SEGURIDAD DIGITAL

Tipos de Ataques

Mensaje o correo de phishing. Intenta engañar a un usuario para hacer un clic en un enlace malicioso, abrir un archivo adjunto infectado o utilizar un formulario en línea para obtener datos personales.

Características:

- Sensación de urgencia para que el usuario cometa un error
- Uso de saludos genéricos en lugar de su nombre o título
- El remitente proviene de una cuenta como Hotmail, Gmail, Gobierno y en otros casos de empresas públicas y privadas.
- Incluye ofertas que despiertan curiosidad o notificaciones de un paquete que nunca llegó

Spear phishing. Parecido al phishing, pero el ataque está dirigido con un objetivo más específico. El atacante investiga a la víctima y crea un correo a medida con más posibilidades de engañarla.

Características:

- El correo parece provenir de un amigo o colega, pero el mensaje no parece escrito por esa persona
- Crea una sensación de urgencia e invita a ignorar las políticas
- Está relacionado con el trabajo, pero proviene de una cuenta como Hotmail, Gmail, Gobierno y en otros casos de empresas públicas y privadas.

Suplantación del CEO. El atacante se hace pasar por un directivo de la organización para instarlo a hacer algo que no debería, como aprobar una transferencia o enviar documentos confidenciales.

Características:

- El correo parece provenir de un amigo o colega, pero el texto no parece escrito por esa persona
- Crea una sensación de urgencia e invita a ignorar las políticas

- El correo es muy breve y urgente, la firma indica que se envió desde un dispositivo móvil
- Está relacionado con el trabajo, pero proviene de una cuenta como Hotmail, Gmail, Gobierno y en otros casos de empresas públicas y privadas.

Llamadas o vishing. Además de enviar correos y mensajes, los atacantes pueden llamar haciéndose pasar por una persona u organización de confianza, como un centro de soporte o un proveedor conocido.

¿Qué hacer?

- Si alguien pretende crear una sensación de urgencia o le pide ayuda sin antes identificarse, sospeche. Siga siempre los protocolos para verificar la identidad de una persona antes de dar información sensible por teléfono.

USB perdidos. Los atacantes entregan o dejan deliberadamente dispositivos, como memorias USB, infectados para que alguien los inserte en una computadora.

¿Qué hacer?

- Jamás use memorias USB ni dispositivos externos desconocidos o no autorizados ni los conecte a su computadora. No permita a nadie conectar dispositivos a su computadora.

La ingeniería social es el arte de la manipulación humana, si cree que está siendo víctima de un ataque de ingeniería social, corte la comunicación con el atacante e informe de lo ocurrido de inmediato.