Guía de ciberataques

Todo lo que debes saber a nivel usuario

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
OSI Oficina de Seguridad del Internauta

MEDIDAS DE PROTECCIÓN

Proponemos el siguiente ***decálogo de buenas prácticas en ciberseguridad para mejorar la protección de los dispositivos y la seguridad de la información*** de los usuarios ***frente a los ciberataques***:

- ***Utiliza un antivirus*** para analizar todas las descargas y archivos sospechosos. Debes mantenerlo siempre actualizado y activo.
- ***Mantén el sistema operativo, navegador y aplicaciones siempre actualizadas*** a su última versión para evitar vulnerabilidades.
- ***Utiliza contraseñas robustas y diferentes*** para proteger todas tus cuentas. Si es posible, utiliza la verificación en dos pasos u otro factor de autenticación.
- ***Desconfía de los adjuntos sospechosos, enlaces o promociones demasiado atractivas.*** La mayoría de los fraudes se basan en ataques de ingeniería social que pueden ser detectados aplicando el sentido común.
- ***Ten cuidado por dónde navegas.*** Utiliza solo webs seguras con *https* y certificado digital y utiliza el modo incógnito cuando no quieras dejar rastro.
- ***Descarga solo de sitios oficiales*** aplicaciones o *software* legítimo para evitar acabar infectado por *malware*. En el caso de las aplicaciones, recuerda dar solo los permisos imprescindibles para su funcionamiento.
- ***Evita conectarte a redes wifi públicas o a conexiones inalámbricas desconocidas.*** Especialmente cuando vayas a intercambiar información sensible, como los datos bancarios. Y, en caso de que tengas que conectarte por una emergencia, trata de utilizar una VPN.
- ***No compartas tu información personal*** con cualquier desconocido ni la publiques o guardes en páginas o servicios webs no fiables.
- ***Haz copias de seguridad*** para minimizar el impacto de un posible ciberataque.

Recuerda que desde INCIBE, ponemos a tu disposición una línea telefónica gratuita de ayuda en ciberseguridad, 017.

017 TU AYUDA EN CIBERSEGURIDAD

OBJETIVOS DE LOS CIBERATAQUES Y SUS CONSECUENCIAS PARA EL USUARIO

Los ciberdelincuentes se encuentran siempre al acecho de nuevas formas con las que atacarnos a los usuarios aprovechándose de nuestro desconocimiento o vulnerabilidades en nuestras defensas.
Sus objetivos son muchos y pueden tener ***distintas consecuencias para el usuario.***

1

Ataques a contraseñas

Los ciberdelincuentes se sirven de ***diversas técnicas y herramientas con las que atacar a nuestras credenciales***. Los usuarios no siempre les dificultamos esta tarea, y solemos caer en malas prácticas que ponen en peligro nuestra seguridad:

- Utilizar ***la misma contraseña para distintos servicios***.
- Utilizar ***contraseñas débiles, fáciles de recordar*** y de atacar
- Utilizar ***información personal a modo de contraseñas***, como la fecha de nacimiento.
- ***Apuntarlas en notas*** o archivos sin cifrar.
- ***Guardar las contraseñas*** en webs o ***en el navegador.***
- Y, finalmente, ***hacer uso de patrones sencillos***, como utilizar la primera letra en mayúscula, seguida de 4 o 5 en minúscula y añadir 1 o 2 números o un carácter especial. Estos patrones acaban por popularizarse, facilitando aún más la tarea a los ciberdelincuentes.

2

Ataques por ingeniería social

Los ataques por ingeniería social ***se basan en un conjunto de técnicas dirigidas a nosotros, los usuarios, con el objetivo de conseguir que revelemos información personal o permita al atacante tomar control de nuestros dispositivos***. Existen distintos tipos de ataques ***basados en el engaño y la manipulación,*** aunque sus consecuencias pueden variar mucho, ya que suelen utilizarse como paso previo a un ataque por *malware*.

TIPOS DE CIBERATAQUES

2 Ataques por ingeniería social

Phishing, Vishing y Smishing | Baiting o Gancho | Shoulder surfing | Dumpster Diving | Spam | Fraudes online

Phishing, Vishing y Smishing

¿Cómo funciona?

Se tratan de tres ***ataques basados en ingeniería social muy similares en su ejecución***. De forma general, el ciberdelincuente ***enviará un mensaje suplantando a una entidad legítima***, como puede ser un banco, una red social, un servicio técnico o una entidad pública, con la que nos sintamos confiados, ***para lograr su objetivo***. Estos mensajes suelen ser de carácter urgente o atractivo, para evitar que apliquen el sentido común y se lo piensen dos veces.

Phishing

Suele emplearse el correo electrónico, redes sociales o aplicaciones de mensajería instantánea.

Vishing

Se lleva a cabo mediante llamadas de teléfono.

Smishing

El canal utilizado son los SMS.

En ocasiones, traen consigo un enlace a una web fraudulenta, que ha podido ser suplantada, fingiendo ser un enlace legítimo, o bien se trata de un ***archivo adjunto malicioso para infectarnos con malware.***

Cuando se trata de un ataque dirigido a una persona en concreto, se conoce como Spear phishing. Esta modalidad centra en una persona específica las técnicas de manipulación, recabando información sobre ella previamente para maximizar las probabilidades de éxito a la hora de hacerse con su información o dinero

TIPOS DE CIBERATAQUES

2 Ataques por ingeniería social

Phishing, Vishing y Smishing | Baiting o Gancho | Shoulder surfing | Dumpster Diving | Spam | Fraudes online

¿Cómo se propaga/infecta/extiende?

El principal medio de propagación es el correo electrónico donde, fingiendo ser una entidad de confianza, el atacante lanza un cebo. Generalmente suele ser un mensaje urgente o una promoción muy atractiva, para motivarnos a hacer clic en el enlace o archivo adjunto, o a compartir los datos que el atacante pide en su mensaje.

¿Cuál es su objetivo?

Su objetivo es obtener datos personales y/o bancarios de los usuarios, haciéndonos creer que los estamos compartido con alguien de confianza. También pueden utilizar esta técnica para que descarguemos *malware* con el que infectar y/o tomar control del dispositivo.

¿Cómo me protejo?

El principal consejo es ser precavido y leer el mensaje detenidamente, especialmente si se trata de entidades con peticiones urgentes, promociones o chollos demasiado atractivos.

Además, otras pautas que podemos seguir para evitar ser víctima de un *phishing* son:

- ***Detectar errores gramaticales en el mensaje***. Y, si se trata de un asunto urgente o acerca de una promoción muy atractiva, es muy probable que se trate de un fraude.
- ***Revisar que el enlace coincide con la dirección a la que apunta***. Y, en cualquier caso, debemos ingresar la url nosotros directamente en el navegador, sin copiar y pegar.
- ***Comprobar el remitente del mensaje***, o asegurarnos de que se trata de un teléfono legítimo.
- ***No descargar ningún archivo adjunto y analizarlo previamente con el antivirus***. En caso de *vishing*, no debemos descargar ningún archivo que nos haya solicitado el atacante, ni ceder el control de nuestro equipo por medio de algún *software* de control remoto.
- ***No contestar nunca al mensaje*** y eliminarlo.

Conoce a fondo qué es el phishing

SMISHING suplantando al BBVA para estafar a usuarios

¿Sabías que el 95% de las incidencias en ciberseguridad se deben a errores humanos?

3

Ataques a las conexiones

Los ataques a las conexiones inalámbricas ***son muy comunes, y los ciberdelincuentes se sirven de diversos software y herramientas con las que saltarse las medidas de seguridad*** e infectar o tomar control de nuestros dispositivos.

Generalmente, este tipo de ataques se basan en interponerse en el ***intercambio de información entre nosotros y el servicio web, para monitorizar y robar*** datos personales, bancarios, contraseñas, etc.

TIPOS DE CIBERATAQUES

3 Ataques a las conexiones

Redes trampa | Spoofing | Ataques a Cookies | Ataques DDoS | Inyección SQL | Escaneo de puertos | Man in the middle | Sniffing

Redes trampa

¿Cómo funciona?

La creación de redes wifi falsas es una práctica muy utilizada por los ciberdelincuentes. ***Consiste en la creación de una red wifi gemela a otra legítima y segura***, con un ***nombre igual o muy similar a la original***, que crean utilizando *software* y *hardware*. Luego, la configuran con los mismos parámetros que la original, esperando que nos conecte a esta.

¿Cómo se propaga/infecta/extiende?

Este tipo de ataques suelen darse en lugares con una red wifi pública, con gran afluencia de usuarios. De modo que su red falsa pueda pasar desapercibida y engañe al mayor número de víctimas posible.

¿Cuál es su objetivo?

El objetivo es conseguir robar nuestros datos cuando accedamos a nuestra cuenta bancaria, redes sociales o correo electrónico, pensando que estamos llevando a cabo una conexión segura. Además, el ciberdelincuente puede llegar a tomar control sobre nuestra navegación, accediendo a determinadas webs fraudulentas o muy similares a la original preparadas para el engaño o para la infección por *malware*.

¿Cómo me protejo?

La mejor forma de prevenir este ataque es aprendiendo a identificar las redes wifi falsas:

- ***El primer indicativo es que existan dos redes con nombres iguales o muy similares***. O, por ejemplo, que añadan la palabra "gratis".
- ***Si las webs a las que accedes tras conectarte solo utilizan el protocolo http***, detén tu actividad y desconéctate.
- ***Es probable que estas redes estén abiertas*** o que permitan introducir cualquier contraseña.

Otra medida preventiva es desconectar la función del dispositivo móvil para conectarse automáticamente a redes abiertas. Finalmente, como protección, no es recomendable utilizar este tipo de redes cuando vamos a intercambiar información sensible, como nuestros datos bancarios. En caso de necesidad, podemos recurrir a una VPN.

Te explicamos qué es una VPN y para qué se usa

¡Conexión gratis a la vista! ¿Conecto mi móvil?

4

Ataques por malware

Los ataques por *malware* se sirven de programas maliciosos cuya funcionalidad ***consiste en llevar a cabo acciones dañinas en un sistema informático y contra nuestra privacidad.*** Generalmente, buscan robar información, causar daños en el equipo, obtener un beneficio económico a nuestra costa o tomar el control de su equipo.

Dependiendo del *modus operandi*, y de la forma de infección, existen distintas categorías de *malware*. ***Las medidas de protección***, por el contrario, ***son muy similares para todos ellos y se basan en mantener activas y actualizadas las herramientas de protección antimalware.***