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*.

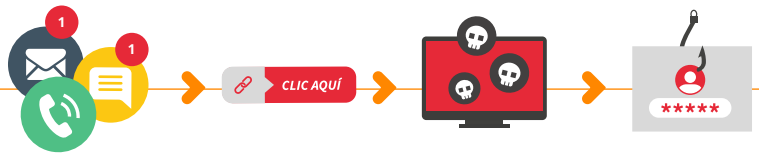
TIPOS DE CIBERATAQUES

2 Ataques por ingeniería social

Phishing, Vishing y Smishing

¿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?

TIPOS DE CIBERATAQUES

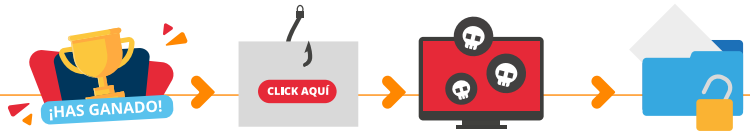
2 Ataques por ingeniería social

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

Baiting o Gancho

¿Cómo funciona?

El *Baiting*, también conocido como "cebo", se sirve de un medio físico y de nuestra curiosidad o avaricia. ***Utilizando un cebo,*** los atacantes ***consiguen que infectemos nuestros equipos o compartamos información personal.***



¿Cómo se propaga/infecta/extiende?

El medio más utilizado son los dispositivos USB infectados que los atacantes colocan en sitios estratégicos, como lugares públicos con mucha afluencia de personas o en la entrada de las empresas. Otro método consiste en utilizar anuncios y webs con las que promocionar concursos y premios que nos incitan a compartir nuestros datos o descargar software malicioso.

¿Cuál es su objetivo?

Conseguir que los usuarios conectemos estos dispositivos infectados en nuestros equipos para ejecutar *malware* con el que robar nuestros datos personales y/o tomar control del equipo, infectar la red y llegar al resto de dispositivos.

¿Cómo me protejo?

La mejor defensa para este tipo de ataques ***es evitar conectar dispositivos desconocidos de almacenamiento externo o con conexión USB a nuestros equipos***. Además, debemos ***mantener nuestro sistema actualizado y las herramientas de protección, como el antivirus, activadas y actualizadas.*** Finalmente, como en todos los ataques por ingeniería social, debemos desconfiar de cualquier promoción demasiado atractiva, o de promesas que provengan de webs o mensajes poco fiables.

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

Prueba de detección de ingeniería social

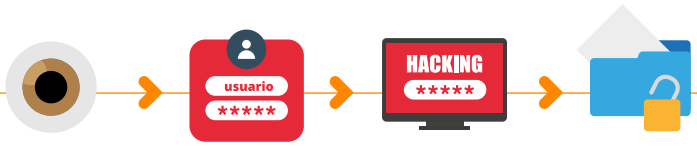
TIPOS DE CIBERATAQUES

2 Ataques por ingeniería social

Shoulder surfing

¿Cómo funciona?

Es una ***técnica mediante la que el ciberdelincuente consigue información*** de nosotros, como usuarios concretos, ***mirando "por encima del hombro" desde una posición cercana,*** mientras que utilizamos los dispositivos sin darnos cuenta.



¿Cómo se propaga/infecta/extiende?

No dispone de un medio de propagación, pero es habitual darse en lugares públicos, como cafeterías o centros comerciales, y en transportes, mientras utilizamos nuestro equipo, o en cajeros automáticos.

¿Cuál es su objetivo?

El objetivo es, como en otros ataques por ingeniería social, el robo de información: documentos confidenciales, credenciales, contactos, códigos de desbloqueo, etc.

¿Cómo me protejo?

La opción más segura es evitar que terceros tengan visión de nuestra actividad y, en sitios públicos, eludir compartir información personal o acceder a nuestras cuentas. ***También se recomienda utilizar gestores de contraseñas y la verificación en dos pasos*** para añadir una capa extra de seguridad a las credenciales.

Finalmente, ***debemos cerciorarnos de que no hay terceras personas observando nuestro dispositivo, especialmente a la hora de ingresar datos personales.*** Podemos utilizar medidas físicas, como los ***filtros "anti-espía"***. Se trata de una lámina fina que podemos colocar sobre la pantalla de nuestro dispositivo para evitar que terceros puedan ver su contenido desde distintos ángulos.

Técnicas de ingeniería social: ¿Cómo consiguen engañarnos?

El ciclo de la Ingeniería Social. ¿Cómo preparan los ciberdelincuentes un ataque de Ingeniería Social?

TIPOS DE CIBERATAQUES

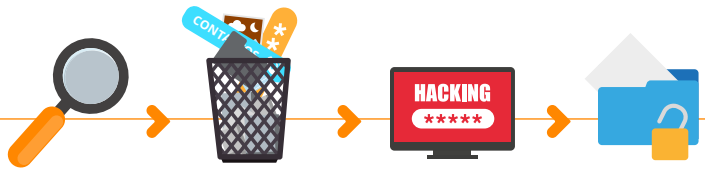
2 Ataques por ingeniería social

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

Dumpster Diving

¿Cómo funciona?

En ciberseguridad, ***se conoce como el proceso de "buscar en nuestra basura" para obtener información útil sobre nuestra persona o nuestra empresa*** que luego pueda utilizarse contra nosotros para otro tipo de ataques.



¿Cómo se propaga/infecta/extiende?

No dispone de un medio de propagación, pero está dirigido principalmente a grandes organizaciones o a individuos en concreto de los que se pueda obtener información sensible. El usuario afectado podría haber tirado a la basura documentos importantes o información personal muy valiosa para un atacante.

¿Cuál es su objetivo?

Su objetivo son documentos, anotaciones y demás información sensible que hayan podido tirar a la basura por descuido, como números de tarjetas de crédito, contactos, anotaciones con credenciales, etc.

También buscan dispositivos electrónicos desechados a los que acceder y sacar toda la información que no haya sido borrada correctamente.

¿Cómo me protejo?

La única medida de protección que debemos seguir es ***la eliminación segura de información***. Desde una trituradora de papel para el formato físico, hasta seguir los pasos para la eliminación segura de información digital.

Técnicas de ingeniería social: ¿Cómo consiguen engañarnos?

¿Sabías que 2 de cada 5 dispositivos vendidos contienen información personal?

TIPOS DE CIBERATAQUES

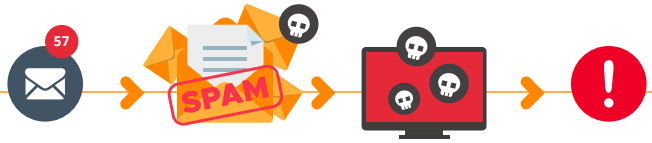
2 Ataques por ingeniería social

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

Spam

¿Cómo funciona?

Consiste en el ***envío de grandes cantidades de mensajes o envíos publicitarios a través de Internet sin haber sido solicitados***, es decir, ***se trata de mensajes no deseados***. La mayoría tienen una finalidad comercial, aunque puede haberlos que contengan algún tipo de *malware*.



¿Cómo se propaga/infecta/extiende?

El canal más utilizado sigue siendo el correo electrónico, pero se sirve de cualquier medio de Internet que permita el envío de mensajes, como las aplicaciones de mensajería instantánea o las redes sociales.

¿Cuál es su objetivo?

Los objetivos son muy variados. Desde el envío masivo de mensajes publicitarios, hasta maximizar las opciones de éxito de un ataque de tipo *phishing* a una gran población, o tratar de infectar el mayor número posible de equipos mediante *malware*.

¿Cómo me protejo?

La recomendación es ***nunca utilizar la cuenta de correo electrónico principal para registrarnos en ofertas o promociones por Internet***. Además, es fundamental configurar el filtro anti*Spam* para evitar la recepción de este tipo de mensajes. Otros medios, como las redes sociales, también cuentan con medidas de protección similares pero lo mejor es ignorar y eliminar este tipo de mensajes.

- *Mis contactos están recibiendo spam y el remitente soy yo ¿por qué?*
- *Filtros de correo antispam: para qué sirven y cómo configurarlos*

TIPOS DE CIBERATAQUES

2 Ataques por ingeniería social

Fraudes online

¿Cómo funciona?

La ingeniería social es utilizada frecuentemente para llevar a cabo todo tipo de fraudes y estafas online con las que engañarnos a los usuarios para que revelemos nuestros datos personales, o con las que obtener un beneficio económico a nuestra costa.

Existen una gran variedad de fraudes, y sus objetivos y medidas de protección pueden variar de un tipo a otro. ***Para aprender a identificarlos y a actuar ante ellos, la OSI pone a nuestra disposición una guía para aprender a identificar fraudes online***, donde se incluye: falsos préstamos, tiendas online fraudulentas, falsos alquileres, falso soporte técnico, sextorsión y muchos otros.

Guía para aprender a identificar fraudes online

Ponle freno a los fraudes y bulos con buenas prácticas