#APRENDECONASUFIN

Ciberfraudes

· Tendencias 2022 ·

MINISTERIO DE CONSUMO

El presente proyecto ha sido subvencionado por el Ministerio de Consumo, siendo su contenido responsabilidad exclusiva de ASUFIN.

asufintech

Finanzas Para Todos

www.tech.asufin.com

Realizado en el marco del programa Educación Financiera y Digital 2022

Las amenazas y el fraude financiero

En una sociedad cada vez más dependiente de los dispositivos electrónicos, el aumento de las amenazas en el mundo digital se acrecienta y se transforma, con el objetivo de aprovechar cualquier debilidad tecnológica para hacerse con los datos más sensibles y ejercer todo tipo de ataques y robos.

El móvil es el principal vector de ataque, debido a toda la información personal que posee. No obstante, no es el único: ordenadores, tablets, cámaras de videoconferencia, smartwatches o drones, entre otros, son sensibles a ser hackeados con fines fraudulentos.

El Instituto Nacional de Ciberseguridad de España (INCIBE) es la organización que trabaja en afianzar la confianza digital, incrementar la ciberseguridad y contribuir al uso seguro del ciberespacio en España. En caso de albergar alguna pregunta, se les puede contactar marcando el 017.

Los ciberataques relacionados con robo de identidad y fraude financiero con más incidencia este año son:

01. **SIM swapping o duplicado de tarjetas móviles**

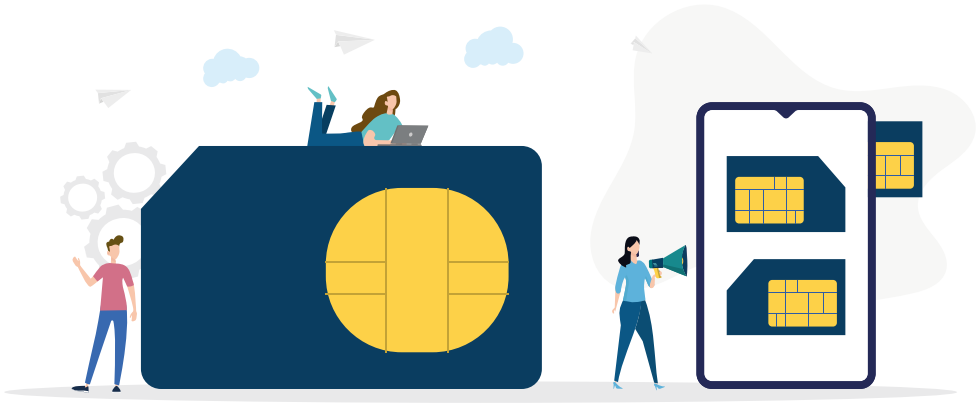
02. **Malware, software hostil o intrusivo**

03. **Phishing, smishing y vishing**

04. **Apps falsas**

05. **Ransomware o secuestro de datos a cambio de dinero**

SIM swapping o duplicado de tarjetas de móviles



La estafa del SIM swapping, consiste en duplicar la tarjeta SIM de un teléfono móvil para acceder a toda la información almacenada en esta.

Cuando el cibercriminal consigue duplicar una tarjeta SIM, no sólo accede a la agenda de contactos de la víctima, sino que, gracias a la autenticación multifactor también puede abrir sus redes sociales (y, por tanto, propagar el virus para infectar y "secuestrar" otros dispositivos u obtener información confidencial) y lo que es peor, puede obtener la clave de acceso o de autorización de una operación bancaria vía SMS y transferir dinero, solicitar un préstamo, etc.

En ocasiones, basta con hacer una llamada telefónica para que dupliquen la SIM, lo que facilita este tipo de estafa.

Consejos

1. **Ser precavido con lo que se comparte en Internet**. Cuanta menos información personal haya, más difícil será que los ciberdelincuentes consigan la información sensible.
2. **Configurar una autenticación en dos o más pasos que no involucre los SMS** (reconocimiento facial, por voz, PIN adicional, etc.).
3. **Reclamar al operador móvil** que refuerce sus sistemas de seguridad cuando se trate de duplicados en tarjetas SIM.
4. **Instalar un antivirus o herramienta de seguridad** que facilite la protección de la tarjeta SIM.

¿Cómo saber si se ha sido víctima de este tipo de ataque?

- Una vez que los ciberdelincuentes tienen acceso al duplicado de la SIM, la tarjeta del usuario se desactivará de forma automática y únicamente funcionará la del criminal. Por tanto, si no se tiene cobertura y no se pueden efectuar llamadas telefónicas ni enviar mensajes de texto, tal vez la tarjeta SIM ha sido duplicada.
- El proveedor telefónico notificará que la tarjeta SIM se ha activado en otro dispositivo.
- Otra pista es la incapacidad de acceder a las cuentas y/o tarjetas bancarias online con las claves habituales.

Malware, software hostil o intrusivo

El malware o software malicioso es un programa hostil o intrusivo que es dañino para el sistema operativo, cuya intención es invadirlo, dañarlo o deshabilitarlo. Es lo que comúnmente se conoce como virus informático.

El objetivo del malware es acceder al dispositivo, pudiendo robar, cifrar, espiar, alterar y/o borrar los datos que se encuentren en el sistema.

La manera más común de infectarse es a través de la descarga de cualquier archivo malicioso (música, películas, archivos adjuntos de email, USB, etc.).

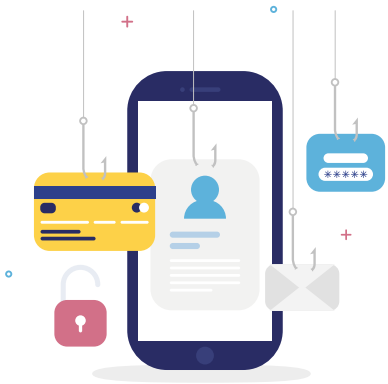
Consejos

1. Utilizar un **software antivirus** para mantener el equipo protegido.
2. **No descargar archivos de desconocidos** que induzcan a pensar que están manipulados. Si el correo, la web o la unidad extraíble (USB) no es fiable, no se debe descargar.
3. **Descargar** programas y archivos desde páginas web oficiales.
4. **Mantener el equipo actualizado** a la última versión para preservar la seguridad del mismo.

¿Cómo saber si se tiene un malware en el ordenador?

- **El ordenador se ralentiza**. La velocidad del sistema operativo irá disminuyendo, la utilización drecursos aumentará, y el ventilador del equipo funcionará a toda velocidad.
- **La publicidad y anuncios emergentes aparecen de forma constante**. Por tanto, si se recibe un mensaje del tipo “¡HAS GANADO UN IPHONE 13!”, puede que el dispositivo tenga un virus.
- **El sistema se bloquea de forma constante** o muestra una pantalla azul indicando que ha encontrado un error grave.
- **El navegador se llena inesperadamente de nuevas barras de herramienta**s, extensiones o complementos.

Phishing, smishing y vishing



El phishing, vishing o smishing son algunos de los fraudes que se utilizan para robar datos privados. El objetivo es engañar a la víctima mediante la suplantación de un tercero de confianza, que busca obtener datos personales para reemplazar la personalidad del usuario y robar sus datos.

Cuando el delito informático llega al dispositivo a través del **correo electrónico**, recibe el nombre de **phishing**, y si lo hace a través de un **SMS**, **smishing**. Existe una tercera modalidad de fraude, el **vishing**, que se comete a través de una **llamada telefónica**.

Si se tiene la sospecha de haber sido víctima de este tipo de estafa, es conveniente acceder a las cuentas (de email, wallet digital, redes sociales...) para cambiar las contraseñas y confirmar que el atacante no ha alterado la configuración de acceso (se recomienda confirmar si se ha modificado la dirección de recuperación de contraseña, las preguntas de seguridad, el teléfono, etc.).

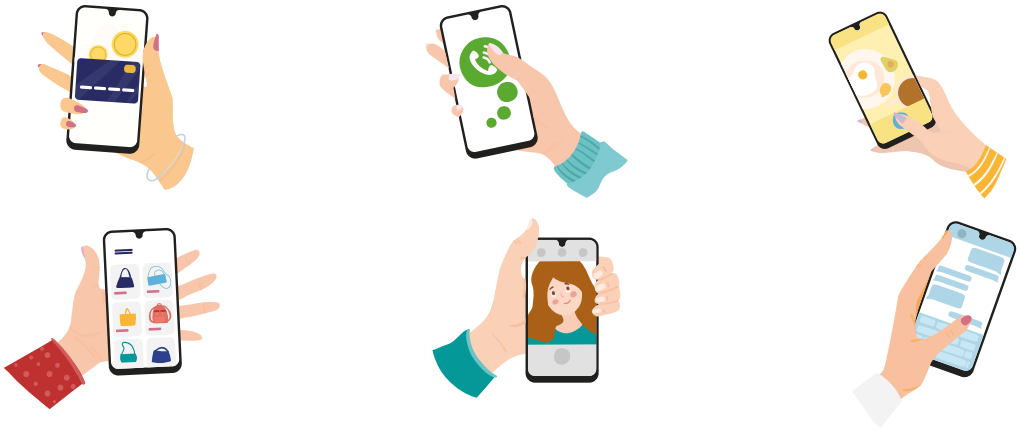
Consejos

1. **Configurar el inicio de sesión mediante la autenticación de múltiples factores** (MFA). Este método requiere probar la identidad de los usuarios a través de dos o más pruebas.
2. **Utilizar conexiones seguras** y comprobar que la web muestre un candado o llave y que su URL comience por “https”.
3. **No facilitar datos sensibles** por internet y/o teléfono, a menos que lo requieran sitios o personas de total confianza.
4. **Desconfiar de SMS, llamadas, o correos** que indican que se ha ganado un sorteo en el que no se ha participado.

¿Cómo saber si se está siendo víctima de este tipo de fraude?

- Advertir que los proveedores de cualquier plataforma nunca pedirán que se proporcionen claves de acceso personales.
- Sospechar de emails mal redactados, con faltas de ortografía o con errores de formato.
- En este tipo de fraude es común establecer plazos urgentes para solucionar el incidente sin consecuencias graves. Este tipo de técnica se lleva a cabo para que se reaccione de forma inmediata.

"Apps" falsas



Otra de las vías principales de acceso del malware a los dispositivos, en especial a smartphones, son las aplicaciones falsas, que contienen un código concreto para el robo de datos sensibles. El aspecto y funcionamiento imita el de la aplicación legítima y oficial, y su objetivo es que los usuarios se la descarguen para poder acceder a contenidos y datos personales sin el consentimiento del usuario. El aspecto de estas apps confunde al usuario, dado que su funcionamiento imita a la perfección el de una aplicación oficial.

Consejos

1. **Verificar la autenticidad** de una aplicación antes de iniciar una descarga.
2. Poner atención en los **comentarios de otros usuarios**.
3. **Confirmar** cuáles son los **permisos** que se solicitan.
4. **Adquirir** un buen producto **antivirus** y realizar **copias de seguridad frecuentes**.

¿Cómo saber si se ha instalado una aplicación falsa?

En caso de que se haya instalado una aplicación falsa, se pueden experimentar los siguientes problemas:

- Una advertencia falsa para el cumplimento de la ley que exige pagar una multa/tasa.
- Un mensaje de un antivirus falso.
- Reorientación a un sitio web o la descarga de una aplicación indeseada.

Ransomware o secuestro de datos a cambio de dinero

El malware de rescate, o ransomware, proviene del término inglés “ransom” que significa “rescate". El objetivo es secuestrar el acceso a los datos sensibles del usuario, impidiéndole la entrada al sistema o a los archivos personales a cambio de un pago, normalmente en criptomonedas o tarjetas de crédito.

Como cualquier malware, la infección puede llegar a través de la apertura de archivos adjuntos de correo electrónico de desconocidos, pinchando en enlaces web corruptos, utilizando unidades extraíbles infectadas (pendrive USB), etc.

Consejos

1. Evitar instalar **programas desconocidos** en los dispositivos.
2. **Actualizar regularmente** el sistema operativo, navegador, antivirus, y otros programas.
3. Si el dispositivo se ha infectado y se pide un rescate por la información, nunca se debe pagar y hay que **ponerse en contacto con el INCIBE en el 017**.
4. **Asegurar los duplicados de los archivos importantes** y verificar que la **copia de seguridad** no esté corrupta.

¿Cómo saber si se ha sido víctima del ransomware?

Se pueden distinguir dos niveles de ransomware o malware de rescate en función del ataque:

- Por un lado, **pueden quedar afectados sólo determinados documentos** de texto, imágenes u otro tipo de archivos, que quedarán bloqueados hasta que se liberen vía contraprestación económica.
- Por otro, en un ataque más masivo, **pueden quedar bloqueados por completo equipos en su totalidad**, como un ordenador o móvil impidiendo el acceso general al sistema y todos los archivos.

Contacto
¿Hablamos?

TELÉFONO
91 532 75 83

EMAIL
info@asufin.com

DIRECCIÓN
Plaza de las Cortes 4, 4°D
28014 - Madrid

HORARIO
De 09:00 a 14:00h.

asufintech

www.tech.asufin.com