Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), mayo-junio 2025,
Volumen 9, Número 3.

https://doi.org/10.37811/cl_rcm.v9i1

CIBERFRAUDE: PRINCIPALES MÉTODOS DE ATAQUE Y ESTRATEGIAS PARA SU PREVENCIÓN

CYBER FRAUD: MAIN ATTACK METHODS AND PREVENTION STRATEGIES

Oscar Morales Ramirez

Escuela Superior de Tlahuelilpan, UAEH

DOI: https://doi.org/10.37811/cl_rcm.v9i3.18122

Ciberfraude: Principales Métodos de Ataque y Estrategias para su Prevención

Oscar Morales Ramirez[1]
oscar2001.pacman@gmail.com
https://orcid.org/0009-0000-4962-9676
Escuela Superior de Tlahuelilpan, UAEH

RESUMEN

El presente artículo tiene como objetivo identificar y analizar los métodos más comunes utilizados por los ciberdelincuentes para cometer fraudes informáticos, así como las vías de ataque más frecuentes y las estrategias preventivas para mitigarlos. A través de una revisión sistemática de literatura reciente (2020-2024), se recopilaron y analizaron fuentes académicas, informes institucionales y casos reales que evidencian el creciente impacto de estos delitos. La metodología consistió en la clasificación temática de los hallazgos en ingeniería social, malware y ataques técnicos, así como la evaluación de vectores de ataque como el correo electrónico, la navegación web y los dispositivos vulnerables. Entre los principales hallazgos, se identificó el uso creciente de técnicas de phishing, vishing y smishing, así como el despliegue de troyanos bancarios, ransomware y keyloggers. Se destaca también el rol de la inteligencia artificial en la sofisticación de las estafas. Finalmente, se proponen medidas preventivas tanto a nivel individual como institucional, incluyendo la autenticación en dos pasos, la educación en ciberseguridad y la colaboración entre gobiernos, empresas y usuarios. Este trabajo contribuye al entendimiento del fenómeno del ciberfraude y refuerza la necesidad de estrategias de protección adaptadas al contexto digital actual.

***Palabras clave*:** ciberdelincuencia, ciberseguridad, malware, phishing, ransomware

[1] Autor principal.
Correspondencia: oscar2001.pacman@gmail.com

Cyber Fraud: Main Attack Methods and Prevention Strategies

ABSTRACT

The purpose of this article is to identify and analyze the most common methods used by cybercriminals to commit computer fraud, as well as the most frequent attack routes and preventive strategies to mitigate them. Through a systematic review of recent literature (2020-2024), academic sources, institutional reports and real cases that demonstrate the growing impact of these crimes were compiled and analyzed. The methodology consisted of the thematic classification of findings into social engineering, malware and technical attacks, as well as the evaluation of attack vectors such as email, web browsing and vulnerable devices. Among the main findings, the growing use of phishing, vishing and smishing techniques was identified, as well as the deployment of banking Trojans, ransomware and keyloggers. The role of artificial intelligence in the sophistication of scams is also highlighted. Finally, preventive measures are proposed at both the individual and institutional levels, including two-step authentication, cybersecurity education and collaboration between governments, businesses and users. This work contributes to the understanding of the cyberfraud phenomenon and reinforces the need for protection strategies adapted to the current digital context.

***Keywords*:** cybercrime, cybersecurity, malware, phishing, ransomware

Artículo recibido 17 mayo 2025
Aceptado para publicación: 18 junio 2025

INTRODUCCIÓN

La reciente revolución de los pagos digitales ha provocado que los consumidores exijan opciones de pago cada vez más flexibles en tiempo real, impulsando una transformación digital en bancos, Fintech o minoristas que están incorporando aplicaciones y ofertas para dar respuesta a las nuevas necesidades. Esto ofrece además nuevas vías de estafa para los ciberdelincuentes por las que atacar y cometer delitos. (Ciberseguridad, 2023)

Con dependencia de la tecnología en la vida cotidiana ha generado que usuarios y organizaciones enfrenten riesgos de fraude digital mediante sistemas y dispositivos informáticos que facilitan las actividades diarias, así como las transacciones bancarias y plataformas de comercios electrónicos, esto ha abierto una posibilidad a los ciberdelincuentes.

Por lo tanto, el hacker y su estafa se benefician de la complejidad de la tecnología de la información para aprovechar las vulnerabilidades de sistemas y usuarios anónimos, empleando la tecnología de manera inapropiada, con el objetivo de manipular, robar o aniquilar datos con propósitos maliciosos y lucrativos. Es crucial mantenerse alerta y adoptar acciones preventivas para reducir la posibilidad de ser víctima de estos fraudes en línea en sus ataques. (Garcia, 2024)

Por otro lado, la velocidad y complejidad de la evolución digital ha hecho que sea más difícil generar que las medidas de seguridad evolucionen al mismo ritmo que las amenazas, este panorama exige una inversión constante en soluciones y enfoques tecnológicos, así como en educación y concientización sobre los riesgos del fraude informático. La prevención comienza por un entendimiento profundo de los métodos de ataque, vías y vulnerabilidades que usan los ciberdelincuentes para atentar contra sus datos. En numerosas ocasiones, los individuos que llevan a cabo este tipo de estafas, se aprovechan de la ignorancia o del descuido que las personas muestran al usar los servicios financieros en línea, transformándose en un blanco sencillo para los estafadores. (*Condusef Tipos-de-fraude*, s. f.)

Se piensa que los fraudes cibernéticos sólo les suceden a grandes empresas como Coca-Cola o Amazon, pero esto es un error; un ataque de este tipo puede sucederle a cualquier empresa o persona sin importar el tamaño o giro comercial. Un sondeo llevado a cabo por ClearSale, líder en soluciones antifraude, reveló que únicamente en la primera mitad del 2020, de los 53,4 millones de pedidos evaluados, 760.301

fueron categorizados como intentos de fraude. Esto impidió la pérdida de más de $765 millones, una cantidad que superó en un 63,5% al ocurrido en el mismo lapso del año previo. (Trafaniuc, s. f.)

METODOLOGÍA

Esta revisión literaria se realizó de manera sistemática para identificar, evaluar y sintetizar la información relevante sobre los métodos de los ciberdelincuentes, las vías de ataque más comunes y las medidas preventivas en el ámbito de la ciberseguridad. Los pasos principales fueron los siguientes:

Selección de Fuentes: Se incluyeron estudios publicados entre 2020 y 2024, priorizando artículos académicos, informes de instituciones de seguridad y literatura relevante de fuentes verificadas. Los estudios que no cumplían con estos criterios fueron excluidos.

Criterios de Inclusión: Se seleccionaron artículos que abordaran de manera directa los métodos de ciberdelincuentes, las formas de fraude informático y las estrategias de defensa, ya sea mediante análisis empíricos o revisiones anteriores.

Análisis de la Literatura: Los estudios seleccionados fueron clasificados en temas clave: métodos de ataque (ingeniería social, malware, ataques técnicos), vías de ataque y medidas preventivas. Se realizó un análisis crítico de los hallazgos, destacando las principales tendencias y vacíos en la investigación actual.

Síntesis de Resultados: Se organizó la información en base a los temas de interés, se compararon los enfoques encontrados y se identificaron las áreas donde se necesita más investigación o donde ya existen soluciones efectivas.

Objetivos de la revisión

- Identificar los principales métodos utilizados por los ciberdelincuentes.
- Analizar las vías de ataque más comunes y cómo se ejecutan.
- Proponer medidas preventivas

RESULTADOS Y DISCUSIÓN

Revisión de la Literatura

Concepto de fraude informático

Generalmente, el fraude en la red se relaciona con el phishing y, en menor medida, con el pharming. En términos prácticos, este último está vinculado con la ejecución de transacciones bancarias, cuya verificación en línea constituye un ambiente favorable para manipular o alterar datos o programas de sistemas informáticos, con el propósito de perjudicar el patrimonio de terceros. (Lux & Calderón, 2020)

El fraude en línea se refiere al empleo de servicios y programas en línea conectados a Internet con el objetivo de engañar o beneficiar a las víctimas. Normalmente, el término "fraude en Internet" alude a la actividad de cibercrimen que se realiza en línea o por correo electrónico, abarcando crímenes como el hurto de identidad, falsificación de identidad y otras acciones de piratería informática diseñadas para estafar a las personas con dinero. (*¿Qué Es el Fraude Por Internet? Tipos de Fraude Por Internet | Fortinet*, s. f.)

Evolución histórica

Inicialmente, las entidades gubernamentales y empresas privadas se preocupaban por proteger grandes almacenes de datos, que eran vulnerables a ataques internos mediante programas maliciosos y fallos de seguridad. Con el lanzamiento de la World Wide Web en 1994, los hackers comenzaron a intercambiar información sobre métodos de ataque en foros, dando paso a incidentes como el virus Melissa en 1999, que causó daños por 80 millones de dólares al realizar spam masivo.

A finales de los años 90 y principios de los 2000, con la masificación del internet, se incrementaron los casos de robo de información, hacking y propagación de malware. Ejemplos como el gusano SQL Slammer, que ralentizó el internet en un 25%, y los macro-virus, que infectaban dispositivos a través de documentos adjuntos en correos electrónicos, ilustran cómo los ciberdelincuentes aprovechaban nuevas tecnologías para perfeccionar sus métodos de ataque. (Tack, 2021)

En conclusión, la evolución de los delitos informáticos ha ido de la mano del avance tecnológico, desde los primeros dispositivos de comunicación hasta los actuales. Esto plantea preguntas sobre si el derecho penal ha logrado abarcar todas las modalidades de estos delitos en un mundo tan globalizado. En entregas futuras, se explorará esta cuestión y se analizarán las lagunas legales en la regulación de los delitos informáticos.

Investigaciones previas:

A nivel global, la ciberdelincuencia se ha convertido en una de las principales amenazas económicas. Se estima que el valor de los delitos cibernéticos supera al del tráfico de drogas, armas y trata de personas combinados, representando casi el 1.5% del PIB mundial. Además, se prevé que para 2025, uno de cada cuatro delitos sea cometido a través de dispositivos tecnológicos. (Varea et al., 2024)

La inteligencia artificial (IA) ha facilitado la ejecución de fraudes digitales, permitiendo a delincuentes menos experimentados llevar a cabo estafas con mayor precisión. Durante 2024, se observó un aumento en los troyanos bancarios y las estafas relacionadas con criptomonedas, impulsados por herramientas de IA que generan correos electrónicos de phishing más realistas. Este fenómeno ha dado lugar al "Phishing-as-a-Service" (PaaS), donde kits completos de phishing se comercializan, facilitando la entrada de atacantes sin experiencia. (De Frutos Sastre et al., 2024)

En México, los desafíos en ciberseguridad también son notables. En 2022, el país enfrentó más de 187,000 millones de intentos de ciberataques, lo que representa un incremento del 20% respecto al año anterior. Este aumento subraya la necesidad de estrategias robustas de ciberseguridad para proteger tanto a instituciones como a usuarios individuales. (Díaz, 2024)

Estos estudios subrayan la importancia de implementar medidas preventivas y de concienciación para mitigar el impacto de los fraudes en internet. Es esencial la colaboración entre entidades gubernamentales, compañías y usuarios para fortalecer la ciberseguridad y reducir la vulnerabilidad ante estas amenazas en aumento.

Métodos de los Ciberdelincuentes

De acuerdo a la revisión sobre la literatura para este artículo se a identificado que los métodos y vías de ataque de los ciberdelincuentes son los que se mencionan y describen a continuación

Ingeniería Social

Se refiere a las diferentes técnicas de manipulación mediante servicios de comunicación informática que usan los ciberdelincuentes para acceder, robar y manipular información confidencial de los usuarios.

- Phishing: El phishing es un ataque que busca sustraer su dinero o su identidad, provocando que revele datos personales (como números de tarjeta de crédito, datos bancarios o contraseñas) en páginas web que simulan ser legítimas. Los ciberdelincuentes a menudo simulan ser empresas de

renombre, amigos o familiares en un mensaje engañoso que incluye una conexión a una página web de phishing. (*Protéjase del phishing*, s/f)

- Vishing: El vishing es un tipo de engaño de ingeniería social por teléfono donde, mediante una llamada, se suplanta la identidad de una compañía, entidad o individuo de confianza, con el objetivo de conseguir datos personales y delicados de la persona afectada. (*Vishing*, s/f)
- Smishing: Smishing es un ataque de ingeniería social que emplea mensajes de texto falsos para persuadir a individuos a que instalen malware, compartan datos personales o transfieran dinero a criminales informáticos. ("¿Qué es el smishing (phishing por SMS)?", 2024)

Paginas falsas de sitios oficiales del gobierno de México

El Instituto para Devolver al Pueblo lo Robado se mantiene alerta acerca de fraudes este 2024, ya que los ciberdelincuentes persisten en su labor de suplantar dominios y páginas web oficiales, junto con los perfiles institucionales en redes sociales, mientras falsifican documentos, firmas, correos electrónicos y cuentas falsas de WhatsApp, todo esto con el fin de estafar tanto a individuos como a gobiernos estatales y municipales, instituciones educativas y organizaciones. (Lo Robado., 2024)

Figura 1: Captura de pantalla de un sitio falso del gobierno de México (Lo Robado., 2024)

Uso de Malware

Según Belcic (2023) El malware es un software o código informático diseñado para infectar, dañar o acceder a sistemas informáticos. a continuación, se explican los más comunes:

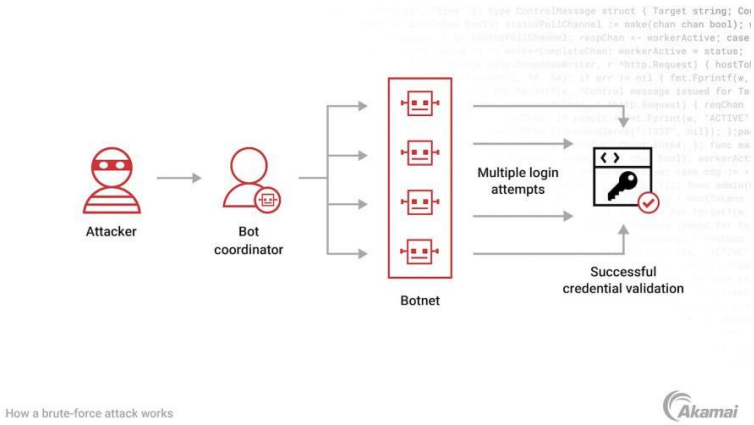
- Troyanos bancarios: Los troyanos bancarios son malware que se disfrazan de software legítimo para infectar computadoras, generalmente a través de correos de phishing o descargas falsas. Una vez instalados, roban credenciales bancarias y datos confidenciales mediante la extracción de información en caché, monitoreo del teclado, búsqueda de contraseñas en archivos y uso de keyloggers cuando el usuario accede a sitios web de banca en línea. (*¿Qué es un troyano bancario? - Software Check Point*, 2023)
- Keylogger: Un keylogger es un hardware o software malicioso que, sin tu permiso o conocimiento, registra todas las teclas que pulsas para operar tu computadora o celular. (¿Qué Es un Keylogger?, 2025). De esta manera al usuario escribir alguna credencial de autentificación tal como una contraseña, pin, código de seguridad o números de tarjetas de crédito, el Keylogger envía esta información al ciberdelincuente pudiendo así hacer uso indebido de esta información de manera remota.
- Ransomware: El ransomware, en informática, es un tipo de malware o código malicioso que impide la utilización de los equipos o sistemas que infecta. El cibercriminal adquiere el control del dispositivo o sistema infectado y lo "secuestra" de diversas formas, encriptándolo, bloqueando la pantalla, entre otras. El usuario es objeto de una coacción, se le solicita un resguardo financiero a cambio de restaurar el funcionamiento normal del aparato o sistema. (Santander, s. f.). Entonces el ransomware se utiliza para realizar una extorción a los usuarios o empresas para obtener un beneficio económico usando como rehenes por así decir los datos y/o dispositivos de los usuarios.

Ataques Técnicos:

- Man-in-the-Middle (MitM): En español como Ataques de hombre en el medio, este consiste en un ataque que intercepta la comunicación entre dos usuarios para robar datos, esto se logra cuando el ciberdelincuente se hace pasar por un intermediario entre los usuarios. (¿Qué es un ataque de hombre en el medio (MitM)? - Software Check Point, 2022)
- Explotación de vulnerabilidades: consiste en aprovechar fallos de seguridad en sistemas, software o redes para cometer delitos cibernéticos. Los atacantes buscan debilidades en programas desactualizados, configuraciones incorrectas o errores de código para infiltrarse en sistemas y obtener información valiosa.

- Ataques de fuerza bruta: Es un metodo de ataque el cual consiste en que el ciberdelincuente hace uso de diferentes nombres de usuario y contraseñas para acceder a una cuenta de un usuario, el atacante hace uso de Botsnets que son redes de bots formadas por miles de ordenadores de usuarios infectados con malware que pueden atacar todos a un mismo usuario. (¿Qué es un ataque de fuerza bruta?, s/f)

Figura 2: anatomía de un ataque de fuerza bruta (Akamai, n.d)



Vías de Ataque

Según *Los 10 vectores de ataque más utilizados por los ciberdelincuentes*, (s/f) estas son las 10 vias de ataque mas usadas por los ciberdelincuentes:

- Correo electrónico y mensajería instantánea: Uso de phishing a través de correos o SMS que suplantan a entidades legítimas para engañar a las víctimas. Buscan robar credenciales, descargar malware o propagar ransomware que secuestra datos a cambio de un rescate.
- Navegación web: Aprovechamiento de vulnerabilidades en navegadores desactualizados, plugins maliciosos o sitios fraudulentos. Técnicas como drive-by download y browser in the browser engañan al usuario para instalar malware o robar credenciales.
- Endpoints y dispositivos vulnerables: Falta de configuraciones seguras en ordenadores, móviles, USB y dispositivos IoT. Configuraciones débiles pueden facilitar ataques como la instalación de malware o la manipulación de redes.
- Aplicaciones web y redes sociales: Webs corporativas e intranets desactualizadas pueden ser explotadas. Redes sociales pueden exponer información sensible utilizada en ataques de spear phishing dirigidos a personas específicas.

- Software de redes y sistemas mal configurado: Equipos de red y servidores sin actualizar o sin parches pueden ser explotados. Ataques como DNS hijacking o denegación de servicio (DoS) pueden afectar la conectividad y seguridad de la empresa.
- Credenciales de usuario comprometidas: Contraseñas filtradas en bases de datos robadas, ataques de fuerza bruta, uso de keyloggers o espionaje de redes Wi-Fi abiertas permiten a los ciberdelincuentes acceder a cuentas sensibles.
- Contraseñas y credenciales predecibles: Uso de claves débiles, credenciales por defecto (admin/admin) o hardcodeadas en dispositivos permite accesos no autorizados y compromete la seguridad de sistemas y aplicaciones.
- Insiders o amenazas internas: Empleados descontentos, exempleados con credenciales activas o personas sobornadas pueden exfiltrar información crítica o ayudar a los atacantes a infiltrarse en sistemas empresariales.
- Carencias en cifrado de datos: Uso de protocolos obsoletos o claves débiles permite la interceptación de información. La falta de cifrado en dispositivos móviles, documentos en la nube o comunicaciones puede exponer datos sensibles.
- Debilidades en la cadena de suministro: Si un proveedor tecnológico sufre un ataque, nuestros datos pueden quedar comprometidos. Es clave revisar acuerdos de seguridad con terceros, especialmente en servicios en la nube.

Estadísticas

En 2023, México enfrentó un panorama complejo en términos de ciberseguridad, destacándose en varios tipos de ataques cibernéticos. A continuación, se presentan algunas estadísticas relevantes:

Ataques de Ingeniería Social

- **Phishing y sus variantes:** Los ataques de phishing, incluyendo técnicas como el callback phishing y el vishing (phishing por voz), aumentaron significativamente. Se registró un incremento del 220% en los ataques de phishing en comparación con 2022. (Ruiz, 2024)
- **Impacto en empresas:** El 80% de las empresas mexicanas fueron víctimas de ataques de ingeniería social, con un costo promedio de 750,000 pesos por incidente.

Malware

- **Infostealers:** En 2023, el 72.9% de las violaciones de datos estuvieron asociadas a malware diseñado para robar información, conocidos como infostealers. Estos malware recopilan datos personales como nombres de usuario, contraseñas y detalles bancarios. (*Fortinet informa que América Latina fue el objetivo de más de 360 mil millones de intentos de ciberataques en 2022*, s/f)
- **Troyanos y Ransomware:** Aunque no se disponen de cifras exactas para cada tipo, se sabe que los troyanos y el ransomware fueron comúnmente utilizados en ataques, a menudo combinados con técnicas de ingeniería social.

Ataques Técnicos

- **Man-in-the-Middle (MitM):** No se encontraron estadísticas específicas sobre ataques MitM en las fuentes consultadas. Sin embargo, es importante destacar que los ataques de ingeniería social a menudo facilitan este tipo de amenazas.
- **Fuerza Bruta:** Similar a los ataques MitM, no se disponen de datos específicos sobre ataques de fuerza bruta en las fuentes revisadas. Estos ataques intentan descifrar contraseñas mediante la prueba exhaustiva de combinaciones.

Otros Datos Relevantes:

- **Intentos de ataques cibernéticos:** México registró cerca de 187,000 millones de intentos de ciberataques en 2022, convirtiéndose en el país de América Latina con la mayor cantidad. (Rodríguez, 2024)

Esta información resalta la importancia de fortalecer las estrategias de ciberseguridad en México, poniendo especial atención en la formación contra métodos de ingeniería social, la puesta en marcha de soluciones de detección y prevención de malware, y el robustecimiento de las defensas frente a ataques técnicos.

DISCUSIÓN

Análisis de los hallazgos

Comparación entre métodos según su frecuencia y efectividad.

Metodos que se basan en la ingeniería social como el vishing y smishing, están en aumento, especialmente a personas de mayor edad o de menos conocimientos en estos temas, Debido a que los

atacantes pueden explotar la confianza que estos usuarios tienen se convierten en algunas de las técnicas más peligrosas.

El uso de virus también sigue siendo usa amenaza muy importante, destacando los troyanos bancarios, ransonware y keyloggers. En el año 2024 aumento la inteligencia artificial que a permitido que los ciberdelincuentes hagan mejoras y desarrollen mejor sus herramientas de ataque, haciendo que los malware sean más difíciles de detectar y por ende más peligrosos.

Los ataques técnicos como Man-in-the-Middle, la explotación de vulnerabilidades y los ataques de fuerza bruta siguen representando riesgos significativos, especialmente para empresas y gobiernos. La falta de actualizaciones de seguridad y configuraciones inadecuadas han permitido que estos ataques sigan siendo efectivos.

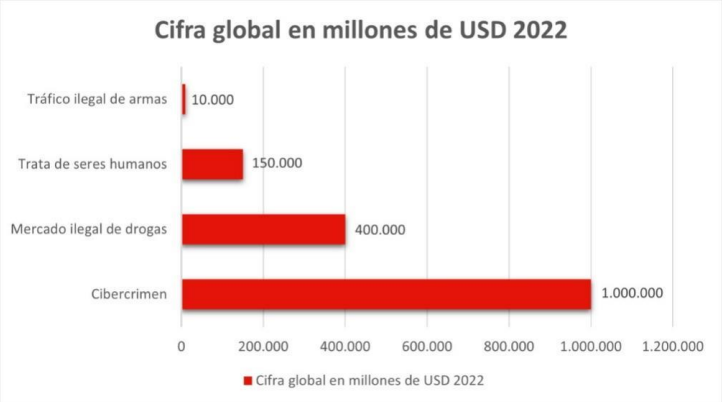
Las vías de ataque como el correo electrónico siguen siendo el canal más utilizado para propagar ataques de phishing y malware, seguido de la navegación web mediante sitios fraudulentos o vulnerabilidades en navegadores desactualizados. Las redes sociales y aplicaciones web también son explotadas para robar información personal de los usuarios.

Impacto del fraude informático

Costos económicos y sociales para las víctimas y las instituciones.

Así como el fraude informático genera pérdidas económicas significativas también tiene un fuerte impacto social. A nivel global se estima que los ataques de ciberdelincuentes superan el valor al trafico de drogas, armas y trata de personas combinados, representando cerda del 1.5% del PIB mundial. Con estas tendencias se espera que en el 2025 uno de cada cuatro delitos sea cometido a través de dispositivos informáticos.

Figura 2: Grafica Cifra global en millones (IT Digital Media Group, 2023)



Para las víctimas individuales, los fraudes en línea pueden significar la pérdida de ahorros, su robo de identidad, etc. En casos extremos estos ataques pueden generar problemas psicológicos y emocionales, como desconfianza en el uso de servicios en línea o dispositivos informáticos, así como ansiedad.

En las organizaciones y empresas sufren graves consecuencias debido más común a los ataques de ransomware, pueden paralizar operaciones enteras obligando a las empresas a pagar recates millonarios para recuperar el control de sus sistemas. También la filtración de datos personales y financieros generan perdidas de confianza en los clientes de dichas empresas, dañando así su reputación.

En el caso de los gobiernos los fraudes informáticos pueden comprometer información sensible, afectando a la prestación de servicios públicos y generar inestabilidad social.

Propuestas para prevenir y mitigar los ataques

En un mundo cada vez más digitalizado, los fraudes por internet se han convertido en una amenaza constante para los usuarios. Para minimizar los riesgos y garantizar una experiencia segura en las transacciones en línea, es fundamental tomar precauciones adecuadas. A continuación, se presentan una serie de recomendaciones para prevenir y mitigar los ataques de fraude en línea:

Protege tu Información Financiera

- Utiliza una tarjeta exclusiva para compras en línea, de preferencia una tarjeta de débito o crédito que no esté vinculada a tus cuentas principales. Esto limitará los daños en caso de fraude.
- **Activas alertas** en tus tarjetas de crédito o débito. Las notificaciones instantáneas pueden ser útiles para detectar movimientos sospechosos.

Navega de Forma Segura

- **Conexiones seguras**: Siempre navega a través de redes seguras y privadas (por ejemplo, evita redes Wi-Fi públicas). Verifica que los sitios web tengan el protocolo **HTTPS** en la URL y un candado verde junto a la dirección, lo cual indica que la conexión está cifrada.
- **Evita enlaces sospechosos**: No accedas a enlaces de anuncios, correos electrónicos desconocidos ni mensajes de mensajería instantánea que no sean de fuentes verificadas.

Protege tus Dispositivos

- Asegúrate de que tus dispositivos estén **actualizados** y cuenten con un software de protección antivirus confiable.

- Realiza escaneos regulares de seguridad para prevenir software malicioso o intrusos.

Verifica la Autenticidad de Ofertas y Páginas Web

- **Valida la página web** donde realizarás compras. Asegúrate de que esté vinculada a una empresa legítima, revisa sus políticas de privacidad, condiciones de venta y datos de contacto.
- Verifica el **correo electrónico** o mensaje con la empresa que ofrece el producto o servicio, asegurándote de que sea el canal oficial. Hazlo directamente desde sus páginas o redes sociales oficiales.
- Si es una oferta que parece demasiado buena para ser verdad, **revisa la reputación** de la empresa o persona que la ofrece mediante comentarios de otros usuarios en línea.

Comprobaciones de la Oferta

- **Valida la oferta**: Investiga si el producto o servicio realmente existe y si la descripción coincide con lo que se está ofreciendo.
- **Datos de contacto**: Asegúrate de que la empresa tenga formas claras de contacto, y verifica la existencia de un número telefónico, dirección física, o servicio de atención al cliente.
- **Revisa la reputación** de los vendedores, mediante comentarios de clientes previos o investigaciones en línea.

Uso de Dispositivos Propios y Redes Privadas

- Siempre utiliza **dispositivos propios** cuando realices compras en línea. Evita realizar compras a través de dispositivos compartidos o públicos que puedan comprometer tus datos.
- Asegúrate de que tu red Wi-Fi doméstica esté **protegida** con una contraseña fuerte y que tu router esté configurado adecuadamente.

Proporciona Solo los Datos Necesarios

- No proporciones **información personal innecesaria**. Limita los datos personales que proporcionas solo a los imprescindibles para completar la transacción.

Verificación en Dos Pasos

- **Habilita la autenticación en dos pasos** en tus cuentas bancarias, tiendas en línea y servicios digitales. Esto proporciona una capa extra de seguridad contra el acceso no autorizado.

Mantén un Registro de tus Operaciones Financieras

- **Guarda los comprobantes de pago** y la información sobre las transacciones realizadas, incluyendo el detalle del producto o servicio adquirido.
- **Mantén un archivo de correos electrónicos** y comunicaciones con los vendedores para poder respaldar tus reclamos en caso de disputas o fraudes.

Educación y Conciencia sobre el Fraude

- Mantente informado sobre las últimas técnicas de fraude y estafas comunes en línea. Conocer las tácticas más recientes te ayudará a identificar señales de alerta.
- Realiza auditorías periódicas de tus cuentas bancarias y tarjetas de crédito para detectar movimientos extraños lo antes posible.

CONCLUSIONES

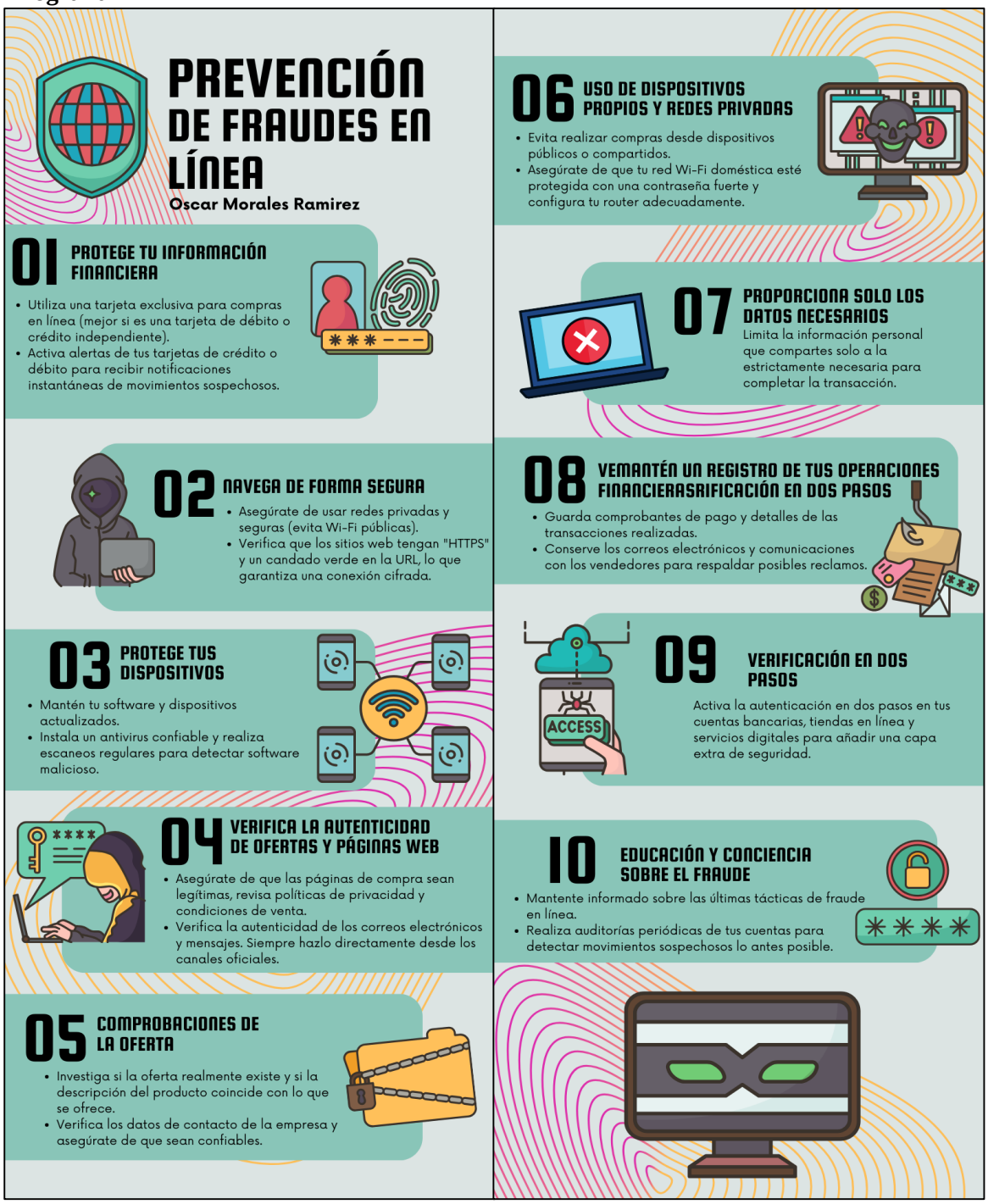
El estudio efectuado en este estudio facilita la identificación de técnicas y rutas de ataque comunes empleadas por los ciberdelincuentes y sus efectos. Se ha comprobado que, junto con las técnicas de phishing, vishing y smishing, la ingeniería social continúa siendo una de las tácticas más eficaces para persuadir y engañar a los usuarios para conseguir su información fiable. De igual forma, la utilización de malware en combinación con troyanos bancarios, ransomware y keyloggers, constituyen una amenaza para entidades y usuarios ordinarios. En el contexto técnico, los ataques de Man-in-the-Middle, la explotación de vulnerabilidades y la fuerza bruta siguen impactando en los sistemas de negocios. En cuanto las vías de ataque como correos electrónicos, sitios web y redes sociales son canales muy explotados por ciberdelincuentes, lo que demuestra la necesidad de fortalecer las medidas de protección en estos entornos.

En este contexto, resulta esencial implementar acciones de prevención y reacción tanto a nivel personal como institucional. Es crucial para los usuarios incrementar su formación en ciberseguridad, aprendiendo a detectar intentos de estafa, además de utilizar la autenticación en dos pasos, que representa un obstáculo más eficaz para prevenir ingresos no permitidos a cuentas bancarias. En cambio, las entidades deben poner en marcha estrategias de vigilancia constante y análisis de conducta para identificar acciones sospechosas en sus sistemas. Al utilizar la inteligencia artificial, se puede potenciar la identificación y prevención de fraudes en tiempo real, identificando patrones de irregularidades en grandes cantidades de información. Finalmente es de suma importancia la colaboración entre gobiernos,

instituciones y usuarios para fortalecer la ciberseguridad y reducir el impacto del fraude informático. La cooperación internacional en la implementación de normativas, el intercambio de información sobre amenazas emergentes y el desarrollo de campañas de concienciación son esenciales para reducir la vulnerabilidad ante estos ataques. En un mundo cada vez más digitalizado, la prevención y la preparación son la clave para enfrentar los desafíos que plantea la ciberdelincuencia.

ANEXOS

Infografía



GLOSARIO

Fintech: Empresas que combinan tecnología y servicios financieros para ofrecer soluciones innovadoras como pagos digitales y banca en línea.

Minoristas: Empresas que venden productos o servicios directamente a los consumidores a través de tiendas físicas o plataformas digitales.

Hacker: Persona con habilidades avanzadas en informática que puede vulnerar sistemas para bien (hacker ético) o con fines maliciosos (ciberdelincuente).

Concientización en ciberseguridad: Proceso de educación y sensibilización sobre los riesgos y mejores prácticas de seguridad digital.

Educación digital: Formación en el uso seguro y eficiente de las tecnologías de la información.

Transformación digital: Integración de tecnología en procesos empresariales y sociales para mejorar eficiencia e innovación.

Instituciones financieras: Bancos y otras entidades que gestionan dinero y ofrecen servicios como préstamos, pagos y ahorro.

Piratería informática: Actividades ilegales que buscan explotar vulnerabilidades en software o sistemas digitales.

Identidad digital: Información personal y credenciales de un usuario que permiten su identificación en línea.

Ciberseguridad: Conjunto de prácticas y tecnologías diseñadas para proteger sistemas y datos de ataques cibernéticos.

Robo de identidad: Uso ilegal de la información personal de alguien para cometer fraude o delitos.

Suplantación de identidad: Acción de hacerse pasar por otra persona para obtener beneficios ilícitos.

Datos personales: Información privada de un usuario, como nombre, dirección, correo electrónico o datos bancarios.

Comercios electrónicos: Plataformas digitales que permiten la compra y venta de productos y servicios en línea.

Derecho penal: Rama del derecho que regula delitos y establece sanciones para quienes los cometen.

Instituciones gubernamentales: Entidades del gobierno encargadas de la gestión pública y la aplicación de normativas.

Malware: Software malicioso diseñado para infectar dispositivos y robar, manipular o destruir datos.

Cadenas de suministro: Red de proveedores, fabricantes y distribuidores que participan en la producción y entrega de bienes o servicios.

Plataformas digitales: Aplicaciones o sitios web que ofrecen servicios en línea como redes sociales, banca digital o comercio electrónico.

Criptomonedas: Activos digitales descentralizados que usan criptografía para garantizar transacciones seguras sin intermediarios.

REFERENCIAS BIBLIOGRÁFICAS

Ciberseguridad, R. (2023, 11 julio). *«Tendencias Mundiales sobre Fraude Digital»*. Revista Ciberseguridad. https://www.revistaciberseguridad.com/2023/07/tendencias-mundiales-sobre-fraude-digital/

Condusef tipos-de-fraude. (s. f.). https://www.condusef.gob.mx/?p=tipos-de-fraude

De Frutos Sastre, A., De Frutos Sastre, A., & De Frutos Sastre, A. (2024, 13 noviembre). El auge de la IA dispara los ciberataques en el sector financiero en 2024. *Cinco Días*. https://cincodias.elpais.com/smartlife/lifestyle/2024-11-13/el-auge-de-la-ia-dispara-los-ciberataques-en-el-sector-financiero-en-2024.html

Díaz, P. F. A. (2024, 6 agosto). *Ciberseguridad en México: Desafíos y Estrategias*. Perito Fernando Amador Díaz. https://fernandoamador.com.mx/informatica-forense/ciberseguridad-en-mexico-desafios-y-estrategias/

Garcia, L. (2024, 16 septiembre). *El fraude informático y sus ciberataques*. OnRetrieval. https://onretrieval.com/el-fraude-informatico-y-sus-ciberataques/

IT Digital Media Group. (2023, 2 junio). *El valor del cibercrimen se aproxima al 1,5% del PIB mundial*. Actualidad | IT Digital Security.

https://www.itdigitalsecurity.es/actualidad/2023/06/el-valor-del-cibercrimen-se-aproxima-al-15-del-pib-mundial

Lo Robado, I. P. D. A. P. (s. f.). *El Instituto para Devolver al Pueblo lo Robado mantiene alerta en 2024 debido a las estafas y sitios web falsos en Internet*. gob.mx. https://www.gob.mx/indep/prensa/el-instituto-para-devolver-al-pueblo-lo-robado-mantiene-alerta-en-2024-debido-a-las-estafas-y-sitios-web-falsos-en-internet?idiom=es

Belcic, I. (2023, enero 19). *¿Qué es el malware y cómo protegerse de los ataques?* ¿Qué es el malware y cómo protegerse de los ataques?; Avast. https://www.avast.com/es-es/c-malware

Los incidentes de ciberseguridad de 2023, gestionados por INCIBE, aumentan en un 24% respecto al año anterior. (s. f.). INCIBE | INCIBE. https://www.incibe.es/incibe/sala-de-prensa/los-incidentes-de-ciberseguridad-de-2023-gestionados-por-incibe-aumentan-en

Lux, L. M., & Calderón, G. O. (2020). The crime of cyber fraud: Definition and delimitation. *Revista Chilena de Derecho y Tecnología*, *9*(1), 151-184. https://doi.org/10.5354/0719-2584.2020.53447

¿Qué es el fraude por Internet? Tipos de fraude por Internet | Fortinet. (s. f.). Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/internet-fraud

¿Qué es un keylogger? (2025, 27 enero). Argentina.gob.ar. https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-un-keylogger

Santander, B. (s. f.). *Ransomware*. Banco Santander. https://www.bancosantander.es/glosario/ransomware

Tack, B. (2021, 9 diciembre). Un breve relato sobre el origen histórico de los delitos cibernéticos. *Lex Diarium*. https://www.lexdiarium.com/derecho-tecnol%C3%B3gico/un-breve-relato-sobre-el-origen-hist%C3%B3rico-de-los-delitos-cibern%C3%A9ticos

Trafaniuc, V. (s. f.). *Victor Trafaniuc*. https://blog.maplink.global/es/tipos-de-fraudes-ciberneticos/

Varea, R., Varea, R., & Varea, R. (2024, 8 diciembre). Fraudes digitales, nadie está a salvo. *El País*.

https://elpais.com/extra/eventos/2024-12-08/fraudes-digitales-nadie-esta-a-salvo.html

Vista de Ataques a celulares a través del uso de aplicaciones móviles: Una revisión narrativa. (s. f.). https://revistascientificas.uach.mx/index.php/tecnociencia/article/view/1584/2579

Belcic, I. (2023, enero 19). *¿Qué es el malware y cómo protegerse de los ataques?* ¿Qué es el malware y cómo protegerse de los ataques?; Avast. https://www.avast.com/es-es/c-malware

Fortinet informa que América Latina fue el objetivo de más de 360 mil millones de intentos de ciberataques en 2022. (s/f). Fortinet. Recuperado el 16 de marzo de 2025, de https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent

Los 10 vectores de ataque más utilizados por los ciberdelincuentes. (s/f). Incibe.es. Recuperado el 16 de marzo de 2025, de https://www.incibe.es/empresas/blog/los-10-vectores-ataque-mas-utilizados-los-ciberdelincuentes

Protéjase del phishing. (s/f). Microsoft.com. Recuperado el 16 de marzo de 2025, de https://support.microsoft.com/es-es/windows/prot%C3%A9jase-del-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44

¿Qué es el smishing (phishing por SMS)? (2024, octubre 24). *Ibm.com*. https://www.ibm.com/mx-es/topics/smishing

¿Qué es un ataque de fuerza bruta? (s/f). Fortinet. Recuperado el 16 de marzo de 2025, de https://www.fortinet.com/lat/resources/cyberglossary/brute-force-attack

¿Qué es un ataque de hombre en el medio (MitM)? - Software Check Point. (2022, agosto 29). Check Point Software. https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-a-man-in-the-middle-mitm-attack/

¿Qué es un troyano bancario? - Software Check Point. (2023, abril 25). Check Point Software. https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-trojan/what-is-a-banking-trojan/

Rodríguez, D. (2024, septiembre 8). *La sofisticación de los ciberataques aumenta el secuestro de datos y redes sociales en México*. Ediciones EL PAÍS S.L. https://elpais.com/mexico/2024-09-08/la-sofisticacion-de-los-ciberataques-aumenta-el-secuestro-de-datos-y-redes-sociales-en-mexico.html

Ruiz, *. Por Víctor. (2024, junio 8). *Sólo el 43.3% de empresas y el 17.2% de entidades gubernamentales en México pueden enfrentrar al cibercrimen*. infobae. https://www.infobae.com/mexico/2024/06/08/solo-el-433-de-empresas-y-el-172-de-entidades-gubernamentales-en-mexico-pueden-enfrentrar-al-cibercrimen/

Vishing. (s/f). Incibe.es. Recuperado el 16 de marzo de 2025, de https://www.incibe.es/aprendeciberseguridad/vishing