South American Publishing

SAP Netnography. 2024;2:98
doi: 10.62486/net202498

ORIGINAL

Criminal profiling of cybercriminals: Analysis on motivations and traits of hackers

Perfilación criminal de los ciberdelincuentes: Análisis sobre motivaciones y rasgos de los hackers

Rocío Magalí Méndez[1]
María Inés Lanza[1]

[1] Universidad Siglo 21, Licenciatura en Criminología y Seguridad. Bahía Blanca, Buenos Aires. Argentina.

Submitted: 28-05-2024 | Revised: 01-09-2024 | Accepted: 22-12-2024 | Published: 23-12-2024

ABSTRACT

The present research conducted an approach to the criminal profiling of cybercriminals, based on the analysis of criminal behavior and statistics of hackers. This descriptive and explanatory analysis, carried out through interviews, surveys, and data collection from cybercrime victims, news, and laws, examined various behaviors, patterns, and traits of hackers. It was possible to conclude the lack or outdated nature of legal regulation on the subject. It is necessary to update our legislation to adapt to the technological changes that occur every day. Despite the fact that the inherent characteristics of cybercrimes involve occurrences in an intangible space, getting to know the types of individuals who commit them could help in preventing them.

Keywords: Hackers; Cybercrimes; Cybercriminals; Technology.

RESUMEN

La presente investigación, realizó una aproximación a la perfilación criminal de los ciberdelincuentes, basado en el análisis de la conducta criminal y estadísticas de los hackers. Este análisis descriptivo y explicativo, realizado en base a entrevistas, encuestas y recopilación de datos obtenidos de víctimas de la ciberdelincuencia, noticias y leyes, examinó las distintas conductas, patrones y rasgos de los hackers. Se pudo concluir la falta o desactualización de regulación legal en la temática. Es necesario actualizar nuestra legislación para que se adapte a los cambios tecnológicos que se desarrollan día a día. Más allá de que las características propias de los delitos informáticos es que ocurran en un espacio intangible, el hecho de acercarnos a conocer los tipos de personas que los realizan podría ayudar a prevenirlos.

Palabras clave: Hackers; Ciberdelitos; Ciberdelincuentes; Tecnología.

Introduction

The analysis of criminal behavior, as a novel specialty, was built on various contributions from criminology and the behavioral sciences applied to the field of criminalistics practice. The use of psychology to understand and prevent criminality must be considered from the origins of psychological science.

The construction of psychological profiles was based mainly on the consideration, use, and development of classifications specific to psychiatry, which ended up pigeonholing criminals into possible diagnoses of mental illnesses. Over time, various theories were developed that began to consider other types of factors beyond psychological ones, which are fundamental for a more precise and accurate approach to the profile of a criminal.

There are multiple methodologies, developments, and conceptual definitions that are beginning to emerge. Ressler considers contributions made from the United States and points out that the criminal profile has been described as a sum of clues, as an attempt to gather specific information, and as a biographical sketch of behavior patterns. On the other hand, Holmes et al. consider three main objectives that emerge from the analysis and psychological study of the offender:

1. An approach to assessing the offender's personality from social and psychological criminology.
2. Consideration of the possible inferences regarding the offender's belongings found at the different crime scenes.
3. To lay the foundations for possible lines of inquiry and key hypotheses in criminal investigation.

These authors suggest that not all cases are analyzable. In this context, criminal profiling seeks to generate an approximation of the characteristics of the alleged aggressor, which allows narrowing the scope of the investigation and focusing on more accurate and defined aspects.

Following Velasco de la Fuente, the technique can be applied in cases of seriality, especially in violent crimes, since repetition makes it possible to determine the presence or absence of a guideline or behavior pattern, which entails high social mobilization and prompt intervention.

The methodology for constructing a criminal profile consists of analyzing and evaluating different aspects:

- The crime scene is the place and space that the offender has chosen to commit a crime.
- Modus operandi refers to the method or manner of operating. It mainly considers the manner or method that the aggressor has used to commit the crime. From its analysis, information is gathered about how the criminal acts, which makes it possible to delimit and approximate the psychological characteristics inferable from their way of acting.
- The detailed study of the information provided by the modus operandi of criminals allows defining clues.
- The signature, according to Robert Keppel, constitutes part of the crime scene that involves different expressions of the criminal's fantasies; that is, it is the set of actions that are not necessary to commit the crime. The signature tends to be among the main patterns that make it possible to establish seriality across different events, making it possible to attribute them to a single offender.
- Serial crime analysis is complemented by geographic analysis. Various theories explain the spatial behavior of the perpetrator of an incident in order to establish whether a relationship exists between these locations and the offender's routines. This profile describes the spatial behavior and the areas in which the offender moves, crime scenes, anchor points of criminal events, risk areas, base of operations, etc.

The objective of this research is to develop the criminal profile of cybercriminals, particularly of "hackers," by conducting an exhaustive analysis of the literature and laws regulating this type of crime, identifying the main trends and gaps in research, collecting and analyzing data from interviews with "ethical hackers," performing a quantitative analysis, analyzing the ethical implications of the research, and contributing to existing knowledge, in order to identify and establish a psychological profile of hackers to uncover them and prevent their crimes early.

The Argentine Justice defines cybercrime as illegal conduct carried out by cybercriminals in cyberspace through electronic devices and computer networks. It consists of scams, theft of personal data and strategic commercial information, identity impersonation, computer fraud, and attacks such as cyberbullying, grooming, and phishing, committed by cybercriminals who act in groups or work alone.(1)

Regarding the laws that address cybersecurity in the country, the following can be mentioned:

- Law 26.388 on Computer Crime: It establishes penalties for the crimes of disseminating photos of minors under 18 years of age, for anyone who improperly accesses an electronic communication, anyone who accesses a computer system or data with restricted access, and for

anyone who defrauds another through any computer manipulation technique that alters the normal functioning of a computer system or data transmission. The last amendment to this law was in 2008. It remains highly outdated for new methods of data access.

- Law 25.326: Personal Data Protection Act, habeas data. Its purpose is the comprehensive protection of personal data stored in files, records, databases, or other technical means of data processing, whether public or private, intended to provide reports, in order to guarantee the right to honor and privacy of individuals, as well as access to the information recorded about them. Its last amendment was in the year 2000.
- Law 25506: Digital Signature Law. It recognizes the use of electronic signatures and digital signatures and their legal validity under the conditions established by this law. Enacted in 2001.
- Law 26904. Grooming Law. It establishes penalties for anyone who, by means of electronic communications, telecommunications, or any other data transmission technology, contacts one person who is a minor, with the purpose of committing any crime against the sexual integrity of that person. It was enacted

in 2013 and is the most recent law on the subject of cybercrime.

Other regulations to mention are:

- Administrative Decision 641/2021. Establishes the minimum information security requirements for public agencies
- Provision 6/2021. Creation of the Advisory Committee for the Development and Implementation of Secure Applications.
- Provision 1/2021. National Center for Computer Incident Response (CERT.ar) within the scope of the National Directorate of Cybersecurity.
- Resolution 580/2011. Creation of the National Program for the Protection of Critical Information Infrastructures and Cybersecurity.
- ONTI Resolution 3/2013. Approval of the Model Information Security Policy.
- Resolution 1523/2019. Definition of Critical Infrastructures.
- Decree 577/2017. Creation of the Cybersecurity Committee.
- Decree 480/2019. Amendment to Decree 577/2017.
- Resolution 829/2019. Approval of the National Cybersecurity Strategy.
- Resolution 141/2019. Presidency of the Cybersecurity Committee.

Cyberspace is an intangible area that any person can access with a computer from their home, workplace, or mobile devices. Cybercriminals use technological means such as: internet, computers, cell phones, 3G and 4G communication networks, fiber optic networks, and software.

Cybercrime can arrive in many ways: insecure websites, social media, holes created by security vulnerabilities, weak passwords on accounts and smart devices, and, above all, email.

Cybercrimes are committed through malicious programs developed to delete, damage, deteriorate, make inaccessible, alter, or suppress computer data without your authorization and for economic and damaging purposes. Some examples are:

- Attacks in your browsing: they redirect your browser to pages that cause infections with malicious programs such as viruses, worms, and Trojans. These programs can erase your operating system, infect your phone and your computer, activate your webcam, extract data, etc.
- Attacks on servers: they can damage or steal your data and deny you access to your information.
- Database corruption: interfering with public or private databases to generate false data or steal information.
- Computer viruses: encrypt files, lock smart locks, steal money from cell phones with text messages that appear to be from the company.
- Spyware: some of the devices have installed software that allows them to turn on and record with the camera and microphone. It can also access your personal information without authorization and without your knowledge.

Cybercriminals use social engineering to deceive, threaten, and obtain personal data or information from other people or organizations, obtain money, impersonate identities, and engage in digital and sexual harassment. Some examples are:

- Phishing or vishing: cybercriminals impersonate service companies, government offices, or friends of a family member and ask you for the data they are missing to impersonate your identity and thereby operate your bank accounts, profiles on platforms and social networks, services, and web applications.
- Cyberbullying: it is harassment via instant messaging, stalking on WhatsApp, Telegram, Facebook Messenger, and on social media with the intention of pursuing, stalking, defaming, and attacking the honor and moral integrity of one person. This is done through the discovery and revelation of secrets, the publication of offensive or discriminatory comments or videos,

the creation of memes, or the tagging of your posts.
- Grooming: this refers to adults who, in a concealed manner, attempt to obtain sexual photographs or videos of minors for subsequent blackmail or prior to sexual abuse.
- Sextortion: consists of asking for money in exchange for not disseminating on social networks images generated for a consensual erotic exchange.
- Cyberhate: it refers to inappropriate content that can harm people. Violence, messages that incite hatred, xenophobia, racism, and discrimination or animal abuse are considered cyberhate.
- Child pornography: This term refers to the corruption of minors and their sexual exploitation for the production and commercialization of images and videos depicting explicit sexual activity.
- Unlawful espionage targeting citizens' private communications.
- Violation of privacy by Internet service provider companies without users' consent, in order to learn their tastes and preferences and establish the aggressive sale of associated products and services.
- Illegal access to a worker's private communications (emails, social media, etc.)

During the last few years we have witnessed the increase in the acceleration in the process of adoption of new technologies, particularly after the long periods of isolation due to the prophylaxis measures due to the COVID-19 pandemic, which meant that many people had to start working through computer devices almost totally, and in many cases without the prevention elements or the necessary training to prevent the aforementioned types of crimes. Investigating the criminal profile of hackers is intriguing for today's society for several reasons. First, it allows for a deeper understanding of the motivations that drive some people to engage in online criminal activities. This is essential for developing effective prevention strategies and cybersecurity policies. In addition, an in-depth study of these profiles can significantly contribute to improving cybersecurity in an increasingly digitized world. Knowledge of how criminal hackers think and operate is essential to strengthen organizations' defenses and better protect sensitive systems and data. It is also important to note that researching the profile of criminal hackers can help identify trends and patterns in their criminal activities. This can be of great use to both law enforcement and cyber security agencies, as it allows them to adapt their strategies to combat online threats more effectively. In addition, contributing to the understanding of the field of cybersecurity is an additional benefit. By documenting and analyzing the criminal profiles of hackers, collective knowledge in this field can be enriched and help the community to be better prepared to face the ever-evolving cyber threats.

It is essential to remember that any research in this field must be conducted ethically and legally, respecting applicable laws and regulations, as well as the privacy of the individuals involved in the research. Furthermore, due to the constantly evolving nature of cybersecurity, it is essential to stay updated on the latest online trends and threats in order to conduct effective and relevant research.

According to the Asociación Argentina de Lucha Contra el Cibercrimen,(2) a slight decrease is observed in consulted cases in 2021 compared with 2020. During 2021, CERT.ar registered a total of 591 computer incidents, a figure that exceeded that of 2020 by 261 %, when 226 incidents were registered. For now, only 18 of the cases registered in 2021 are open, so work is still being done on them. The remaining 573 incidents are closed. In 2020, the rise in cases compared with previous years was considerable, mainly cases of fraud, data theft, and digital extortion due to the strict quarantine decreed in the country in the second and third quarters. In 2021, a significant percentage normalized their usual way of working, others managed to train in preventive matters, and the different awareness campaigns by government, civil society organizations, and the media likewise achieved, to a certain extent, a positive effect on prevention.

In Argentina, according to the Characterization of Organized Crime published by the official Argentine government website "argentina.gob.ar",(3) the most common crimes are: drug trafficking, arms trafficking, illegal sale of auto parts, smuggling of merchandise, money laundering, and cybercrimes.

Cybercrime has grown in importance as computers have become a central part of commerce, entertainment, and government. A cybercriminal does not differ from a criminal in the physical world. Undoubtedly, some manifestations are new, but a large number of crimes committed with or against computers differ only in terms of the medium used. In the book "The Digital Trace of Crime: Technical, Legal, and Strategic Aspects of Computer Forensics,"(4) its authors conclude regarding computer forensics; the dynamics of human evolution and its technological advancement have brought a new paradigm in the field, generating new crime scenes with virtual characteristics that coexist with physical ones; new writings that are not on paper media and to which it is not possible to apply the scopometric method that has yielded such good results for Documentology. The digitization of information has made it so that a trace of a fingerprint must no longer be sought

with a chemical or magnetic reagent, but with complex computational tools that search for that hidden clue, that trace, in a binary code, an algorithm.

Real-world criminals make the decision to commit crimes, so, faced with a change in the paradigm of citizens' habits, it is to be expected that criminals would have the motivation to shift toward cybercrime. According to the RAE, one hacker or computer pirate is a person with great computer-handling skills who investigates a computer system in order to report faults and develop improvement techniques. Fortunately, not all hackers or computer pirates use their knowledge in the same way; there are different types of hackers.

The general classification is composed of three types: Black Hat, Grey Hat, and White Hat, but over the years it has diversified the types until forming a long list; the main ones would be:(5)

- Black Hats, also called cybercriminals, are hackers who access unauthorized systems or networks to inflict damage, gain access to financial information, personal data, and passwords, and introduce viruses. Within this classification, there are two types: Crackers and Phreakers; the former modify software, create malware, crash servers, and infect networks, while the latter operate in the field of telecommunications.
- For Grey Hats, ethics depend on the time and place; they provide their services to intelligence agencies, large corporations, or governments, and disclose useful information for a modest price.
- White Hats, or ethical hackers, dedicate themselves to research and report vulnerabilities or flaws in security systems.
- Newbies have little experience or knowledge, as they have just entered the field of cybersecurity; they are the novices of hacking.
- Hacktivists have grown in number in recent years; they use their skills to attack networks for political purposes. Among the most representative examples is Anonymous.

Other Types of Hackers

- Phreakers: They are hackers who focus on manipulating or exploiting telecommunications technology, especially telephone systems.
- Social engineering hackers: They are hackers who use psychological manipulation techniques to obtain confidential information or gain access to computer systems. They may use tactics such as deception, impersonation, persuasion, and emotional manipulation.
- Hardware hackers: They are hackers who focus on the manipulation or exploitation of physical devices, such as credit cards, security cameras, or industrial control systems.
- Network hackers: They are hackers who focus on exploiting vulnerabilities in computer networks and communication systems.

Computer security involves not only the use of strong passwords and updating software and antivirus, but also education and awareness about potential threats. Citizens can take simple measures, such as avoiding sharing confidential information on social media or using complex passwords, while organizations must implement security policies and conduct risk assessments and penetration tests to identify potential vulnerabilities.

Among the main threats is malware (computer viruses), especially the type known as ransomware, malicious software that encrypts computer files and then demands money or, generally, cryptocurrencies in exchange for returning the hijacked information.

Both private companies and state organizations are victims on a daily basis. Some examples of companies and public agencies hacked in recent years in our country include: the Public Prosecutor's Office,(6) CONICET,(7) the Senate of the Nation,(8) Migraciones,(9) Correo Argentino,(10) PAMI,(11) among others.

In August 2022, the computer system of the Poder Judicial de la Provincia de Córdoba suffered an attack that affected its official website, digital services, and the databases containing the case files. This event led to technological investment becoming a priority for the Poder Judicial de Córdoba for the year 2023.(12,13,14)

METHODS

In this research work, a methodology will be adopted that is framed within a descriptive and qualitative approach. This approach has been carefully selected due to its suitability for the objective of our study, which is to understand and analyze in depth the criminal profile of hackers.

The descriptive methodology will focus on the collection of data from various sources to provide a detailed and accurate description of the relevant aspects related to criminal hackers. To this end, a bibliographic review of the area will be carried out, reviewing books, academic articles,

and other resources that address topics related to cybersecurity and hacking.

In addition to the literature review, online research will be conducted to track and analyze web publications related to the topic. Since the field of cybersecurity and hacking is highly dynamic and constantly evolving, this online research will make it possible to capture the most recent trends and developments in the area of criminal hackers.

A fundamental part of the qualitative methodology will consist of conducting interviews with specialists at conventions and conferences related to hackers and cybersecurity. These interviews will provide valuable first-hand information, insights, and perspectives from experts in the field, which will significantly enrich the analysis.

In summary, this research will be based on a solid qualitative database collected from bibliographic sources, web publications, and interviews with specialists. The descriptive approach will allow us to provide a complete and detailed overview of the criminal profile of hackers, while the qualitative approach will help to better understand the motivations, strategies, and trends behind their criminal activities. This comprehensive approach will make it possible to effectively address the complexity of this constantly evolving topic.

RESULTS

Black Hat is a security conference that brings together hundreds of hackers from around the world; it demonstrated the existence of vulnerabilities in objects that would be unthinkable for ordinary users. However, a curious aspect is the very nature of the presenters at Black Hat: security gurus who refer to themselves, and proudly, as "hackers." At this point, a brief clarification is necessary: unlike cybercriminals, hackers do not necessarily dedicate themselves to stealing people's money. To understand the motivations of these computer geniuses, Thycotic, a well-known security company, conducted a survey of more than 100 hackers who attended Black Hat, with the aim of determining what drives them to hack certain systems and what their preferred strategies are.

The survey yielded several striking results. 86% of hackers are convinced that they will never be punished for their actions and assume no responsibility whatsoever for the consequences. Apparently, impunity is the initial motivation for cybercrime.

40% of hackers state that their primary target for an attack would be the company's contractors.

Another interesting point is whom hackers would choose among a company's personnel as the target of an attack in order to infiltrate a system. 40% of respondents state that their first option would be the company's contractors, since they have access to corporate networks and are not fully regulated by security policies.

Interestingly, IT administrators (IT being the English acronym for "Information Technology") are the second option. Although IT staff, at least in theory, should be fully prepared to handle an attack of this type, 30% of hackers stated that they would target these administrators to gain access to the company's network.

The survey results surprised us, since Thycotic's list did not include human resources staff, who are traditionally identified as the potentially most vulnerable target for an attack.

On the other hand, the survey also revealed that 51% of hackers usually carry out attacks for the mere fun of doing so. However, 30% of respondents claim that they never violate their ethical principles.

Finally, 88% of hackers state that, despite having extensive computing capabilities and knowledge, even they are not exempt from becoming victims of an attack or of a massive data theft perpetrated by other hackers.

DISCUSSION

Analysis of the data obtained indicates that the profile of hackers is mostly male (approximately 90%). 80% are under 30 years of age. Most have above-average logical-mathematical intelligence compared with the general population and come from upper-middle-class socioeconomic backgrounds. They are not the type of offenders who act out of economic necessity. The main motive of most of them is self-improvement and the search for "new sensations," fun, and the adrenaline from offending, in addition to proving to themselves that they are capable and better than large companies. They are people who, even though they could use their skills for good and have no socioeconomic needs to meet, decide to offend. In their exact words, "I analyze people, look for

vulnerabilities, and manipulate them." That is, they are people who use social engineering; on a large scale, they are people with narcissistic traits (15,16).

For the psychological analysis, I used Eysenck's PEN model of personality (17). This model is based on the idea that personality can be understood in terms of three fundamental factors: psychoticism (P), extraversion (E), and neuroticism (N). Psychoticism refers to one's tendency to display traits such as aggression, impulsivity, emotional insensitivity, and lack of empathy. People with high levels of psychoticism tend to be more daring, dominant, and prone to antisocial behaviors. They may show a lower ability to understand others' emotions and may lack empathy toward others. The extraversion factor (E) is related to sociability, stimulation seeking, and energy. Extraverted people tend to be energetic, sociable, and talkative and to seek social interaction. They enjoy being surrounded by other people and may display greater extraversion in social situations. Extraverts often seek external stimuli and may enjoy activities that involve interaction with other people. Neuroticism (N) is another important factor in the PEN model. It refers to the tendency to experience negative emotions, such as anxiety, emotional instability, and a propensity to worry. People with high levels of neuroticism tend to be more prone to experience stress and negative emotions in challenging situations. They may be more sensitive to changes in their environment and may have difficulty managing stress. It is important to note that these factors are not absolute or determinative, but rather represent general tendencies in personality. Each individual is unique and may show different levels of each factor at different times and in different situations.

A characteristic trait of hackers is coolness and the absence of nervousness—the ability to maintain control no matter what happens. They are individuals who can tolerate high levels of stress, tension, and anxiety. According to the PEN model of personality, they would score very low on neuroticism; they are individuals with considerable emotional stability. They do not become nervous and do not display anxiety or nervousness.

On the other hand, being a hacker requires spending a great deal of time alone, analyzing and studying. Hackers tend to be solitary people, less sociable than others. They are strongly introverted, analytical, calm, forward-thinking, and planning-oriented people. Many hackers are on the autism spectrum, with a high level of perception of detail and systematization. Other traits common to autism and hackers include obsessive-compulsive traits and a high capacity for concentration.

To conclude with the PEN concepts of personality, they are individuals with high psychoticism; they tend to have difficulties integrating into and adapting to society. They find it difficult to internalize social norms and are less sensitive to punishment. They have less social awareness. They are prone to criminal behaviors. They are intellectual, solitary, and independent individuals, socially viewed as "strange".

CONCLUSIONS

Another conclusion that can be drawn from this research is that, because technology is in constant development worldwide, and particularly in our country, it has not been possible to find a balance that would allow legal systems to adapt to its turbulence and constant change. Argentine legislation is not up to date; the laws that address cybercrime were amended more than 10 years ago, which lags far behind the permanent changes in cybercrime.

A prevention measure would be to implement a global cyber system to monitor and regulate online activities more effectively, identifying suspicious patterns and behaviors through advanced algorithms created by experts. In addition, the creation of a global database, permanently updated and shared among government entities and law enforcement agencies, could improve the capacity to track and pursue those engaged in online criminal activities. As another measure, more rigorous authentication mechanisms could be established to mitigate the problem of anonymity, requiring verifiable identification in various online interactions. Likewise, international cooperation would be fundamental, enabling the rapid transfer of information and the execution of coordinated actions to address cybercrimes that transcend borders. To strengthen this system, it would be crucial to invest in cutting-edge security technologies and in the continuous training of professionals dedicated to cybersecurity. Public awareness of cyber threats and the promotion of safe online practices should also be integral components of any global strategy to combat digital criminal activity.

REFERENCES

1. Argentina.gob.ar. Qué es el ciberdelito. 2023. Disponible en: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito
2. AALCC. Estadísticas 2021: informe sobre consultas en materia de delitos configurables a través de internet. 2021. Disponible en: https://www.cibercrimen.org.ar/2021/12/28/estadisticas-2021/
3. Argentina.gob.ar. Caracterización de la criminalidad organizada. 2022. Disponible en: https://www.argentina.gob.ar/seguridad/abordaje-crimen-organizado/criminalidad-organizada
4. Di Iorio AH, Castellote MA, et al. El rastro digital del delito: aspectos técnicos, legales y estratégicos de la informática forense. Mar del Plata: Grupo de Investigación en Sistemas Operativos e Informática Forense, Universidad FASTA; 2016.
5. Campus Ciberseguridad. Tipos de hackers. Disponible en: https://www.campusciberseguridad.com/blog/item/133-tipos-de-hackers
6. Diario Perfil. Un hackeo en el Ministerio Público Fiscal generó preocupación en el poder judicial. 2021. Disponible en: https://www.perfil.com/noticias/politica/hackeo-ministerio-publico-fiscal-genero-preocupacion-poderjudicial.phtml
7. Clarín. El CONICET víctima de ciberdelincuentes: roban datos y piden dinero para devolverlos. 2022. Disponible en: https://www.clarin.com/tecnologia/conicet-victima-ciberdelincuentes-roban-datos-piden-dinero-devolverlos_0_LFRRFW39jx.html
8. Clarín. El Senado de la Nación sufrió un ciberataque de tipo ransomware. 2021. Disponible en: https://www.clarin.com/tecnologia/senado-nacion-sufrio-ciberataque-ransomware-secuestrandatos-publicos_0_13uPrKQNd.html
9. La Nación. Migraciones: cómo fue el ataque del ransomware Netwalker y qué datos revela. 2020. Disponible en: https://www.lanacion.com.ar/tecnologia/migraciones-como-fue-ataque-del-ransomware-netwalker-nid2446451/
10. Correo Argentino. Alerta: usan el nombre de Correo Argentino para una nueva estafa virtual. 2021. Disponible en: https://www.correoargentino.com.ar/alerta-usan-el-nombre-de-correo-argentino-para-una-nuevaestafa-virtual
11. Infobae. Hackearon el sistema de PAMI: qué pasará con los turnos y con las recetas para medicamentos. 2023. Disponible en: https://www.infobae.com/economia/2023/08/02/hackearon-el-sistema-de-pami-que-pasara-con-los-turnos-y-con-las-recetas-para-medicamentos/
12. Comercio y Justicia. En 2023, la inversión tecnológica será prioridad para el Poder Judicial de Córdoba. 2022. Disponible en: https://comercioyjusticia.info/suplementoaniversario/2022/10/31/en-2023-la-inversion-tecnologica-sera-prioridad-para-el-poder-judicial-de-cordoba/
13. La Voz. Por el hackeo, el TSJ determinaría que el martes sea feriado judicial. 2022. Disponible en: https://www.lavoz.com.ar/sucesos/por-el-hackeo-el-tsj-determinaria-que-el-martes-sea-feriado-judicial/
14. La Voz. Colegio de Abogados, preocupado por ciberataque a la Justicia, pide explicaciones al Tribunal Superior. 2022. Disponible en: https://www.lavoz.com.ar/sucesos/colegio-de-abogados-preocupado-por-ciberataque-a-la-justicia-y-pide-explicaciones-al-tribunal-superior/
15. Kaspersky LATAM. Cuáles son las principales motivaciones de los hackers. Disponible en: https://latam.kaspersky.com/blog/cuales-son-las-principales-motivaciones-de-los-hackers/3853/
16. United Nations Office on Drugs and Crime (UNODC). Crimen organizado transnacional. 2020. Disponible en: https://www.unodc.org/ropan/es/organizedcrime.html
17. Mentes Abiertas Psicología. El modelo PEN de Eysenck: comprendiendo la personalidad desde una perspectiva científica. Disponible en: https://www.mentesabiertaspsicologia.com/blog-psicologia/blog-psicologia/el-modelo-pen-de-eysenck-comprendiendo-la-personalidad-desde-una-perspectiva-cientifica

FUNDING

None.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

AUTHORSHIP CONTRIBUTIONS

Conceptualization: Rocío Magalí Méndez, María Inés Lanza.
Data curation: Rocío Magalí Méndez, María Inés Lanza.
Formal analysis: Rocío Magalí Méndez, María Inés Lanza.
Investigation: Rocío Magalí Méndez, María Inés Lanza.
Methodology: Rocío Magalí Méndez, María Inés Lanza.
Project administration: Rocío Magalí Méndez, María Inés Lanza.
Software: Rocío Magalí Méndez, María Inés Lanza.
Supervision: Rocío Magalí Méndez, María Inés Lanza.
Validation: Rocío Magalí Méndez, María Inés Lanza.
Visualization: Rocío Magalí Méndez, María Inés Lanza.
Writing – original draft: Rocío Magalí Méndez, María Inés Lanza.
Writing – review and editing: Rocío Magalí Méndez, María Inés Lanza.