Data and Metadata. 2025; 4:930
doi: 10.56294/dm2025930

ORIGINAL

Vulnerability analysis in the university community using social engineering and phishing applications

Análisis de vulnerabilidades en la comunidad Universitaria mediante aplicaciones de Ingeniería Social y phishing

Javier Guaña-Moya[1], Sofía Villacís[1], Danilo Miniguano Miniguano[2]

[1]Pontificia Universidad Católica del Ecuador, Facultad de Hábitat, Infraestructura y Creatividad. Quito. Ecuador.
[2]Universidad Técnica de Ambato, Facultad de Ingeniería en Sistemas Electrónica e Industrial. Ambato. Ecuador.

Cite as: Guaña-Moya J, Villacís S, Miniguano Miniguano D. Vulnerability analysis in the university community using social engineering and phishing applications. Data and Metadata. 2025; 4:930. https://doi.org/10.56294/dm2025930

Submitted: 12-08-2024 **Revised:** 21-12-2024 **Accepted:** 14-05-2025 **Published:** 15-05-2025

Editor: Dr. Adrián Alejandro Vitón Castillo

Corresponding author: Javier Guaña-Moya

ABSTRACT

Introduction: the project focused on analyzing the impact of social engineering on the security of confidential information in a university community, highlighting the risks which individuals are exposed to when falling victim to such an attack. A controlled phishing attack was implemented.
Objetive: identify the main vulnerabilities that allow unauthorized access to personal data.
Method: the methodology used was descriptive, allowing for the analysis of factors such as the type of passwords used and the level of prior knowledge of social engineering.
Resul: the results revealed that the group most affected by the attack was people between 23 and 27 years of age, representing 27,5 % of the total, followed by older adults between 58 and 63 years of age at 19,6 %, demonstrating that both young and older adults are the most susceptible. Furthermore, it was found that 43,1 % of users used passwords composed of names and numbers, reflecting a low complexity in their construction. Only 5,9 % used password managers, and only 11,8 % incorporated special characters, indicating a low adoption of secure practices. The first phase of the attack, investigative in nature, was key to identifying exploitable personal patterns.
Conclusions: finally, after an awareness campaign was launched, it became clear that the main cause of vulnerability is a lack of knowledge about social engineering, highlighting the importance of strengthening cybersecurity education within the academic environment.

Keywords: Vulnerabilities; University Community; Social Engineering; Phishing.

RESUMEN

Introducción: el proyecto se centró en el análisis del impacto de la ingeniería social sobre la seguridad de la información confidencial en una comunidad universitaria, destacando los riesgos a los que se expone una persona al ser víctima de un ataque de este tipo. Para ello, se implementó un ataque de phishing controlado,
Objetivo: identificar las principales vulnerabilidades que permiten el acceso no autorizado a datos personales.
Método: la metodología utilizada fue de carácter descriptivo, permitiendo analizar factores como el tipo de contraseñas utilizadas y el nivel de conocimiento previo sobre ingeniería social.
Resultados: los resultados obtenidos revelaron que el grupo más afectado por el ataque fue el de personas entre 23 y 27 años, representando el 27,5 % del total, seguido por adultos mayores entre 58 y 63 años con un 19,6 %, evidenciando que tanto jóvenes como adultos mayores son los más susceptibles. Asimismo, se detectó que el 43,1 % de los usuarios utilizó contraseñas compuestas por nombres y números, lo cual refleja una baja

complejidad en su construcción. Solo el 5,9 % empleó gestores de contraseñas, y apenas un 11,8 % incorporó caracteres especiales, indicando una escasa adopción de prácticas seguras. La primera fase del ataque, de tipo investigativo, fue clave para identificar patrones personales aprovechables.
Conclusions: Finalmente, tras el envío de una campaña de concientización, se evidenció que la principal causa de vulnerabilidad es el desconocimiento sobre ingeniería social, por lo que se destaca la importancia de fortalecer la educación en ciberseguridad dentro del entorno académico.

Palabras clave: Vulnerabilidades; Comunidad Universitaria; Ingeniería Social; Phishing.

INTRODUCTION

The term “social engineering” first appeared in the context of computing in 1990, introduced by so-called “crackers,” who, unlike hackers, used their technical knowledge for malicious purposes. Crackers began employing psychological techniques such as persuasion and manipulation to breach systems.[1] Importantly, these psychological methods proved more effective than attempting to breach computer systems directly.[2] Rather than attempting to force their way into a system, crackers realized that it was easier to obtain sensitive information by manipulating the people using it.

One of the pioneers in the use of social engineering is Kevin Mitnick, who was captured by the FBI on February 15, 1995, and sentenced to 5 years in prison for carrying out acts considered illegal using this technique. But how did Mitnick manage to obtain the information he needed? His strategy consisted of not directly asking for what he needed, but pretending to already have that information, but incorrectly, so that people would correct their mistakes with the correct information. In this way, Mitnick demonstrated that people are the weakest link in computer security. By applying these psychological techniques together with his technical skills, he was able to access systems and obtain a large amount of information.[3]

From this perspective, identity theft, psychological manipulation, deceptive emails, and other methods became commonplace for hackers.[4] This evolved, and today, phishing has become the most popular social engineering attack.[5]

According to [6] Social Engineering, it is considered a manipulation technique that takes advantage of people’s vulnerabilities to obtain confidential information.[7]

The main objective of this type of attack is to take advantage of the lack of knowledge on this subject and it has become very common, since a person can give their information without realizing it and with this, they can access different platforms without the user knowing that someone violated their privacy, so applying social engineering takes less time than the usual attacks developed by cyber attackers.[8]

It is important to note that social engineering represents one of the most significant threats in the field of cybersecurity, as it exploits human behavior to gain access to confidential information. In the university context, this threat takes on relevance due to the intensive use of digital platforms by students, teachers, and administrative staff. Various studies have shown that a lack of specific training in digital security increases exposure to these types of attacks.[9,10] Phishing, as a social engineering technique, has been identified as one of the most effective for deceiving users and obtaining credentials or personal data, taking advantage of users’ trust and ignorance.[11]

An analysis conducted on a university community through a controlled phishing attack revealed multiple vulnerabilities, both technical and human. Most users use weak passwords or passwords related to personal information and social media, which makes it easier for attackers to reconnoiter or gather data. As stated by [12] and [13] the human factor remains the weakest link in the security chain, and it is precisely at this point where social engineering finds its greatest potential. A lack of understanding of how these attacks operate increases their likelihood of success, putting not only individual privacy at risk but also institutional integrity.

To mitigate these vulnerabilities, it is essential to implement awareness programs and ongoing cybersecurity training focused on early detection of digital social threats. As stated,[14] educational strategies should be aimed at developing practical skills in users so they can recognize suspicious patterns and act with caution when faced with unverified emails and links. Strengthening digital literacy in academic environments not only reduces the number of victims but also promotes a more resilient community prepared for emerging threats.

Social engineering relies on the psychological manipulation of people to obtain confidential information or access to restricted systems. Attackers do not need to breach sophisticated computer systems; rather, they exploit the trust, fear, or urgency they can induce in their victims.[15] The most common means include phone calls, fraudulent emails (phishing), SMS messages (smishing), and social media. Phishing has become one of the most widely used techniques due to its effectiveness and low implementation cost.[16] Through these channels, attackers pretend to be trustworthy entities to induce users to share credentials, download malware, or follow malicious links.

In general, it can be said that social engineering is an attack that uses psychological techniques to extract information in order to gain access to a system, banking data, cause fraud, impersonate identities, among others, in order to often obtain financial gain.[6]

Social Engineering Attack Means

Attackers use different means for different situations where they want to apply social engineering, so using the basic principles of social engineering is likely to make the attack more successful.[17] Below are the four different means, according to the article " Social Engineering Attacks".[18]

- *Phone:* This is where social engineering began, getting people to pretend to be someone they're not, creating the necessary importance and thereby obtaining the necessary permissions for the attacker to access the information they desire. This is a method that is still used today, and the results are often successful.
- *Internet:* This is the most common and widely used medium today. Phishing is one of the most common social engineering attacks used on this medium to steal information or infect with malware via a link. Another uncommon technique used on this medium is to display a pop-up window in which the user believes they are on the correct page and enters their information.
- *Dumpster Diving:* This method is rarely used, and its main objective is to search through garbage to extract information, usually from companies. The attacker can use the information they find to their advantage and obtain positive results when applying social engineering attack.
- *Psychological Manipulation:* This method can be combined with other methods and primarily focuses on manipulating people so that they unwittingly give away information.

It's important to note that the ninth State of Phishing report conducted by ProofPoint shows that 44 % of people trust an email when they see a familiar domain. However, the report mentions that around 30 million phishing emails were in a Microsoft context. Furthermore, of the 75 million threats, 1 in 10 were reported by users, demonstrating a lack of knowledge about how to avoid and protect against phishing.[19]

According to a study conducted by NordPass, which analyzed 3TB of password data in 2022, it mentions that the most used passwords remain weak due to individual habits. The study shows that people typically use social topics like movies, sports, or family-related topics. Regarding the use of special characters, the results of these studies show that people don't use these characters unless required.[20]

METHOD

For this research, the descriptive method was used, as the goal was to determine the factors that determine the outcomes that lead people to fall prey to social engineering attacks. The following describes the process carried out during this type of controlled attack to analyze user vulnerabilities in the university sector.

Analysis of the principles of social engineering

The following principles are mentioned by Christopher Hadnagy in his book "Social Engineering the Science of Human Hacking". This book describes how social engineering works and how the following principles are fundamental to its application.[15]

Principle 1: Reciprocity

The principle of reciprocity can be described in one word: altruism. When you offer something that the other person wants to hear or needs, they may feel a kind of emotional debt, which can generate a desire to reciprocate. This creates the opportunity to mention what you want, resulting in obtaining the desired information.

Principle 2: Obligation

The principle of obligation is based on getting people to behave in accordance with what is considered socially correct. In the context of social engineering, this principle can be used to establish a relationship of trust with a victim, so that they allow actions without the need for the necessary permissions.[15] In his book, he explains that, to enter a place without a badge, all you need to do is create a situation in which the other person feels the need to do the right thing. For example, entering a place with many heavy boxes and having the other person open the door. While the person may ask for the badge, the manipulator may ask for help to remove it from the pocket, which creates an awkward situation and leads the other person to give in.

Principle 3: Concession

The principle of concession is based on getting the other person to give in to what is needed indirectly. That is, you offer something exaggerated first, and then, when they refuse, you offer something you know the person

is willing to give. When analyzing the two options, the person will likely give in to the second option, which is what the attacker wanted all along. This same principle can be applied to obtaining information. You simply provide false information so that the victim will hand over the correct information.

Principle 4: Scarcity

The scarcity principle refers to turning a situation that may not be very important into one that requires immediate attention. To achieve this, in various situations, attempts are made to make it seem as though failure to act immediately will result in serious consequences. This leads the other person to give in and take immediate action to resolve the issue and avoid any potential problems. However, this can also allow the attacker full access to sensitive information or take complete control of a situation.

Principle 5: Authority

The principle of authority is based on investigating who has the highest rank or authority in the organization or situation you want to access. Once this person has been identified, their name or position can be used to influence others and get what you need. This works because the authority figure generates fear in people of making mistakes or acting against what has been ordered, so they will often defer to the name or position of the authority figure.

Principle 6: Consistency and Commitment

The Principle of Constancy and Commitment shows that, to successfully obtain the desired information, the attacker must have a clear strategy that allows them to establish a relationship of trust or friendliness with the victim. It is essential for the attacker to be able to anticipate possible situations and adapt their strategy as needed to achieve their goal.

Furthermore, it's important to keep in mind that the process of obtaining information should be gradual and not started immediately. This way, the attacker can gradually build trust with the victim, which will increase the chances of successful manipulation. Ultimately, perseverance and patience are key to achieving the goals of social engineering.

Research design

Investigation is the first phase of a social engineering attack. It determines the most suitable scenario for carrying out the attack. For a person to become a victim, a relationship of trust must be established, so the different types of social engineering must be considered.

For this research, a controlled social engineering attack was carried out, using an advertisement offering something attractive to entice people to check it out. This is referred to as Quid Pro Quo.

Attack execution

A website was developed using PHP and MySQL. To upload the website to the internet, a hosting service and a domain were used. Additionally, advertisements with the QR code were placed in specific locations at several higher education institutions.

Ethical procedures

This investigation does not aim to carry out malicious activities with the data obtained; it was used solely for analysis and to conduct an awareness campaign against social engineering. The data, as well as the website, were subsequently deleted. Victims received an email informing them of the precautions they should take when entering personal information.

Process for reporting phishing pages

There are various websites that are responsible for categorizing whether a website is detected as phishing or suspicious, so it's essential to report the hosting provider where the website is located. To find out which hosting provider it belongs to, you can enter the domain name on the website: https://www.whois.com/. This provides all the information about the domain, as well as contact information for reporting abuse and the hosting provider to which it belongs.

Regarding websites that classify a page as malicious or phishing, you can use the reporting pages of: Fortinet, ESET, Palo Alto, Safebrowsing, google, among others. On each of them, you must specify the website you want to report on and fill out the required fields. After submitting the reports, depending on the analysis performed, it will be classified as malicious. If you check the URL in the VirusTotal tool, it will already have indicators of compromise. This will help prevent people from falling for attacks like phishing.

Regarding the hosting report, it will depend on the hosting you're using. Once you've identified which hosting it belongs to, simply search for the report option and follow the same procedure above, filling out the

requested information. Hosting staff will conduct the respective analysis and take the necessary action.

RESULTS

Targeted attack development

The following details the processes carried out in each phase for the controlled phishing attack.

Phase 1. Research

In this phase, the victim's motive for entering the QR code and their information was determined. Three popular social themes were proposed for this attack, as the ideal target for a controlled attack is to obtain user registration data.

An organization to be cloned was also investigated, and publications and information were sought to be used on the website to make it as like the original as possible.

Finally, a link to the website was sent as bait, and advertisements were placed in specific locations where people were heavily trafficked. The advertisements offered services that could help people and thereby attract the interest of potential victims. It was also important to establish a relationship of trust with the victim. In this project, the website was made to appear authentic so that visitors would feel they were on the official site.

Phase 2. Design

When designing the advertising campaign, we considered that, to be convincing, it must be as similar as possible to the advertisement the organization publishes on its social media. Furthermore, it must be high-quality and highly produced. To achieve this result, we researched the organization's posting style on the social media platform Instagram.

Once the style to be used was determined, the page was cloned with an identical model of how the advertisement was, which had the following characteristics.

- Image of the cloned institution, attractive information for the victim, steps to follow for registration, eye-catching footer, QR code and the institution's slogan

2.1. Advertising design structure

When people recognize something familiar, they tend to trust the information they see, which is why the cloned institution's logo was included. A saying was placed next to the logo because it's always included in the organization's original publications. To facilitate access to the website, a QR code was used. These codes generate curiosity, and people often scan them just to see what's inside. Next to the QR code are the steps to follow, which indicate what to do to register. The title is the most important part of the advertisement, so an attractive phrase was included. To entice users to register, the flyer stated that several benefits would be obtained if they registered.

2.2. Structure of the website design

CSS was used for page design. The design is a simple page with a header, a body containing a registration form, and a footer. The registration fields are: first name, last name, date of birth, ID, address, phone number, email, password, and password confirmation. No controls were placed on the latter field to evaluate the user's input.

Phase 3. Execution

In this research project on social engineering, advertisements were placed in specific locations, containing relevant information and QR codes. The QR code redirected to the cloned website, which remained operational for two months. The designed website included a database that allowed data collection, which was subsequently used to analyze the collected information.

The operation of the attack was as follows:

- Distribution of advertising
- The person scans the QR code which will redirect them to the registration page.
- It is expected that the requested data be entered
- By clicking register, the data is stored in the database.
- Once the data is obtained, the information obtained is analyzed.
- An awareness email was sent informing them that they have been victims of a social engineering attack in a controlled environment.
- Information was sent on how to avoid these types of attacks.

Phase 4. Exit

Since this was an investigation, awareness was raised for those who entered their information, and an email was sent to all users to raise awareness about this type of cyberattack. In the case of a real attack, attackers at this stage use the obtained data for malicious purposes, by attempting to access other accounts. The obtained information is often also sold on the Deep Web.

DISCUSSION

Analysis of Results by Gender and Age

Below are the results of the data collected based on the age and gender of the users who clicked on the link sent.

It's evident that among the 51 people who entered their information, 28 were women and 23 were men. Therefore, there's a trend toward women being the most interested in the advertising in this controlled phishing attack.

Age range analysis

Figure 1 shows that of the 51 people who entered their data, the majority were between the ages of 23 and 27. It should be noted that the targeting of this attack was aimed at a technology-intensive audience. This is why the age group of young people who are likely employed and highly knowledgeable about using technology predominates.

The next group is 58 to 63-year-olds who may have some technological knowledge but filled out their information solely for the benefit the advertisement was offering, without considering that it could be a scam.

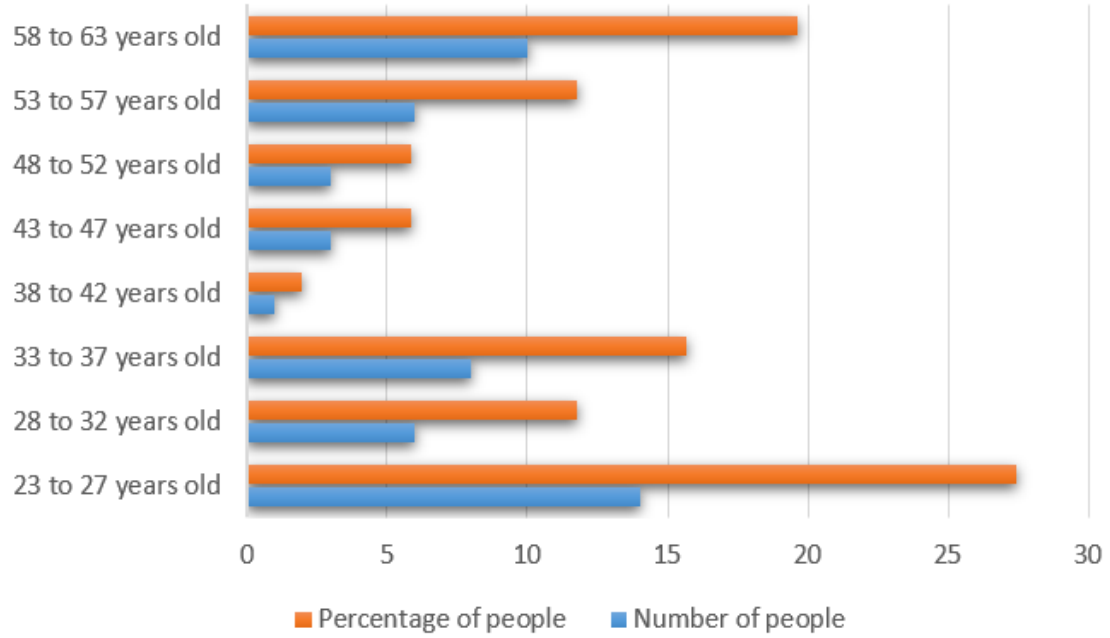

Figure 1. Result of Information by Age

Most vulnerable group

The 23- to 27-year-old age group accounted for the largest number of victims (14), representing more than a quarter of the total (27,5 %). This may be due to:

- Greater use of digital platforms.
- Overconfidence or lack of experience in cybersecurity.

Another critical group:

The 58-63 age group represents 19,6 %, showing that older adults are also vulnerable, possibly due to:

- Less familiarity with emerging technologies.
- Difficulties in identifying digital scams.

Less affected groups:

The 38-42 age range had only one affected person (2 %), which may reflect a medium level of digital

experience combined with caution.

Intermediate distribution (28 to 57 years):
They represent a more balanced dispersion, ranging between 5,9 % and 15,7 %, suggesting moderate awareness, although not without risk.

Password Results Analysis
Regarding passwords, since this data is sensitive, only the tendency of people to use one password will be mentioned. It's worth mentioning that no restrictions were placed on the password for the attack, as the goal was to analyze what people enter (see figure 2).

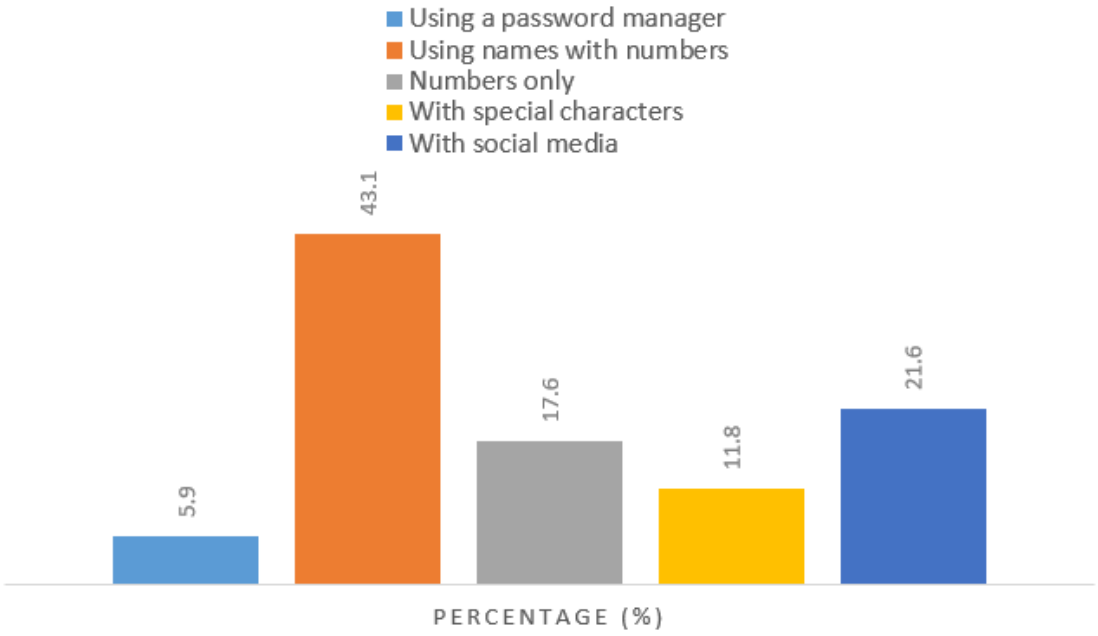

Figure 2. Password by Category

Below is an interpretive analysis of the categories found based on the use of passwords:
Prevalent weak passwords:
The largest group corresponds to the use of names with numbers (43,1 %), a risky practice due to its ease of being guessed through dictionary attacks or social engineering techniques.

Exclusive use of numbers (17,6 %):
It also represents a significant risk, as pure numeric passwords are typically short and more vulnerable to automated attacks.

Few strong passwords:
Only 11,8 % incorporate special characters, which is a key component to increasing password strength.

Social issues as inspiration (21,6 %):
Although creative, these passwords are also predictable if the attacker knows the user's public information or interests.

Low use of password managers:
Only 3 people (5,9 %) make use of managers, indicating a low level of awareness or adoption of technological tools specifically designed to improve security.

CONCLUSIONS

Attacks using social engineering demonstrate how attackers can exploit people's vulnerabilities and control them to obtain sensitive information. The controlled attack identified that people are more vulnerable when offered something attractive, which, as mentioned above, refers to the type of social engineering called quid pro quo.

https://doi.org/10.56294/dm2025930

The middle groups showed a more balanced distribution, although not exempt from vulnerability. These results highlight the need to implement differentiated cybersecurity training strategies by age group, particularly strengthening preventative campaigns for new users and older adults, to reduce susceptibility to this type of threat.

Awareness of social engineering is of utmost importance in both personal and business settings. An organization must implement social engineering campaigns to identify the most vulnerable employees. Therefore, proper training on how to identify and prevent these types of attacks will help reduce the risks and vulnerabilities of institutions.

Regarding the passwords analyzed, it's clear that if restrictions aren't set that the password must be at least 8 digits long, contain a capital letter, non-consecutive numbers, and special characters, people set a simple password that's very easy to crack and is likely to be used for multiple accounts.

Finally, the data reveals a worrying trend toward the use of weak and predictable passwords, with names with numbers being the most common practice (43,1 %), followed by passwords composed solely of numbers (17,6 %) and those inspired by social themes (21,6 %). Only a small percentage of users incorporate special characters (11,8 %) or use password managers (5,9 %), reflecting a low adoption of secure practices. This situation highlights the urgent need to strengthen cybersecurity awareness, promoting the creation of strong passwords and the use of specialized tools that help mitigate the risks of unauthorized access.

REFERENCES

1. Moya JG,VJCC,CGB,VAM,&GMJ. Análisis de vulnerabilidades en sectores industriales: Un estudio sobre Ciberseguridad 2021-2023. Revista Ingenio global. 2025;: p. 219-236.

2. Tumbaico BDT. Ciberseguridad en educación y política: Desafíos éticos y tecnológicos. Horizon International Journal. 2024;: p. 28-39.

3. Pastor J. Xataka. [Online].; 2018. Available from: https://www.xataka.com/seguridad/kevin-mitnick-genio-o-figura-de-uno-de-los-hackers-mas-famosos-de-la-historia.

4. Vélez LFC. Influencia de la ingeniería social en la educación y política digital. Alpha International Journal. 2023; 1(1): p. 44-56.

5. Guaña-Moya J,CCMA,dCJFP,NVD,MZER,&LTLG. Phishing attacks and how to prevent them. 17th Iberian Conference on Information Systems and Technologies. 2022.

6. Guaña-Moya J,&ÁPD. Social Engineering as the Art of Deception in Cyber-Attacks: A Mapping Review. In World Conference on Information Systems and Technologies. Springer Nature Switzerland. 2023;: p. 155-163.

7. Breda F,BH,&MT. Social engineering and cyber security. INTED2017 Proceedings. 2017;: p. 4204-4211.

8. Salama R,&ATF. Cyber-security countermeasures and vulnerabilities to prevent social-engineering attacks. Artificial intelligence of health-enabled space. 2023;: p. 133-144).

9. Hadnagy C. Social engineering: The art of human hacking. John Wiley & Sons. 2010.

10. Mitnick KD,&SWL. The art of deception: Controlling the human element of security. John Wiley & Sons. 2003.

11. Granger S. Social engineering fundamentals, part I: hacker tactics. Security Focus. 2001.

12. Abawajy J. User preference of cyber security awareness delivery methods. Behaviour & information technology. 2014; 33(3): p. 237-248.

13. Albladi SM,&WGR. Predicting individuals' vulnerability to social engineering in social networks.. Cybersecurity. 2020; 3(1).

14. Kumar P,SM,&BB. Social engineering attacks and defense mechanisms: Current trends and future challenges. Journal of Information Security and Applications. 2021;(58).

15. Hadnagy C. Social Engineering The science of Human Hacking: John Wiley & Sons, Inc; 2018.

16. Jagatic TN,JNA,JM,&MF. Social phishing. Communications of the ACM. 2007; 50(10): p. 94-100.

17. Salahdine F, Kaabouch. Social Engineering Attacks: A Survey. Future Internet. 2019; 11(4): p. 89.

18. Koyun A, Al Janabi E. Social Engineering Attacks. Multidisciplinary Engineering Science and Technology (JMEST). 2017; 4(6): p. 7533-7538.

19. Proofpoint. Proofpoint. [Online].; 2022. Available from: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish.

20. Nordpass. Nordpass. [Online].; 2022. Available from: https://nordpass.com/most-common-passwords-list/.

FINANCING

The research is funded by the Pontifical Catholic University of Ecuador.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION:

Conceptualization: Sofía Villacís, Danilo Miniguano Miniguano.
Data curation: Javier Guaña-Moya.
Formal analysis: Danilo Miniguano Miniguano, Sofía Villacís, Javier Guaña-Moya.
Research: Javier Guaña-Moya, Danilo Miniguano Miniguano.
Methodology: Sofía Villacís, Javier Guaña-Moya.
Writing - original draft: Sofía Villacís, Javier Guaña-Moya, Danilo Miniguano Miniguano.
Writing - review and editing: Javier Guaña-Moya.