
Phishing

Phishing

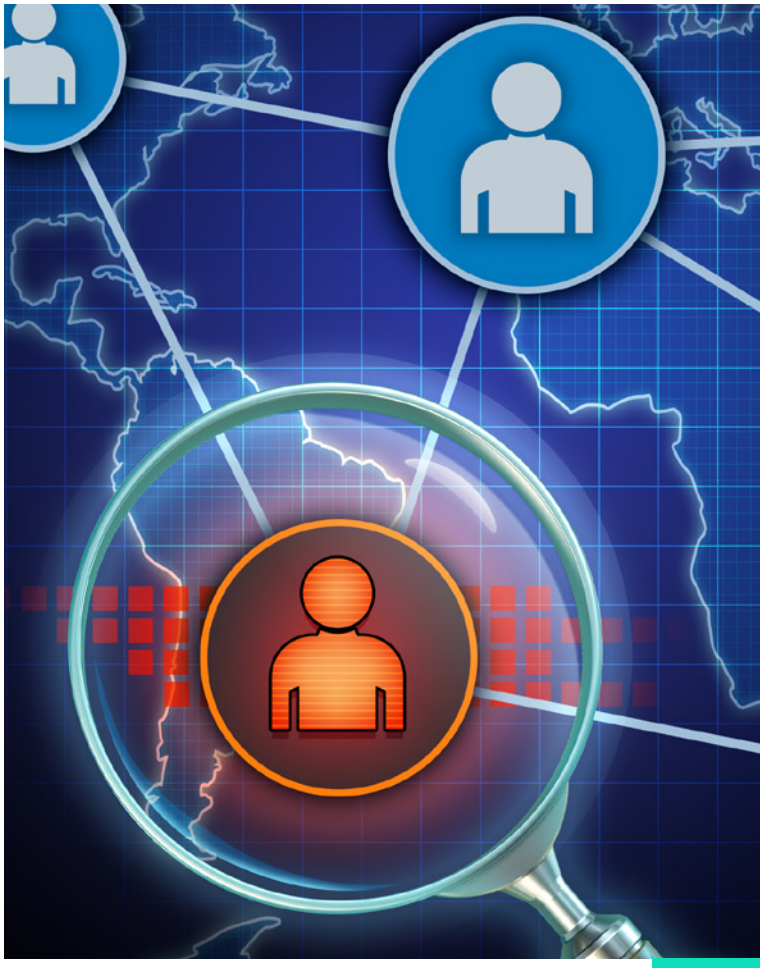
El phishing es un tipo de fraude que utiliza técnicas de ingeniería social para obtener información confidencial de las personas.

Este tipo de prácticas tiene tres componentes:

1. Se realiza a través de comunicaciones como correo electrónico, redes sociales o incluso mensajes de texto.
2. El ataque viene de usuarios que se hacen pasar por organizaciones o personas de confianza.
3. Tiene como objetivo recabar información confidencial como datos sobre cuentas o tarjetas bancarias, contraseñas para inicio de sesión y otros datos personales.

Estas son las estrategias más comunes de phishing (Belcic, 2023):

- ***De engaño:*** los atacantes se hacen pasar por personas u organizaciones para obtener información. Existen casos donde el atacante crea perfiles falsos en redes sociales que alimenta por años y de esa manera ir ganando la confianza de las víctimas.
- ***Personalizado:*** se adapta el ataque de acuerdo con el perfil de la potencial víctima y el atacante les hace llegar contenido relacionado con sus intereses, gustos o afinidades personales.
- ***Fraude del CEO:*** los atacantes se hacen pasar por directores ejecutivos o CEO's de compañías importantes como Amazon, Mercado Libre, Tesla, entre otras, para obtener información confidencial o pagos de las víctimas.
- ***Clonación:*** los atacantes crean correos electrónicos o páginas web similares a plataformas de renombre, por ejemplo, una página falsa de inicio de sesión para Facebook o un correo de algún servicio de mensajería para agregar enlaces maliciosos.
- ***Manipulación de enlaces:*** los atacantes crean enlaces similares a URLs de sitios con alta reputación o alto tráfico de usuarios pero integran cambios en las letras o errores ortográficos deliberados para provocar que las personas entren al sitio malicioso y tomar su información personal. Un ejemplo sería myfacebook.com o instagram.me que son direcciones web diferentes a las oficiales (facebook.com e instagram.com).



Algunos tipos de phishing en redes sociales son los siguientes (Norton, 2022):

- ***De inicio de sesión:*** los atacantes crean un sitio web de nombre y apariencia similar a una red social para robar información como nombre del usuario y contraseña.
- ***Avisos de cuentas bloqueadas:*** el atacante hace llegar a los usuarios mensajes con información falsa sobre un acceso no autorizado o un nuevo "filtro de seguridad" donde se le pide a la persona que agregue sus datos personales o credenciales de inicio de sesión.
- ***Servicios de hackeo:*** los atacantes crean campañas falsas donde ofrecen a los usuarios hackear el perfil de algún usuario, pero las personas terminan siendo redirigidas a otras páginas que generan ganancias monetarias a los atacantes.
- ***Servicios para ganar seguidores:*** al igual que los servicios de hackeo, los atacantes crean páginas donde ofrecen a las potenciales víctimas generarles más seguidores.
- ***Fraude de pago:*** los atacantes crean páginas con apariencia similar a alguna red social e integran un mensaje relacionado con un pago rechazado, junto con el mensaje se agregan campos para agregar información sobre la tarjeta de crédito o débito de la potencial víctima.

Estas prácticas pueden causar consecuencias en los usuarios vulnerados como robo de dinero, de identidad o de datos por lo que se recomienda siempre verificar las páginas que soliciten datos personales, no hacer clic en enlaces sospechosos que sean vistos en las redes sociales o bien, que algún usuario haga llegar por medio de mensajes directos.

Referencias bibliográficas

- Belcic, I. (2023). *Guía esencial del phishing: cómo funciona y cómo defenderse*. Recuperado de https://bit.ly/3NqsaCf

- Norton. (2022). *Nuevo estudio detecta 8 ataques de phishing en redes sociales*. Recuperado de https://bit.ly/43y4EKa

La obra presentada es propiedad de ENSEÑANZA E INVESTIGACIÓN SUPERIOR A.C. (UNIVERSIDAD TECMILENIO), protegida por la Ley Federal de Derecho de Autor; la alteración o deformación de una obra, así como su reproducción, exhibición o ejecución pública sin el consentimiento de su autor y titular de los derechos correspondientes es constitutivo de un delito tipificado en la Ley Federal de Derechos de Autor, así como en las Leyes Internacionales de Derecho de Autor.

El uso de imágenes, fragmentos de videos, fragmentos de eventos culturales, programas y demás material que sea objeto de protección de los derechos de autor, es exclusivamente para fines educativos e informativos, y cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por UNIVERSIDAD TECMILENIO.

Queda prohibido copiar, reproducir, distribuir, publicar, transmitir, difundir, o en cualquier modo explotar cualquier parte de esta obra sin la autorización previa por escrito de UNIVERSIDAD TECMILENIO. Sin embargo, usted podrá bajar material a su computadora personal para uso exclusivamente personal o educacional y no comercial limitado a una copia por página. No se podrá remover o alterar de la copia ninguna leyenda de Derechos de Autor o la que manifieste la autoría del material.