Prevención de extorsión y como evitar estafas digitales

Autores:

Moreno, Irma
Universidad UMECIT, Panamá
Licenciatura en Derecho y Ciencias Políticas
irmadanela2510@gmail.com
https://orcid.org/0009-0004-0366-212X

García, Leonel
Universidad UMECIT, Panamá
Licenciatura en Derecho y Ciencias Políticas
leo8043508@gmail.com
https://orcid.org/0009-0008-1364-125X

Alba, Anibal
Universidad UMECIT, Panamá
Licenciatura en Derecho y Ciencias Políticas
albaanibal2552@gmail.com
https://orcid.org/0009-0007-0541-6362

Ortiz, Melvin
Universidad UMECIT, Panamá
Licenciatura en Derecho y Ciencias Políticas
melvissvasquez90@gmail.com
https://orcid.org/0009-0000-2904-9404

Docente Asesor:
Tuñon, Zuley
Universidad UMECIT, Panamá
Asignatura: Derecho Económico y Financiero
zuley0530@gmail.com
https://orcid.org/0009-0003-4027-6431

Sede: Santiago

DOI: 10.37594/sc.v1i7.1887

Resumen

En la era digital, donde la tecnología facilita innumerables aspectos de la vida cotidiana, también surgen riesgos que requieren atención inmediata: la extorsión y las estafas digitales se han convertido en amenazas frecuentes y sofisticadas, afectando a personas, empresas e incluso instituciones. Estos delitos aprovechan la confianza, la desinformación o los descuidos en el manejo de datos personales para manipular, robar información o sustraer recursos económicos. En este contexto, es fundamental comprender las estrategias de prevención y las medidas prácticas para proteger la integridad física, emocional y financiera. Mecanismos clave para prevenir la extorsión, incluyendo la protección de datos sensibles y el manejo de situaciones de chantaje. Tácticas para identificar y evitar estafas digitales, como el phishing, fraudes en redes sociales o ofertas fraudulentas. Acciones inmediatas que deben tomarse si se es víctima de estos delitos. La importancia de la educación continua y las herramientas tecnológicas como pilares de la seguridad en línea. El objetivo es brindar un panorama claro y práctico que permita navegar en el entorno digital con mayor conciencia y resiliencia, reduciendo al mínimo la exposición a estos riesgos.

Palabras clave: Prevención de extorsión y como evitar la estafa digital: Educación, Tecnología, estafas, encuestas, teorías, argumentos, extorsión, leyes, derecho informático.

Extortion prevention and how to avoid digital scams

Abstract

In the digital age, where technology facilitates countless aspects of daily life, risks also arise that require immediate attention: digital extortion and scams have become frequent and sophisticated threats, affecting individuals, companies, and even institutions. These crimes exploit trust, misinformation, or carelessness in handling personal data to manipulate, steal information, or subtract economic resources. In this context, it is fundamental to understand prevention strategies and practical measures to protect physical, emotional, and financial integrity. Key mechanisms to prevent extortion include protecting sensitive data and managing blackmail situations. Tactics to identify and avoid digital scams, such as phishing, social media fraud, or fraudulent offers. Immediate actions that should be taken if one is a victim of these crimes. The importance of continuous education and technological tools as pillars of online security. The objective is to provide a clear and practical overview that allows navigating the digital environment with greater awareness and resilience, minimizing exposure to these risks.

Keywords: Extortion prevention and how to avoid digital scams: Education, technology, scams, surveys, theories, arguments, extortion, laws, computer law.

1. INTRODUCCIÓN

Justificación:

En la era digital actual, la interconexión global y la dependencia de la tecnología han traído consigo un aumento significativo en la sofisticación y frecuencia de delitos como la extorsión y las estafas digitales. Estos actos delictivos no solo generan considerables pérdidas económicas para individuos y organizaciones, sino que también provocan un profundo impacto emocional y psicológico en las víctimas, minando la confianza en las interacciones digitales y, en el caso de la extorsión, la seguridad personal.

La evolución constante de las tácticas empleadas por los ciberdelincuentes y extorsionadores exige una ciudadanía informada y preparada. Muchas personas desconocen las señales de alerta, las medidas preventivas básicas o cómo actuar adecuadamente al ser confrontadas con una situación de este tipo. Por lo tanto, la prevención activa, basada en el conocimiento y la adopción de buenas prácticas de seguridad, se convierte en una herramienta fundamental.

Es por lo que este tema, busca dotar al público de una comprensión clara de los riesgos existentes y las medidas concretas que pueden tomar para salvaguardar su seguridad personal, financiera y digital, fomentando una actitud proactiva y vigilante.

Descripción de la temática o problema de investigación

El tema "PREVENCIÓN DE EXTORSIÓN Y CÓMO EVITAR ESTAFAS DIGITALES" aborda de manera integral las estrategias y conocimientos necesarios para que los individuos puedan protegerse activamente contra dos de las modalidades delictivas con mayor impacto en la actualidad.

En relación con la prevención de la extorsión, el tema cubre, definición y tipos de extorsión comprensión de qué es la extorsión y sus diversas manifestaciones (ej. llamadas telefónicas, sextorsión, secuestro virtual), modus operandi de los extorsionadores: Cómo suelen actuar los delincuentes para intimidar y manipular a sus víctimas, medidas preventivas específicas: Consejos prácticos sobre cómo proteger la información personal, qué hacer ante llamadas o mensajes sospechosos, y cómo evitar convertirse en un blanco fácil, protocolos de actuación: Pasos a seguir en caso de recibir una amenaza extorsiva, incluyendo la importancia de mantener la calma, no ceder a las demandas y contactar a las autoridades.

En cuanto a cómo evitar las estafas digitales, el tema explora, panorama de las estafas digitales identificación de los fraudes más comunes en el entorno online (ej. phishing, smishing, vishing, ransomware, estafas en compras online, fraudes románticos, ofertas de inversión falsas), técnicas de ingeniería social: Cómo los estafadores manipulan psicológicamente a las personas para obtener información confidencial o dinero, prácticas de seguridad digital esenciales: Recomendaciones sobre la creación de contraseñas seguras, la activación de la autenticación de dos factores, la identificación de sitios web y correos fraudulentos, el uso seguro de redes Wi-Fi, y la protección de dispositivos, hábitos de navegación segura: Consejos para realizar transacciones en línea de forma segura, verificar la legitimidad de ofertas y ser crítico con la información encontrada en internet, mecanismos de denuncia: Información sobre las entidades y canales disponibles (como el Ministerio Público y la Policía Nacional en Panamá) para reportar estos delitos y buscar ayuda.

Antecedentes investigativos:

La investigación sobre la extorsión y las estafas digitales ha experimentado un crecimiento significativo en los últimos años, impulsada por el aumento de estos delitos y la necesidad de comprender sus dinámicas. Diversos estudios han abordado estos fenómenos desde diferentes perspectivas:

Investigaciones han examinado los perfiles de los delincuentes, sus motivaciones y las metodologías empleadas. Se ha observado una tendencia hacia la especialización y la organización de grupos criminales que operan a través de fronteras, aprovechando la anonimidad y la dificultad de rastreo que ofrece el entorno digital (Grabosky, 2014). Se han realizado estudios para comprender el impacto de estos delitos en las víctimas, incluyendo las pérdidas económicas, el daño psicológico y las barreras para la denuncia. Estos estudios revelan la vulnerabilidad de ciertos grupos de población y la necesidad de ofrecer apoyo y recursos adecuados a las víctimas (Button et al., 2014). Expertos en ciberseguridad han analizado las técnicas utilizadas en los ataques de extorsión y estafas digitales, como el uso de malware, la ingeniería social y las vulnerabilidades de los sistemas informáticos. Esta investigación es fundamental para desarrollar herramientas y estrategias de detección y prevención (Kshetri, 2016). Se ha investigado la efectividad de las campañas de concientización y los programas de educación en la prevención de estos delitos. Los resultados sugieren que la información clara y accesible, adaptada a diferentes audiencias, puede aumentar la capacidad de las personas para reconocer y evitar las amenazas (Anderson et al., 2017). Se han realizado análisis sobre el marco legal existente para combatir la extorsión y las estafas digitales, así como sobre la efectividad de las políticas públicas implementadas. Estos estudios a menudo señalan la necesidad de una mayor cooperación internacional y la adaptación de las leyes a la naturaleza transfronteriza de estos delitos (Ryder & Wall, 2015).

Estos antecedentes investigativos resaltan la complejidad de la extorsión y las estafas digitales, así como la necesidad de un enfoque multidisciplinario para su prevención y combate.

Formulación de Interrogantes

¿Qué estrategias preventivas pueden reducir la vulnerabilidad de los usuarios ante la extorsión y las estafas digitales en entornos virtuales?

Objetivos

Objetivo general: Analizar las estrategias de prevención contra la extorsión y estafas digitales.

Breve desarrollo teórico conceptual

El desarrollo conceptual de este estudio se centra en el análisis detallado de los factores que inciden en la extorsión y las estafas digitales, con un enfoque multidisciplinario que incluye aspectos legales, psicológicos y tecnológicos. Se busca establecer un marco teórico que permita comprender la dinámica de estos delitos y las estrategias más efectivas para su prevención.

En la actualidad, el uso cotidiano de internet y tecnologías de la información ha dado paso a

nuevas formas de delincuencia, en especial la extorsión y las estafas digitales. Estos delitos, muchas veces invisibles hasta que la víctima ya ha sido afectada, se aprovechan del desconocimiento, la urgencia emocional y la ingenuidad de los usuarios para materializarse. La extorsión digital puede manifestarse de múltiples maneras, desde amenazas con divulgar información privada, hasta ataques con software malicioso como el ransomware que bloquea dispositivos hasta recibir un pago. Por otro lado, las estafas digitales, como el phishing, el fraude por suplantación de identidad o los engaños en redes sociales, se presentan con una apariencia de legalidad o confianza, lo que las hace especialmente peligrosas.

Comprender estos delitos requiere no solo una mirada jurídica, sino también psicológica y tecnológica. Desde la psicología se puede entender cómo la ingeniería social explota emociones como el miedo, la vergüenza o la necesidad de ayuda. Tecnológicamente, es esencial conocer los mecanismos que utilizan los delincuentes: desde correos electrónicos fraudulentos, páginas web clonadas, hasta malware sofisticado. Pero quizás el aspecto más crítico sea el conocimiento social: muchas personas no están preparadas para detectar señales de alerta ni conocen los protocolos básicos de seguridad digital.

Este desarrollo conceptual busca justamente cimentar una base sólida desde la cual puedan implementarse medidas concretas de prevención. Comprender el fenómeno desde múltiples dimensiones no solo enriquece el análisis, sino que habilita una acción más eficiente y articulada entre ciudadanía, instituciones y sector privado.

2. METODOLOGÍA

La presente investigación adopta un enfoque mixto, con un diseño no experimental y de tipo descriptivo. Se emplearon dos métodos complementarios: la revisión documental y la recolección de datos mediante encuestas.

En la fase documental, se analizó el Proyecto de Ley N.º 61, “Por el cual se adoptan medidas contra la ciberdelincuencia”, así como el Convenio sobre Ciberdelincuencia suscrito en Budapest el 23 de noviembre de 2001. Estos documentos fueron seleccionados por su relevancia en el marco jurídico panameño e internacional relacionado con la prevención del delito digital.

Paralelamente, se aplicó una encuesta estructurada al público en general, con el propósito de conocer el nivel de exposición, percepción y frecuencia de estafas digitales en la vida cotidiana. El instrumento fue diseñado con preguntas cerradas y de escala ordinal, permitiendo cuantificar aspectos clave sobre el conocimiento y la vivencia de extorsión y fraudes digitales. La muestra fue

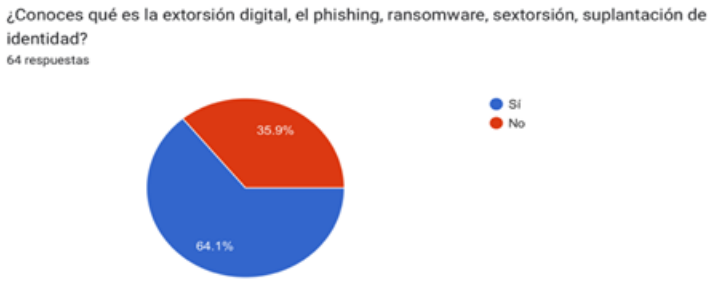
seleccionada por conveniencia, considerando la accesibilidad y disposición de los participantes.

3. RESULTADOS Y DISCUSIÓN

Se realizó una encuesta con la ciudadanía panameña sobre la Prevención de extorsión y de cómo evitar las estafas digitales, donde se estas fueron las siguientes interrogantes:

- ¿Conoces qué es la extorsión digital, el phishing, ransomware, sextorsión, suplantación de identidad?
- ¿Conoces qué leyes regulan estos temas en Panamá?
- ¿Has escuchado sobre casos de extorsión o estafas digitales en tu entorno?
- Si respondiste "Sí" en la anterior, ¿cuál fue la forma de contacto utilizada? (Llamada telefónica, correo electrónico, Redes Sociales, otros)
- ¿Sueles verificar la autenticidad de los mensajes o correos electrónicos antes de responder?
- ¿Qué métodos utilizas para proteger tus datos personales en línea? (Selecciona todas las que apliquen)
- ¿Crees que la educación en temas de ciberseguridad debería ser obligatoria o implementarse en centros educativos y lugares de trabajo?

- Donde iniciamos preguntando, si conocía sobre la extorsión digital, el phishing, ransomware, sextorsión, suplantación de identidad, cuyo resultado fue el siguiente:



Esto nos indica que, hay ciertas personas de la cual, si tiene conocimiento, pero es preocupante que hay un 35.9% de la población de que no conoce de que son estos conceptos de extorsión y estafas digital.

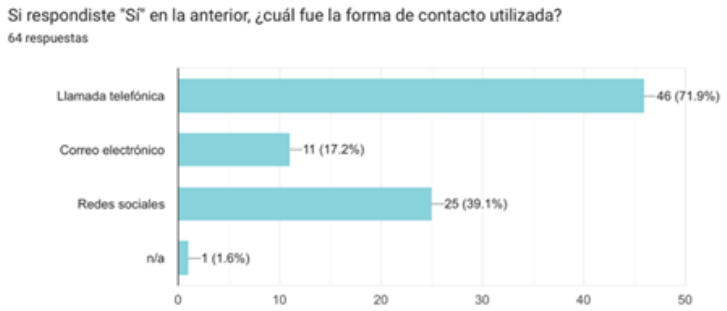
- También preguntamos si conocían alguna ley que regulara estos conceptos en Panamá

Conocimiento sobre leyes que regulan temas digitales en Panamá: Un 81.3% de los encuestados conoce las leyes que regulan los temas digitales en Panamá, mientras que un 18.8% no tiene conocimiento al respecto.

- Además, preguntamos si habían escuchado mencionar sobre casos de extorsión o estafas digitales en su entorno

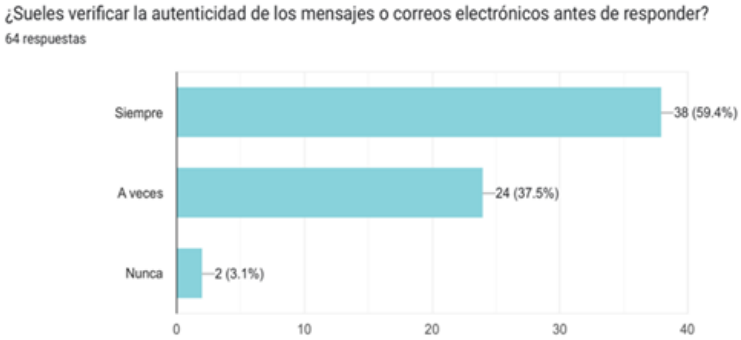
Casos de extorsión o estafa digital en el entorno: Un 93.8% ha escuchado sobre casos de extorsión o estafa digital en su entorno, mientras que solo un 6.3% no ha tenido conocimiento de estos casos.

- En esta pregunta, fue adoptada con la anterior, pero quisimos saber cuál era la estafa más común aquí en Panamá:



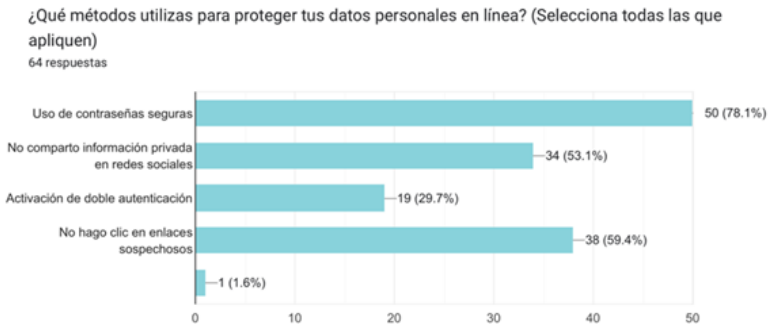
Vemos como las llamadas suelen ser el medio más utilizado para gestionar este tipo de ataques y fraudes digitales, seguido de las redes sociales que hoy en día se han convertido en algo muy utilizado por la sociedad, haciéndolo un entorno perfecto para los ciberdelincuentes.

- Aquí preguntamos si solían verificar la autenticidad de los mensajes o correos electrónicos antes de responder y este fue el resultado:



Si bien una gran parte de los encuestados reveló verificar la autenticidad de sus mensajes y correos electrónicos, no debes dejar de pasar por alto que un 37.5% suele tomar estas medidas a veces, es importante recalcar que igualmente a pesar de lo alerta que se puede estar no estamos exentos de ser blancos para los estafadores informáticos.

- Preguntamos qué métodos utilizan para proteger sus datos personales en línea, y los resultados nos parecieron interesantes:



Basándonos en la encuesta realizada dentro de nuestro artículo, pudimos identificar diferentes métodos de respaldo que utilizan los diferentes usuarios encuestados. Con un gran margen de diferencia, la opción más votada fue el uso de contraseñas seguras en las diferentes plataformas y aplicaciones digitales y a su vez van de la mano con la segunda opción más votada que es el no compartir información privada.

- Lo último que preguntamos fue si creían o consideraban que la educación sobre la ciberseguridad es importante en las escuelas y lugares de trabajo:

Siendo este un tema de suma importancia, claramente todos somos conscientes de que a nivel nacional no hay un mucho interés en orientar o concientizar a las personas sobre los diferentes tipos de delitos informáticos y las consecuencias que esto trae.

Al finalizar esta encuesta pudimos coincidir con casi el 90% de los encuestados sobre la falta de interés tanto por parte del gobierno, como también por otras entidades que también podrían involucrarse como en este caso podrían ser las escuelas, universidades e incluso dentro de las

diferentes áreas de trabajo, ya sean empresas públicas o privadas.

4. CONCLUSIONES

La extorsión y las estafas digitales representan una amenaza creciente en el entorno digital actual. La sofisticación de las tácticas empleadas por los delincuentes y la facilidad con la que pueden operar a través de fronteras exigen una respuesta integral y coordinada. La investigación académica ha proporcionado valiosos conocimientos sobre la naturaleza, el alcance y el impacto de estos delitos, pero aún existen interrogantes importantes que requieren mayor exploración.

La prevención efectiva de la extorsión y las estafas digitales se basa en la adopción de medidas de seguridad proactivas, la educación y la concientización de la población, y la colaboración entre individuos, empresas, autoridades y la sociedad civil en general. Es crucial fomentar una cultura de ciberseguridad y promover la denuncia de estos incidentes para debilitar las redes criminales y proteger a las posibles víctimas.

La lucha contra la extorsión y las estafas digitales es un desafío continuo que requiere una adaptación constante a las nuevas amenazas y el desarrollo de estrategias innovadoras para garantizar un entorno digital más seguro y confiable para todos.

La prevención combina prudencia, herramientas tecnológicas y conocimiento. Mantén un escepticismo saludable ante solicitudes inusuales y prioriza la protección de tu información. Ante cualquier incidente, actuar rápido y reportar es crucial para minimizar daños.

REFERENCIAS BIBLIOGRÁFICAS

- Alonso, J. A. (2018). Ciberseguridad para todos: Protege tu vida digital.
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588–608.
- Cressey, D. R. (1953). Other People's Money: A Study in the Social Psychology of Embezzlement. Free Press.
- Europol. (2022). Internet Organised Crime Threat Assessment (IOCTA).
- Ministerio Público de Panamá (2021) "El Ciberdelito es Real" Ministerio Público y Policía Nacional lanzan campaña de prevención del delito. Obtenido de: https://ministeriopublico.gob.pa/notas-de-prensa/el-ciberdelito-es-real-ministerio-publico-y-policia-nacional-lanzan-campana-de-prevencion-del-delito/
- INTERPOL. (2023). Cybercrime.
- Kaspersky. (2022). IT Threat Evolution in Q2 2022.

- Mitnick, K. D., & Simon, W. L. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley.
- Symantec. (2021). Internet Security Threat Report.