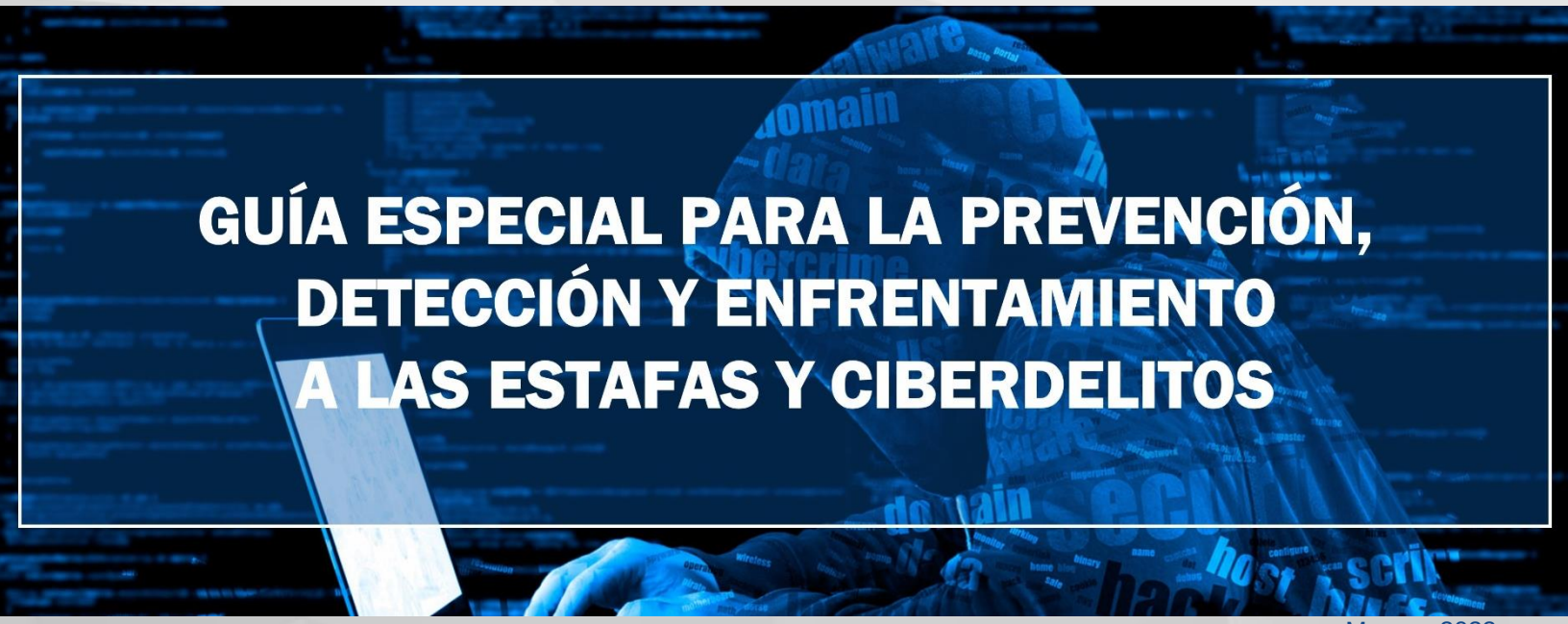

GUÍA ESPECIAL PARA LA PREVENCIÓN, DETECCIÓN Y ENFRENTAMIENTO A LAS ESTAFAS Y CIBERDELITOS

Marzo • 2022

Con el contenido del presente documento, la Unidad de Análisis Financiero de la República de Nicaragua, ***pretendemos fortalecer las alertas, aunar y dirigir acciones a la prevención, disminución y erradicación de las estafas y ciberdelitos***, por ende, a la ***protección permanente del patrimonio personal y empresarial,*** lo que no es más que reafirmar nuestro lema permanente de, ***"Por una Economía Sana y Segura"*** y nuestro lema de décimo aniversario, ***"Diez años defendiendo la economía".***

Conforme datos públicos relacionados a la incidencia del cibercrimen en América, (https://assets.kpmg/content/dam/kpmg/xx/pdf/2022/01/fraud-survey-report-spanish-mx-version.pdf) durante el año 2021 se presentó un aumento significativo, en el que evidentemente se aprovecharon de la pandemia COVID 19, destacándose como las principales modalidades utilizadas por los ciberdelincuentes las ya identificadas como ***estafas virtuales:*** Phishing (44%), Scamming (33%) y Social Hacking (17%); asimismo, ***en Nicaragua las denuncias por estafa en el año 2020 incrementaron en un 36.6%*** con respecto al 2019, aunque no se especifica la modalidad utilizada.
(https://www.policia.gob.ni/wp-content/uploads/2021/05/Anuario-PN-2020-marzo.pdf)

En correspondencia con las acciones que implica el aumento de la inclusión financiera, actualmente las instituciones financieras han optimizado los servicios ofertados a sus clientes, brindándoles mayores facilidades, comodidad, ahorro de tiempo y seguridad, por tanto, ***los clientes, en su mayoría, hacen un constante uso del Internet*** para ejecutar todo tipo de gestiones y transacciones financieras y comerciales que le son permitidas por esta vía, no obstante, es importante destacar ***que el riesgo a ser víctimas de la ciberdelincuencia aumenta***, máxime cuando existen ***prácticas insuficientes y falta de medidas de seguridad*** por parte de los usuarios en el uso de las tecnologías de la información y comunicación (TIC).

Asociado a lo anterior, es un hecho que la mayoría de los usuarios del Internet mantienen en la nube una cantidad increíble de sus datos personales, así como, de parientes y de amistades, lo que permite a los ciberdelincuentes poder ***conocer previamente a sus potenciales víctimas, caracterizarlos*** con solo leer sus publicaciones en las diferentes redes sociales, además, de aquellos formularios que los mismos llenan en línea en la búsqueda de empleo o la oferta de bienes o servicios.

El **Código Penal de Nicaragua** establece en su **artículo 229** la tipificación del delito de **Estafa** como: ***"Quien con el propósito de obtener un provecho ilícito, para sí o para un tercero,*** *mediante* ***ardid o engaño, induzca o mantenga en error a otra persona*** *para que realice una disposición total o parcial* ***sobre el patrimonio propio o ajeno,*** *siempre que el valor del perjuicio patrimonial exceda la suma equivalente a dos salarios mínimos mensuales del sector industrial,* ***será penado con prisión de uno a cuatro años y noventa a trescientos días multa****. La misma pena se impondrá a quien con el propósito de obtener un provecho ilícito, consiga la* ***transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero, mediante la manipulación de registros informáticos o programas de computación o el uso de otro artificio semejante."***

Continúa en página 2...

Viene de portada...

Así mismo, la **Ley N° 1042 "Ley Especial de Ciberdelitos"**, tiene por **objeto** la prevención, investigación, persecución y sanción de los delitos cometidos por medio de las Tecnologías de la Información y la Comunicación, en perjuicio de personas naturales o jurídicas, así como, la protección integral de los sistemas que utilicen dichas tecnologías; esta Ley define los **Ciberdelitos** como: *"Acciones u omisiones, típicas, antijurídicas, continuas o aisladas, de carácter penal, cometidas en contra de personas naturales y/o jurídicas, utilizando como método, como medio o como fin, los datos, sistemas informáticos, Tecnologías de la Información y la Comunicación y que tienen por objeto lesionar bienes jurídicos personales, patrimoniales o informáticos de la víctima".*

30-10-2020 LA GACETA - DIARIO OFICIAL 201

ASAMBLEA NACIONAL

EL PRESIDENTE DE LA REPÚBLICA DE NICARAGUA

A sus habitantes, hace saber:

Que,

LA ASAMBLEA NACIONAL DE LA REPÚBLICA DE NICARAGUA

Ha ordenado lo siguiente:

LA ASAMBLEA NACIONAL DE LA REPÚBLICA DE NICARAGUA

En uso de sus facultades,

HA DICTADO

La siguiente:

LEY Nº. 1042

LEY ESPECIAL DE CIBERDELITOS

Capítulo I

Disposiciones Generales

Artículo 1 Objeto

La presente Ley tiene por objeto la prevención, investigación, persecución y sanción de los delitos cometidos por medio de las Tecnologías de la Información y la Comunicación, en perjuicio de personas naturales o jurídicas, así como la protección integral de los sistemas que utilicen dichas tecnologías, su contenido y cualquiera de sus componentes, en los términos previstos en esta Ley.

Artículo 2 Ámbito de aplicación

La presente Ley es de orden público y se aplicará a quienes cometan los delitos previstos en ésta, dentro o fuera del territorio nacional.

Artículo 3 Definiciones

Para los efectos de la presente Ley se entenderá:

1. **Acceso a sistemas de información:** Es la entrada a dichos sistemas, incluyendo los accesos remotos.

2. **Acceso a la información contenida en un dispositivo que permita el almacenamiento de datos:** Es la lectura, copia, extracción, modificación o eliminación de la información contenida en dicho dispositivo.

3. **Copia de datos:** Es la reproducción total o parcial de la información digital.

4. **Ciberdelitos:** Acciones u omisiones, típicas, antijurídicas, continuas o aisladas, de carácter penal, cometidas en contra de personas naturales y/o jurídicas, utilizando como método, como medio o como fin, los datos, sistemas informáticos, Tecnologías de la Información y la Comunicación y que tienen por objeto lesionar bienes jurídicos personales, patrimoniales o informáticos de la víctima.

5. **Datos informáticos:** Es cualquier representación de hechos, información o conceptos en un formato digital o análogico, que pueden ser generados, almacenados, procesados o transmitidos a través de las Tecnologías de la Información y la Comunicación.

6. **Datos relativos al tráfico:** Todos los datos relativos a una comunicación realizada a través de cualquier medio tecnológico, generados por este último, que indiquen el origen, el destino, la ruta, la hora, la fecha y el tipo de servicio o protocolo utilizado, tamaño y la duración de la comunicación.

7. **Datos personales:** Es la información privada concerniente a una persona, identificada o identificable, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, número telefónico o otra similar.

8. **Datos personales sensibles:** Es toda información privada que revele el origen racial, étnico, filiación política, credo religioso, filosófico o moral, sindical, relativo a su salud o vida sexual, antecedentes penales o faltas administrativas, económicos financieros, así como información crediticia y financiera y cualquier otra información que pueda ser motivo de discriminación.

9. **Dispositivo:** Es cualquier mecanismo, instrumento, aparato, medio que se utiliza o puede ser utilizado para ejecutar cualquier función de la Tecnología de la Información y la Comunicación.

10. **Dispositivos de almacenamiento de datos informáticos:** Es cualquier medio a partir del cual la información es capaz de ser leída, grabada, reproducida o transmitida con o sin la ayuda de cualquier otro medio idóneo.

11. **Entrega de datos y archivos informáticos:** Se entiende la transferencia de informaciones, documentos o datos en formato electrónico que obren en poder de particulares, entidades públicas o privadas.

12. **Identidad informática:** Información, datos o cualquier otra característica que individualice, identifique o distinga una persona de otra o a un usuario de otro usuario, dentro de un sistema informático.

13. **Intercepción y depósito de sistemas informáticos o dispositivos de almacenamiento de datos:** Se entiende su ocupación física y su requerimiento por las autoridades competentes.

14. **Interceptar:** Acción de apropiarse o interrumpir datos informáticos contenidos o transmitidos por medio de las Tecnologías de la Información y la Comunicación antes de llegar a su destino.

15. **Interferir:** Obstaculizar, perturbar o obstruir por medio

9319

La Ley 1042 tipifica el "**Hurto por medios informáticos**": ***"El que, por medio del uso de las Tecnologías de la Información y la Comunicación, se apodere de bienes o valores tangibles o intangibles de carácter patrimonial, sustrayéndolos a su propietario, tenedor o poseedor, con el fin de obtener un provecho económico para sí o para otro, siempre que el valor de lo hurtado sea mayor a la suma resultante de dos salarios mínimos mensuales del sector industrial será sancionado con prisión de dos a cinco años y trescientos a seiscientos días multa."***.

De igual esta Ley tipifica el delito de **"Utilización de datos personales"** como: ***"El que, sin autorización utilice datos personales a través del uso de las Tecnologías de la Información y la Comunicación, violando sistemas de confidencialidad y seguridad de datos, insertando o modificando los datos en perjuicio de un tercero, se le impondrá pena de cuatro a seis años de prisión y doscientos a quinientos días multa".***

La Unidad de Análisis Financiero (UAF) tiene como propósito proteger la economía nacional y la integridad del Sistema Financiero Nacional; disminuir la capacidad económica y operativa de las organizaciones delictivas nacionales o internacionales, a través de su misión de prevenir y enfrentar el lavado de activos provenientes de actividades ilícitas.

Sobre la base de todo lo anterior, en la presente Guía Especial se pretende brindar una serie de contenidos que podrían contribuir a visualizar oportunamente algunos tipos de delitos que han estado y continuarán afectando el patrimonio personal, familiar y empresarial de las víctimas, así como, proporcionar una serie de medidas básicas dirigidas a prevenir y enfrentar estos delitos en función de irlos mitigando.

Técnicas más utilizadas para ejecutar estafas

Dado el crecimiento de la popularidad de los servicios de banca en línea, el robo de información bancaria se ha vuelto uno de los tipos más comunes de actividad delictiva en Internet. Además de robar códigos de acceso de cuentas bancarias personales y corporativas, los cibercriminales también roban los números de las tarjetas de crédito y otros tipos de tarjetas de pago.

Los criminales usan diversas técnicas para obtener acceso a información bancaria para luego robar fondos a través de retiros en cajeros automáticos, transferencias electrónicas y compras en línea, siendo la principal la **Ingeniería Social**; conocida por el uso del engaño para manipular a las personas con el fin de que permitan el acceso o la divulgación de información o datos, por ello, para llevar a cabo esta técnica, los criminales utilizan varios tipos de ataques o modos de operar, entre los que se destacan:

Tipos de ataques

Baiting: implica la creación de una trampa, como una memoria USB cargada con malware. Alguien que quiere ver el contenido del dispositivo lo introduce en su unidad USB, lo que hace que el sistema se vea comprometido.

Pretexting: Este ataque utiliza un pretexto para obtener la atención de la víctima e inducirla a que proporcione información. Por ejemplo, una encuesta por Internet podría parecer bastante inocente al principio, pero luego solicitar los datos de una cuenta bancaria.

Phishing y Spam: Los ataques de phishing implican un correo electrónico o mensaje de texto que pretenden ser de una fuente de confianza y en los que se solicita información. Un tipo muy conocido es el correo electrónico que supone ser de un banco y quiere que sus clientes "confirmen" su información de seguridad y los dirige a un sitio falso donde se registran sus credenciales de acceso.

Tipos de ataques

Vishing y Smishing: Estos tipos de ataques de ingeniería social son variantes del phishing, "phishing de voz", que consiste simplemente en llamados telefónicos para pedir datos. El delincuente puede hacerse pasar por un compañero de trabajo, por ejemplo, y fingir ser del servicio de asistencia informática para pedir información de acceso. El Smishing utiliza mensajes SMS para tratar de obtener esta información.

Intercambio (in)justo: Dicen que "el intercambio justo no es un robo", pero en este caso lo es. Muchos ataques de ingeniería social hacen creer a las víctimas que están recibiendo algo a cambio de los datos o el acceso que proporcionan.

Spoofing: Es el uso de técnicas de suplantación de identidad. Hay diferentes tipos de Spoofing, entre ellos el envío de correos electrónicos o páginas fraudulentas, falsificación de dispositivos o de direcciones IP. Independientemente del tipo, los ataques de Spoofing son maliciosos. Es decir, quienes realizan este tipo de fraudes buscan hacerse pasar por otras personas, organizaciones o empresas para acceder a datos personales, distribuir malware o generar algún tipo de perjuicio. El phishing y el Spoofing suelen ir de la mano, mientras el phishing es una técnica de cibercrimen en la que los piratas informáticos tratan de pescar a sus víctimas para robarles sus datos personales, el Spoofing hace referencia a una de las técnicas que usan los delincuentes para realizar esa pesca.

Farming y Hunting: Otros ataques de ingeniería social son mucho más avanzados. La mayoría de los enfoques simples que hemos descrito son una forma de "Hunting". Consisten, básicamente, en entrar, tomar la información y salir.

SIM Swapping: permite a los criminales robar tu identidad mediante el secuestro del número de teléfono al obtener un duplicado de tu tarjeta SIM.

En este tipo de estafa, los delincuentes tratan de obtener las credenciales del usuario; normalmente aquellas relacionadas con la banca online para maximizar el beneficio económico; una vez conseguidas las credenciales, los delincuentes tratan de obtener un clonado de la SIM de la víctima para así poder recibir los códigos de verificación por SMS (doble factor de autenticación). Para eso, los cibercriminales se aprovechan de las pobres medidas de verificación de la identidad que suelen solicitar algunos operadores. Tras recopilar la información personal de sus víctimas, por ejemplo, a través de las redes sociales, realizan una llamada o se presentan físicamente en una tienda de la compañía telefónica responsable de la SIM que quieren clonar para solicitar un duplicado de la tarjeta. Una vez conseguido este duplicado, los delincuentes pueden entrar a la cuenta bancaria de la víctima, realizar transferencias o incluso solicitar créditos en su nombre. A la hora de confirmar la operación no tendrán problema, puesto que reciben los mensajes con el doble factor de autenticación (2FA) en la SIM clonada.

Modos de operar

- Los ciberdelincuentes realizan llamadas telefónicas o te contactan vía WhatsApp o correo electrónico en nombre de; funcionarios de una autoridad reguladora y/o supervisora vinculada a servicios financieros, comercio y/o migración o una empresa privada relacionada a exportaciones e importaciones (almacenes comerciales, gestores y similares) y de Bancos.

- Ventanas de sitios web falsos, los virus troyanos pueden atacar las computadoras de las víctimas y mostrar una ventana de diálogo o imagen en la computadora de cada usuario. La ventana imita la apariencia del sitio web del banco del usuario y te pide que ingreses tu nombre de usuario y contraseña.

- Por razones de negocios en línea, piden a la futura víctima una cuenta a la que le depositarán el dinero con el cual le realizarán compra de algún producto que tiene en venta, indicándole ingresar sus credenciales en Banca en Línea al Link "X"; Si la víctima revisa y les dice no tener el depósito, le indican que alguien del banco la contactará para solucionar; casi de inmediato otro delincuente haciéndose pasar por trabajador del banco "X", le indica que sí tiene un depósito de "X cantidad" y para lograr hacer efectivo requiere le facilite sus credenciales: usuario, contraseña, etc.

- Algunos estafadores o sus cómplices le solicitan a la víctima el préstamo de su cuenta para recibir dinero, pagándole por este favor.

- Utilización de cuentas de una persona natural en el papel de "comisionista", más bien de "trampolín" para estar recibiendo dinero estafado y luego transferirlo a otra(s) cuenta(s); por esto se gana una cantidad acordada (realmente podría estar siendo utilizada a ciegas o por necesidad).

- La víctima en potencia recibiendo llamada del área de tecnología de "X" banco para realizar mantenimiento de sistema, requiriendo los datos necesarios para poder hacerlo, seguido de algunas pruebas consistiendo en hacer varias transferencias de dinero, mismas que posteriormente serían anuladas.

- En el actuar de los ciberdelincuentes, realizan llamadas telefónicas a los que han perfilado, para lo cual piden un número de cuenta y banco para poder realizar el depósito, pero, además, piden otros datos como la verificación de los dos nombres y apellidos, lugar y fecha de nacimiento, si utiliza tarjetas de crédito y/o débito, si quieren que se acredite el dinero a una de ellas, entonces piden la identificación completa de la misma.

Modos de operar

- Los ciberdelincuentes realizan llamada para comunicar con gran felicidad que la suerte les ha favorecido, en un sorteo en "X" país, la potencial víctima es ganadora de un automóvil, pero, para poder enviarlo en barco, debe asumir los gastos de envío en el menor tiempo posible y piden la cantidad "X" que ellos necesitan (no es exagerada, para ser creíble y en correspondencia a lo que cuesta este servicio).
- Los ciberdelincuentes realizan llamada para comunicar que le vino una mercancía de "X" país y se encuentra en Aduana (o un almacén) para lo cual la potencial víctima debe depositar el costo necesario para la entrega. Pueden aprovechar para extraer otras informaciones vinculadas a cuentas bancarias, tarjetas de crédito y más.
- Estafadores presentándose personalmente a un negocio como supuesto colaborador del área de Tecnología de "X" empresa, para realizar actualizaciones de los sistemas. Una vez ganada la confianza del personal de la tienda, les indica que tienen que realizar una prueba con el POS de Agente del Banco "X", debido a que se actualizará automáticamente con el sistema. La prueba consiste en realizar depósitos mediante el Agente del Banco "X" a diferentes cuentahabientes de ese Banco y que dichos depósitos serán anulados posteriormente.
- A la potencial víctima la llama el delincuente estafador identificándose como trabajador del área de seguridad bancaria, alertándolo e indicándole que está siendo víctima en proceso de una estafa y que por ello requiere le facilite de inmediato los datos de su cuenta para poder bloquear el delito en marcha; si la potencial víctima cae en el engaño, de inmediato le sustraen el dinero.

Errores y/o descuidos en los que reinciden los usuarios

- → Usuario que dan clic a ventanas emergentes en los navegadores web.
- → Usuarios que atienden llamadas telefónicas de supuestos ejecutivos de entidades financieras, que les requieren datos personales y no solicitan o verifican la identidad de la persona que la requiere.
- → Usuarios que acceden a los enlaces proporcionados en correos electrónicos que reciben sin antes verificar la dirección de dominio del remitente.
- → Usuarios que pierden sus tarjetas de crédito o débito y no la reportan de inmediato.
- → Usuarios que por algún motivo facilitan o prestan sus tarjetas de crédito o débitos a algún pariente o amistad.
- → Usuarios que prestan sus cuentas bancarias a terceros para ser utilizadas como puente a cambio de recibir dinero.
- → Usuarios que no atienden las recomendaciones de seguridad brindadas por las entidades financieras para evitar ser víctimas de estafas.

Medidas y recomendaciones técnicas y de seguridad para la protección de nuestro patrimonio

- Instruirnos permanentemente sobre el modo de operar, tipologías (vías, canales, formas, métodos y procedimientos creíbles, pero, fraudulentos, que utilizan para apropiarse de tu dinero).
- Identificar con la mayor y mejor exactitud el(los) sitio(s) del Internet al que desea ingresar o en el que ya ha ingresado.
- Suscribirse a sitios en el Internet que nos resulten bien seguros; no acceder al home banking (banca online o e-banking) o apps financieras desde equipos públicos y redes WIFI abiertas.

- Activar la autenticación de dos factores en cuentas de redes sociales y WhatsApp o las plataformas digitales que utilices. Esta herramienta es una capa adicional de seguridad que ayuda a verificar que solo la persona usuaria de la cuenta pueda acceder a sus redes sociales y plataformas digitales. Se activa ingresando al menú de ajustes o configuración de la cuenta que se quiere proteger, opción "Autenticación en dos pasos".
- Asegurarse de que los datos e informaciones personales, familiares, de amistades y de trabajo que ingresaremos, realmente serán protegidos y se les garantizará seguridad, confidencialidad y manejo limitado.
- No excedernos en facilitar cuantos datos e informaciones nos requiera alguna persona natural por vía telefónica, WhatsApp, Chat, sitios oficiales de Facebook, Twitter e Instagram.
- No nos confiemos y primero verifiquemos, si nos llamaron para realizar una "encuesta" de "X" empresa, en la que primero nos piden "comprobar" nuestros datos personales y de cliente.
- Cualquier duda, insuficiencia o ampliación de datos que nos requiera alguna institución bancaria, financiera, institución pública, empresa en donde goce de crédito y/o similares, no permitamos que se haga extensiva vía telefónica, correo electrónico, WhatsApp, Redes Sociales o similares, deberíamos o podríamos interrumpir la comunicación expresando que nos den un tiempo prudencial para verificar los datos de quien lo está indagando o entrevistando, o sencillamente manifestar que preferimos presentarnos físicamente a las instalaciones de la institución.

Medidas y recomendaciones técnicas y de seguridad para la protección de nuestro patrimonio

- No debemos abrir cualquier enlace que nos llegue por correo, el mismo se debe verificar antes; los ciberdelincuentes tienen la posibilidad de crear páginas web fraudulentas.
- Mantener actualizado el navegador, el sistema operativo de los equipos, antivirus y las aplicaciones, además de eliminar las que no se utilizan o innecesarias.
- No debemos facilitar nuestra información sensible, tales como: identidad y demás datos personales; usuario o contraseña en línea; dirección y contraseña de correo electrónico; datos de cuentas bancarias; numeración o PIN de tarjetas; códigos o PIN para transferencias; entre otras.
- Descargar de gratis en el Internet programas que no conocemos nos ubica en una situación de alto riesgo para ser hackeado, nos exponemos a que nos instalen programas maliciosos o espías, virus o programas que más tarde nos bloquean totalmente nuestra computadora y nos obliguen a pagar dinero para poder recuperar nuestra información.
- Nunca se debe acudir a un cajero automático, abrir la app o acceder al home banking cuando se recibe una llamada supuestamente proveniente de la entidad bancaria. El cliente comúnmente debe ser el que origina la llamada.

- No debemos mantener conectada nuestra computadora las 24 horas, mucho menos en las horas nocturnas de nuestro descanso. Mientras la computadora esté conectada a una fuente de poder, las posibilidades de que la interfieran y te instalen programas espías o virus, así como, te sustraigan la información que deseen los ciberdelincuentes, son reales.
- Evitar descargar apps móviles desde la web y hacerlo desde las diferentes plataformas de distribución digital de aplicaciones móviles desarrolladas por fabricantes reconocidos: Google, Apple, Samsung, Huawei, entre otras.
- Antes de descargar apps móviles, verificar los diferentes accesos que requiere la app en nuestros dispositivos móviles, para evitar que la misma acceda a una función o información innecesaria.
- Debemos mantener cuantas medidas de seguridad sean posible en nuestros dispositivos móviles, ya que, mientras nos expongas al Internet correremos el riesgo de exponer todo lo que en este se procese, inclusive, que nos monitoreen las llamadas y hasta nuestra ubicación.
- Denunciar las estafas, lo que podemos hacer en el **formulario en línea de la Policía Nacional**, que está en su página web eligiendo el método de denuncia en línea, se nos guiará paso a paso por su formulario donde plasmar la denuncia por phishing.
- Pagar una suscripción de VPN, lo que proporcionaría seguridad en la navegación web, principalmente para usuarios que usan servicios financieros en línea.
- Para el caso de ***las criptomonedas***, de las cuales existen miles operando para todos los continentes, en estas no hay ganancias aseguradas; se debe tener claro que el mercado de ***las criptomonedas es volátil y nada está garantizado***. Sin embargo, los estafadores intentarán convencernos de que ganaremos mucho dinero en poco tiempo, incluso si están respaldadas con testimonios de personas o celebridades, asimismo, si se pretende invertir en criptomonedas en alguna casa de cambio o Exchange, aplicación o en algún mercado digital, asegúrate de hacerlo solo cuando sea necesario y no dejes allí ningún remanente. Estas plataformas no son monederos de bitcoin; tus fondos pueden estar en riesgo allí, ya sea por algún hackeo o por una estafa de salida eventual.

UAF
X Aniversario
2012-2022

"Diez años defendiendo la economía"

UNIDAD DE ANÁLISIS FINANCIERO

Dirección de Inteligencia Financiera

Managua, Nicaragua

(505) 2255-8333

www.uaf.gob.ni