South American Publishing

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

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 21, Especialización en Cibercrimen. Argentina.

Cite as
Bof SI. The evolution and classification of digital scams in the technological age. SAP Netnography. 2024; 2:95. https://doi.org/10.62486/net202495

Publication History
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.

© 2024; The Authors. This Open access article is distributed under the Creative Commons Attribution 4.0 license (https://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

INTRODUCCIÓN

El presente trabajo tiene su motivación en la necesidad de abordar un tema de gran relevancia social y jurídica como lo son las ciberestafas. En un mundo que se encuentra cada vez más conectado, estas modalidades delictivas representan un desafío creciente para las autoridades y la sociedad en su conjunto.

Las ciberestafas en Argentina han experimentado un auge significativo en los últimos años. Según dato de la Unidad Fiscal Especializada sobre Ciberdelincuencia entre abril de 2022 y marzo de 2023 hubo un aumento del 38,5 % en ciberdelitos con respecto al año anterior.(1)

De igual manera, durante el período comprendido entre el 1 de enero y el 31 de diciembre de 2023, el CERT.ar registró en su plataforma de administración un total de 379 incidentes informáticos, cifra que aumentó en un 13 % respecto a la del 2022, cuando se registraron 335.(2,3,4,5)

Esta alarmante tendencia se ve agravada por la sofisticación de las técnicas utilizadas por los estafadores, quienes constantemente buscan nuevas formas de engañar a sus víctimas.

"Los casos de fraude, con 288 incidencias, representan el 76 % del total de incidentes reportados, denotando que esta tipología fue el delito informático que más se registró durante el período mencionado. Entre los tipos detectados, se incluyeron uso no autorizado de los recursos, derechos de autor, suplantación de identidad y phishing".(2,6,7,8,9)

DESARROLLO

El avance de las tecnologías de la información y la comunicación (TICs) trajo muchísimos beneficios para el desarrollo, personal, profesional, económico y comercial, no obstante, también trajo consigo un nuevo escenario para la comisión de delitos: las ciberestafas.(10,11)

En la era digital actual, las ciberestafas se han convertido en una amenaza cada vez más frecuente y sofisticada. Estas modalidades delictivas, que se llevan a cabo a través de medios electrónicos o informáticos, generan un impacto significativo en las víctimas, tanto a nivel individual como económico, dándose frecuentemente por medio de redes sociales, aplicaciones de citas, emails y páginas de ventas, entre otras.(12,13)

Las Ciberestafas son un tipo de delito que se comete utilizando las Tecnologías de Información y Comunicación para engañar a la víctima y obtener un beneficio económico, y "al igual que en todas las causas de estafa, requiere para su configuración el causar un perjuicio de contenido patrimonial a otra persona. El bien jurídico protegido es el patrimonio en general y lo que se castiga son las conductas que afectan el patrimonio mediante el uso de sistemas informáticos por parte del causante".(14,15,16)

Las ciberestafas pueden ser muy variadas en su forma de comisión, pero entre las nuevas modalidades se incluyen:(17,18,19,20,21)

a) Ingeniería social: Técnicas utilizadas por los ciberdelincuentes para manipular a las personas y obtener información confidencial o acceso a sistemas informáticos.(22)

b) Phishing: El phishing es un tipo de ciberataque que utiliza correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web fraudulentos para engañar a las personas y hacer que compartan datos confidenciales, descarguen malware o se expongan de otro modo a la ciberdelincuencia.(23,24)

c) Pharming: similar al Phishing pero saquí no hay un señuelo, sino una redirección a una página web falsa, con la finalidad de obtener información confidencial.(25)

d) Ransomware: El ransomware es un tipo de software utilizado generalmente por los cibercriminales para cifrar archivos o sistemas informáticos. El término incluye a todas las formas de código malicioso, como virus y gusanos informáticos. Su finalidad es "secuestrar información" y, de esta manera, impedir a una persona u organización el cceso a sus datos o dispositivos hasta que se haya pagado un dinero como rescate, que frecuentemente suele ser en criptomonedas para permitir al ciberdelincuente ocultar su rastro .(26)

e) Vishing: Es un tipo de estafa de ingeniería social, en al que a través de una llamada se suplanta la identidad de una persona o empresa o entidad a los fines de obtener de la víctima información sensible.

f) Malware: Se trata de software malicioso que se instala en los dispositivos de las víctimas sin su consentimiento, con el objetivo de robar información, controlar el dispostivo o extorsionar a la víctima.

Si bien actualmente, las ciberestafas se encuentran siendo investigadas y penalizadas, la falta de un marco normativo específico genera diversas dificultades:(27,28,29)

- Tipificación imprecisa: Las figuras penales existentes no siempre se ajustan perfectamente a las nuevas modalidades de ciberestafas, lo que dificulta su aplicación efectiva.
- Penalidades insuficientes: Las penas previstas para las ciberestafas suelen ser leves en comparación con la gravedad de los daños que pueden ocasionar.
- Falta de especialización: En muchos departamentos judiciales, no existe un cuerpo de investigadores y jueces especializados en delitos informáticos, lo que puede afectar la calidad de las investigaciones y los juicios.

CONCLUSIONES

El análisis realizado permitió evidenciar que las ciberestafas constituyeron uno de los principales desafíos del siglo XXI en materia jurídica y social. La creciente digitalización de las actividades cotidianas incrementó las oportunidades para la comisión de delitos informáticos, cuyos impactos económicos y personales resultaron cada vez más significativos. Si bien Argentina contó con avances legislativos, como la Ley 26.388 y la adhesión al Convenio de Budapest, se observó que la normativa vigente no logró

https://doi.org/10.62486/net202495

abarcar plenamente la complejidad y diversidad de las nuevas modalidades delictivas.

Asimismo, la falta de tipificación específica, las sanciones insuficientes y la escasa capacitación de los operadores judiciales dificultaron la persecución penal efectiva de los ciberdelincuentes. Ante este panorama, se consideró indispensable la actualización del marco legal, la creación de unidades especializadas en ciberdelito y la promoción de políticas públicas orientadas a la prevención y educación digital.

En definitiva, el estudio concluyó que la lucha contra las ciberestafas requiere un abordaje integral, interdisciplinario y coordinado entre el Estado, las instituciones privadas y la sociedad civil. Solo mediante la combinación de legislación moderna, cooperación internacional y concientización ciudadana será posible enfrentar con eficacia este fenómeno delictivo en constante evolución.

FINANCIACIÓN

Los autores no recibieron financiación para el desarrollo de la presente investigación.

CONFLICTO DE INTERESES

Los autores declaran que no existe conflicto de intereses.

CONTRIBUCIÓN DE AUTORÍA

Conceptualización: Sabrina Ivana Bof.
Curación de datos: Sabrina Ivana Bof.
Análisis formal: Sabrina Ivana Bof.
Investigación: Sabrina Ivana Bof.
Metodología: Sabrina Ivana Bof.
Administración del proyecto: Sabrina Ivana Bof.
Recursos: Sabrina Ivana Bof.
Software: Sabrina Ivana Bof.
Supervisión: Sabrina Ivana Bof.
Validación: Sabrina Ivana Bof.
Visualización: Sabrina Ivana Bof.
Redacción – borrador original: Sabrina Ivana Bof.
Redacción – revisión y edición: Sabrina Ivana Bof.

REFERENCIAS BIBLIOGRÁFICAS

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. Grupo Ático 34. El scamming o los peligros de las estafas por internet. https://protecciondatos-lopd.com/empresas/scamming/

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. Peña M, Lofeudo I. Fraudes: cuáles son las modalidades de ciberdelitos más habituales. Infobae; 2023 sep 21. https://www.infobae.com/opinion/2023/09/21/fraudes/

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. Martínez M. Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico: implicancias y consecuencias en materia penal y de responsabilidad civil. En: Cibercrimen y delitos informáticos. Buenos Aires: Errepar; 2018. p. 33–47.

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. Bisquert SO. La figura del "phishing" como modalidad delictiva: problemática en cuanto a su encuadre jurídico. 2006. http://www.saij.gob.ar/doctrina/dacf060096-bisquertfiguraphishingcomomodalidad.htm

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. Saij. G. R. M. s/ Procesamiento. Estafa. http://www.saij.gob.ar/camara-nacional-apelaciones-criminal-correccional-nacional-ciudad-autonoma-buenos-aires--procesamiento-estafa-fa22060033-2022-1102

28. Weidenslaufer C, Juan Pablo, Cifuentes P. Jurisdicción y ciber-delitos. Biblioteca Nacional del Congreso de Chile; 2022 nov. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/33744/1/BCN_jurisdiccion_ciber_delitos_CW_JPC_PC_2022.pdf

29. Ámbito Financiero. Quién fue Carlo Ponzi, uno de los estafadores más famosos de la historia. 2024 oct 12. https://www.ambito.com/economia/quien-fue-carlo-ponzi-unolos-estafadores-mas-famosos-la-historia-n6069767

https://doi.org/10.62486/net202495