South American Publishing

SAP Netnography. 2024;2:95
doi: 10.62486/net202495

MINI-REVIEW

The evolution and classification of digital scams in the technological age

Evolución y tipificación de las estafas digitales en la era tecnológica

Sabrina Ivana Bof[1]

[1] Universidad Siglo XXI, Especialización en cibercrimen. Argentina.

Submitted: 25-05-2024 | Revised: 20-08-2024 | Accepted: 11-12-2024 | Published: 12-12-2024

ABSTRACT

Introduction: the purpose of the study was to analyze the phenomenon of cyber scams in Argentina, a problem that has become increasingly relevant in recent years. It was observed that the widespread use of information technology has created a new criminal landscape, where digital scams affect both individuals and institutions. According to data from the Specialized Cybercrime Prosecution Unit and CERT.ar, between 2022 and 2023 there was a significant increase in the number of computer incidents, especially fraud and identity theft, highlighting the expansion of the problem. Development: the paper addressed the main types of cyber scams, such as phishing, pharming, ransomware, vishing, malware, and social engineering, highlighting their sophistication and ability to adapt to new technologies. It also examined current Argentine legislation, in particular Law 26,388 on computer crimes and the Penal Code, noting that, although there had been regulatory advances, the provisions were insufficient to cover the complexity of these practices. Weaknesses were also identified in judicial specialization and inter-institutional coordination in the fight against cybercrime. Conclusion: the analysis concluded that cyber scams were a real and growing threat. It highlighted the need to update the legal framework, strengthen cooperation between public and private agencies, and promote digital education as a prevention tool. The fight against this type of crime required a comprehensive legal and technological approach that kept pace with digital transformation.

Keywords: Cyber Fraud; Computer Crimes; Phishing; Social Engineering; Argentine Criminal Code.

RESUMEN

Introducción: el estudio tuvo como propósito analizar el fenómeno de las ciberestafas en Argentina, un problema que adquirió creciente relevancia en los últimos años. Se observó que el uso masivo de las tecnologías de la información generó un nuevo escenario delictivo, donde las estafas digitales afectaron tanto a individuos como a instituciones. De acuerdo con datos de la Unidad Fiscal Especializada en Ciberdelincuencia y del CERT.ar, entre 2022 y 2023 se registró un aumento significativo en la cantidad de incidentes informáticos, especialmente en fraudes y suplantaciones de identidad, evidenciando la expansión del problema. Desarrollo: el trabajo abordó las principales modalidades de ciberestafas, tales como phishing, pharming, ransomware, vishing, malware e ingeniería social, destacando su sofisticación y capacidad para adaptarse a las nuevas tecnologías. Asimismo, se examinó la legislación argentina vigente, en particular la Ley 26.388 de delitos informáticos y el Código Penal, señalándose que, si bien existieron avances normativos, las disposiciones resultaron insuficientes para abarcar la complejidad de estas prácticas. También se identificaron debilidades en la especialización judicial y en la coordinación interinstitucional frente a la ciberdelincuencia. Conclusión: el análisis permitió concluir que las ciberestafas constituyeron una amenaza real y en expansión. Se evidenció la necesidad de actualizar el marco legal, fortalecer la cooperación entre organismos públicos y privados, y promover la educación digital como herramienta de prevención. La lucha contra este tipo de delitos exigió un enfoque integral, jurídico y tecnológico que acompañara el ritmo de la transformación digital.

Palabras clave: Ciberestafas; Delitos Informáticos; Phishing; Ingeniería Social; Código Penal Argentino.

INTRODUCTION

This work is motivated by the need to address a topic of considerable social and legal relevance: cyber fraud. In an increasingly connected world, these criminal modalities pose a growing challenge for authorities and society as a whole.

Cyber scams in Argentina have risen significantly in recent years. According to data from the Specialized Fiscal Unit on Cybercrime, cybercrimes increased by 38.5% between April 2022 and March 2023 compared with the previous year.(1)

Similarly, during the period between January 1 and December 31, 2023, the CERT.ar registered a total of 379 computer incidents on its management platform, a figure that increased by 13% compared to 2022, when 335 were registered.(2,3,4,5)

This trend is exacerbated by the sophistication of the techniques used by fraudsters, who constantly seek new ways to deceive their victims.

"Fraud cases, with 288 occurrences, represent 76% of the total reported incidents, indicating that this category was the most frequently recorded computer crime during the period analyzed. The detected types included unauthorized use of resources, copyright, identity theft, and phishing."(2,6,7,8,9)

DEVELOPMENT

The advancement of information and communication technologies (ICTs) has brought numerous benefits for personal, professional, economic, and commercial development; however, it has also created a new scenario for the commission of crimes: cyber frauds.(10,11)

In today's digital era, cyber scams have become an increasingly frequent and sophisticated threat. These criminal modalities, which are carried out through electronic or computer-based means, often occur through social media, dating applications, emails, and sales pages, among others, and have a significant impact on victims at both the individual and economic levels.(12,13)

Cyber scams are a type of crime committed by using information and communication technologies to deceive the victim and obtain an economic benefit, and "as in all cases of fraud, their configuration requires causing harm of a patrimonial nature to another person. The legally protected interest is patrimony in general, and what is punished are conducts that affect patrimony through the use of computer systems by the perpetrator."(14,15,16)

Cyber scams can vary greatly in how they are committed, but new forms include the following:(17,18,19,20,21)

a) Social engineering: Techniques used by cybercriminals to manipulate people and obtain confidential information or access to computer systems.(22)
b) Phishing: Phishing is a type of cyberattack that uses emails, text messages, phone calls, or fraudulent websites to deceive people and make them share confidential data, download malware, or otherwise expose themselves to cybercrime.(23,24)
c) Pharming: similar to Phishing, but here there is no decoy, rather a redirection to a fake web page, with the purpose of obtaining confidential information.(25)
d) Ransomware: Ransomware is a type of software generally used by cybercriminals to encrypt files or computer systems. The term includes all forms of malicious code, such as viruses and computer worms. Its purpose is "to hijack information" and, in this way, to prevent one person or organization from accessing their data or devices until a sum of money has been paid as ransom, which is often in cryptocurrencies to allow the cybercriminal to hide their trace. (26)
e) Vishing: It is a type of social engineering scam, in which the identity of a person or company or entity is impersonated through one phone call in order to obtain sensitive information from the victim.
f) Malware: This refers to malicious software that installs itself on victims' devices without their consent, with the objective of stealing information, controlling the device, or extorting the victim.

Although cyber frauds are currently being investigated and penalized, the absence of a specific regulatory framework creates various difficulties: (27,28,29)

- Imprecise legal classification: Existing criminal offenses do not always align perfectly with new forms of cyber fraud, which hinders their effective application.
- Insufficient penalties: The penalties prescribed for cyber fraud are often lenient relative to the severity of the damage they can cause.

- Lack of specialization: Many judicial departments lack a specialized body of investigators and judges for cybercrime, which can affect the quality of investigations and trials.

From a legal perspective, one of the main difficulties posed by cyber fraud is that technological developments occur more rapidly than legislative reforms. Criminal conduct can change its technical characteristics without altering its essential purpose: deceiving victims to obtain an unlawful economic benefit. Consequently, the legal response cannot depend exclusively on the creation of a separate criminal offense for every new fraudulent technique. It also requires technologically neutral provisions that can be applied to emerging methods without violating the principles of legality, precision, and legal certainty.

Another relevant aspect is the transnational nature of many cyber scams. The offender, the victim, the digital platform, and the financial accounts used to receive or transfer the funds may be located in different jurisdictions. This geographical dispersion creates difficulties in determining jurisdiction, obtaining electronic evidence, identifying perpetrators, and recovering stolen assets. Therefore, international cooperation and the rapid exchange of information among judicial authorities, financial institutions, telecommunications companies, and digital platforms are essential for an effective investigation.

The preservation of digital evidence also represents a central challenge. Emails, messages, access records, IP addresses, transaction data, and other electronic traces may be modified, deleted, or become unavailable over time. For this reason, victims must report incidents promptly and preserve all available documentation, while investigative authorities must apply procedures that protect the integrity, authenticity, and traceability of the evidence. An inadequate collection process may reduce its evidentiary value and hinder the identification and prosecution of those responsible.

The impact of cyber fraud should not be evaluated exclusively in terms of the amount of money lost. Victims may also experience anxiety, fear, loss of confidence in digital services, reputational damage, and the unauthorized disclosure of personal information. In cases involving identity theft, the consequences may continue even after the initial fraudulent transaction because the stolen data can be reused to commit additional crimes. Accordingly, the institutional response should include not only criminal investigation but also guidance, psychological support when necessary, protection of personal data, and mechanisms for reporting fraudulent financial operations.

Finally, prevention constitutes an indispensable component of any comprehensive strategy against cyber fraud. Criminal prosecution generally begins after the damage has already occurred, whereas digital literacy and early-warning mechanisms can reduce the likelihood of victimization. Public awareness campaigns should explain how to identify suspicious communications, verify the identity of alleged representatives of institutions, protect authentication credentials, and report fraudulent activities. At the same time, companies and public agencies should strengthen their security and verification systems, since responsibility for prevention cannot be placed exclusively on individual users. Thus, an effective response requires the coordinated participation of the State, the private sector, educational institutions, and civil society.

CONCLUSIONS

The analysis carried out made it possible to show that cyber scams were among the principal challenges of the XXI century in legal and social matters. The growing digitalization of everyday activities increased the opportunities for the commission of computer crimes, whose economic and personal impacts became increasingly significant. Although Argentina had legislative advances, such as Law 26.388 and its accession to the Budapest Convention, it was observed that the current regulations failed to fully encompass the complexity and diversity of the new criminal modalities.

Likewise, the lack of specific legal classification, insufficient sanctions, and limited training of judicial officials hindered the effective criminal prosecution of cybercriminals. Given this scenario, updating the legal framework, creating specialized cybercrime units, and promoting public policies aimed at prevention and digital education were considered indispensable.

In short, the study concluded that combating cyber fraud requires a comprehensive, interdisciplinary, and coordinated approach among the State, private institutions, and civil society. Only through the combination of modern legislation, international cooperation, and citizen awareness will it be possible to effectively confront this constantly evolving criminal phenomenon.

REFERENCES

1. Unidad Fiscal Especializada en Ciberdelincuencia. Informe de gestión 2023. https://www.fiscales.gob.ar/ciberdelincuencia/la-unidad-fiscal-especializada-en-ciberdelincuencia-senalo-un-alza-continua-de-los-delitos-informaticos-en-su-informe-de-gestion-2023
2. CERT.ar. Incidentes informáticos: informe anual de incidentes de seguridad registrados en 2023. Dirección Nacional de Ciberseguridad; 2024. https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/informes-de-la-direccion-7
3. Secretaría de Innovación Tecnológica del Sector Público. Delitos informáticos en Argentina: modalidades detectadas durante la pandemia COVID-19. Recomendaciones preventivas para los ciudadanos. 2022. https://www.argentina.gob.ar/sites/default/files/2022/04/ciberdelitos_en_pandemia.pdf
4. Brodowski D, Linares MB. Los delitos informáticos en el Código Penal Argentino. En: Cibercrimen y protección de la seguridad informática. Buenos Aires: Ad-Hoc; 2021. p. 155–91.
5. Singh T, Kumar M, Kumar S. Walkthrough phishing detection techniques. Computers and Electrical Engineering 2024;118. https://doi.org/10.1016/j.compeleceng.2024.109374
6. Luján S. El problema de phishing en Argentina. Infobae; 2024 jul 1. https://www.infobae.com/opinion/2024/07/01/el-problema-de-phishing-en-argentina/
7. Departamento de Delitos Tecnológicos de la Policía Federal Argentina. Denunciar un delito informático. https://www.argentina.gob.ar/servicio/denunciar-un-delito-informatico
8. Ahmad I, Khan S, Iqbal S. Guardians of the vault: unmasking online threats and fortifying e-banking security, a systematic review. Journal of Financial Crime 2024;31:1485-501. https://doi.org/10.1108/JFC-11-2023-0302
9. Pérez-Colomé J. Las ciberestafas ya son el segundo delito más denunciado: nadie está a salvo de caer en la trampa. El País; 2024 mar 10. https://elpais.com/tecnologia/2024-03-10/las-ciberestafas-ya-son-el-segundo-delito-mas-denunciado-nadie-esta-a-salvo-de-caer-en-la-trampa.html
10. IBM. ¿Qué es el phishing? https://www.ibm.com/es-es/topics/phishing
11. Abogacía Española, Consejo General. Delitos en internet: ciberestafas. https://www.abogacia.es/actualidad/opinion-y-analisis/delitos-en-internet-ciberestafas/
12. Ministerio de Justicia de la Nación. Qué es el ciberdelito. https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito
13. Aboso G. Ciberdelitos: análisis doctrinario y jurisprudencial. Buenos Aires: elDial Libros; 2022.
14. Brown D, Batra G, Zafar H, Saeed K. Reducing fraud in organizations through information security policy compliance: An information security controls perspective. Computers and Security 2024;144. https://doi.org/10.1016/j.cose.2024.103958.
15. Código Penal Argentino. https://www.argentina.gob.ar/normativa/nacional/ley-11179-16546/texto
16. Donna EA. Derecho penal: parte especial. Tomo II-B. 2ª ed. Santa Fe: Rubinzal-Culzoni; 2012.
17. Centro de Ciberseguridad del Gobierno de la Ciudad de Buenos Aires. Delitos y contravenciones en el mundo digital: las normas que nos amparan. 2024 may. https://buenosaires.gob.ar/sites/default/files/2024-05/B4_Delitos%20y%20contravenciones%20en%20el%20mundo%20digital.pdf
18. Defensa del Consumidor. Cuadernillos COFEDEC. https://www.argentina.gob.ar/produccion/defensadelconsumidor/cuadernilloscofedec
19. Ministerio de Seguridad de la Provincia de Buenos Aires. Cibercrimen y delitos informáticos: guía de estudio 2. 2021. https://www.mseg.gba.gov.ar/areas/Vucetich/GUIAS%20DE%20MATERIAS%202021/2%20Cibercrimen.pdf
20. Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires. Delitos informáticos. 2018 mar 9. https://mpfciudad.gob.ar/tematicas/2020-03-09-18-42-38-delitos-informaticos
21. Centro Europeo del Consumidor de España. Noticias: Ley de Servicios Digitales. 2023 ago 25. https://cec.consumo.gob.es/CEC/comunicacion/noticias/2023/NI_Ley_De_Servicios_Digitales_25_08_2023.htm
22. Interpol. Fraudes basados en la ingeniería social. https://www.interpol.int/es/Delitos/Delincuencia-financiera/Fraudes-basados-en-la-ingenieria-social
23. Departamento de Ciberdelitos y Tecnologías Aplicadas de la SPC. Ciberseguridad, phishing y estafas digitales. https://www.mpba.gov.ar/phishing
24. Gopali S, Namin AS, Abri F, Jones KS. The Performance of Sequential Deep Learning Models in Detecting Phishing Websites Using Contextual Features of URLs, 2024, p. 1064-6. https://doi.org/10.1145/3605098.3636164.
25. Santander. "Pharming": otro motivo para detenerse y pensar antes de hacer clic. 2022 sep 12. https://www.santander.com/es/stories/pharming
26. Toki K. Acciones prohibidas bajo la Ley Japonesa de Prohibición de Acceso No Autorizado. 2024 mar 21. https://monolith.law/es/it/unauthorized-computer-access
27. Gupta G, Bohara S, Kovid RK, Pandla K. Deepfakes and their impact on business. 2024. https://doi.org/10.4018/979-8-3693-6890-9.
28. Kadyshevitch D. Generative AI has democratised fraud and cybercrime. Computer Fraud and Security 2024;2024. https://doi.org/10.12968/S1361-3723(24)70018-9.
29. Omar M, Zangana HM, Mohammed D. Integrating artificial intelligence in cybersecurity and forensic practices. 2024. https://doi.org/10.4018/979-8-3373-0588-2

FUNDING

The authors received no funding for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTIONS

Conceptualization: Sabrina Ivana Bof.
Data curation: Sabrina Ivana Bof.
Formal analysis: Sabrina Ivana Bof.
Investigation: Sabrina Ivana Bof.
Methodology: Sabrina Ivana Bof.
Project administration: Sabrina Ivana Bof.
Software: Sabrina Ivana Bof.
Supervision: Sabrina Ivana Bof.
Validation: Sabrina Ivana Bof.
Visualization: Sabrina Ivana Bof.
Writing – original draft: Sabrina Ivana Bof.
Writing – review & editing: Sabrina Ivana Bof.