
PROTEGIENDO TU IDENTIDAD
EN LA ERA DIGITAL
OPERINTCO.COM

INDICE

Nota. Éste E-Book es Interactivo, por lo tanto, podrás encontrar imagenes que, al darle click, te llevarán a un video que explique a profundidad del tema. A su vez, los enlaces que aparezcan en color azul, también están habilitados para cliquear y llevarte directamente a la página de información sugerida.

Créditos.
Comunicadora Social, Rocío Rueda A.
info@operintco.com

Año de Publicación. 2024

Diseño y Maquetación.
Operintco.com

Introducción

Vivimos en un mundo cada vez más interconectado, donde nuestras vidas personales y profesionales están profundamente integradas en el vasto universo digital.

La tecnología nos ha brindado innumerables beneficios, desde la facilidad de realizar transacciones bancarias en línea hasta la comodidad de hacer compras desde nuestros dispositivos móviles. Sin embargo, junto con estos avances, también han surgido amenazas invisibles pero devastadoras: **el cibercrimen.**

Imagina recibir un correo electrónico de tu banco pidiéndote que verifiques tu cuenta. Todo parece legítimo, así que haces clic en el enlace y **proporcionas tu información personal.** Poco después, descubres que tus ahorros han desaparecido. O tal vez recibes una llamada de alguien que se hace pasar por un representante de soporte técnico, **convenciéndote de compartir tus datos confidenciales.** O aún peor, un mensaje de texto aparentemente inofensivo te lleva a un sitio web fraudulento que roba tu identidad. Estos son solo algunos ejemplos de cómo el phishing, vishing y smishing pueden cambiar tu vida en un instante.

Si has sido víctima de estos engaños, no estás solo. Hombres y mujeres de todas las edades, desde los 18 hasta los 70 años, han sufrido la pérdida de información personal valiosa y han visto cómo sus identidades eran suplantadas para cometer fraudes en comercios electrónicos, tiendas en línea y otros sectores comerciales. La sensación de vulnerabilidad y desesperanza puede ser abrumadora, pero hay esperanza.

Este eBook está diseñado para ser tu guía en la defensa contra estos ataques cibernéticos. Aquí aprenderás a identificar las señales de advertencia, a comprender las tácticas utilizadas por los cibercriminales y, lo más importante, a protegerte y a proteger a tus seres queridos. Acompáñanos en este viaje para recuperar tu seguridad digital y fortalecer tus defensas contra las amenazas invisibles del mundo moderno.

¿Cómo te roban el Acceso al WhatsApp?

Tener acceso a tus redes sociales, es uno de los objetivos que tienen los ciberdelincuentes dedicados al ciberataque a través del WhatsApp, plataforma que permite la recepción de mensajes de números desconocidos y sin registrar, y cuyos mensajes son totalmente persuasivos, que conllevan un saludo, una presentación de una persona o idea que ofrece un producto, un servicio e incluso, opciones de ganar dinero.

El acceso a tu cuenta de WhatsApp puede ser comprometido de diversas maneras por ciberdelincuentes. Aquí te explicamos algunos de los métodos más comunes que utilizan para robar tus datos y acceder a tu cuenta:

1. Ingeniería Social y Phishing.

La ingeniería social es una técnica que aplican los atacantes que manipulan a las víctimas para que revelen información confidencial como nombres completos, número de identificación personal, códigos enviados por mensajes de texto, entre otro tipo de información personal que **no debe ser compartida a contactos desconocidos.** En el contexto de WhatsApp, esto puede implicar el uso de mensajes fraudulentos para engañarte y obtener tu código de verificación de seis dígitos.

Ejemplo:
Si Recibes un mensaje de texto o de WhatsApp que parece ser de un amigo o conocido. El mensaje dice que accidentalmente han enviado un código de verificación de WhatsApp a su número y te piden que se lo reenvíes. En realidad, **el atacante está intentando registrar su número en otro dispositivo.** Al proporcionar el código, le estarás dando acceso completo a tu cuenta, arriesgando información de chats privados, fotografías o videos enviadas, números de cuentas o cualquier otro tipo de información que la persona maneje a través de éste canal.

¿Se puede recuperar? Si. Puesto que, el código de verificación siempre deberá llegar como mensaje de texto al celular, logrando ingresar nuevamente a la aplicación con el número registrado. A continuación encontrarás los pasos a seguir.

1. Habla con tus contactos por teléfono u otra vía de comunicación acerca de la situación y detallen que la persona que está controlando su WhatsApp está suplantando su identidad, así se evitará que puedan compartir información con él o ella.

2. Registre de nuevo su cuenta de WhatsApp con su número de teléfono. Ingresa el código de seis dígitos que llega por SMS (Mensaje de Texto). Si se han hecho muchos intentos, es posible que el SMS no llegue hasta dentro de unas horas, en ese caso intenta la llamada. En cuanto inicies sesión, se cerrará la sesión del ladrón.

3. Si además del código de seis dígitos le pide otro código adicional de otros seis dígitos, es posible que el atacante haya activado la verificación en dos pasos. En este caso WhatsApp no brinda muchas opciones, pero tendrás que esperar al menos siete días para poder volver a usar dicha cuenta de usuario.

Nota. Lo positivo de éste tercer paso es, que la sesión que el ciberdelincuente tiene abierta, también se cerrará, por lo que en ese tiempo tampoco podrá usar tu cuenta y no te suplantará.

2. Mensajes de Soporte Técnico Falsos.

Otro método común es hacerse pasar por el soporte técnico de WhatsApp. Los ciberdelincuentes envían mensajes que parecen ser oficiales, solicitando que verifiques tu cuenta proporcionando tu código de verificación.

Identificando los Ciberataques.

1. Éste mensaje es de un número falso que no representa el chat real de WhatsApp.

2. El mensaje tiene errores en la ortografía puntual y de acentuación.

3. Usa Ingeniería Social, advirtiendo al usuario que su cuenta será eliminada si no responde.

4. La cuenta oficial de WhatsApp no invita a añadir a los contactos. Por lo tanto, aparece el aviso que indica que no es un contacto registrado y, por seguridad, la aplicación móvil invita a bloquear dicho canal con el ciberatacante.

5. Recomendación: No Responder.

El malware es otro método utilizado para robar el acceso a WhatsApp. Los ciberdelincuentes pueden engañarte para que descargues aplicaciones maliciosas que contienen software diseñado para capturar tu información personal.

Ejemplo:
Descargas una aplicación aparentemente inofensiva de una tienda de aplicaciones no oficial. Esta aplicación contiene un troyano que registra las pulsaciones de teclas y otras actividades en tu dispositivo. El atacante utiliza esta información para acceder a tu cuenta de WhatsApp.

4. Redes Wi-Fi No Seguras.

Conectarte a redes Wi-Fi públicas o no seguras también puede poner en riesgo tu cuenta de WhatsApp. Los atacantes pueden interceptar tu tráfico de datos y capturar información sensible, incluyendo códigos de verificación y mensajes.

Ejemplo:
Te conectas a una red Wi-Fi pública en una cafetería. Un atacante en la misma red utiliza herramientas de interceptación de tráfico para capturar tu información de inicio de sesión de WhatsApp y otros datos sensibles.

5. Duplicación de SIM.

La duplicación de SIM, o SIM swapping, es un ataque en el que los ciberdelincuentes consiguen que la compañía telefónica transfiera tu número de teléfono a una nueva tarjeta SIM en su posesión. Esto les permite recibir todos los mensajes y llamadas destinados a tu número, incluyendo los códigos de verificación de WhatsApp.

Ejemplo:
El atacante se pone en contacto con tu proveedor de servicios móviles y, haciéndose pasar por ti, convence al representante del servicio al cliente para transferir tu número a una nueva tarjeta SIM. Una vez que tienen tu número, reciben el código de verificación de WhatsApp y acceden a tu cuenta.

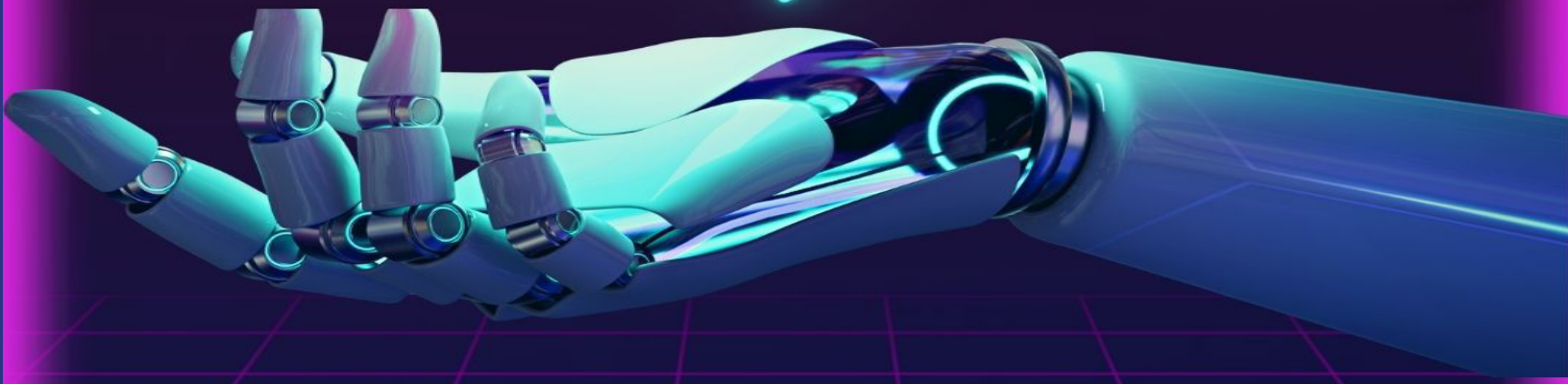
Medidas de Protección. Para proteger tu cuenta de WhatsApp de estos ataques, sigue estas recomendaciones:

- Activar la Verificación en Dos Pasos: WhatsApp ofrece una capa adicional de seguridad mediante un código PIN de seis dígitos que tendrás que ingresar además del código de verificación.

- Códigos de Verificación: Nunca compartas tu código de verificación con nadie, ni siquiera con amigos o familiares.

IDENTIFIQUE LOS MENSAJES DE CIBERESTAFADORES EN WHATSAPP

Ciberseguridad



Click Aquí

WWW.OPERINTCO.COM

¿Cómo te roban el Acceso al Instagram y Facebook?

Protege tus Redes Sociales de los Ciberdelincuentes

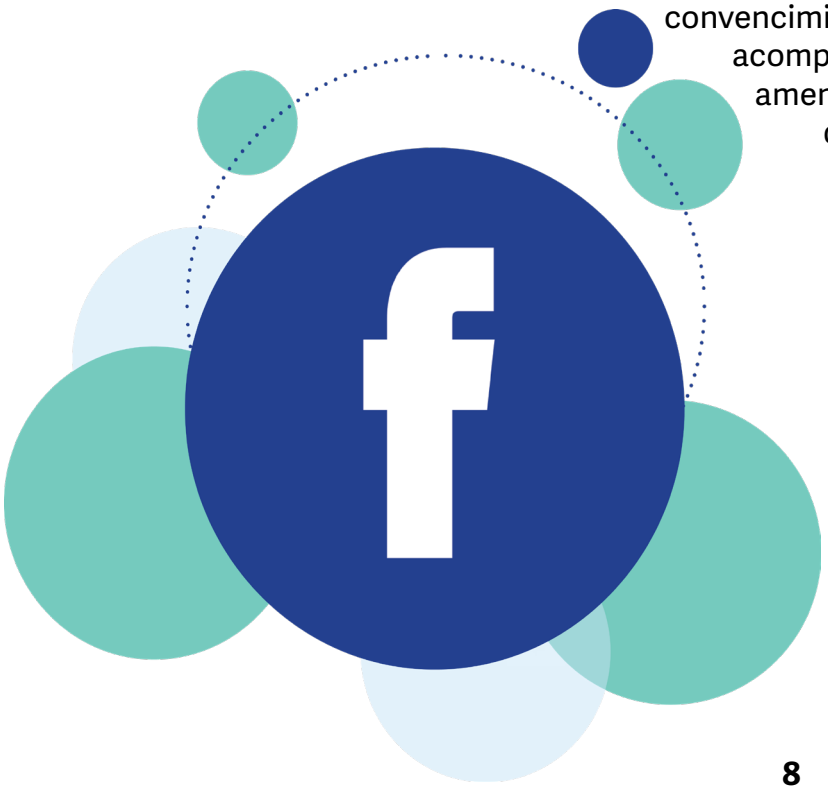
Imagina un día típico: te despiertas, y antes de tomas tu desayuno, decides revisar tus redes sociales como Instagram y Facebook. Pero te encuentras que algo no está bien. No puedes iniciar sesión. Tu corazón late más rápido mientras intentas restablecer tus contraseñas sin éxito. De repente, te das cuenta de que tus cuentas han sido comprometidas. Fotos, mensajes y recuerdos importantes ahora están en manos de desconocidos que están suplantando tu identidad en línea.

En un mundo donde se comparte la vida diaria en plataformas como Instagram y Facebook, los ciberdelincuentes están constantemente al acecho, buscando la oportunidad de acceder a nuestras cuentas y a nuestras vidas. Desde sofisticados ataques de phishing hasta el uso de software malicioso y la explotación de redes Wi-Fi inseguras, las amenazas son más reales que nunca. Estos ataques no solo ponen en riesgo tu privacidad, también pueden causar daños irreparables a tu reputación y seguridad personal.

Pero, **¿cómo logran estos ciberdelincuentes acceder a tus cuentas? ¿Qué tácticas emplean y cómo puedes protegerte de ellas?**

¡Es hora de tomar el control y proteger lo que es tuyo!

Es importante que tengas en cuenta que todo inicia con un inocente mensaje a través del correo electrónico o WhatsApp, los Ciberdelincuentes son expertos en realizar mensajes persuasuvos a través de la conocida Ingeniería Social. Es quí en donde el poder del convencimiento cumple su papel, además de estár acompañado de mensajes de advertencia que amenazan al usuario con el cierre definitivo de su red social, invitando al final que el usuario de clic y acceda a enlaces frau--dulentos cuyo fin es obtener acceso a la red social, nombre de usuario, correo electrónico y contraseñas.



Ésta modalidad de Ciberataque es conocida como Phishing, cuyo significado es “Suplantación”.

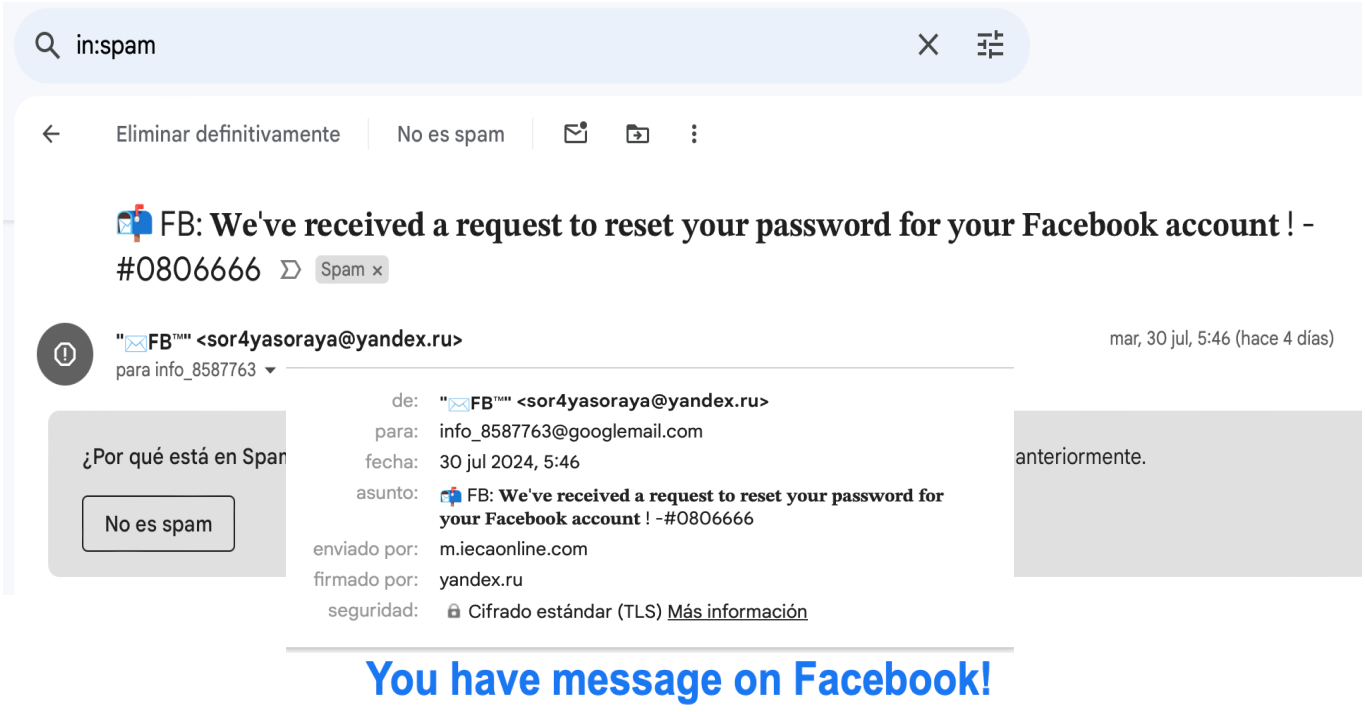
Por lo tanto, nuestro primer tipo de ataque es el PHISHING.

1. Phishing.

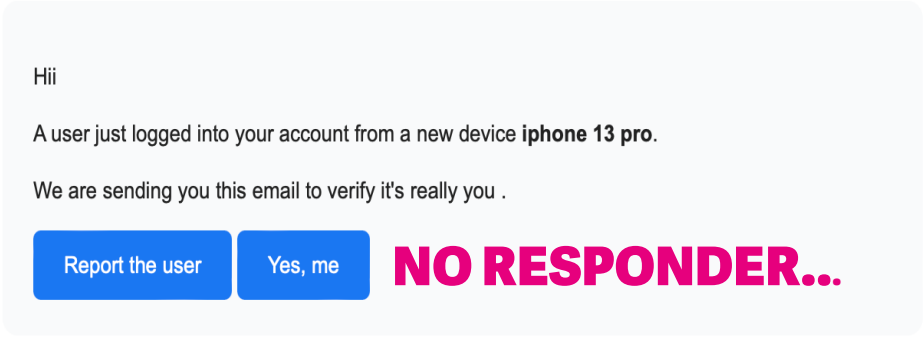
Es una de las tácticas más comunes que utilizan los ciber-delincuentes para robar el acceso a tus cuentas de redes sociales.

Esto implica la creación de sitios web falsos o el envío de mensajes que parecen legítimos pero están diseñados para robar tus credenciales de inicio de sesión.

Ejemplo:
Recibes un correo electrónico o mensaje directo que parece ser de Instagram o Face-book, indicando que debes verificar tu cuenta para evitar su desactivación. El mensaje incluye un enlace que te lleva a una página de inicio de sesión falsa. Al ingresar tus cre-denciales, estas son capturadas por los atacantes.



You have message on Facebook!



NO RESPONDER...

2. Ataques de Fuerza Bruta.

En un ataque de fuerza bruta, los ciberdelincuentes intentan adivinar tu contraseña probando múltiples combinaciones hasta encontrar la correcta. Este método es más efectivo contra cuentas con contraseñas débiles o comunes.

Ejemplo:
Un atacante utiliza un programa automatizado para probar miles de combinaciones de contraseñas en tu cuenta de Instagram o Facebook hasta encontrar la correcta.

Consejos de Prevención.

Una excelente protección de contraseñas está al utilizar frases cifradas entre letras Mayúsculas y minúsculas, números, además de signos como *** $! ¡ @ # % ( ) .** La frase a utilizar no debe ser fácil de adivinar, no deben contener letras de canciones conocidas y de ser posible, nombres ni fechas de nacimiento, pues los Ciberdelincuentes pueden tener acceso a estos

datos personales y adivinar su contraseña por el nombre y fechas de nacimiento o días importantes para usted.

Recuerde también que, una buena contraseña debe tener al menos 8 o más caractéres. Y, si suele olvidar sus contraseñas, puede apoyarse al utilizar un gestor de contraseñas: Este tipo de herramientas pueden generar y almacenar contraseñas fuertes para ti.

No comparta sus credenciales: Nunca compartas tu contraseña con nadie, incluso si parece ser alguien de confianza.

Verifica las solicitudes inusuales: Si alguien te pide información sensible, verifica su identidad por otro medio antes de proporcionar cualquier dato.

Pasos a seguir si sospechas que tu cuenta ha sido comprometida.

1. Recupera el Acceso a tu Cuenta: Restablece tu contraseña. Usa la opción "¿Olvidaste tu contraseña?" en Instagram o Facebook para restablecer tu contraseña. **Inicia sesión desde un dispositivo confiable:** Esto puede ayudar a verificar tu identidad más rápidamente.

2. Revisa la Actividad de tu Cuenta. Verifica sesiones activas: Revisa la lista de dispositivos conectados y cierra sesión en los que no reconozcas. **Revisa tu historial de actividad.** Asegúrate de que no haya publicaciones, mensajes o interacciones que no hayas realizado.

3. Habilita la Autenticación en Dos Pasos. Añade una capa adicional de seguridad: Activa esta opción en la configuración de seguridad de tu cuenta.

4. Informa a tus Contactos. Avisa a tus amigos y seguidores: Informa que tu cuenta fue comprometida para que ignoren mensajes o publicaciones sospechosas.

5. Contacta con el Soporte de Instagram o Facebook. Informa del incidente: Usa los canales oficiales de soporte para informar sobre la situación y obtener ayuda adicional.

Si en llegado caso ya estás siendo víctima de Phishing, podrás enviar un correo electrónico antes de las 24 horas de la suplantación con captures de pantalla, al correo electrónico: phish@instargam.com

Para el caso de Facebook, podrás ingresar al siguiente enlace: https://es-es.facebook.com/help/434918221794966/?helpref=uf_share y dale clic al mensaje en azul que dice: **denuncia cualquier mensaje sospechoso en Messenger.**

Las cuatro amenazas digitales que ponen en riesgo tu Seguridad en Linea

En esta era digital, la sociedad se ha vuelto cada vez más conectada, con interacciones diarias que ocurren a través de correos electrónicos, mensajes de texto y llamadas telefónicas.

Sin embargo, este mundo interconectado también ha abierto la puerta a una serie de amenazas cibernéticas que buscan explotar nuestras vulnerabilidades. Entre las tácticas más insidiosas empleadas por los ciberdelincuentes se encuentran cuatro tipos específicos de ataques: el phishing, el vishing, el smishing y el whaling. Cada uno de estos métodos tiene como objetivo engañar a las víctimas para que revelen información confidencial, poniendo en riesgo no solo su privacidad, sino también su seguridad financiera y personal.

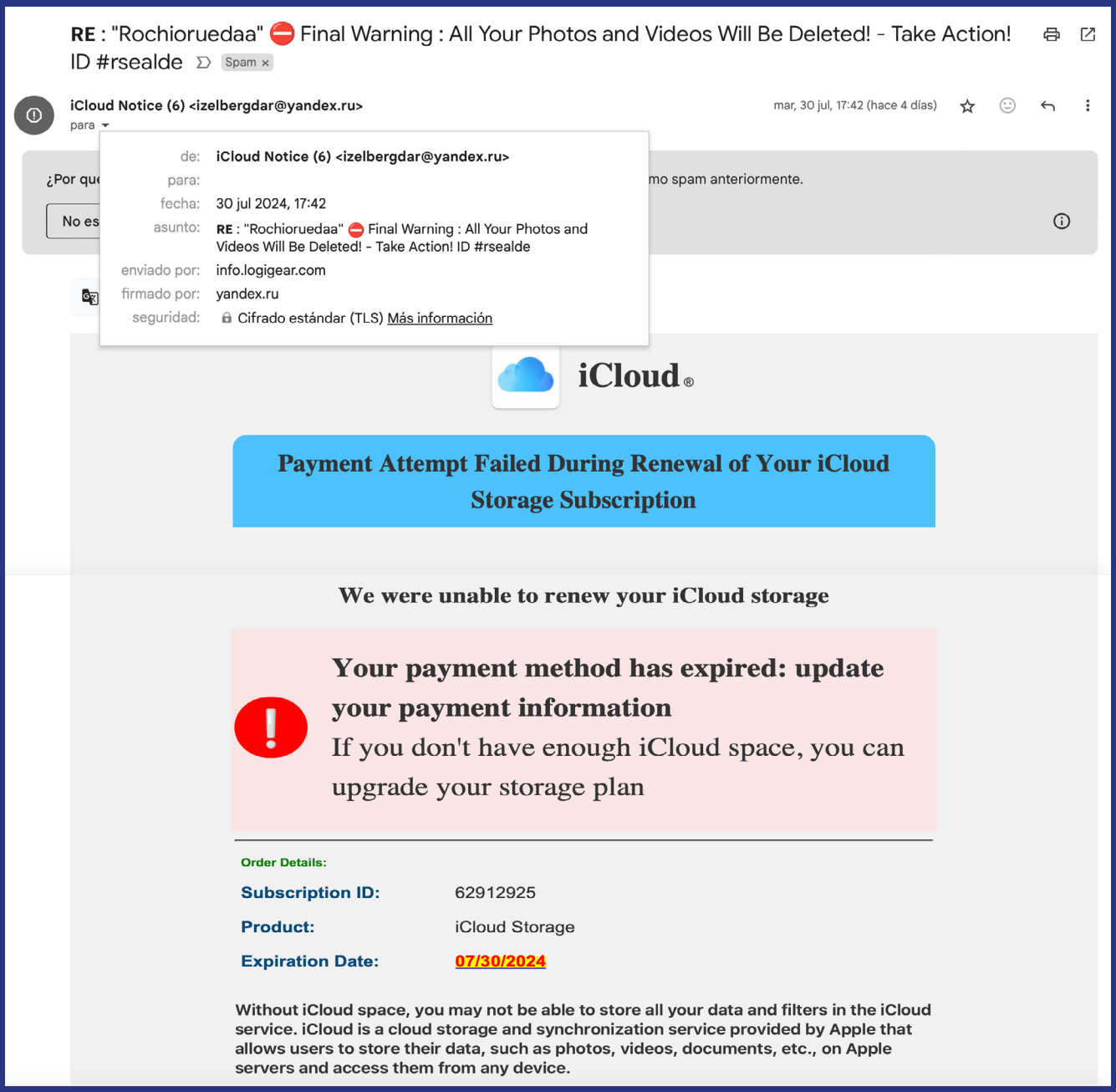
El phishing, quizás el más conocido de estos ataques, utiliza correos electrónicos falsos para engañar a las personas y hacerles revelar sus datos sensibles. Por otro lado, el vishing lleva esta táctica al ámbito de las llamadas telefónicas, donde los atacantes se hacen pasar por representantes legítimos para robar información valiosa. No menos peligrosos son los ataques de smishing, que emplean mensajes de texto fraudulentos con el mismo objetivo de engaño. Y para aquellos en posiciones de poder, el whaling es una amenaza aún más sofisticada, dirigida específicamente a altos ejecutivos con la intención de acceder a información corporativa crítica.

Estos ciberataques no solo son cada vez más frecuentes, también más sofisticados, adaptándose rápidamente a las prácticas digitales y haciéndose más difícil de detectar.

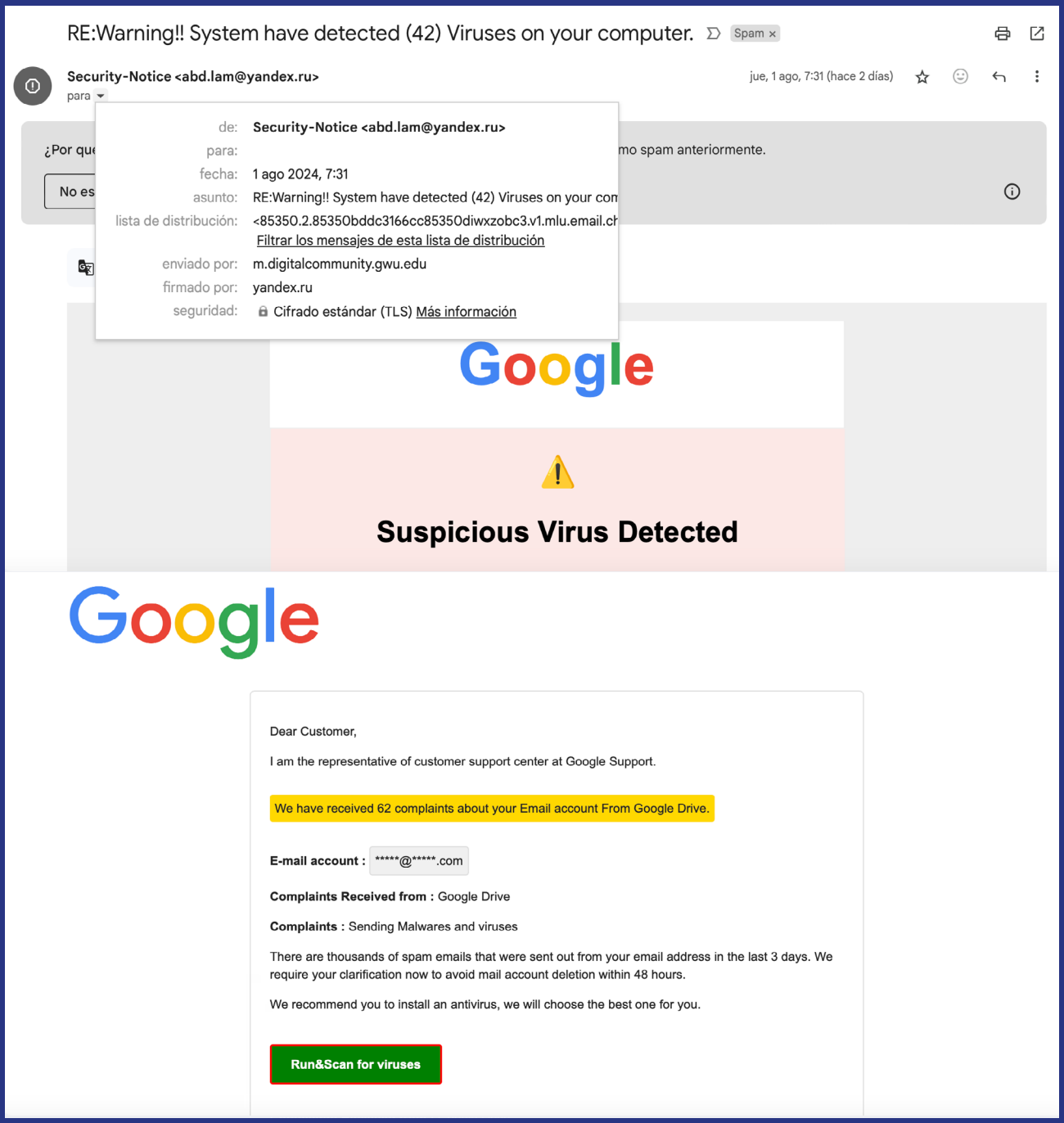
Comprender estos cuatro tipos de amenazas es el primer paso crucial para protegese en el entorno digital actual. En este capítulo, exploraremos en detalle cada uno de estos ataques, revelando cómo operan, a quiénes están dirigidos y, lo más importante, cómo podemos defendernos de ellos.

A continuación encontrarás imagenes de correos phishing reales, para que puedas identificarlos en tu correo electrónico y evitar caer en las trampas de los ciberdelincuentes. Algunos ejemplos comunes llegan a tu bandeja de entrada de tu correo electrónico.

1 Ejemplo Phishing de iCloud, plataforma que ofrece el servicio de resguardo de contenido multimedia como imagenes, videos, contactos telefónicos, agenda con actividades programadas entre otro tipo de información personal. Y, al ser una herramienta clave para archivar información personal, los Ciberdelincuentes están en busca de acceder a la plataforma del usuario que caiga en su trampa.



2 Ejemplo Phishing en Google. Al igual que iCloud, en Google se guarda la mayor parte de la base de datos personales de un usuario en línea, como fotografías, videos, documentos, bases de datos, números de contactos e incluso, el registro de los movimientos que hace una persona en su día a día, registrandolo en Google Maps de cada cuenta de Gmail, facilitando una información detallada de las actividades diarias. Por esta razón, las cuentas de Google son apetecidas, porque, a través de ellas se tiene acceso a una buena parte de la información personal e incluso, financiera, si fuere el caso que los datos personales registrados en una entidad bancaria se correspondan con el correo gratuito de Gmail.



Teniendo presente dichas imagenes, **el phishing es una técnica de ciberataque que utiliza correos electrónicos fraudulentos** para engañar a las personas y hacerles revelar información confidencial, como contraseñas, números de tarjetas de crédito y otros datos personales. Los correos electrónicos de phishing suelen parecer legítimos, simulando provenir de instituciones de confianza como bancos, empresas de tecnología o incluso contactos personales. Estos mensajes a menudo contienen enlaces que dirigen a las víctimas a sitios web falsos diseñados para capturar la información ingresada.

Uno de los aspectos más peligrosos del phishing es su capacidad para evolucionar y adaptarse a nuevas tácticas. Los atacantes constantemente perfeccionan sus métodos, creando correos electrónicos y sitios web falsos que son cada vez más difíciles de distinguir de los legítimos. **Pueden emplear tácticas de ingeniería social, como generar una sensación de urgencia o miedo, para inducir a las víctimas a actuar rápidamente sin cuestionar la autenticidad del mensaje.** Por ejemplo, **un correo electrónico puede afirmar que tu cuenta ha sido comprometida y que necesitas actualizar tu información inmediatamente para evitar el cierre de la cuenta.**

Para protegerse contra el phishing, es crucial ser cauteloso con los correos electrónicos no solicitados y **verificar siempre la autenticidad del remitente antes de hacer clic en cualquier enlace** o proporcionar información personal. Utilizar herramientas de filtrado de correo electrónico y software de seguridad también puede ayudar a detectar y bloquear intentos de phishing. Además, activar la autenticación en dos pasos en todas las cuentas importantes añade una capa adicional de seguridad, haciendo más difícil para los atacantes acceder a tus datos incluso si consiguen robar tu contraseña.

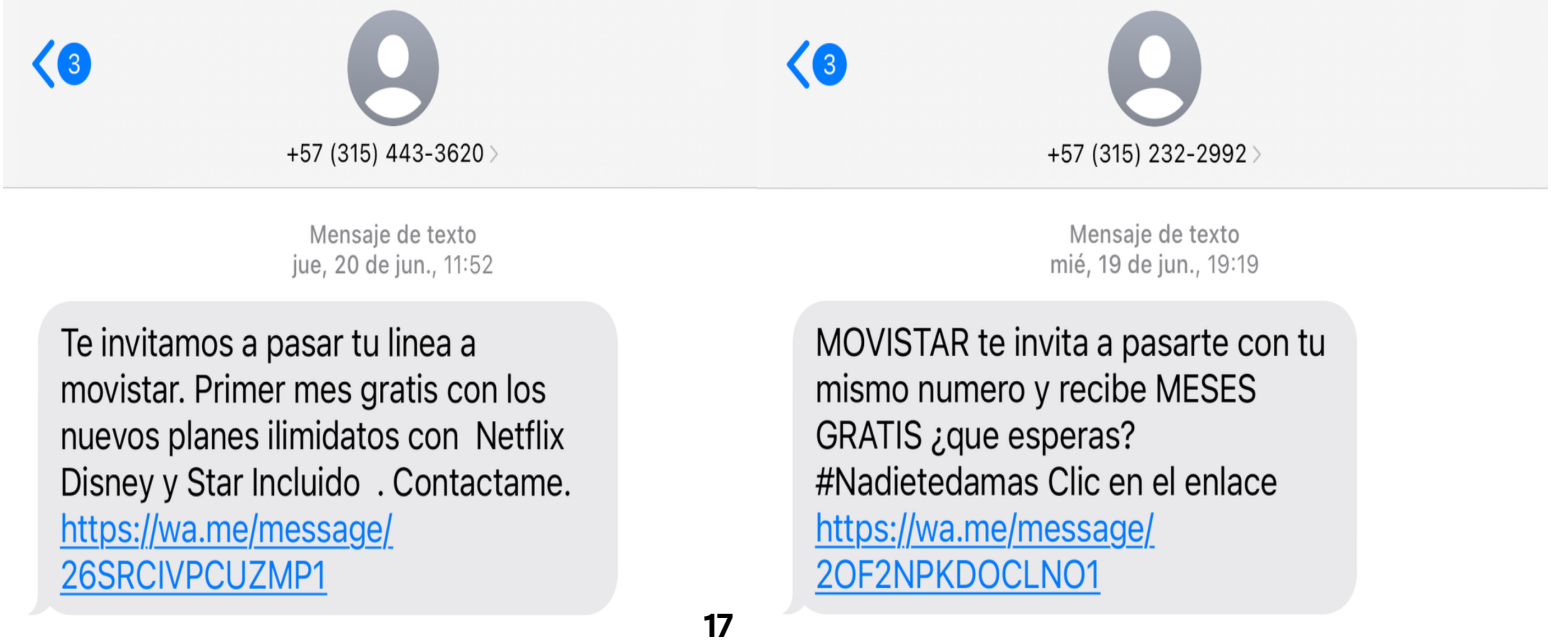
El segundo tipo de Ciberestafa es el Vishing, caracterizado por ser estafa a través de la voz, es decir, ciberataque que se lleva a cabo mediante llamadas telefónicas. En estos ataques, los ciberdelincuentes utilizan tácticas de ingeniería social para convencer a las víctimas de que proporcionen información confidencial, como datos de tarjetas de crédito, números de seguro social o contraseñas. Los atacantes suelen hacerse pasar por representantes de instituciones legítimas, como bancos, proveedores de servicios técnicos o agencias gubernamentales, para ganar la confianza de la víctima.

A diferencia del phishing tradicional, el vishing aprovecha la inmediatez y el carácter personal de las llamadas telefónicas para ejercer presión sobre las víctimas.

Los atacantes pueden utilizar técnicas como la falsificación de números de teléfono (caller ID spoofing) para que las llamadas parezcan venir de fuentes confiables. Por ejemplo, una víctima podría recibir una llamada de alguien que dice ser del soporte técnico de su banco, informándole de una actividad sospechosa en su cuenta y solicitando datos personales para "verificar" su identidad.

Para protegerse contra el vishing, es importante desconfiar de cualquier llamada que solicite información confidencial, especialmente si es inesperada. Nunca proporciones información personal por teléfono a menos que hayas iniciado la llamada a un número conocido y verificado. Además, utilizar aplicaciones de identificación de llamadas y reportar números sospechosos puede ayudar a reducir el riesgo de ser víctima de este tipo de estafa. Si tienes dudas sobre la legitimidad de una llamada, cuelga y contacta directamente a la institución a través de los canales oficiales.

Como tercer tipo de Ciberataque está el Smishing. Una característica clave de esta ciberestafa es su capacidad para explotar la confianza que las personas tienen en los mensajes de texto, ya que estos suelen ser considerados más personales y menos susceptibles a fraudes que los correos electrónicos. Los atacantes pueden crear un sentido de urgencia en los mensajes, como una supuesta alerta de seguridad de tu banco que requiere una acción inmediata para "evitar" la suspensión de tu cuenta. Al hacer clic en el enlace o responder al mensaje, las víctimas pueden ser dirigidas a un sitio web falso que solicita información personal o pueden ser inducidas a descargar una aplicación maliciosa.



El smishing, una combinación de “SMS” y “phishing”, es una táctica de ciberataque que **utiliza mensajes de texto para engañar a las víctimas y obtener información confidencial o inducirlas a descargar malware.**

Los mensajes de smishing suelen parecer legítimos y pueden hacerse pasar por alertas de bancos, notificaciones de servicios de entrega, o incluso mensajes de amigos o familiares. Al igual que en el phishing, los mensajes de smishing suelen contener enlaces que dirigen a sitios web falsos o números de teléfono que conectan directamente con los atacantes.

Para protegerse contra el smishing, es esencial ser cauteloso con los mensajes de texto no solicitados, especialmente aquellos que contienen enlaces o solicitan información personal. Verifica siempre la autenticidad de cualquier solicitud directamente con la empresa o persona que supuestamente envió el mensaje, utilizando un canal de comunicación conocido y confiable. Además, mantener actualizado el software de seguridad en tu dispositivo móvil y evitar descargar aplicaciones de fuentes no oficiales puede ayudar a prevenir la instalación de malware a través de smishing.

Por último, está el whaling, o phishing dirigido a altos ejecutivos y personas en posiciones de poder. Es una forma sofisticada de ciberataque que busca obtener acceso a información corporativa crítica o recursos financieros significativos. A diferencia de otros tipos de phishing que pueden dirigirse a una amplia audiencia, el whaling está específicamente diseñado para engañar a individuos con roles ejecutivos, como CEO, CFO y otros altos directivos. Los ataques de whaling suelen involucrar correos electrónicos muy personalizados que imitan de manera convincente la correspondencia legítima dentro de la empresa.

Estos ataques suelen utilizar información detallada sobre la organización y sus operacio-

nes para hacer que los correos electrónicos parezcan auténticos. Por ejemplo, un atacante puede enviar un correo electrónico que parece provenir del CEO de la empresa, solicitando una transferencia bancaria urgente o acceso a documentos confidenciales. Los correos electrónicos de whaling a menudo se redactan de manera profesional y pueden incluir firmas electrónicas y logotipos corporativos para aumentar su credibilidad.

Para mitigar el riesgo de ser víctima de un ataque de whaling, las empresas deben implementar políticas de seguridad rigurosas y educar a sus empleados, especialmente a aquellos en posiciones de liderazgo, sobre las tácticas de los ciberdelincuentes. Es fundamental verificar cualquier solicitud de transferencia de fondos o acceso a información confidencial a través de un segundo canal de comunicación, como una llamada telefónica directa. Además, la implementación de medidas de seguridad avanzadas, como la autenticación en dos pasos y el uso de cifrado para correos electrónicos sensibles, puede ayudar a proteger la información crítica de la empresa contra estos ataques dirigidos.

Identidad en Línea: Una perspectiva desde la Seguridad Informática

En el mundo de la Ciberseguridad, cada usuario que navega en la web, es un usuario en línea que interactua con el mundo de la información y datos digitales. Por lo tanto, es una representación digital de una persona o entidad en el mundo virtual.

Comprende también una combinación de credenciales de autenticación, datos personales y perfiles en redes sociales, entre otros elementos. A medida que la dependencia de las tecnologías digitales aumenta, también lo hacen los riesgos asociados con la identidad en línea.

Sin embargo, existen dos características que diferencian a los usuarios activos de los no activos, como lo son, la identidad sin conexión y la identidad con conexión.

La identidad sin Conexión, es la misma identidad fuera de línea, es decir, aquellas per-

sonas que en la vida real comparten momentos especiales con amigos y familiares, experiencias laborales y de crecimiento personal, sin éstas ser publicadas a través de plataformas sociales. Por lo tanto, esta área de la identidad sin conexión es la vida real en si, es lo que nuestros amigos, familiares, compañeros de trabajo ven, escuchan y conocen de nosotros mismos.

La identidad sin conexión es clave, puesto que solamente las personas que comparten con nosotros, conocen datos personales como dirección de residencia, nombres de familiares, amigos, gustos. Pero es aquí, cuando el peligro realmente llega, debido a la ausencia y participación en red, pues no se tiene control sobre los datos personales y pueden ser estos robados facilmente, justo, cuando no estás mirando lo que sucede en el mundo digital.

Existe también la Identidad con Conexión, haciendo referencia a datos personales como nombre de pila o nombre de usuario, que es lo que te representa ante los demás en el mundo en línea.

Así como la identidad social que se establece con la comunidad en la vida real, también se establecen dichas conexiones digitales a través de las redes sociales, correos electrónicos, plataformas de comunicación instantánea como WhatsApp, Facebook Messenger, Telegram, entre otras plataformas digitales.

Cuando la conexión en línea o la Identidad con Conexión está disponible al público, existen precauciones que cada usuario debe tomar, debido a la información compartida y que se publica para identificarse en las redes sociales, como viajes, encuentros familiares, fiestas de amigos, visitas a restaurantes e incluso, momentos personales compartidos públicamente para los demás.

Independientemente de las dos formas de relacionarnos a diario, es importante proteger y cuidar su información y la de sus hijos, amigos y conocidos, ya que, independientemente de la interacción con el mundo digital, así no se tengan redes sociales, cada usuario si tiene identidad en línea. Si usas la web para buscar información, ya eres considerado un usuario con identidad digital.

¿Cómo proteger tu Identidad en Línea?

Existen las Credenciales de Autenticación en dos pasos, que son esenciales para verificar la identidad de un usuario en línea, cuando éste ingresa e interactúa en redes sociales u otras plataformas digitales, antes de ingresar, deberá proceder a los pasos de seguridad que permitirá el ingreso a su cuenta virtual.

Éstas incluyen las contraseñas, tokens de seguridad, datos personales, identificación biométrica entre otros tipos de seguridad que las redes sociales, plataformas bancarias, correos electrónicos e incluso, acceso a la nube de Google o iCloud solicitan a cada usuario para comprobar que es la persona correcta que ingresa al perfil solicitado.

Las contraseñas, son la forma más segura de ingresar, pero, todo dependerá del tipo de clave de acceso que cada usuario registre en la red social o plataforma digital. Las contraseñas son combinaciones de caracteres como letras y números, ya sean en Mayúsculas, minúsculas, lleven puntos, comas, astericos, entre otro tipo de caracter que permitan ser indecifrables para los ciberdelincuentes. Por ello, las contraseñas sirven como barrera inicial contra el acceso no autorizado.

¿Cómo identificar una contraseña totalmente segura?
Para que una contraseña sea totalmente segura, deberá cumplir con una serie de normas establecidas por el Instituto Nacional de Normas y Tecnología (NITS) de los Estados Unidos, y dentro de las 8 reglas a seguir, se encuentran:

1. Las contraseñas deben tener por lo menos 8 caracteres, pero no más de 64.
2. No utilizar contraseñas comunes, ni que se puedan adivinar con facilidad, por ejemplo, (abc123).
3. No deben haber reglas de composición, como incluir números y letras mayúsculas o minusculas.
4. Los usuarios deben poder ver las contraseñas al escribir, para ayudar a mejorar la precisión.
5. Se deben permitir todos los caracteres de impresión y espacios.
6. No debe haber sugerencias para la contraseña.
7. No debe haber periodo de caducidad para la contraseña.
8. No debe haber autenticación basada en el conocimiento, como tener que pro porcionar respuestas a preguntas secretas o verificar el historial de transacción.

Como recomendaciones para proteger su identidad en línea y sus perfiles digitales, tenga en cuenta que sus contraseñas tampoco deberán llevar fechas de nacimiento, nombres de familiares o amigos, tampoco, letras de canciones favoritas, puesto que, a través de la técnica FUERZA BRUTA, los Ciberdelincuentes ingresan varios tipos de contraseñas hasta identificar la correcta.

Es recomendable que, su contraseña contenga frases que solamente usted conozca, y cumplir con los requerimientos de seguridad que la NITS sugiere a los usuarios en línea.

Como segundo tipo de ciberseguridad, están Los Tokens: Dispositivos o aplicaciones que generan códigos de autenticación de un solo uso. Para éste ejemplo, es característico de iCloud que, cuando se ingresa a la nube a través de un computador o navegador web, siempre llega un Token de seguridad al celular de cada usuario.

De ésta misma forma, aplicaciones como Facebook e Instagram y Gmail están aplicando esta herramienta de seguridad.

Para finalizar, existen otros tipos de seguridad virtual como los Certificados Digitales y la biometría (Características físicas únicas como huellas dactilares y reconocimiento facial que se utilizan cada vez más para la autenticación).

La identidad en línea es un aspecto crucial de la ciberseguridad que requiere una gestión y protección adecuadas para prevenir riesgos como el robo y la suplantación de identidad.

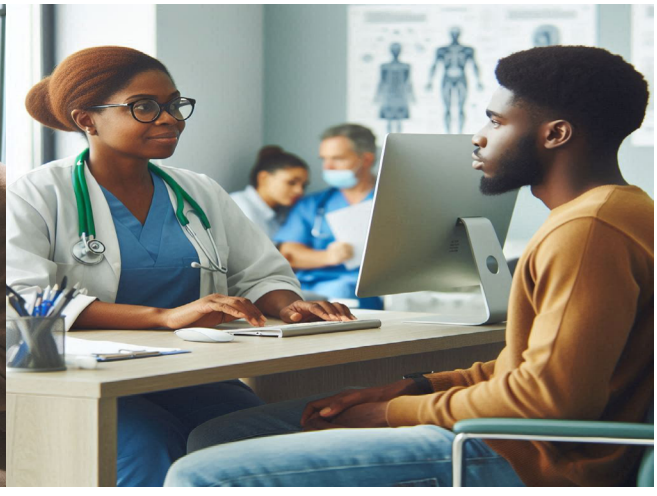
Las organizaciones y los individuos deben adoptar prácticas robustas de autenticación, educarse continuamente sobre las amenazas cibernéticas y utilizar tecnologías avanzadas para proteger su información personal. A medida que el entorno digital continúa evolucionando, la seguridad de la identidad en línea debe mantenerse como una prioridad para garantizar la privacidad y la integridad de los usuarios en el mundo virtual.

La Importancia de los Datos Personales en el Mundo Digital

En esta época de la digitalización de la sociedad, los datos personales se han convertido en un recurso invaluable para diversas industrias. En el sector salud, la educación, la industria y el comercio, la recopilación y el manejo de estos datos son fundamentales para la eficiencia operativa, la personalización de servicios y la mejora continua de procesos. Sin embargo, la importancia de estos datos también conlleva una gran responsabilidad en cuanto a su protección y uso ético.

En el sector salud, los datos personales son esenciales para la atención médica eficaz y personalizada. La información como el historial médico, los resultados de pruebas diagnósticas y los registros de tratamientos permiten a los profesionales de la salud tomar decisiones informadas y proporcionar una atención adecuada. Además, estos datos facilitan la continuidad de la atención, asegurando que los pacientes reciban un tratamiento coherente y bien coordinado, independientemente de los cambios en el personal médico o las instalaciones.

Los datos personales también juegan un papel crucial en la investigación médica y el desarrollo de nuevos tratamientos. Al analizar grandes volúmenes de datos de pacientes, los investigadores pueden identificar patrones, evaluar la eficacia de diferentes tratamientos y desarrollar nuevas terapias más rápidamente. Sin embargo, esto debe hacerse con estrictas medidas de privacidad para proteger la identidad y los derechos de los pacientes.



La información personal, también cumple un papel importante en el ámbito educativo, los datos personales permiten una educación más personalizada y efectiva. Los registros académicos, los perfiles de aprendizaje y las evaluaciones ayudan a los educadores a entender mejor las necesidades y capacidades de sus estudiantes. Esto facilita la adaptación de métodos de enseñanza y la oferta de recursos específicos que optimicen el aprendizaje individual. Además, los datos personales son vitales para la administración educativa. Desde la inscripción y la gestión de asistencia hasta la evaluación del desempeño y la planificación curricular, los datos ayudan a las instituciones educativas a funcionar de manera más efi-

ciente. Sin embargo, es fundamental garantizar la seguridad de estos datos para proteger la privacidad de los estudiantes y evitar el mal uso de la información.

Generalmente, en el área de la Industria y el Comercio, los datos personales impulsan la innovación y la eficiencia operativa. La información de los empleados, como sus habilidades, experiencias y rendimiento, es crucial para la gestión del talento y la asignación de tareas. Los datos personales también facilitan la mejora de los procesos internos y la toma de decisiones estratégicas, permitiendo a las empresas mantenerse competitivas en un mercado globalizado. La personalización de productos y servicios es otra área donde los datos personales son fundamentales. Al entender mejor las preferencias y necesidades de los consumidores, las empresas pueden desarrollar productos más adecuados y campañas de marketing más efectivas. No obstante, este uso debe equilibrarse con la protección de la privacidad del cliente para evitar la explotación indebida de su información.

para el caso del comercio, la información personal es la base de las estrategias de ventas y marketing. Los historiales de compras, las preferencias de productos y la demografía de los clientes permiten a los minoristas crear experiencias de compra más personalizadas y atractivas. Las tiendas en línea, en particular, dependen en gran medida de los datos personales para ofrecer recomendaciones precisas y promociones dirigidas. Además, los datos personales ayudan a mejorar la logística y la gestión de inventarios. Con información detallada sobre las compras y las tendencias del mercado, las empresas pueden optimizar sus cadenas de suministro y reducir costos. Sin embargo, la recopilación de datos en el comercio debe hacerse de manera transparente y con el consentimiento del cliente para mantener la confianza y cumplir con las regulaciones de privacidad.

A pesar de los beneficios evidentes que los datos personales aportan a estos cuatro sectores económicos, los ciberdelincuentes están pendientes de poder acceder a dicha información personal de los usuarios registrados, con el objetivo de suplantarlos en cualquiera de estos cuatro sectores expuestos.

Un ejemplo de suplantación en el sector de la medicina, es cuando un ciberdelincuente logra obtener la información de un paciente, y éste, bajo la identidad de dicha persona accede a las atenciones médicas, generando un registro médico que la verdadera persona no ha recibido por parte de la entidad.

No siempre los ciberataques están dirigidos a estafar a los usuarios, también, están direccionados a generar un beneficio a otra persona que suplanta la identidad del titular.

Por todo esto, es crucial reflexionar sobre la cantidad de información que se comparte y cómo se maneja. Cada vez que se proporcionan los datos personales, ya sea para recibir atención médica, realizar una inscripción o matrícula en una institución educativa, ser parte de una empresa o realizar compras en línea, las personas está cediendo una parte de su privacidad.

La protección de los datos personales no es solo responsabilidad de las organizaciones, también de cada persona. Recuerda que eres vigilante sobre la información que compartes, entender cómo se utilizará y asegurarse de que las decisiones estén informadas. Al hacerlo, podrás disfrutar de los beneficios de una sociedad digital mientras proteges tu privacidad y seguridad.

t

La Fortaleza Invisible para sus Datos Personales

"La fortaleza más resistente no es aquella hecha de piedra y acero, sino la construida con conocimiento y prevención".

En un mundo donde las fronteras físicas han sido superadas por las virtuales, la ciberseguridad se ha convertido en la principal defensa contra los asaltos invisibles de los ciberdelincuentes. La seguridad en el ámbito digital no es un lujo, sino una necesidad imperiosa para individuos y organizaciones por igual.

Los ciberdelincuentes emplean una variedad de técnicas sofisticadas para infiltrarse en sistemas y robar información valiosa. Desde el phishing, que engaña a las personas para que revelen sus contraseñas, hasta el ransomware, que secuestra datos a cambio de un rescate, las amenazas son numerosas y en constante evolución. La creciente interconexión de dispositivos y la dependencia de servicios en línea han ampliado la superficie de ataque, haciendo que la protección digital sea más compleja y crucial que nunca.

Desde el uso de contraseñas robustas y la autenticación multifactor, hasta la implementación de software de seguridad y la educación continua sobre las tácticas de los atacantes, te explicaremos algunos de los ciberataques y tipos de malware utilizados por los ciberdelincuentes, así como los tipos de protección que debes tener para el celular inteligente, tables o iPad, laptos y computadores. Es importante entender y aplicar estos conceptos, ya que son la clave para navegar en el mundo digital con seguridad y confianza, transformando cada usuario en un guardián informado de su propia información y privacidad.

¿En donde se guarda su información personal?

Los datos personales son la descripción de cualquier información relacionada con un usuario, este tipo de datos incluyen sus nombres y apellidos completos, fechas de nacimiento, seguridad social, número de identificación personal, ciudad de nacimiento, e incluso fotografías tomadas desde el momento del registro, hasta las capturadas por su dispositivo móvil.

Sin una protección y cuidado responsable, los ciberdelincuentes pueden ingresar a sus cuentas y utilizar su información confidencial para identificarlo, seguidamente de suplantar su identidad, infringiendo su seguridad, además de causar daños a la reputación de cada persona que descuida su información personal.

Cada registro que se realice en la web, en las redes sociales, en los historiales clínicos, educativos, bancarios, además de su información personal como fotografías y videos, siempre quedan registrados en una base de datos, ya sea en la nube de sus correos electrónicos, o en las bases de datos de una entidad gubernamental o privada.

Un ejemplo común con el cuidado de los datos personales de la sociedad en línea es, cuando en una reunión social las personas toman fotografías, éstas quedan guardadas en la nube del usuario que tomó dicha foto y, además es compartida entre el circulo social de amigos, generando varias copias de un mismo archivo y en dispositivos móviles diferentes al original. Y sin mala voluntad, uno de esos amigos orgulloso de la fotografía decide publicarla en línea, y personas que tú no conoces tienen ahora acceso a la fotografía que describe el lugar de encuentro, da detalles de su ubicación, nombres personales o nombres de usuarios registrados en las redes sociales, siendo ahora usted identificable para los ciberdelincuentes.

Como segundo ejemplo, están las famosas tarjetas de fidelidad de la tienda, o las tarjetas regalo. Además de ser una estrategia conveniente de ahorrar dinero en las compras, la tienda está usando la tarjeta para crear un perfil del cliente, analizar el comportamiento del comprador y luego usar la información registrada para enviar correos de ofertas especiales.

Para éste segundo caso, si el comercio tiene un excelente manejo de datos de sus clientes, los ciberdelincuentes no podrán acceder a sus datos personales, pero, si la tienda maneja con deficiencia cada información de sus clientes, la información será revelada para los famosos Hackers.

¿Quién quiere sus DATOS?

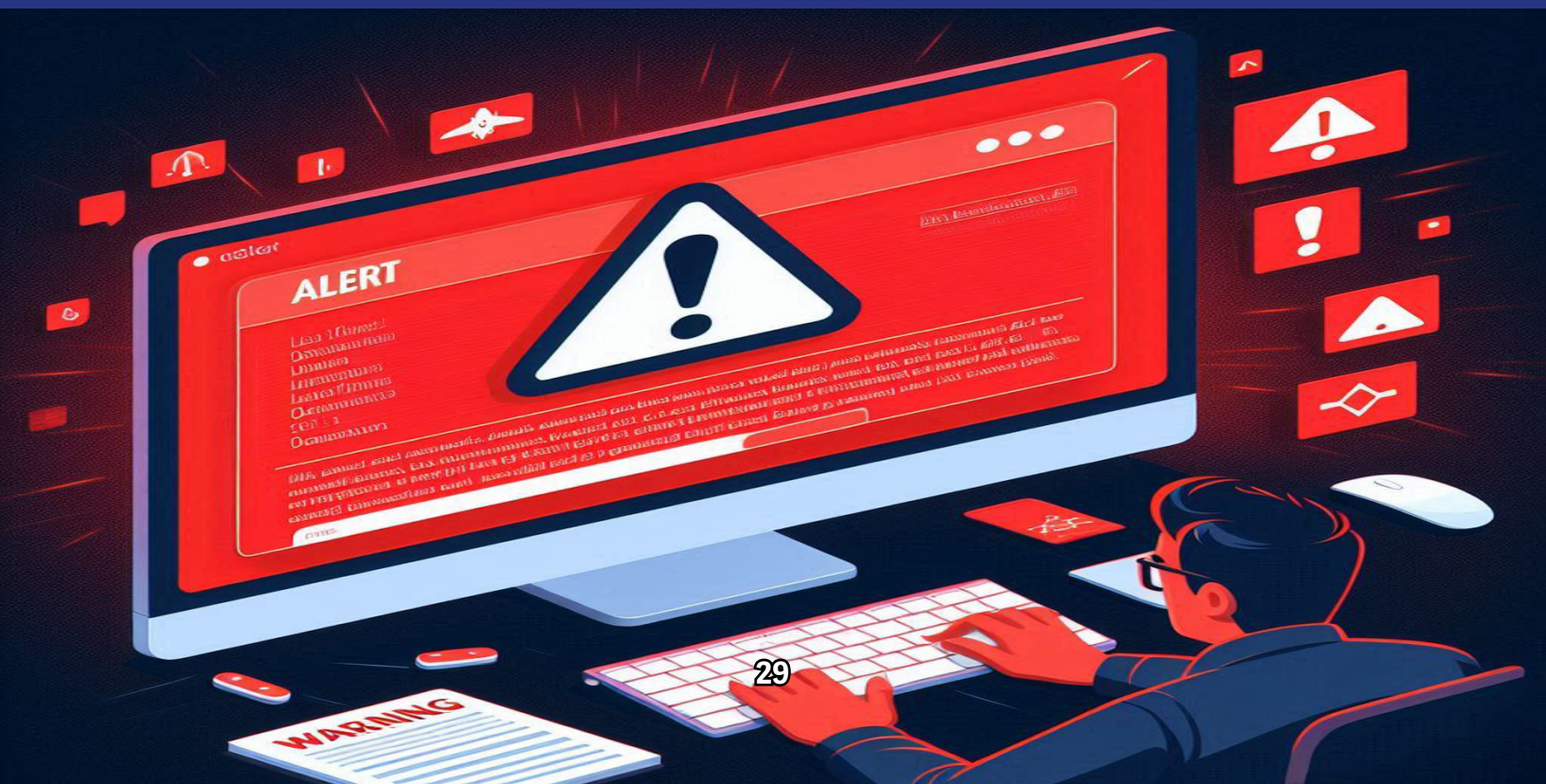
A demás de los Hackers que buscan tu dinero, y los ciberdelincuentes que buscan tu información personal para suplantarte la identidad, existen otras entidades que están en busca de la información de los usuarios en línea para identificar a sus clientes y futuros nuevos clientes.

Por tal razón, existen comercios como los proveedores de servicios de Internet (ISP), quienes hacen seguimiento de una actividad en línea y, en algunos países, éstos pueden incluso vender la información obtenida a los anunciantes con fines de lucro. Existen también circunstancias gubernamentales que obligan a las ISP, a compartir la información con las agencias o autoridades de vigilancia del Gobierno.

Los anunciantes de cada campaña comercial, especialmente la publicidad dirigida, también integran la lista de los que buscan tus datos personales como gustos, actividades, busquedas en internet e incluso tendencias en línea, con el objetivo de monitorear y rastrear las actividades de los usuarios, los hábitos de compra y las preferencias personales, por tal razón, cada que un usuario ve un anuncio en sus redes sociales o buscadores web, es debido a la información obtenida por los anunciantes.

Como tercero en la lista están los motores de busqueda y plataformas de Redes Sociales. A través de sus algoritmos, cada interacción en línea brinda información sobre su género, geolocalización, números de contacto e ideologías políticas y religiosas. Toda la información se va acomodando de acuerdo a la identidad en línea que tiene el usuario. Ésta información obtenida, también es vendida a los anunciantes con fines de lucro.

Por último en la lista, se encuentran los sitios web, siendo éstos servidores digitales diseñados con herramientas informáticas como los Cookies, para rastrear sus actividades con el fin de ofrecer una experiencia más personalizada. Ésta herramienta no deja rastros de datos del usuario, pero, si registran los movimientos e intereses de los usuarios.

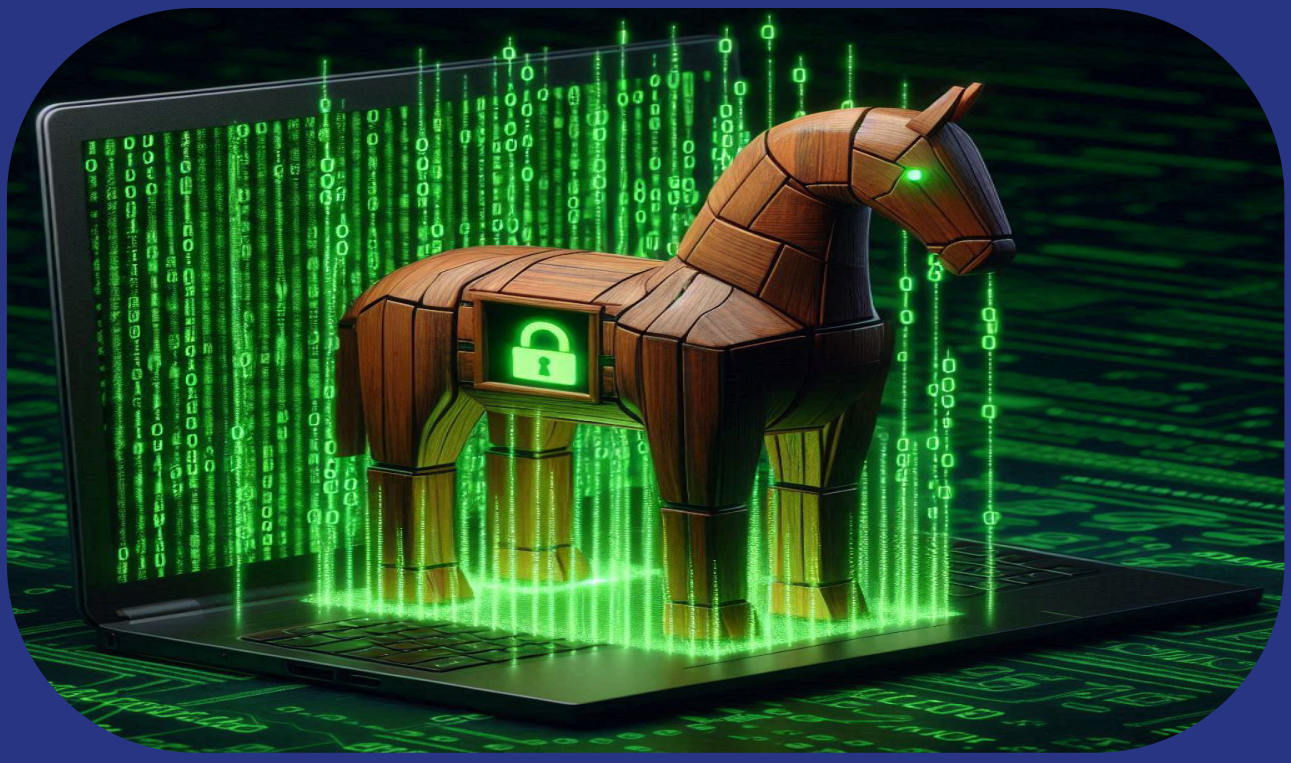


Ataques a través de Malware

Estos tipos de ataques son conocidos como Virus, Troyanos, Spyware, Puerta Trasera, Ransomware, Gusanos, entre otros tipos de programaciones diseñadas por los famosos Hackers, quienes desarrollan materiales descargables como programas gratuitos, pero que en sí, llevan una programación que abre las puertas a los ciberdelincuentes.

Dentro de las programaciones de software malicioso reconocidos, está el **Spyware,** diseñado para rastrear y espiar a los usuarios en línea. Éste tipo de Malware monitorea la actividad y registra cada tecla presionada en el smartphone o iPhone, Tablet o iPad, Laptops o Computadores. También está destinado a capturar información confidencial, como datos bancarios en línea. Este tipo de software espía y modifica la configuración de seguridad de sus dispositivos, y con frecuencia se camufla con software legítimos o con los famosos Caballos de Troya.

El Caballos de Troya es un tipo de Malware programado a llevar a cabo operaciones maliciosas, camuflando su verdadera intención. Estas programaciones se camuflan con programas legítimos, pero, de hecho, es bastante peligroso, puesto que los Troyanos aprovechan sus privilegios de usuarios y se encuentra con mayor frecuencia en archivos de imagenes, archivos de audios o juegos.



A diferencia de los virus, los Troyanos no se replican a sí mismos, pero actúan como señuelo para colar software malicioso a usuarios desprevenidos.

t

Por otro lado, Los Virus, son un programa informático que, cuando es ejecutado en un dispositivo con conexión a internet, se replica y se adjunta a otros archivos ejecutables como documentos, insertando su propio código malicioso.

Los virus pueden ser inofensivos, como los que conllevan a una imagen divertida. También pueden ser destructivos como los que modifican o eliminan datos. La mayoría de virus se esparcen a través de USB, discos ópticos, recursos de red compartidos o correos electrónicos.

Sintomas de Malware en un dispotivo

Sin importar el tipo de programación maliciosa, se encuentran una serie de sintomas que identifican la presencia de software malicioso en su dispositivo inteligente.

Lo primero es analizar el aumento en el uso de la Unidad de Procesamiento Central (CPU), provocando que el sistema operativo sea lento a la hora de utilizarse. Como segunda medida está el bloqueo o congelación frecuente del computador, laptop, celulares inteligentes y cualquier otro dispositivo con acceso a internet. Mientras se está utilizando el aparato electrónico, especialmente, en el uso de los navegadores web, y este con frecuencia es lento para acceder a la busqueda en internet, también es el tercer tipo de sintoma de presencia de Malware.

Si al encender el computador o dispositivo inteligente, presenta fallas de conexión a la red, sin tener un daño interno en el aparato electrónico, es otro síntoma clave que debe tener presente para identificar la presencia de virus.

Como quinto sintoma están las modificaciones de archivos o documentos eliminados sin que usted lo haya realizado. Este punto es clave de VIRUS, puesto que su programación como malware consiste precisamente en ello, eliminar o modificar sin su autorización.

Si en su ordenador o dispositivo inteligente usted detalla programas o aplicaciones que usted no ha instalado, también represena la presencia de Malware.

Como sintomas finales están las ejecuciones de procesos o servicios desconocidos que su dispositivo móvil realiza, así como el cierre inesperado de programas o, las reconfiguraciones independientes de los programas instalados. A su vez, el envío de correos electrónicos sin su conocimiento, es sintoma real de infección de programación software maliciosa en sus dispositivos inteligentes.

Por éstas razones, es importante que usted aprenda a identificar este tipo de amenazas, para que pueda proteger sus documentos privados, archivos multimedia personales y, por supuesto, todo lo confidencial que usted tenga en sus ordenadores, como información corporativa, financiera, bases de datos, entre otros tipos de contenidos privativos para los Ciberdelincuentes.

Por una forma segura de conexión en el mundo digital

OPERINTCO.COM