evaluate the effectiveness of existing cybersecurity awareness measures (Alawida et al., 2022). To achieve this objective, the study aimed to simulate a phishing campaign targeting university students, faculty, and staff, with the goal of gathering personal information and user credentials under the guise of updating personal data for the COVID-19 vaccine. By conducting a controlled phishing attack in this context, the study sought to uncover insights into the response patterns of university community members to phishing attacks and identify opportunities for enhancing cybersecurity awareness and prevention efforts within the university community (Pinto et al., 2022).



Figure 2: Pipeline for security awareness training

The methodology involves several steps to execute the controlled phishing attack, as illustrated in the Chevron process (Figure 2). Once the objective of the hacking is defined and the ethical guidelines are established and approved, the next technical phases begin. Thus, phishing emails should be crafted to mimic official communication from the university's heads, specifically for this experiment, informing recipients of a mandatory update requirement for COVID-19 vaccination records. These emails should be developed using a specific tool for this purpose; we chose Gophish in advance because we already had experience with this tool. Next, the phishing emails should be distributed to a sample of university community members via their university email accounts. Although in this type of experiment, participants are not informed in advance about the simulated phishing attack (to ensure the authenticity of their responses), data collection procedures should adhere to ethical guidelines to protect the privacy and well-being of participants and minimize the likelihood that the phishing attack causes harm or distress to individuals.

Throughout the phishing simulation, participants' interactions with the phishing emails should be monitored and recorded, including the number of individuals who clicked on the malicious links, entered sensitive information, and reported suspicious activity. The validity and reliability step includes a dotted arrow toward the previous steps since it is key to ensuring the integrity of the study findings, addressing potential sources of bias or limitations in the study design, and considering factors such as sample size and the realism of the phishing simulation.

Finally, the results of the study should be used to inform cybersecurity education and awareness efforts within the university community, with outputs including class sessions with teachers and students, as depicted in the report and education step. However, acknowledge any limitations or constraints of the methodology, such as the generalizability of findings to other university communities or the potential for participant awareness of the phishing simulation.

1) **Open-source Platform Settings**

The GoPhish software is open-source for conducting simulated phishing attacks and security awareness training. We used it to create and execute a controlled phishing campaign to evaluate the university community's susceptibility to phishing attempts and enhance their awareness of phishing threats.

This software is easy to customize for phishing templates, email content, and landing pages, allowing simulations to be tailored to specific requirements and to emulate evolving phishing tactics (Rodríguez-Corzo et al., 2018). To ensure greater reliability, cloned page certification was employed to present the site as secure. An SSL certificate, a global security standard, was utilized to enable the encrypted transfer of data between browsers and web servers, thereby mitigating the risk of theft and manipulation of confidential information by hackers and identity thieves. Before the execution of the attack, the following stages were completed:

Installation: The initial step entailed accessing the official GoPhish page and selecting the installation button, which directed to a GitHub path housing the GoPhish repository. Depending on the operating system, the appropriate file was chosen, and GoPhish was subsequently installed from the GitHub path onto Ubuntu VPS.

Settings: Following installation, the "nano" command was employed to edit the "config.json" file, incorporating the IP and port of the VPS (the latter being optional). Port "3333" was designated as the default port for GoPhish, and the public IP "159.203.70.255" was inputted into the "admin_server" and "phish_server" attributes of the.json file. Special permissions were then granted to the "gophish" command via the "chmod u+x gophish" command to establish the GoPhish service.

Running. Subsequently, the GoPhish application was executed using the "./gophish" command. The IP address "https://159.203.70.225:3333" was accessed, and upon reaching the GoPhish page, the admin username and password were entered to log in and initiate attack setups.

4 Results

The domain universityean.cf was configured to be displayed in the email address. This domain was then registered on the VPS, and the email template was utilized to craft the campaign. The email notified the university community of the necessity to update their data for the COVID-19 vaccination process. Notably, the attack was designed solely to capture information from victims' email accounts and provide feedback to prevent future scams. The email contained a greeting, a description of the email's purpose, a link for data submission, a note regarding the link's active duration and restrictions, and university logo

and information in the footer. Intentional spelling errors and incorrect wording were included to underscore the educational nature of the exercise and prevent individuals from easily falling victim to deception.

Mass emails were dispatched to the previously selected university community. During the monitoring phase, the cybersecurity team tracked metrics such as recipients' interactions with the email, including clicking on malicious links, entering login credentials, or reporting suspicious emails.



Figure 3: Controlled phishing attack results

Figure 3 shows the two bar charts presented offer a valuable comparison between controlled phishing attack campaigns conducted within a university community, each targeting distinct groups-students in the blue bar chart and administrative workers in green. These charts provide similar insights within these demographic segments, shedding light on the varying levels of susceptibility and incident reporting.

In the student-focused campaign, 8712 phishing emails were sent, yet the engagement levels were relatively lower, with 4740 emails read and 2567 clicks on the links. However, a notable proportion of students fell for the phishing attempt, resulting in 2098 individuals submitting sensitive data, and 92 event reports indicated a degree of vigilance within this demographic. In contrast, the administrative worker campaign reached a smaller, more specific audience with 497 emails sent but showcased a higher proportion of active engagement, with 410 emails read and 258 clicks on links. These findings underscore the need for tailored cybersecurity education and training programs to address the varying susceptibility levels and responses among university community segments, ensuring a holistic approach to effectively mitigating phishing threats.

Actualización de datos para vacunación covid-19	Did you not realize it? Check the irregularities in the message:
covid@universidadean.edu.co Para	Although the message was sent from an account on the university's domain, cybercriminals often mask legitimate email accounts. For this
Apreciado Eanista	reason, it is important to review the body of the message very carefully.
De manera atenta nos permitimos invitarte a participar en la actualización de datos para VACUNACIÓN COVID-19 2021 desde el día de/hoy 27 de mayo y hasta el día 5 de junio de 2021 https://universidadean.cf.80/ndsioiA3/y pasos: Haga díe o pube para seguir vínculo.	 ☑ It had a date mismatch; it said as of today, May 27, and the message was sent on June 1. ☑ It had some spelling errors, a mixture of capital letters and
1. [Ingresa]al siguiente vínculo: [www.universidadean.com/actualizacion] 2. [Diligencie] los campos que allí se solicitan y verifica la [informacion] antes de enviar NOTA IMPORTANTE:	In the same paragraph. ☐ The domain of the University page was misspelled (universidadean.edu.co): the link is also directed to a false page
El enlace será válido durante la vigencia de la convocatoria o hasta que diligencie y envie la inscripción (lo que ocurra primero). Por lo anterior <u>ABSTENGASE de compartir su enlace y no notifique</u>]sobre este correo al servicio médico ni al personal de seguridad y salud en el trabajo.	 managed by the managers of the controlled attack. ☑ It included messages that encouraged not to share the link nor report the event to the responsible processes. Additionally, a final note with
Recuerde que al no diligenciar esta información se puede quedar sin vacuna.	an incentive in exchange for providing information.
[Saludos!	
Universidad Ean	

In the next few days, you will receive an invitation to participate in a webinar on cybersecurity topics you should consider daily. Remember that these events must always be reported to the account segurinfo@universidadean.edu.co.

Figure 4: Email body with annotations to indicate perilous items

Once the attack data was collected and processed, it was reported to university management. Finally, Figure 4 shows the informative email with the phishing attack that was sent, showing clues that made the email suspicious.

5 Discussion and Recommendations

The results of the controlled phishing attack campaigns within the university community offer valuable insights into the multifaceted nature of cybersecurity awareness, susceptibility, and incident reporting among different demographic segments. While much research traditionally focuses on enhancing computer network systems and software development to bolster information security (Kaur & Ramkumar, 2022; Zheng et al., 2022), it is crucial to acknowledge that cyber attackers can exploit vulnerabilities in human behavior. As highlighted (Moustafa et al., 2021), attackers may manipulate the minds of computer system users through social engineering and cognitive hacking techniques, effectively bypassing technical defenses to gain unauthorized access to networks or systems. This underscores the importance of considering the human element in cybersecurity strategies. The similar levels of engagement and response observed among university students and administrative workers in our campaigns emphasize the need for customized cybersecurity education and training initiatives. By addressing the specific vulnerabilities and behaviors of different user groups, organizations can bolster their defenses against phishing attacks and enhance overall cybersecurity resilience.

While technological safeguards are undoubtedly crucial in cybersecurity, it is essential to recognize that human behavior often serves as the linchpin determining the success or failure of cybersecurity measures. As mentioned in previous work (Rodríguez-Corzo et al., 2018), the human factor is frequently the weakest link in the chain of computer security. The campaign within the university community highlighted the profound impact of human behavior on email engagement, susceptibility to phishing attacks, and incident reporting. These findings underscore the critical need for cultivating a cybersecurity-aware culture within organizations as another authors (Arabia-Obedoza et al., 2020). Comprehensive education and training programs are paramount in equipping individuals with the

knowledge and skills necessary to identify and respond effectively to phishing attempts. By addressing the human element in cybersecurity strategies, organizations can bolster their defenses against evolving threats. Furthermore, our results emphasize the importance of tailoring these initiatives to the specific needs and vulnerabilities of different user groups, recognizing that susceptibility levels can vary significantly among various demographics.

In researching simulated phishing attacks within the university community, we recognize and prioritize ethical considerations as fundamental to the integrity of our study. Throughout the design and execution of the phishing simulation, ethical guidelines and participant welfare were paramount. To address concerns about privacy and confidentiality, stringent measures were implemented to safeguard participants' personal information. Data collected during the phishing simulation was anonymized to prevent the identification of individual participants, and strict protocols were followed to ensure the secure storage and handling of sensitive data. By adhering to these principles as other authors recommend (Jones et al., 2015), we aimed to protect participants' privacy rights and maintain the trust and confidence of our university community.

Moreover, we acknowledge the importance of considering the psychological well-being of participants when conducting research involving potentially sensitive or distressing stimuli. While authors such as (Carroll et al., 2022) highlight the enduring and evolving nature of phishing attacks, emphasizing the heightened sense of alertness and nervousness experienced by participants when encountering these threats, your approach also emphasizes the need to minimize any potential harm or discomfort experienced by participants. Specifically, in this study, we outline measures taken to mitigate stress or anxiety induced by the phishing simulation, such as carefully crafting the phishing emails to avoid undue stress and allowing participants to opt out of the study or seek support if needed.

In the era of Industry 4.0, where rapid technological advances and the proliferation of interconnected devices are redefining our digital landscape, opportunities and challenges in cybersecurity continue to evolve. Opportunities arise from the integration of technologies such as the Internet of Things (IoT), artificial intelligence (AI), and blockchain, which improve efficiency, automation, and data-driven decision-making (Agrawal et al., 2022; Piedrahita et al., 2022). However, these technologies also introduce new cybersecurity challenges; for instance, (Bettín-Díaz et al., 2022) show how smart contracts implemented on blockchain offer an interesting spectrum of industrial applications, but their adoption success makes them a valuable target for cybercriminals. In fact, the increased connectivity of IoT devices expands the attack surface, making networks more susceptible to breaches (Ramírez et al., 2022). While AI is a powerful tool for threat detection, cybercriminals can also use it to launch sophisticated attacks (Capuano et al., 2022). Therefore, today, more than ever, building a solid cybersecurity culture within an organization requires more than implementing technical solutions. It involves furthering a mentality of vigilance and responsibility among all members of the community, which will be achieved with continuous training that emphasizes the importance of cybersecurity.

6 Conclusions

As phishing attacks evolve, they incorporate increasingly sophisticated social engineering tactics, making them more challenging to recognize. Consequently, organizations and individuals must implement robust email filtering, educate users about phishing red flags, and promote cautious interaction with any message links and attachments. By acknowledging the evolving challenges and embracing cybersecurity education and awareness initiatives, universities and companies can empower their communities to become resilient against the ever-evolving cyber threats.

The controlled phishing attack made to this community have proven instrumental in helping numerous members of the university community recognize the signs of phishing attempts and acquire the skills to respond effectively. The results of this security exercise underscore the pivotal role of cybersecurity education in mitigating the human factor's vulnerability within computer security systems.

It is essential to recognize that cybersecurity training must be ongoing and adaptable, as people represent the most critical allies in security processes. Furthermore, this training should be integrated with a robust and up-to-date technological infrastructure. The results of controlled attacks should serve as the foundation for strengthening information security.

The dynamic nature of cyber threats demands continuous vigilance and adaptation. As a future direction, research could integrate Industry 4.0 technologies into threat detection. The sheer volume and diversity of IoT devices connected to networks create a vast attack surface, heightening the potential for security breaches. Consequently, exploring cybersecurity issues through a big data focus entails analyzing vast volumes of data, identifying patterns indicative of malicious activities, and proactively mitigating emerging threats in real-time. By doing so, we can bolster our collective resilience to cybersecurity challenges and stay ahead of the curve.

References

- [1] Agrawal, K., Aggarwal, M., Tanwar, S., Sharma, G., Bokoro, P. N., & Sharma, R. (2022). An Extensive Blockchain Based Applications Survey: Tools, Frameworks, Opportunities, Challenges and Solutions. *IEEE Access*, 10, 116858 116906. https://doi.org/10.1109/ACCESS.2022.3219160
- [2] Alawida, M., Omolara, A.E., Abiodun, O.I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University -Computer* and *Information* Sciences, 34(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003
- [3] Aldawood, H., & Skinner, G. (2019). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. *Proceedings of 2018 IEEE International Conference* on Teaching, Assessment, and Learning for Engineering, TALE 2018, 62–68. https://doi.org/10.1109/TALE.2018.8615162
- [4] Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, *314*(5799), 610–613. https://doi.org/10.1126/science.1130992
- [5] Arabia-Obedoza, M.R., Rodriguez, G., Johnston, A., Salahdine, F., & Kaabouch, N. (2020). Social Engineering Attacks A Reconnaissance Synthesis Analysis. 11th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2020, 0843–0848. https://doi.org/10.1109/UEMCON51285.2020.9298100
- [6] Arora, G. (2024). Desing of VLSI Architecture for a flexible testbed of Artificial Neural Network for training and testing on FPGA. *Journal of VLSI Circuits and Systems*, 6(1), 30-35.
- [7] Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics* (*Switzerland*), 12(6), 1333. https://doi.org/10.3390/electronics12061333
- [8] Bettín-Díaz, R., Rojas, A.E., & Mejía-Moncayo, C. (2022). Colombian Origin Coffee Supply Chain Traceability by a Blockchain Implementation. *Operations Research Forum*, *3*(4), 64. https://doi.org/10.1007/s43069-022-00174-4
- [9] Bubukayr, M.A.S., & Almaiah, M.A. (2021). Cybersecurity concerns in smart-phones and applications: A survey. *In international conference on information technology (ICIT)*, 725-731. https://doi.org/10.1109/ICIT52682.2021.9491691

- [10] Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable artificial intelligence in cybersecurity: A survey. *IEEE Access*, 10, 93575-93600. https://doi.org/10.1109/ACCESS.2022.3204171
- [11] Carroll, F., Adejobi, J.A., & Montasari, R. (2022). How good are we at detecting a phishing attack? Investigating the evolving phishing attack email and why it continues to successfully deceive society. SN Computer science, 3(2), 170. https://doi.org/10.1007/s42979-022-01069-1
- [12] Caviglione, L., Wendzel, S., Mileva, A., & Vrhovec, S. (2021). Guest Editorial: Multidisciplinary Solutions to Modern Cybersecurity Challenges. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 12*(4), 1-3.
- [13] Desolda, G., Ferro, L.S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human factors in phishing attacks: a systematic literature review. ACM Computing Surveys (CSUR), 54(8), 1-35. https://doi.org/10.1145/3469886
- [14] Fan, Y., Saeidi, M., Lai, K.K., Yang, J., Cai, X., & Chen, Y. (2023). Corruption and Infrastructure Development Based on Stochastic Analysis. *Arhiv za tehničke nauke*, 1(28), 11-28.
- [15] Fatima, R., Yasin, A., Liu, L., & Wang, J. (2019). How persuasive is a phishing email? A phishing game for phishing awareness. *Journal of Computer Security*, 27(6), 581–612. https://doi.org/10.3233/JCS-181253
- [16] Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. In Human Aspects of Information Security, Privacy, and Trust: Third International Conference, HAS 2015, Held as Part of HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015. Proceedings 3, pp. 36-47. https://doi.org/10.1007/978-3-319-20376-8_4
- [17] Fette, I., Sadeh, N., & Tomasic, A. (2007). Learning to detect phishing emails. In Proceedings of the 16th international conference on World Wide Web, 649-656. https://doi.org/10.1145/1242572.1242660
- [18] Fonseca-Herrera, O.A., Rojas, A.E., & Florez, H. (2021). A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard. *IAENG International Journal of Computer Science*, 48(2), 1–10.
- [19] Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. *In international conference on computing, communication and automation* (*ICCCA*), 537-540. https://doi.org/10.1109/CCAA.2016.7813778
- [20] Gupta, V., Sharma, P., & Gill, H. (2014). Wireless Data Routing with Security Keys. *International Journal of Communication and Computer Technologies (IJCCTS)*, 2(2), 135-138.
- [21] Hijji, M., & Alam, G. (2021). A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions. *IEEE Access*, 9, 7152-7169. https://doi.org/10.1109/ACCESS.2020.3048839
- [22] Jagatic, T.N., Johnson, N.A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, 50(10), 94-100. https://doi.org/10.1145/1290958.1290968
- [23] Jones, H.S., Towse, J.N., & Race, N. (2015). Susceptibility to email fraud: A review of psychological perspectives, data-collection methods, and ethical considerations. *International Journal of Cyber Behavior, Psychology and Learning*, 5(3), 13-29. https://doi.org/10.4018/IJCBPL.2015070102
- [24] Kashif, R. (2019). A Compact Circular Polarized Antenna for Fixed Communication Applications. *National Journal of Antennas and Propagation (NJAP)*, 1(1), 1-4.
- [25] Kaur, J., & Ramkumar, K.R. (2022). The recent trends in cyber security: A review. Journal of King Saud University-Computer and Information Sciences, 34(8), 5766-5781. https://doi.org/10.1016/j.jksuci.2021.01.018
- [26] Mahendiren, D.B., & Kushwaha, B.P. (2023). Impact of Leadership Style and Perceived Organizational Support on the Organizational Citizenship Behaviour of Librarians in Indian Universities. *Indian Journal of Information Sources and Services*, *13*(2), 22–29.

- [27] Moustafa, A.A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology*, *12*, 561011. https://doi.org/10.3389/fpsyg.2021.561011
- [28] Mujtaba, G., Shuib, L., Raj, R. G., Majeed, N., & Al-Garadi, M. A. (2017). Email classification research trends: review and open issues. *IEEE Access*, 5, 9044-9064. https://doi.org/10.1109/ACCESS.2017.2702187
- [29] Nivia, R.M., Cortés, P.E., & Rojas, A.E. (2018). Implementation phase methodology for the development of safe code in the information systems of the ministry of housing, city, and territory. *In International Conference on Computational Science and Its Applications*, 34-49. https://doi.org/10.1007/978-3-319-95165-2_3
- [30] Piedrahita, D., Bermejo, J., & Machío, F. (2021). A Secure Email Solution Based on Blockchain. In International Congress on Blockchain and Applications, Cham: Springer International Publishing, 355-358. https://doi.org/10.1007/978-3-030-86162-9_36
- [31] Pinto, L., Brito, C., Marinho, V., & Pinto, P. (2022). Assessing the Relevance of Cybersecurity Training and Policies to Prevent and Mitigate the Impact of Phishing Attacks. *Journal of Internet Services and Information Security*, *12*(4), 23-38.
- [32] Purkait, S. (2012). Phishing counter measures and their effectiveness Literature review. *Information Management and Computer Security, 20*(5), 382-420. https://doi.org/10.1108/09685221211286548
- [33] Ramírez, C., Rojas, A.E., & García, A. (2022). A cold chain logistics with IoT and Blockchain scalable project for SMEs: first phase. *IFAC-PapersOnLine*, 55(10), 2336-2341. https://doi.org/10.1016/j.ifacol.2022.10.057
- [34] Rodríguez-Corzo, J.A., Rojas, A.E., & Mejía-Moncayo, C. (2018). Methodological model based on Gophish to face phishing vulnerabilities in SME. *In ICAI Workshops (ICAIW)*, 1-6. https://doi.org/10.1109/ICAIW.2018.8555006
- [35] Sreenivasulu, G. (2024). A Hybrid Optical-Acoustic Modem Based on Mimo Ofdm for Reliable Data Transmission in Green Underwater Wireless Communication. *Journal of VLSI Circuits and Systems*, 6(1), 36-42.
- [36] Sundararaj, A., & Kul, G. (2021). Impact Analysis of Training Data Characteristics for Phishing Email Classification. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 12*(2), 85-98.
- [37] Syafitri, W., Shukur, Z., Asma' Mokhtar, U., Sulaiman, R., & Ibrahim, M. A. (2022). Social engineering attacks prevention: A systematic literature review. *IEEE access*, 10, 39325-39343. https://doi.org/10.1109/ACCESS.2022.3162594
- [38] Taib, R., Yu, K., Berkovsky, S., Wiggins, M., & Bayl-Smith, P. (2019). Social engineering and organisational dependencies in phishing attacks. *In IFIP Conference on Human-Computer Interaction*, 564-584. https://doi.org/10.1007/978-3-030-29381-9_35
- [39] Time. (2023). They alert about a scam via SMS that impersonates 4-72: they send an alleged delivery guide.
- [40] Timko, D., & Rahman, M.L. (2023). Commercial anti-smishing tools and their comparative effectiveness against modern threats. *In Proceedings of the 16th ACM Conference on Security* and Privacy in Wireless and Mobile Networks, 1-12. https://doi.org/10.1145/3558482.3590173
- [41] Veksler, V.D., Buchler, N., LaFleur, C.G., Yu, M.S., Lebiere, C., & Gonzalez, C. (2020). Cognitive models in cybersecurity: learning from expert analysts and predicting attacker behavior. *Frontiers in Psychology*, 11, 1049. https://doi.org/10.3389/fpsyg.2020.01049
- [42] Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2022). Dynamic defenses in cyber security: Techniques, methods and challenges. *Digital Communications and Networks*, 8(4), 422-435. https://doi.org/10.1016/j.dcan.2021.07.006

A Controlled Phishing Attack in a University Community: A Case Study

Authors Biography



Diego Esteban Díaz Vivas achieved a bachelor's degree in Systems Engineering from Universidad Ean in Bogota, Colombia. This article summarizes the research project conducted within the university's cybersecurity and ethical hacking research hotbed, where Diego played pivotal roles as a developer and a junior researcher.



William Yecid Gutierrez Pena obtained a bachelor's degree in Systems Engineering at the Universidad Ean. As a cybersecurity and ethical hacking research hotbed member, he played the roles of developer and junior researcher to carry out this research at Universidad Ean.



Sandra Patricia Cristancho Botero is the Director of the Systems Engineering Program at Ean University, and a mentor of the Apps.co program of the Ministry of Information and Communications Technologies. She led the cybersecurity project 'Hackers Wanted,' which received funding from the OAS (Organization of American States), CISCO Latam, and Citi Foundation, and she carried out the Equity Scholarships: Women in IT Generation 5.0 initiative. She is currently the head of the cybersecurity and ethical hacking research hotbed.



Alix E. Rojas is an associate professor at Ean University, a recognized associate researcher by the Ministry of Science, Technology, and Innovation, and a mentor of the Apps.co program of the Ministry of Information and Communications Technologies. She leads research projects focused on the gender gap, agile practices, and the application of Industry 4.0 technologies. She is currently the head of the Blockchain and STEM Girls research hotbeds.