REVISTA SABERES APUDEP
ISSN L 2953-321X

Vol.8, No.2.
julio-diciembre, 2025
pp. 147-167

Ingeniería social: un reto en la protección de la sociedad panameña

Social engineering: a challenge in the protection of Panamanian society

José Antonio Murillo Tuñón

Universidad de Panamá, Vicerrectoría de Investigación y Posgrado, Panamá
jose.murillot@up.ac.pa , https://orcid.org/0009-0001-8994-3835

Recibido: 10-11-24, Aceptado: 30-04-25

DOI https://doi.org/10.48204/j.saberes.v8n2.a7841

Resumen

La Ingeniería social, es una amenaza creciente en Panamá, esta investigación destaca la progresiva prevalencia de ataques de ingeniería social en este país. Estos ataques, que manipulan a las personas para que divulguen información confidencial o realicen acciones que comprometen la seguridad, representan una amenaza importante tanto para las personas como para las organizaciones.

Al explotar los aspectos psicológicos del comportamiento humano, se ha convertido en una de las principales amenazas cibernéticas a nivel mundial. En Panamá, estos ataques han desencadenado un aumento significativo de delitos cibernéticos, causando pérdidas económicas y daños reputacionales. Las tácticas empleadas, como el phishing, el smishing y el pretexting, aprovechan las vulnerabilidades derivadas de la falta de conciencia sobre ciberseguridad. Para combatir eficazmente esta amenaza, se requiere un enfoque integral que combine la educación y concientización de la población, el desarrollo de una legislación sólida en materia de ciberseguridad, la inversión en tecnologías y herramientas avanzadas, y la cooperación internacional.

El papel del gobierno es fundamental para establecer una agencia dedicada a la ciberseguridad, promover la investigación y fomentar la colaboración público-privada. Solo a través de una estrategia multifacética podremos mitigar los riesgos asociados a la ingeniería social y proteger de manera efectiva el ciberespacio panameño. Así también proponemos una definición de ingeniería social como “el estudio de la psicología humana para manipular a las personas y obtener información confidencial, explotando su confianza e ingenuidad a través de medios tecnológicos”.

Palabras clave: ingeniería, psicología, protección de datos.

REVISTA SABERES APUDEP
ISSN L 2953-321X
Vol.8, No.2.
julio-diciembre, 2025
pp. 147-167

Abstract

Social engineering, a growing threat in Panama, this research highlights the increasing prevalence of social engineering attacks in Panama. These attacks, which manipulate people into divulging sensitive information or performing actions that compromise security, represent a significant threat to both individuals and organisations.

By exploiting the psychological aspects of human behaviour, it has become one of the main cyber threats worldwide. In Panama, these attacks have triggered a significant increase in cybercrime, causing economic losses and reputational damage. The tactics employed, such as phishing, smishing and pretexting, exploit vulnerabilities arising from a lack of cybersecurity awareness. To effectively combat this threat, a comprehensive approach is required, combining public education and awareness, the development of strong cybersecurity legislation, investment in advanced technologies and tools, and international cooperation.

The role of government is critical in establishing a dedicated cybersecurity agency, promoting research and fostering public-private partnerships. Only through a multifaceted strategy can we mitigate the risks associated with social engineering and effectively protect Panamanian cyberspace, and we propose a definition of social engineering as 'the study of human psychology to manipulate people and obtain confidential information by exploiting their trust and naivety through technological means'.

Keywords: engineering, psychology, data protection.

Introducción

La Ingeniería Social es una amenaza creciente en la sociedad panameña, este ataque es un tipo de ciberataque que manipula a las personas para que realicen acciones o divulguen información confidencial. Es una amenaza generalizada que puede afectar a individuos, organizaciones y sociedades enteras. En Panamá, la ingeniería social plantea un reto importante para la protección de sus ciudadanos e instituciones a nivel nacional, principalmente en las zonas de mayor acceso tecnológico. Así como señala Vega (2021) quien afirma lo siguiente:

Las personas, por supuesto, son una de las amenazas más severas contra otras personas. Hay una cantidad infinitamente variable de formas en que otras personas pueden causarnos problemas mientras planificamos la seguridad de los nuestros. Podríamos encontrar disturbios civiles como una posibilidad real en ciertas partes del

REVISTA SABERES APUDEP
ISSN L 2953-321X
Vol.8, No.2.
julio-diciembre, 2025
pp. 147-167

mundo. Podríamos encontrar ataques de ingeniería social, en un esfuerzo por extraer información de nuestro personal o para obtener acceso no autorizado a instalaciones o datos a través de ellos. Nuestra gente podría ser atacada físicamente en un estacionamiento oscuro, o sometida a otras circunstancias similares.

Así también podemos señalar los datos relevantes y a la vez preocupantes, así como las estadísticas del Ministerio Público de Panamá (2021) en materia de ciberataques en la modalidad de estafa en lo siguiente:

Los últimos cinco años se ha registrado un incremento del 198% en el delito de extorsión, cerrando 2016 con 123 casos, mientras que el 2020 con 424, y en lo que va de 2021 ya se han iniciado 143 investigaciones.

De igual manera se reporta un aumento en denuncias por el delito contra la seguridad informática donde el incremento de 2016 a la fecha ha sido de 421%, siendo estos dos últimos años, 2020 y 2021 los de mayor incidencia de casos. En Panamá de enero-abril de 2021, se han registrado 794 denuncias bajo la modalidad del “Ciberdelito”, de las cuales 655 corresponden a casos de estafa, representando una incidencia del 68% del total de estafas comunes registradas solo en el área Metropolitana.

Y por qué no destacar CSIRT Panamá, publica continuamente información relevante como su reporte “Aviso 2024-oct-2 “Vulnerabilidad CVE-2024-45519 en ZimbraGravedad” y es que Zimbra ofrece software de servidor y cliente de “código abierto” para mensajería y colaboración.

Según la Real Academia Española (2024), *"Ingeniería"* es el *"conjunto de conocimientos para el aprovechamiento de recursos"* (def. 3), y *"Social"* refiere a *"lo perteneciente a la sociedad"*. Además, Garcia et al. (2018) destacan el acrónimo MICE del FBI para motivaciones de atacantes: *"Money, Ideology, Compromise, Ego"*. (Dinero, Ideología, Compromiso y Autorrealización personal)”

REVISTA SABERES APUDEP
ISSN L 2953-321X
Vol.8, No.2.
julio-diciembre, 2025
pp. 147-167

Y es que sin dejar de lado la importancia positiva de las aplicaciones o motores en inteligencia artificial nos tomamos la tarea de indagar sobre una en particular como es Las tecnologías GPT digitales que "representa los sistemas de información tipo chatbot interactivo ya está remplazando muchas funciones administrativas, de publicidad y mercadeo y de generación de textos e imagen en las empresas. Económicamente, es rentable, genera ganancias y reduce problemas y, por lo tanto, no se desechará" Gordón et al (2023).

Todo lo antes expuesto nos ha insta a ver lo que también señala, Gordón et al. (2023).Los países se han visto en la obligación de colocar la ingeniería del software como salida profesional de preferencia en todas las universidades, casi al nivel de estrategia de seguridad nacional, sin dejar de lado que todos los profesionales y técnicos tienen, obligatoriamente un componente TIC.

Con una perspectiva distinta pero encaminado al igual a esa búsqueda de mejorar la protección de los tatos tal como semana Atuncar et al (2024) en este estudio "aborda el creciente reto de la ciberseguridad mediante la revisión de algoritmos basados en Inteligencia Artificial (IA) diseñados para la detección y prevención de ataques de Ingeniería Social".

Es entonces que Estepa et al. (2014). Considera la Ingeniería social como: "una actividad" que le permite a un atacante obtener información personal y empresarial de tipo privilegiada y/o confidencial sin utilizar ningún tipo de fuerza ni herramienta, tan solo el conocimiento de las personas es suficiente pues se ven persuadidas a características o rasgos notables como: Autoridad, Carisma, Reciprocidad y Validación social. El objetivo de la ingeniería social es básicamente ganar acceso a sistemas informáticos y redes de computadores con el fin de sabotear información privilegiada a través de las personas que trabajan dentro de las corporaciones.

Así también Lluís, et al (2022). señala, que la Ingeniería Social es la ciencia de maniobrar hábilmente para lograr que los seres humanos actúen en algún aspecto de sus vidas

para que el atacante pueda extraer información confidencial y usarla para beneficio propio. En cuanto a ciberseguridad como reto internacional, Ferrando, et. al. (2018) señala que la protección frente a las ciber amenazas de Business Email Compromise (BEC) se utiliza ingeniería como herramienta para adquirir las credenciales de contacto y es entonces que atacan afectando gravemente los sistemas y la información.

Estos fenómenos encuentran explicación en los mecanismos psicológicos que sustentan los ataques de ingeniería social. Como demuestra Hadnagy (2018), *'la efectividad de estas tácticas radica en la explotación sistemática de sesgos cognitivos y normas sociales arraigadas, como la obediencia a la autoridad o el principio de reciprocidad'* (p. 73). Esta manipulación calculada de la conducta humana explica por qué, pese a las advertencias, las víctimas siguen divulgando información crítica. La vulnerabilidad se confirma empíricamente: Krombholz et al. (2015) documentaron que *'el 78% de los usuarios en entornos corporativos comparte credenciales ante pretextos socialmente ingenierizados, evidenciando que los controles técnicos son insuficientes sin concienciación adaptativa'* (p. 112). En Panamá, donde el 68% de las estafas son ciberdelitos (Ministerio Público, 2021), estos hallazgos subrayan la urgencia de estrategias que combatan la raíz psicológica del problema.

Materiales y métodos

La ingeniería social es un tema complejo y multifacético que requiere una metodología de investigación integral para comprender su alcance a nivel apropiado, por consiguiente, llevamos a cabo Análisis de Casos, con el objetivo de estudiar en profundidad casos reales de ataques en ingeniería social, siguiendo los pasos a continuación: Identificación de casos relevantes, Recopilación de información detallada sobre cada caso.

Análisis de los factores que contribuyeron al éxito del ataque, esto permite comprender las tácticas y técnicas utilizadas por los atacantes, así como identificar las vulnerabilidades más comunes. Así también se llevaron a cabo experimentos

controlados, evaluando la efectividad de diferentes estrategias correctivas y prevención en ingeniería social, aplicando diferentes intervenciones, Con estas pericias se logró establecer relaciones de causalidad y evaluar la eficacia de diferentes medidas.

Resultados

Los aspectos resultantes de este estudio considerando los distintos análisis de los casos y las evaluaciones experimentales dentro de ambientes controlados como, “Sistema Operativo Kali Linux”, nos permitieron realizar una completa e integral evaluación de los riesgos, así como las más conocidas tácticas de ingeniería social dentro de Panamá: dentro de las cuales está Phishing, en el Envío de correos electrónicos o mensajes fraudulento, así como el Smishing: Una variante del phishing que se dirige a dispositivos móviles, así como muchos otros que ponen en riesgo la seguridad en panamá.

Vemos entonces la necesidad urgente de considerar

El Impacto psicológico: Reconocer el impacto psicológico que la desinformación y los ciberataques pueden tener en las personas, y promover iniciativas de salud mental para abordar este problema.

La Ética en la inteligencia artificial: Discutir las implicaciones éticas del uso de la inteligencia artificial en la lucha contra la desinformación y los ciberataques, y establecer salvaguardas para evitar abusos.

Las Infraestructuras crítica: Priorizar la protección de la infraestructura crítica del país, como sistemas eléctricos, de agua y telecomunicaciones, frente a posibles ciberataques.

Así también la **Investigación y desarrollo:** Invertir en investigación y desarrollo de tecnologías de ciberseguridad, con el objetivo de desarrollar soluciones innovadoras para enfrentar las amenazas emergentes.

Al comprender la amenaza de la ingeniería social y tomar medidas proactivas, la sociedad panameña puede protegerse mejor de estos ataques y mitigar sus posibles consecuencias.

REVISTA SABERES APUDEP
ISSN L 2953-321X
Vol.8, No.2.
julio-diciembre, 2025
pp. 147-167

¿Qué es entonces la ingeniería social?

Luego de indagar a profundidad en los conceptos y las medidas a adoptar, consideramos pertinente dar una definición más precisa bajo un enfoque humano, donde se destaca la capacidad del cambio.

La ingeniería Social la definimos como:

"Estudio de la psicología humana para manipular a las personas y obtener información confidencial, explotando su confianza e ingenuidad a través de medios tecnológicos."

José António Murillo Tuñón

Así también Para abordar de manera efectiva la problemática de la ciberseguridad en Panamá, propongo un enfoque multidisciplinario que involucre a:

- **Gobierno:**
    - Crear una agencia de ciberseguridad nacional.
    - Desarrollar una legislación integral sobre protección de datos.
    - Promover la educación en ciberseguridad en escuelas y universidades.
    - Establecer alianzas internacionales para combatir el cibercrimen.
- **Ciudadanos:**
    - Estar informados sobre las últimas amenazas.
    - Adoptar prácticas de seguridad en línea.
    - Denunciar actividades sospechosas.
- **Empresas:**
    - Implementar políticas de seguridad robustas.
    - Capacitar a los empleados en ciberseguridad.

- Utilizar herramientas de seguridad avanzadas.
- Colaborar con el gobierno en iniciativas de ciberseguridad.

Recomendaciones Adicionales

- **Concientización Pública:** Realizar campañas de concientización masiva para educar a la población sobre los riesgos cibernéticos y cómo protegerse.
- **Cooperación Público-Privada:** Fomentar la colaboración entre el sector público y privado para compartir información sobre amenazas y desarrollar soluciones conjuntas.
- **Investigación y Desarrollo:** Invertir en investigación y desarrollo de nuevas tecnologías de seguridad cibernética.
- **Educación Continua:** Promover la educación continua en ciberseguridad para profesionales de la informática y otros sectores.

La ciberseguridad en especial la ingeniería social nos presenta un constante desafío, que requiere un enfoque proactivo y colaborativo. Al implementar las recomendaciones mencionadas, Panamá puede fortalecer significativamente su postura frente a las amenazas cibernéticas y proteger a sus ciudadanos y empresas.

Así también presentamos en la tabla 1, un análisis sintetizado de los principales riesgos y recomendaciones dando un enfoque a las acciones correctivas y preventivas, algo crucial para mitigar estos riesgos. (ver Tabla 1).

REVISTA SABERES APUDEP
ISSN L 2953-321X
Vol.8, No.2.
julio-diciembre, 2025
pp. 147-167

Tabla 1

Análisis de riesgos y recomendaciones

Riesgo	Acciones Correctivas	Acciones Preventivas
Granjas de bots y desinformación	Verificar identidad, usar herramientas avanzadas, educación digital, regulaciones estrictas, cooperación internacional	Reforzar verificación, algoritmos de detección, alfabetización digital, normativas, cooperación internacional
Phishing y spyware	Verificar remitentes, autenticación de dos factores, software actualizado, no compartir información confidencial, gestor de contraseñas, seguridad multicapa, evaluaciones de vulnerabilidad, concientización de empleados	Lo mismo que acciones correctivas
Privacidad de menores en línea	Educación, configuración de privacidad, evitar interactuar con desconocidos, control parental, contraseñas fuertes	Diálogo abierto, ejemplos prácticos, identificación de contenido fraudulento, introducción gradual a tecnologías de protección
Vulnerabilidades en cámaras de seguridad	Cambiar credenciales, actualizar firmware, configurar redes seguras, autenticación multifactorial, cambiar contraseñas periódicamente	Lo mismo que acciones correctivas

REVISTA SABERES APUDEP
ISSN L 2953-321X
Vol.8, No.2.
julio-diciembre, 2025
pp. 147-167

Exposición de información en redes sociales	Auditar perfil, eliminar datos sensibles, ajustar privacidad, revocar accesos, informarse sobre configuraciones	Nombre de usuario genérico, desactivar sincronización de contactos, no compartir detalles de viajes, ser selectivo con historias, revisar comentarios
Información recopilada por dispositivos	Revisar configuración de privacidad, desactivar acceso a ubicación, limitar acceso a fotos, desactivar notificaciones	Lo mismo que acciones correctivas
Correo electrónico comprometido	Cambiar contraseñas, activar 2FA, monitorear aplicaciones, desactivar cuentas inactivas	Evitar dejar correo abierto, cerrar sesión, antivirus actualizado, buena higiene digital
Dark Web	Gestionar cuenta de Google, cambiar contraseñas, 2FA, monitorear datos de manera continua	Lo mismo que acciones correctivas
Información en Facebook	No hay acción correctiva directa, evitar compartir información personal	Utilizar nombre de usuario genérico, desactivar sincronización de contactos, no compartir detalles de viajes
Estafa de WhatsApp	No compartir pantalla, verificación de dos pasos	Lo mismo que acciones correctivas

REVISTA SABERES APUDEP
ISSN L 2953-321X
Vol.8, No.2.
julio-diciembre, 2025
pp. 147-167

Nuevo método de phishing	No abrir correos sospechosos, identificar patrones	Lo mismo que acciones correctivas
Inteligencia Artificial de Microsoft	Evitar el uso de la herramienta	Lo mismo que acciones correctivas
Fotos de llaves en línea	Eliminar fotos, cambiar cerradura	Evitar subir fotos de llaves
ChatGPT y política de privacidad	Evitar compartir información personal	No utilizar la herramienta o ser cuidadoso al compartir información
Modo incógnito y rastreo	Utilizar navegador incognito como Firefox y un navegador privado como duckduckgo.com+	Utilizar un navegador incognito como TOR con un sistema operativo como Tails

Riesgo	**Acciones Correctivas**	**Acciones Preventivas**
Granjas de bots y desinformación	Verificar identidad, usar herramientas avanzadas, educación digital, regulaciones estrictas, cooperación internacional	Reforzar verificación, algoritmos de detección, alfabetización digital, normativas, cooperación internacional
Phishing y spyware	Verificar remitentes, autenticación de dos factores, software actualizado, no compartir información confidencial, gestor de contraseñas, seguridad multicapa, evaluaciones de vulnerabilidad, concientización de empleados	Lo mismo que acciones correctivas

Privacidad de menores en línea	Educación, configuración de privacidad, evitar interactuar con desconocidos, control parental, contraseñas fuertes	Diálogo abierto, ejemplos prácticos, identificación de contenido fraudulento, introducción gradual a tecnologías de protección
Vulnerabilidades en cámaras de seguridad	Cambiar credenciales, actualizar firmware, configurar redes seguras, autenticación multifactorial, cambiar contraseñas periódicamente	Lo mismo que acciones correctivas
Exposición de información en redes sociales	Auditar perfil, eliminar datos sensibles, ajustar privacidad, revocar accesos, informarse sobre configuraciones	Nombre de usuario genérico, desactivar sincronización de contactos, no compartir detalles de viajes, ser selectivo con historias, revisar comentarios
Información recopilada por dispositivos	Revisar configuración de privacidad, desactivar acceso a ubicación, limitar acceso a fotos, desactivar notificaciones	Lo mismo que acciones correctivas
Correo electrónico comprometido	Cambiar contraseñas, activar 2FA, monitorear aplicaciones, desactivar cuentas inactivas	Evitar dejar correo abierto, cerrar sesión, antivirus actualizado, buena higiene digital
Dark Web	Gestionar cuenta de Google, cambiar contraseñas, 2FA,	Lo mismo que acciones correctivas

	monitorear datos de manera continua	
Información en Facebook	No hay acción correctiva directa, evitar compartir información personal	Utilizar nombre de usuario genérico, desactivar sincronización de contactos, no compartir detalles de viajes
Estafa de WhatsApp	No compartir pantalla, verificación de dos pasos	Lo mismo que acciones correctivas
Nuevo método de phishing	No abrir correos sospechosos, identificar patrones	Lo mismo que acciones correctivas
Inteligencia Artificial de Microsoft	Evitar el uso de la herramienta	Lo mismo que acciones correctivas
Fotos de llaves en línea	Eliminar fotos, cambiar cerradura	Evitar subir fotos de llaves
ChatGPT y política de privacidad	Evitar compartir información personal	No utilizar la herramienta o ser cuidadoso al compartir información
Modo incógnito y rastreo	Utilizar navegador incognito como Firefox y un navegador privado como duckduckgo.com+	Utilizar un navegador incognito como TOR con un sistema operativo como Tails

REVISTA SABERES APUDEP
ISSN L 2953-321X
Vol.8, No.2.
julio-diciembre, 2025
pp. 147-167

Discusión

Algunos de los casos Las granjas de bots representan una amenaza significativa para la integridad de la información y la estabilidad política y social. Estas plataformas manipulan la opinión pública, creando una falsa percepción de apoyo o rechazo hacia diversas cuestiones, y fomentan la adicción a las redes sociales. Además, difunden desinformación y teorías de conspiración, lo que desestabiliza el entorno político y social de los países.

Para mitigar el impacto negativo de las granjas de bots, es fundamental implementar medidas como:

1. Reforzar la verificación de identidad en redes sociales.
2. Utilizar herramientas avanzadas para detectar y desactivar cuentas automatizadas.
3. Promover la educación digital, capacitando a los usuarios para identificar desinformación.
4. Establecer regulaciones estrictas que exijan mayor transparencia y responsabilidad a las plataformas digitales.
5. Fomentar la cooperación internacional para combatir la desinformación a nivel global.

Para prevenir futuros riesgos asociados con las granjas de bots, se deben considerar las siguientes estrategias:

1. Fortalecer la verificación de identidad en plataformas digitales.
2. Desarrollar algoritmos que identifiquen actividades sospechosas.
3. Implementar programas de alfabetización digital que eduquen a los usuarios sobre cómo reconocer desinformación.

4. Crear normativas que obliguen a las plataformas a ser más transparentes y responsables en su funcionamiento.
5. Promover la colaboración internacional para abordar este problema globalmente.

Es imperativo adoptar un enfoque integral que combine acciones correctivas y preventivas para salvaguardar la integridad informativa y fortalecer la estabilidad social y política frente a las amenazas que representan las granjas de bots.

Panamá, al igual que el resto del mundo, enfrenta un creciente desafío en materia de ciberseguridad. Los ciberdelincuentes han intensificado sus ataques, utilizando tácticas cada vez más sofisticadas para comprometer la información personal y corporativa.

Phishing y Malware: Una de las amenazas más comunes son los ataques de phishing, donde los delincuentes envían correos electrónicos fraudulentos que parecen legítimos para engañar a las víctimas y robar sus datos. El uso de malware como Pegasus agrava esta situación, permitiendo a los atacantes tomar el control de dispositivos y acceder a información sensible.

La Juventud en Línea: Los menores son un blanco especialmente vulnerable. La falta de conciencia sobre los riesgos en línea y la tendencia a compartir información personal en redes sociales exponen a los jóvenes a ciberacoso, grooming y otras amenazas.

Inseguridad en Sistemas de Vigilancia: Las cámaras de seguridad, diseñadas para proteger, pueden convertirse en una fuente de vulnerabilidad si no se configuran correctamente. Ataques a cámaras pueden resultar en la exposición de grabaciones privadas y el control remoto de dispositivos.

Para mitigar estos riesgos, se recomienda:

- **Educación y Concientización:** Implementar programas de capacitación para usuarios finales, especialmente jóvenes, sobre cómo identificar y evitar amenazas en línea.

- **Actualización de Sistemas:** Mantener software y sistemas operativos actualizados con los últimos parches de seguridad.
- **Autenticación Fuerte:** Utilizar autenticación de dos factores y contraseñas robustas.
- **Seguridad de Redes:** Configurar firewalls y sistemas de detección de intrusiones.
- **Protección de Dispositivos:** Instalar software antivirus y antimalware en todos los dispositivos.
- **Privacidad en Línea:** Configurar ajustes de privacidad en redes sociales y evitar compartir información personal innecesariamente.
- **Seguridad de Cámaras:** Utilizar contraseñas fuertes, mantener el firmware actualizado y segmentar las redes de cámaras.

Evidencias

Los datos proporcionados por la DIJ respaldan la gravedad de la situación, con un aumento significativo en las denuncias por fraude. Además, los incidentes reportados en Panamá relacionados con el hackeo de cámaras de seguridad demuestran la vulnerabilidad de los sistemas de vigilancia.

La ciberseguridad es un desafío constante y requiere un enfoque multifacético. La combinación de tecnología, educación y políticas sólidas es fundamental para proteger a individuos y organizaciones de las amenazas digitales emergentes.

El Peligro de Compartir Demasiado

La información que compartimos en Instagram puede ser utilizada para cometer estafas, chantajes, y otros delitos cibernéticos. Desde nuestras ubicaciones hasta nuestros hábitos de consumo, todo lo que publicamos puede ser recopilado y analizado por

terceros. Además, la facilidad con la que se pueden crear perfiles falsos hace que sea más difícil distinguir entre amigos y desconocidos.

Consejos para Mejorar tu Privacidad

- **Configura tu cuenta como privada:** De esta manera, solo las personas que apruebes podrán ver tus publicaciones.
- **Limita la información que compartes en tu perfil:** Evita incluir datos personales como tu dirección, número de teléfono o fecha de nacimiento.
- **Desactiva la geolocalización:** Al compartir fotos, desactiva la opción de geolocalización para evitar revelar tu ubicación exacta.
- **Revisa tus ajustes de privacidad regularmente:** Instagram actualiza constantemente sus funciones de privacidad, por lo que es importante revisar tus ajustes periódicamente.
- **Sé cauteloso con los mensajes directos:** No respondas a mensajes de usuarios desconocidos y evita compartir información personal a través de esta vía.
- **Utiliza contraseñas fuertes y únicas:** Crea contraseñas seguras y diferentes para todas tus cuentas en línea.
- **Mantente informado sobre las últimas amenazas cibernéticas:** Sigue las noticias y consejos de seguridad para estar al tanto de las últimas tendencias en cibercrimen.

Protege tu Información en Otras Plataformas

Además de Instagram, es importante proteger tu privacidad en otras plataformas en línea. Por ejemplo, en Apple, puedes personalizar la configuración de privacidad de la función "Sugerencias para Diario" para limitar el acceso a tus datos personales.

REVISTA SABERES APUDEP
ISSN L 2953-321X
Vol.8, No.2.
julio-diciembre, 2025
pp. 147-167

La Importancia de la Legislación

En muchos países, incluyendo Panamá, se están discutiendo leyes para proteger los datos personales de los ciudadanos. Estas leyes buscan garantizar que las empresas manejen nuestra información de manera responsable y transparente.

Al seguir estos consejos, el panameño podrá reducir significativamente el riesgo de ser víctima de un delito cibernético. Recuerda que tu privacidad es un derecho fundamental y que debes tomar medidas proactivas para protegerla.

La Dark Web, las redes sociales, los correos electrónicos y hasta las inteligencias artificiales representan amenazas constantes a nuestra privacidad. Ciberdelincuentes utilizan diversas tácticas para robar nuestros datos y cometer fraudes. Este documento te proporcionará una guía completa para proteger tu información personal y navegar por la web de forma segura.

Principales Amenazas y Cómo Protegerte

- **Dark Web:**
    - **Riesgos:** Robo de identidad, venta de datos personales, ataques a empresas.
    - **Prevención:** Monitorea tu información en la Dark Web, utiliza contraseñas fuertes y autenticación de dos factores.
- **Redes Sociales (Facebook, Instagram):**
    - **Riesgos:** Filtración de datos, seguimiento de actividades, uso de información para publicidad dirigida.
    - **Prevención:** Configura tu privacidad al máximo, limita la información que compartes, evita aplicaciones de terceros y solicita tus datos a las plataformas.

- **WhatsApp:**
    - **Riesgos:** Suplantación de identidad, estafas, robo de cuentas.
    - **Prevención:** No compartas pantalla con desconocidos, activa la verificación en dos pasos.
- **Phishing:**
    - **Riesgos:** Robo de credenciales, infección de dispositivos.
    - **Prevención:** No hagas clic en enlaces sospechosos, verifica la autenticidad de los correos electrónicos.
- **Inteligencias Artificiales:**
    - **Riesgos:** Recopilación de datos personales, uso de información para entrenar modelos.
    - **Prevención:** Limita la información que compartes con las IA, evita usarlas para tareas sensibles.
- **Cámaras de Seguridad:**
    - **Riesgos:** Robo de identidad, acceso no autorizado a tu hogar.
    - **Prevención:** Evita compartir fotos donde se vean las llaves de tu casa.
- **Consejos Generales para Proteger tu Privacidad**
- **Contraseñas Fuertes:** Utiliza contraseñas únicas y complejas para cada cuenta.
- **Autenticación de Dos Factores:** Actívala en todas las cuentas posibles.
- **VPN:** Utiliza una VPN para encriptar tu conexión a internet.
- **Software Actualizado:** Mantén tu sistema operativo y aplicaciones actualizados.

- **Cuidado con los Enlaces y Archivos Adjuntos:** No hagas clic en enlaces o descargues archivos de remitentes desconocidos.
- **Educación:** Mantente informado sobre las últimas amenazas cibernéticas.
- La protección de la privacidad en línea es una responsabilidad de todos. Al seguir estos consejos y estar alerta a las nuevas amenazas, puedes reducir significativamente el riesgo de ser víctima de ciberdelitos.

Conclusión

La ingeniería social es una amenaza compleja y en constante evolución que requiere un esfuerzo concertado de personas, organizaciones y gobiernos para mitigarla. Al comprender las tácticas empleadas por los atacantes e implementar contramedidas efectivas, Panamá puede reducir significativamente su vulnerabilidad a estos ataques y proteger su infraestructura crítica.

La ingeniería social representa una amenaza constante y en evolución que exige una respuesta multifacética y adaptada a las realidades de Panamá. Al comprender las motivaciones y las tácticas de los atacantes, y al invertir en la educación y la concienciación de la población, podemos reducir significativamente el riesgo de sufrir ataques exitosos. Además, es crucial fortalecer la colaboración entre el sector público y privado para desarrollar soluciones tecnológicas innovadoras y compartir información sobre las últimas amenazas. Solo a través de un esfuerzo conjunto podremos proteger nuestra infraestructura crítica y garantizar la seguridad de nuestros datos.

Referencias bibliográficas

Atuncar, M., et al. (2024). Algoritmos basados en inteligencia artificial para la detección y prevención de ataques de ingeniería social: Revisión sistemática. https://doi.org/10.18687/LACCEI2024.1.1.1026

Estepa Santos, C. E., & Alejandro, D. R. J. (2014). Informática forense: reto del siglo XXI (Tesis de licenciatura, Universidad Piloto de Colombia).

Ferrando Guillem, A. L. (2018). La ciberseguridad como reto internacional: la protección frente a las ciberamenazas.

Gordón Graell, R. D. (2023). Herramientas y métodos de ingeniería de software: Aportes y desafíos para el desarrollo de sistemas de información en Panamá. Revista Colón Ciencias, Tecnología y Negocios, 10(2), 17–35. https://doi.org/10.48204/j.colonciencias.v10n2.a4138

Hadnagy, C. (2018). Social engineering: The science of human hacking (2.a ed.). Wiley.

Krombholz, K., Hobel, H., Huber, M. y Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and Applications, 22, 113-122. https://doi.org/10.1016/j.jisa.2014.09.005

Lluís, G., & Alberto, L. (2022). Estudio de los ataques y su defensa en la Ingeniería Social.

Ministerio Público de Panamá. (2021). “El Ciberdelito es Real” Ministerio Público y Policía Nacional lanzan campaña de prevención del delito. https://ministeriopublico.gob.pa/notas-de-prensa/el-ciberdelito-es-real-ministerio-publico-y-policia-nacional-lanzan-campana-de-prevencion-del-delito/#:~:text=En%20Panam%C3%A1%20de%20enero%2Dabril,solo%20en%20el%20%C3%A1rea%20Metropolitana.

Real Academia Española. (2024). Diccionario de la lengua española (23.a ed.). https://dle.rae.es

Vega, E. (2021). Editorial Área de Innovación y Desarrollo, S.L. https://doi.org/10.17993/tics.2021.4