Unveiling the code: A review of the knowledge and awareness of computer engineering students-UPE-CPF on the mechanisms of digital appropriation

María Luisa Hermosilla de Olmedo
Faculty of Computer Science, Universidad Privada del Este. City Pdte. Frank. Paraguay
E-mail: maluolme31@gmail.com
ORCID: https://orcid.org/0000-0003-4910-6562

Rodolfo Fernando Oliver Ayala
Faculty of Computer Science, Universidad Privada del Este. City Pdte. Frank. Paraguay
E-mail: rodolfo_oliver@hotmail.com
ORCID: https://orcid.org/0009-0008-4050-420X

Jaqueline Olmedo Hermosilla
E-mail: 990.hermosilla@gmail.com
ORCID: https://orcid.org/0000-0002-4158-1169

Daisy Beatriz Paredes Segovia
Faculty of Computer Science, Universidad Privada del Este. City Pdte. Frank. Paraguay
E-mail: paredesdaisy82@gmail.com

Victor Ariel Córdoba Bordón
Faculty of Computer Science, Universidad Privada del Este. City Pdte. Frank. Paraguay
E-mail: victorarielcordobabordon830@gmail.com

Ariel de Jesús Duarte Núñez
Faculty of Computer Science, Universidad Privada del Este. City Pdte. Frank. Paraguay
E-mail: duarteariel353@gmail.com

Ángel Ramón Servían González
Faculty of Computer Science, Universidad Privada del Este. City Pdte. Frank. Paraguay
E-mail: angelserviangonzalez@gmail.com

Leandro David Cáceres Ferreira
Faculty of Computer Science, Universidad Privada del Este. City Pdte. Frank. Paraguay
E-mail: leandrocaceresinformatica570@gmail.com

Salvador Cano Chávez
Faculty of Computer Science, Universidad Privada del Este. City Pdte. Frank. Paraguay
E-mail: 999999.azaazaz@gmail.com

ABSTRACT

The study investigated the level of knowledge and awareness of Computer Engineering students at the Private University of the East with respect to the technological mechanisms used for malicious purposes for information theft. The research had a mixed approach, with a non-experimental descriptive design. With a population of 258 students, being 1774 the number of elements in the sample, which was chosen with a non-probabilistic method and cluster technique. Google form was used for data collection. The findings revealed a significant gap in their understanding of these cyber threats, highlighting the urgent need to improve cybersecurity education in the curriculum. In addition, the importance of awareness about ethical responsibility in information management was highlighted and the need for interdisciplinary collaboration in this constantly evolving field was underlined. In conclusion, the study highlights the importance of preparing future computer professionals to address security and data protection challenges in a constantly evolving digital environment.

Keywords: Security, Computer Science, Knowledge-theft, Information.

1 INTRODUCTION

In the context of the increasing number of cyberattacks, it is essential that the public is informed about the schemes and mechanisms that are often used to steal information. Cyberattacks can have devastating consequences for victims, who may suffer financial loss, reputational damage, or even loss of privacy. For example, a victim of a phishing attack may lose access to their bank account or credit cards, which can lead to large financial losses. A victim of a malware attack may have their computer infected with a virus that can steal their personal data, such as their social security number or email address. And a victim of a brute force attack may have their password compromised, which can allow cybercriminals to access their online accounts.

This research is developed with the general purpose, to identify the knowledge that students of the Computer Science Engineering career have, about the technological schemes and mechanisms used for malicious purposes for the theft of information. This is due to the fact that modern society is increasingly immersed in a digital environment, which makes it susceptible to various cyber threats, such as the theft of confidential data, scams and bribes, among other risks. Therefore, it is crucial to keep people informed and empowered in the face of these threats, and for this the professional must be highly prepared.

To achieve the objectives, a series of in-depth investigations and analyses were carried out that addressed the following aspects: Protection and Prevention Measures. Survey on student knowledge: A survey was carried out among students of the Computer Science Engineering program at the Universidad Privada del Este, CPF; to review your level of knowledge about computer security threats and information theft.

The research seeks to contribute significantly to the protection of personal and confidential information, as well as to the preparation of IT professionals to face today's cyber threats.

In the digital age, where information has become an invaluable asset and cybersecurity stands as a critical issue, it is essential to evaluate the degree of knowledge and understanding of Computer Engineering students at the Universidad Privada del Este, Campus Ciudad Presidente Franco (UPE-CPF), about the mechanisms of digital appropriation.

This problem statement is based on the need to address the following aspects: Importance of Cybersecurity: Digital information is an essential resource in today's society, used in daily and professional activities. A lack of cybersecurity understanding and preparation can leave individuals and organizations exposed to significant risks, such as loss of sensitive data, disruption of critical services, and reputational damage.

Current Challenges: Technological advancements and the sophistication of cyber threats pose constant challenges in protecting data and systems. Digital appropriation, in its various forms, represents a latent threat that needs to be addressed proactively.

Academic Background: Computer Engineering students at UPE-CPF are future professionals who will play a crucial role in information security. Reviewing your current knowledge of digital appropriation mechanisms is critical to ensure proper training and preparation of cybersecurity experts.

Knowledge Gaps: It is necessary to identify potential gaps in students' knowledge, including understanding the tactics used by malicious actors online, prevention methods, and best practices in cybersecurity.

Repercussions on Digital Security: Insufficient knowledge of digital appropriation mechanisms can have serious consequences, both at the individual and organizational levels. Lack of preparation can lead to vulnerabilities that are exploited by cyber attackers.

Therefore, the following general question arises, what is the knowledge and awareness that the students of Computer Engineering of the Universidad Privada del Este have about the technological mechanisms that are used maliciously for the theft of information? and its respective objective, to determine the level of knowledge and awareness of the students of Computer Engineering at the Universidad Privada del Este, Campus Ciudad Pdte. Franco (UPE-CPF), on digital appropriation mechanisms. The researchers made the following proposition; Hi: The level of knowledge and awareness of the students of Computer Engineering at the Universidad Privada del Este, Campus Ciudad Pdte. Franco (UPE-CPF), on the mechanisms of digital appropriation is **high**.

To test this hypothesis, a survey was carried out, with the instrument called questionnaire, applied to the students of Computer Engineering of the UPE-CPF. The survey included questions on the following aspects: Definition of Digital Appropriation, Types of Digital Appropriation, Examples of Digital Appropriation, and Risks of Digital Appropriation.

2 METHODOLOGY

2.1 RESEARCH FOCUS

This work adopts a multimodal approach by combining quantitative data collection with detailed characterization of the phenomenon under study. This methodology allows us to gain a more complete and holistic understanding of the research topic.

2.2 RESEARCH DESIGN

This study is characterized by its descriptive scope, since its main objective is to collect information in an exhaustive manner. This is a non-experimental design, since the environment in which the research is carried out is not modified. In addition, it adopts a mixed approach, as the proposed questionnaire will provide statistical data, thus combining quantitative and qualitative elements in the analysis.

2.3 SCOPE OF RESEARCH

This study is characterized by its descriptive scope, since its main objective is to collect information in an exhaustive manner. This is a non-experimental design, since the environment in which the research is carried out is not modified. In addition, it adopts a mixed approach, as the proposed questionnaire will provide statistical data, thus combining quantitative and qualitative elements in the analysis.

2.4 POPULATION AND SAMPLE

The study will focus on the 258 undergraduate students of the Computer Engineering program at the Universidad Privada del Este, Ciudad Pdte. Frank. From this population, a representative sample will be selected, thus guaranteeing the relevance and applicability of the results obtained.

2.5 SAMPLING TECHNIQUE

The sample will be selected using the non-probabilistic method with the cluster selection technique, in which a specific subset of students from the Universidad Privada del Este will be identified and selected.

2.6 DATA COLLECTION TECHNIQUE

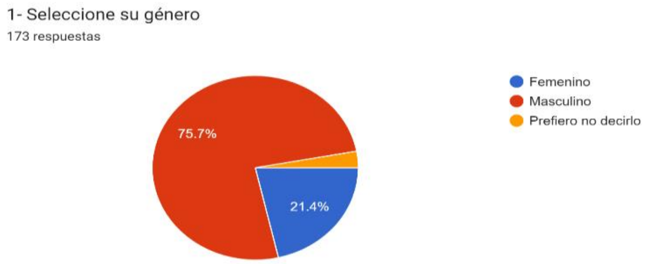
Data collection will be carried out through a survey, using a questionnaire as an instrument. This questionnaire will consist of closed-ended questions with answer options, which will be implemented in a Google form. These questions help to gather valuable information about students' level of knowledge and awareness in relation to information security and digital appropriation mechanisms, as well as identify areas for improvement in their academic training.

2.7 ANALYSIS OF COLLECTED DATA

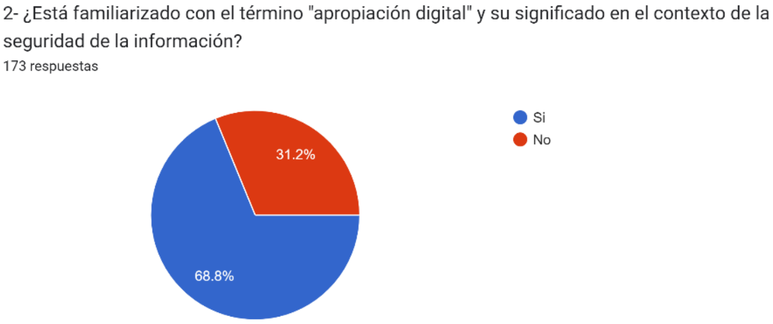
The analysis of the collected data was carried out using a quantitative approach. To do this, the Excel tool was used to process and analyze the data. Subsequently, the results of the analysis were presented in the form of demonstration graphs for ease of interpretation. Data cleansing: This is a crucial step, it's the way to ensure that the data is complete, consistent, and error-free.

3 RESULTS

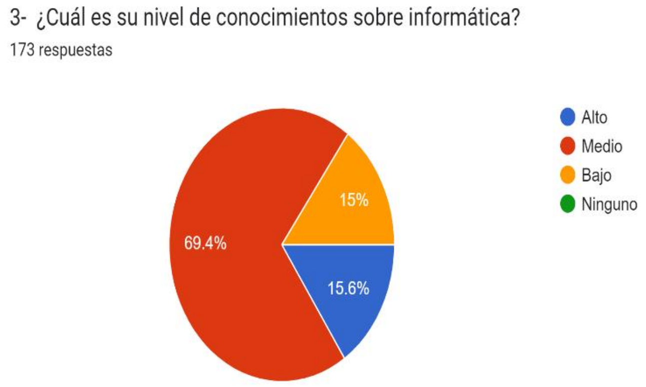
3.1 AFTER THE RESPECTIVE ANALYSIS, THE RESULTS ARE PRESENTED UNDER THE QUANTITATIVE AND QUALITATIVE PARADIGMS



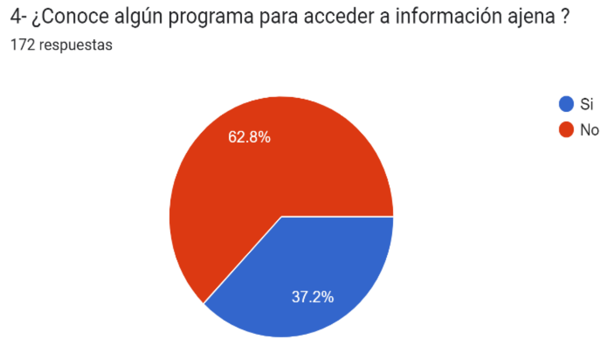
In this case, 174 people responded to a questionnaire. It responds to the Gender Distribution, in which 75.7% of the students in the sample identify their gender as male. 21.4% of the people in the sample identified their gender as female. Non-Preference Rest: The "rest" refers to people who did not choose to identify as male or female. In other words, they either did not disclose their gender in the questionnaire or preferred not to specify it. To calculate the percentage of Students who did not prefer to say their gender, you can reset the sum of the percentages of known gender (male and female) to 100%. In this case: 100% - (75.7% + 21.4%) = 100% - 97.1% = 2.9%. Then, 2.9% of the students in the sample did not prefer to say their gender.



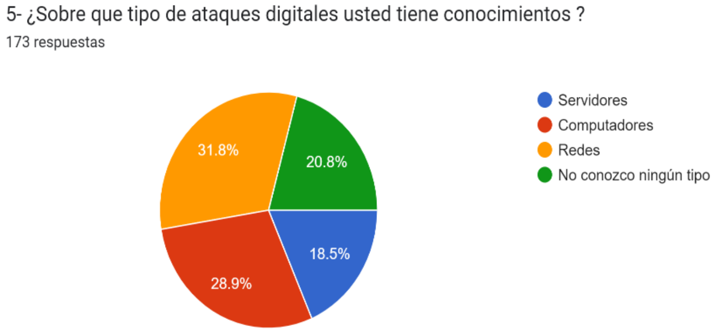
The sample size constitutes a group of students and this group consists of a total of 100%. In this case, the sample is divided into two categories: Familiar people: 68.8% of the students in the sample are familiar with the term "Digital Appropriation". This means that approximately two-thirds of the students in the sample mean or have heard of this term. Unfamiliar students: 31.2% of the people in the sample do not know the term "Digital Appropriation". This implies that about one-third of the people in the sample are either unaware of this term or unfamiliar with it. These percentages indicate the proportion of people in the sample who are or are not familiar with the term "Digital Appropriation." This information is useful for understanding the spread or awareness of a concept or term in a group of people.


3- ¿Cuál es su nivel de conocimientos sobre informática?
173 respuestas

Distribution of levels of computer literacy: 69.4% of the population has an "average" level of computer literacy. This means that the majority of students in the population have an average level of knowledge in this area. 15.6% of the population has a "High" level of computer literacy. This indicates that a significant, but smaller, part of the population has a high level of computer literacy. The remaining 15% of the population has a "Low" level of computer skills. This means that a relatively small percentage of the population has a low level of knowledge in this area. These percentages indicate how the levels of computer knowledge are distributed in the population. It is important to have this information to understand the level of computer proficiency of the population and to make decisions related to education, training or decision-making in technology projects.

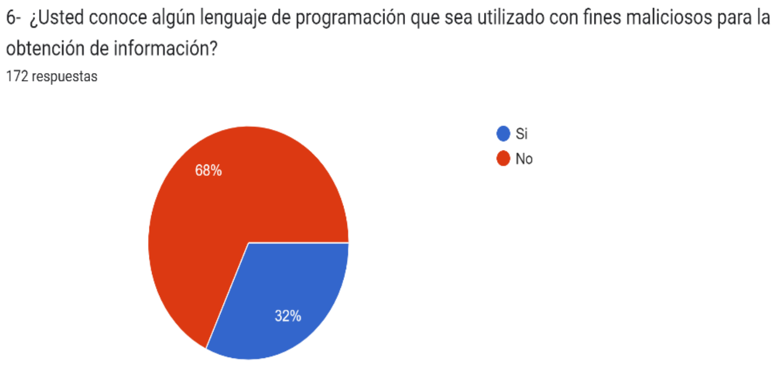

4- ¿Conoce algún programa para acceder a información ajena ?
172 respuestas

This statement refers to the entire population of interest. Students with knowledge: 62.8% of the population is aware of a program that is used to access private information. This means that approximately two-thirds of people in the population are aware of the existence of programs designed to access information that should normally be private. Students without knowledge: The remaining 37.2% of the population is not aware of these programs. This implies that about one-third of the population is uninformed or unaware of the existence of such programs. This information is used to understand how many people in the population are aware of risks related to privacy and information security. It is important for decision-making and education on cybersecurity and privacy issues.


5- ¿Sobre que tipo de ataques digitales usted tiene conocimientos ?

173 respuestas

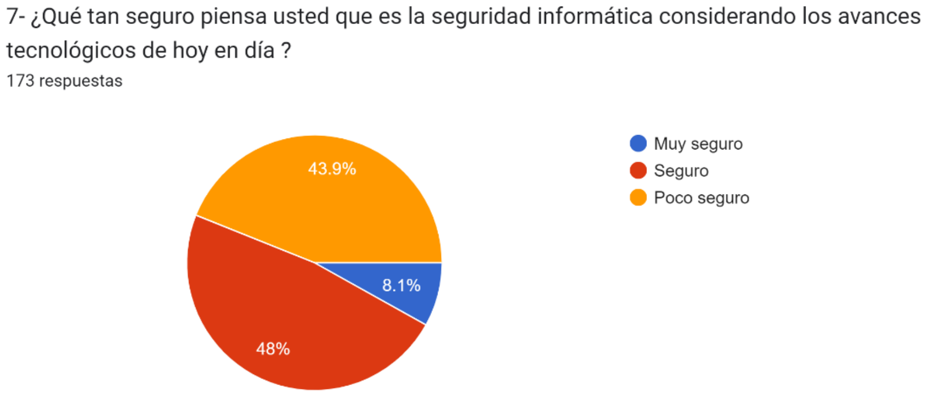
Students with knowledge about network attacks: 31.8% of the population has knowledge about digital attacks aimed at networks. This indicates that about one-third of students in the population understand what network attacks are and how they work. Students with knowledge about computer attacks: 28.9% of the population has knowledge about digital attacks aimed at computers. This implies that just under a third of the population is familiar with cyberattacks targeting individual computer systems. Students who are not aware of any type of computer attack: 20.8% of the population has no knowledge about any type of computer attack. This means that one-fifth of the population is unaware of digital attacks. Students with knowledge about attacks on servers: The remaining 18.5% of the population has knowledge about digital attacks targeting servers. This indicates that a significant proportion of the population understands attacks targeting information servers.



6- ¿Usted conoce algún lenguaje de programación que sea utilizado con fines maliciosos para la obtención de información?

172 respuestas

The statement describes the distribution of the population's knowledge regarding the programming languages used for the theft of digital information. Students who do not know any programming language for information theft: 68% of the population has no knowledge of any programming language that is used for digital information theft. This means that the majority of students in the population are not informed about these languages. Students who know a programming language for information theft: The remaining 32% of the population does have knowledge of at least one programming language used for digital information theft. This indicates that a minority of the population is aware of the existence of programming languages used in illicit activities related to the theft of data or digital information. This information is relevant to understanding the population's awareness of cybersecurity and programming in illegal contexts. It can assist in decision-making related to education and cybersecurity.

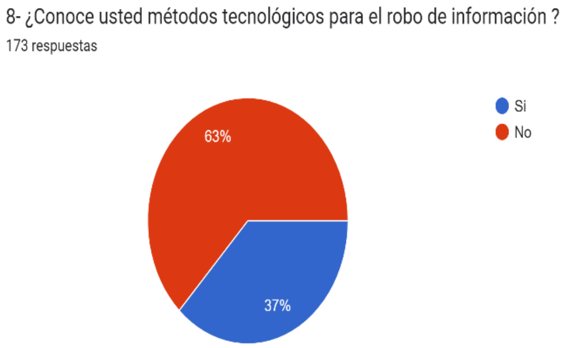


7- ¿Qué tan seguro piensa usted que es la seguridad informática considerando los avances tecnológicos de hoy en día ?

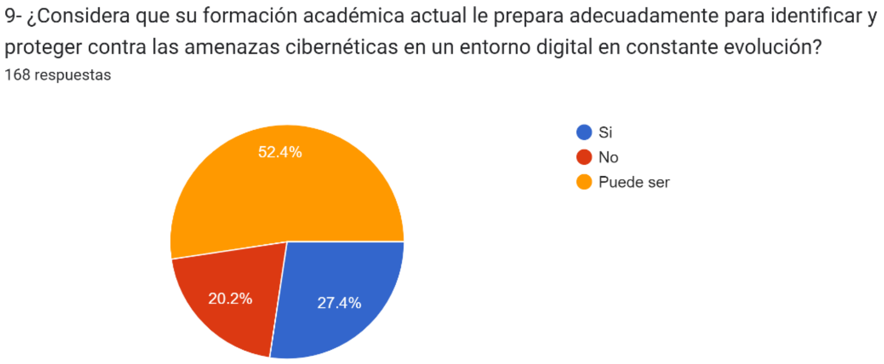
173 respuestas

The statement describes the population's perceptions of today's computer security. Students who think computer security is "Secure": 48% of the population believes that today's computer security is "Secure." This indicates that almost half of the population considers that computer security is sufficient and that their data and information are protected. Students who think computer security is "Not very secure":

43.9% of the population thinks that computer security is "Not very secure". This means that a significant proportion of the population has doubts or concerns about the security of their online data. Students who say that computer security is "Very secure": 8.1% of the population believes that computer security is "Very secure". This indicates that a minority of the population has high confidence in the security of today's computer technology. This information is useful for understanding people's perceptions of cyber security and may be relevant for cybersecurity policy planning and public education on online safety issues.


8- ¿Conoce usted métodos tecnológicos para el robo de información ?
173 respuestas

Students who do not know technological methods for information theft: 63% of the population is not aware of technological methods used for information theft. This means that most students in the population are not aware of the techniques and tools that can be employed for the theft of data or digital information. Students who know methods for stealing information: The remaining 37% of the population does have knowledge of technological methods used to steal information. This indicates that a minority of the population is informed about the techniques and tools related to the theft of data or digital information. This information is relevant to understanding how many students in the population are aware of threats to computer security and cybersecurity. It can be important for decision-making related to cybersecurity education and cybercrime prevention.


9- ¿Considera que su formación académica actual le prepara adecuadamente para identificar y proteger contra las amenazas cibernéticas en un entorno digital en constante evolución?
168 respuestas

Perception of educational background: The majority of respondents indicate that their educational background could adequately prepare them to identify and protect against cyber threats. This implies that the majority of students surveyed believe that their education provides them with at least a reasonable basis for dealing with cybersecurity issues, although not necessarily with a high degree of preparation. 27% of respondents say yes, their training prepares them adequately. This indicates that just over a quarter of respondents feel well prepared by their educational background to deal with cyber threats. 20% of respondents say no, their training does not prepare them adequately. This means that one-fifth of respondents do not believe that their education has provided them with adequate preparation to deal with cyber threats. These responses reflect respondents' perceptions of the effectiveness of their academic training in the field of cybersecurity. It may be important to take these opinions into account when assessing the quality of cybersecurity education and consider improvements to cybersecurity training or awareness programs.

10- Have you ever experienced a situation where your personal data or sensitive information was compromised online? If so, what steps did you take to address the situation? 150 replies
Fifty of the respondents reported no incidents with the security of their online accounts. However, the others established these events, which are detailed below Changing passwords to strong ones, encrypting files I had an occasion in my work, that there was an attempt to steal the data of users of the company by the Phishing method, which I intervened by blocking the attacking email addresses in the anti-spam server that we have Yes, I looked for solutions to the problem and asked for help Against viruses, I was installing antivirus on my computer Full PC Formatting Something similar, they took some money from me, I didn't do anything, I cried. Change my password Change Password Two-step verification I didn't manage to delete it, but I did manage to save those emails. If it already happened to me, ask for help from that app's support Luckily I haven't experienced that situation It was on Facebook, I turned on 2-step verification Much longer and varied-character passwords (#$@abc123) First of all, I protected all my information If on several occasions, the measures I took were to change passwords for more secure ones, I activated two-step verification. Yes, change my passwords and turn on authentication methods At that time, I went to "recover password" and use an auxiliary email (both on time) report I couldn't make any countermeasures, since at the time I found out they had already taken over my accounts, I had to create new accounts. In addition to erasing my personal information, I changed passwords and turned on two-step security Hack attempt, strengthen security, implement 2-step verification, and if possible migrate the information to another account Yes, I changed the password and unlinked all devices from the account If it has already been compromised, change my social media password. I tried to delete everything and I could change/edit everything that was publicly seen on the internet about me The only experience is theft attempts, for example, ip loggers that through a camouflaged link try to steal your information if you enter them, I never fell into one, but they are very well known and people usually fall for them

I never had an experience of exposing personal information, but if I lost some accounts due to the cyberattack, the first thing I usually see the root/cause of the problem may be applications of dubious origin or unsafe sites, then I proceed to delete them and then clean up my account Yes, they tried to hack my Instagram from another distant city (Luque) it came directly to my email and asked me for verification which I only had to cancel
11- Can you name any basic security measures that organizations typically implement to protect their information against digital appropriation?154 replies
Seventeen sample items indicated that they did not have names of basic security measures used by the organizations. While the others indicated this, which is described below: Passwords What if you were a robot VPN Basic security measures that organizations typically implement include the use of firewalls, antivirus and up-to-date security software, strong password policies, two-factor authentication, employee security training, and regular data backups. Have strong passwords, at least 12 digits, with numbers, uppercase, lowercase, and characters. First of all, a good antivirus and spam stop servers Pins, fingerprints, facial scans, etc Implement network firewalls to control and monitor traffic in and out of the organization's network and block potential threats. Two-factor authentication One of the most common ones that people don't take seriously is about social media, they just add passwords related to their pet's name or something easier like: 123456, it's best to avoid that kind of thing. Private ID Two-step verification, by a single key 2-Step Verification Call an engineer who specialized in that area Changing passwords from time to time Physical servers. Standard Antivirus Backup/Use Harder Passwords Passwords and so on Two-step security Use antivirus or a secure browser Two-factor authentication Phone Number Physical Keys 2-step security and mobile confirmation Falcon Strike Make a password or backup depending on the app you're using A strong password and 2-factor authentication. VPNs and security practices that depend on the area of work The measure is that we should always be discreet with our online passwords By signing up for a security package that contains antivirus, etc. Encryption of information. Use a strong password Put a good password don't get into any side or pages Antivirus Changing your password Don't Install Unknown Apps Not for security, but for invasion, several, one of them the Pegasus Passwords and keys password Change Password Two-factor authentication QoS Protection Strong password Use of anti-virus on computers, awareness of safe computer use

Two-step insurance Cloud Security Support and back-up? Strong passwords Two-step verification Have a password, hire a security package Two-factor authentication for security Do not enter unknown websites and make the backup Backup, to save data and protect it. Cookies Cloud Security Two-factor authentications Constant change of passwords, reinforcement in the I.P Tighter data access controls Pattern & Fingerprint 2-step verification Two-step verification VPN Avat Antivirus Strong passwords, anti-virus and anti-malware and backups. Change your password from time to time Data Encryption 2-Factor Authentication Method Constantly changing my passwords and not revealing too much information. Log off -Change your password every 1 month -Keep your account up to date Two-step authentication security They often use passwords of numbers and letters, patterns, and fingerprint locks Secure emails and passwords One of the most basic security measures would be to change the password multiple times Hire ethical hackers to detect vulnerabilities and fix security issues Do not enter illegal pages because they have ads, and may some of the ads are malicious, use an ad blocker or do not enter the page. No knowledge Work in the cloud
12- Can you name at least three examples of digital appropriation mechanisms used to obtain information in an unauthorized way? 146 replies
Twenty respondents did not mention any examples, indicating that they did not know them. While the others wrote names of the appropriate mechanisms: Pishing They include phishing, malware, ransomware, brute force attacks, social engineering, and phishing attacks. Phishing - Malware - Social Engineering Phishing Spam Malware Antivirus, security software, plans and pins Phishing: Attackers send spoofed emails that appear to come from legitimate sources, such as banks or online services, with the goal of tricking people into revealing sensitive information Brute force attacks: In these attacks, cybercriminals try to guess passwords by repeatedly trying different combinations until they find the right one Malware and viruses: Attackers can use malicious software, such as viruses, Trojans, or ransomware, to infiltrate computer systems and gain unauthorized access to sensitive information. Fishing, spoofing, social engineering Phishing: Phishing is a technique in which attackers send fake emails or messages that appear to be from legitimate sources, such as well-known banks or companies. Social engineering attacks: In social engineering attacks, criminals manipulate people into divulging sensitive information. Malware: Malware is malicious software that is installed on a victim's device without their knowledge or consent. Social Media, Virtual Assistants, and Streaming Platforms

Obtaining data by impersonating a website, scanning keys by means of a virus, by means of unofficial programs

Pishing, malware, spoofing

Emails, passwords, fake pages that ask you to fill in your details

Pishing Rich Identity Scams

Phishing. Maleante. Form grabbing

Data Hijacking (Rasomware)

Fhishing

Computer Damage Pishing Virus

Nmap, camphish

Pishing, malware, ataque DOS

Other URLs

Masking Pages for Stealing Passwords, Remote Desktop Access, Write Grabbers

Keylogger, Pishing y Malware

It could be participation in online communities, which can be related to personal interests. Online learning, they can find tutorials, videos, and gain knowledge or information. Using hacking unethically to steal data.

I don't have the slightest idea

Computer viruses, tracking and spyware disguised as commonly used programs and viruses that overload computers with illicit intentions (mining, extortion, violation of privacy, use of IP in the name of another, illegal mining, etc.)

Using false identity, stealing photos, impersonating another person

Firewall, antivirus, firewall

Fake pages

Hack

By link, by stikes the truth there are many things that can be accessed to your information

Phishing, Trojans, email spam.

Fishing back door and the use of the various malicious viruses used (which are extremely effective)

I have no idea how to do it

hackers, go on a hacking page and enter your data and write down your data and valuable information instead of anyone being able to access it

Pishing, doS attack

-installation of malicious apps that access personal information - -

Through spam emails, or files with viruses

Ndaikuaai

Obtain information from data-stealing sites

No, I don't have clear examples

Cloning, kchers and by network

The vdd nose

QR Scanning, Malicious Virus Link, Artificial Intelligence

Keyloggers, chip clones, page clones

It can be extortion, some copies of devices

Malware, SQL injection, Phishing.

Lever: A rigid device that pivots on a point (fulcrum) and is used to transmit force. Pulley: A disc with a hole or groove for a rope, used to lift or move loads by transmitting force through the rope. Gear: A set of sprockets that trick each other to transmit motion and change the speed or direction of motion.

At the moment I don't know yet

Malicious links

Pishing- Keylover- Attacks through free wifi networks

I don't know of any

Phishing, key loger

Phishing Malware Social Engineering

Extortion, malware, some kind of malicious link.

-scam -spyware -malware

Phishing, key logger

By means of links, cookies or strange calls

-Enter your email and password -Personal data -Confidential information

Phishing Keylogger Robo de cookies

Don't trust any app Don't open attachments from unknown emails Keep your operating system up to date

Emails that have never been changed Sharing inappropriate links

By means of links Cookies on the pages
Pishing, account access, scams.
Blackmail, unauthorized access to someone else's computer, some program created that asks for the user's data.
Fhishing
Hacking, Malware, and Social Engineering
Impersonating a Google assistant, making fake prizes online in order to get someone to register and enter an account and password, impersonating WhatsApp support to ask for account verification codes, and stealing WhatsApp numbers
Through unsafe links. Malware. Virus
Phinshing Malware Social Engineering
Malicious links and virtual scammers
Extortion or copying of bank details
Misleading Messages or Links
social media, scams, and phishing.
Entering unknown links Sharing password and email carelessly
Viruses, malicious pages
Blackmail, network invasion, hacked of personal information
-Installation of malicious applications - -
Phishing Social Engineering Brute Force Attack

4 CONCLUSION AND RECOMMENDATIONS

The research entitled "Unveiling the Code: A Review of the Knowledge and Awareness of Computer Engineering Students at UPE-CPF on Digital Appropriation Mechanisms" provides in-depth and valuable insight into the understanding and awareness of Computer Engineering students in relation to digital appropriation mechanisms. From the findings presented in this work, several key conclusions can be drawn, fulfilling the different specific objectives and in relation to the research hypothesis, it was refuted, since the students do not have a high level of knowledge about the mechanisms of digital appropriation:

1. Need for Awareness: The research highlights the importance of increasing awareness among computer engineering students about the mechanisms of digital appropriation. Digital appropriation has become essential in today's age of technology, and students in this discipline must be prepared to understand and apply it effectively.
2. Knowledge Gap: It also highlights that there is a gap in students' knowledge regarding digital appropriation mechanisms. This suggests the need for improved education and training in this field to ensure that future IT professionals are well-informed and can address digital challenges effectively.
3. Importance of Education: The results of the questionnaire responses underscore the importance of a solid education in Computer Engineering that includes a solid understanding of aspects related to digital appropriation. Educational programs should be reviewed and updated to ensure that they address these issues appropriately.
4. Challenges and Opportunities: The review also identifies challenges and opportunities in the realm of digital appropriation. Students should be prepared to face challenges such as

cybersecurity, data privacy, and digital ethics, but they can also take advantage of opportunities for innovation and the development of responsible technology solutions.

5. Shared Responsibility: The findings in the fieldwork highlight that the responsibility for improving knowledge and awareness of digital appropriation mechanisms does not fall solely on students, but must also be assumed by educational institutions, teachers, and the technology industry.

In conclusion, "Unveiling the Code" sheds light on the importance of addressing digital appropriation in the education of Computer Engineering students and underlines the need for action to close the knowledge gap in this area. This review serves as a call to action to improve the readiness of future IT professionals and ensure they are equipped to effectively navigate an increasingly digital world.

REFERENCES

Aguilerra López, P. Editerc. (s.f.) Troyanos. Informática y comunicación. https://books.google.es/books?hl=es&lr=&id=Mgvm3AYIT64C&oi=fnd&pg=PA1&dq=que+es+un+Adwares+&ots=PrppWzCHR2&sig=o8MWjP4HZDqnhkfYvGxZwaX8hr4#v=onepage&q=troy

Adwares. https://books.google.com.py/books?id=WHCUYnQ2hz0C&pg=PA9&dq=que+es+un+Adware&hl=es&sa=X&ved=2ahUKEwi33dqt3_z6AhUZjZUCHZ8mBmkQ6AF6BAgKEAI#v=onepage&q=que%20es%20un%20Adware&f=false

Castañeda Meza, L. R. (2021). Revisión sistemática de literatura sobre competencias de uso y apropiación de las TIC en estudiantes virtuales de posgrado (Doctoral dissertation, Corporación Universitaria Minuto de Dios). https://repository.uniminuto.edu/handle/10656/14037

Cerra, M. (2010). Spyware. Seguridad. USERS. https://books.google.com.py/books?id=WHCUYnQ2hz0C&pg=PA102&dq=que+es+el+Spyware&hl=es&sa=X&ved=2ahUKEwj2qdj73_z6AhUIr5UCHd_7D1EQ6AF6BAgIEAI#v=onepage&q=que%20es%20el%20Spyware&f=false

de Luna, E. L. B., García, S. M. A., & de Dios Naranjo, M. E. P. ESTADO DEL ARTE DE LAS COMPETENCIAS DIGITALES PARA LA INNOVACIÓN DOCENTE EN EL ÁMBITO UNIVERSITARIO. PRÁCTICAS SOCIOEDUCATIVAS EN INVESTIGACIÓN, 59. https://ri.ujat.mx/bitstream/20.500.12107/3595/1/4.pdf#page=59

de Cali, S. (2022). PROYECTO EDUCATIVO DEL PROGRAMA DE INGENIERÍA INFORMÁTICA. https://www.uao.edu.co/wp-content/uploads/2023/09/PEP-Ingenier%C3%ADa-Inform%C3%A1tica.pdf

Ferreres Franco, C. (2011). La integración de las tecnologías de la información y de la comunicación en el área de la educación física de secundaria: análisis sobre el uso, nivel de conocimientos y actitudes hacia las TIC y de sus posibles aplicaciones educativas. https://www.tdx.cat/handle/10803/52837

Giraldo Gómez, L. Y. (2014). Competencias mínimas en pensamiento computacional que debe tener un estudiante aspirante a la media técnica para mejorar su desempeño en la media técnica de las instituciones educativas de la alianza futuro digital Medellín (Doctoral dissertation, Universidad EAFIT). https://repository.eafit.edu.co/handle/10784/4488?locale-attribute=es

Herrera Leyva, R. Y. (2018). Nivel de conocimiento que tienen estudiantes de pregrado de Lima sobre mecanismos para el robo de información digital. https://repositorio.usil.edu.pe/items/62895322-f1a3-4e41-923b-d0567c0bf021

Jara Delgado, C. J. (2017). Relación entre el nivel de conocimiento y el uso de las Tecnologías de Información y Comunicación en la formación académica de los estudiantes de Estomatología del Octavo y Noveno Ciclo en el año 2017. https://repositorio.uap.edu.pe/handle/20.500.12990/1417

Luz, C. G. M. (2018). Educación y tecnología: estrategias didácticas para la integración de las TIC. Editorial UNED. https://books.google.es/books?hl=es&lr=&id=KG5aDwAAQBAJ&oi=fnd&pg=PT5&dq=REVISI%C3%93N+DEL+CONOCIMIENTO+Y+CONCIENCIACI%C3%93N+DE+LOS+ESTUDIANTES+DE+INGENIER%C3%8DA+INFORM%C3%81TICA+SOBRE+LOS+MECANISMOS+DE+APROPIACI%C3%93N+DIGITAL&ots=Ov-QKzboMy&sig=O--KaqVeosQ8CKtHCn0dcYZrJDQ#v=onepage&q&f=false

Quintana-Nevárez, A. Robo de información, mas común de lo que todos creen. https://www.researchgate.net/profile/Alberto-Quintana-Nevarez/publication/314772203_Robo_de_informacion_mas_comun_de_lo_que_todos_creen/links/58c5e88fa6fdcce648e8b804/Robo-de-informacion-mas-comun-de-lo-que-todos-creen.pdf Robo de información, más común de lo que todos creen.

Quintana Narvaez, A. (2017). Robo de información, mas común de lo que todos creen. /links/58c5e88fa6fdcce648e8b804/Robo-de-informacion-mas-comun-de-lo-que-todos-creen.pdf

Rivera, F. C., Hermosilla, P., Delgadillo, J., & Echeverría, D. (2021). Propuesta de construcción de competencias de innovación en la formación de ingenieros en el contexto de la industria 4.0 y los objetivos de desarrollo sostenible (ODS). Formación universitaria, 14(2), 75-84. https://www.scielo.cl/scielo.php?pid=S0718-50062021000200075&script=sci_arttext&tlng=en

Rootkit

https://books.google.com.py/books?id=ZqHDDwAAQBAJ&pg=PT143&dq=que+es+es+un+Rootkit&hl=es&sa=X&ved=2ahUKEwjF1_iU3_z6AhURiJUCHZU4D-IQ6AF6BAgNEAI#v=onepage&q=que%20es%20es%20un%20Rootkit&f=false

Spam de Correos

https://books.google.es/books?hl=es&lr=&id=Mgvm3AYIT64C&oi=fnd&pg=PA1&dq=que+es+un+Adwares+&ots=PrppWzCHR2&sig=o8MWjP4HZDqnhkfYvGxZwaX8hr4#v=snippet&q=Spam&f=false

Torres, M. I. (2021). Aportes para una apropiación crítica de conocimientos y usos de hardware y software de programación y robótica en la educación para la primera infancia de Argentina (Master's thesis). https://rdu.unc.edu.ar/handle/11086/23970

Postigo Palacios, A. (20220) Smishing. Sistemas microinformáticos y redes. Paraninfo. Gráfica Summa. España.
https://books.google.com.py/books?id=UCjnDwAAQBAJ&pg=PA126&dq=que+smishing&hl=es&sa=X&ved=2ahUKEwiNmNLL3vz6AhVmI7kGHQXbBwsQ6AF6BAgNEAI#v=onepage&q=que%20smishing&f=false