Edición No. 2 – Enero 2021

Seguridad Informática en el sector Salud

¡Porque la seguridad es de todos!

TIPOS DE CIBERATAQUES

El objetivo de los ciberdelincuentes siempre será conseguir la información almacenada en nuestras cuentas, por eso les contaremos algunos tipos de Ciberataques.

Ataques por ingeniería Social

Los ataques por ingeniería social se basan en un conjunto de técnicas dirigidas a 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.

Phishing, Vishing y Smishing

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.

Smishing: El canal utilizado son los SMS.

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

Vishing: Se lleva a cabo mediante llamadas de teléfono

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

¿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.

Edición No. 2 – Enero 2021

Seguridad Informática en el sector Salud

¡Porque la seguridad es de todos!

¿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 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.
- **Comprobar el remitente del mensaje**, o asegurarnos de que se trata de un **teléfono legítimo**.
- **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.
- 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 el mensaje y eliminarlo.

Te invitamos a tomar las siguientes medidas preventivas:

- **NO abrir archivos adjuntos** ni abrir enlaces que provengan de correos de destinatarios desconocidos, que alerten sobre cobros jurídicos, demandas o similares y en caso de recibirlo, se debe reportar de inmediato al correo de Seguridad de tu institución o al área de informática, adjuntando el correo sospechoso.
- No descargue contenido multimedia por redes de intercambio tales como Ares.
- Apagar el equipo de cómputo cuando termine su jornada laboral, no solo previene que sea blanco de un ataque, sino que mejora el rendimiento, ahorra energía y previene el desgaste innecesario de este.
- Evitar ingresar a páginas de orígenes desconocidos.

Fuente: INCIBE y la Oficina de Seguridad del Internauta (OSI).