Guía de ciberataques

ATAQUES POR INGENIERÍA SOCIAL # 2

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.*

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

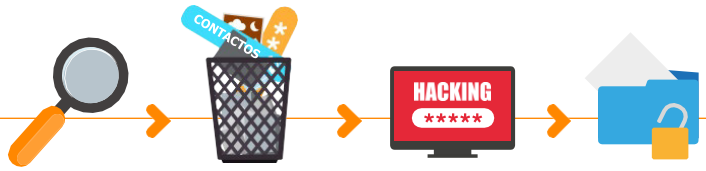
2 *Ataques por ingeniería social*

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

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, historias clínicas, información confidencial, 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

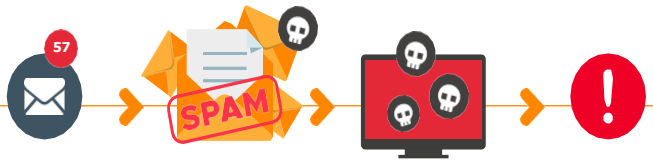
2 Ataques por ingeniería social

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 institucional para registrarnos en ofertas o promociones por Internet*. **Además, es fundamental configurar el filtro antiSpam 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*

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

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, ponemos a 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 timos con buenas prácticas

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.