Guía de ciberataques

ATAQUES POR INGENIERÍA SOCIAL # 1

Todo lo que debes saber a nivel usuario

Instituto Nacional de Cancerología-ESE
Colombia
Por el control del cáncer

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.*

TIPOS DE CIBERATAQUES

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*.

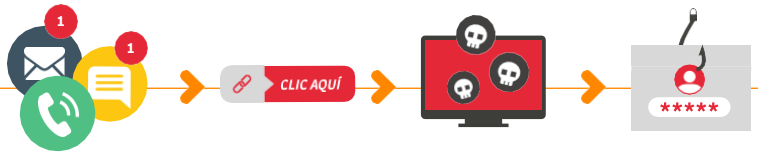
TIPOS DE CIBERATAQUES

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 piense 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 o mensajes de texto .

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 u entidad en concreto, se conoce como Spear phishing. **Esta modalidad centra en una persona o entidad 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 y noticias demasiado atractivas que apelen a una reacción emocional inmediata.

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 de remitentes desconocidos, 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 sospechoso , reportarlo a sistemas,* **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

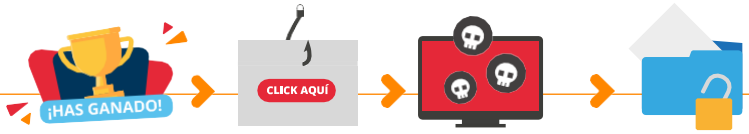
2 *Ataques por ingeniería social*

*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

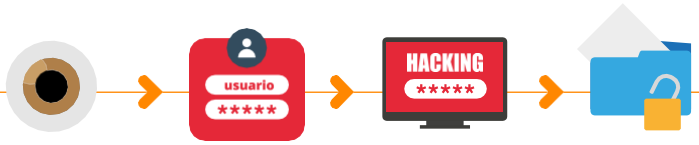
2 Ataques por ingeniería social

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

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?

Fuente:

INCIBE - https://www.incibe.es

Instituto Nacional de Ciberseguridad (INCIBE), publicación de INCIBE bajo una licencia Reconocimiento Internacional de Creative Commons 4.0-No comercial-CompartirIgual. Texto completo de la licencia: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es_ES

OSI - Servicio de la Oficina de Seguridad del Internauta (OSI) - https://www.osi.es.