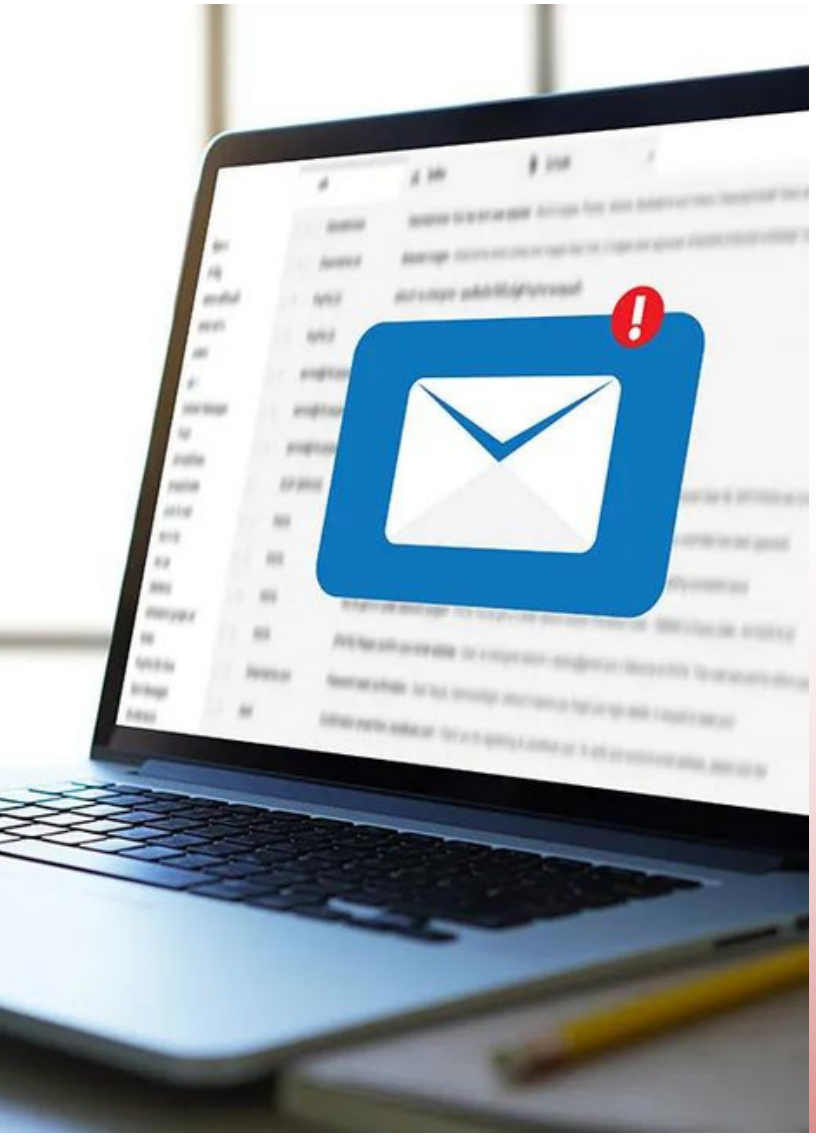
¿QUE ES EL PHISHING?

IMG



IMG

¿Que es el PHISHING?

El phishing ocurre cuando un atacante le engaña para que abra un enlace malicioso o un archivo adjunto de correo electrónico tras haberlos disfrazado de algo interesante. Siga leyendo para obtener más información sobre qué es el phishing y cómo puede protegerse.

P H I S H I N G

También se puede utilizar para infectar su dispositivo con malware.

Este tipo de virus se denominan troyanos , por el caballo de Troya de la mitología griega.

Lo engañan para que proporcione sus datos, como las credenciales de inicio de sesión y otros datos confidenciales, a los delincuentes.

Todos son métodos utilizados por ladrones de identidad y utilizan tecnología avanzada para obtener sus datos personales y utilizarlos para propósitos ilegales.

PHISHING

Lo engañan para que proporcione sus datos, como las credenciales de inicio de sesión y otros datos confidenciales, a los delincuentes.

SMISHING

Utiliza mensajes de texto en lugar de correos electrónicos para engañar a sus víctimas.

VISHING

Puede usar llamadas reales o software de texto a voz automatizado

5 FORMAS DE EVITAR ESTAFAS DE PHISHING

Las medidas antiphishing empiezan sabiendo qué es y cómo funciona el phishing. Estos son 5 consejos que pueden ayudarle a evitar estafas de phishing.

1. Recuerda que tú eres tu mayor vulnerabilidad

Nadie se convierte en víctima de una estafa de phishing sin ser engañado para implicarse. Una estafa de phishing exitosa generalmente requiere que abra un correo electrónico de phishing, haga clic en un enlace o abra un archivo adjunto. Por lo general, hay pasos adicionales, como hacer clic en Habilitar contenido para permitir que un troyano o ransomware infecte su dispositivo o ingresar sus datos privados en un formulario de estafa.

2. Comprender que cualquiera puede convertirse en víctima

Actualmente, los ataques de phishing son realizados por delincuentes profesionales y pueden ser extremadamente difícilesde detectar. Los ataques de phishing a menudo se alimentan de nuestro deseo de buenas noticias y nuestro miedo a las cosas malas. Por ejemplo, los delincuentes saben que existe una alta probabilidad de que una víctima o un miembro de su hogar esté esperando una entrega. Y si no esperábamos algo, podríamos estar recibiendo un regalo. Las estafas de phishing relacionadas con el envío son comunes, especialmente durantelas temporadas de Hot Sale, El Buen Fin y Navidad.

IMG

3. Los muchos tipos de phishing a menudo involucran fuentes que parecen creíbles

Los tipos más comunes de phishing son los archivos adjuntos de correo electrónico y los enlaces. Como vimos anteriormente, los ataques de phishing tambiénse pueden enviaren un SMS o mensajeinstantáneo. Cualquier cosa que mejore la credibilidad de un ataque de phishing ayuda a que la estafa funcione. Muy a menudo, los ataques de phishing utilizan la apariencia falsa de grandes marcas en las que confía y de las que espera comunicarse, como Amazon, su banco, FedEx o cualquier otra empresa de envío.

4. Cuidado con la urgencia

Los correos electrónicos de phishing a menudo lo atraen con urgencia. Un correo electrónico que quiere que actúes con prisa debería generar una advertencia. Si realmente fuera urgente, no se le contactaría solo por correo electrónico o unmensaje. De hecho, fuentes como bancos y compañías de tarjetas de crédito nunca le pedirán que verifique su tarjeta o información por correo electrónico. Si dicen que es urgente, haz lo inteligente y no hagas clic. Tome el teléfono para llamar al remitente y ver si el mensaje es genuino. Para cuando comience a marcar, es posible que lo haya descubierto por símismo.

IMG

5. Confía en tu instinto

Los tipos más comunes de phishing son los archivos adjuntos de correo electrónico y los enlaces. Como vimos anteriormente, los ataques de phishing tambiénse pueden enviaren un SMS o mensajeinstantáneo. Cualquier cosa que mejore la credibilidad de un ataque de phishing ayuda a que la estafa funcione. Muy a menudo, los ataques de phishing utilizan la apariencia falsa de grandes marcas en las que confía y de las que espera comunicarse, como Amazon, su banco, FedEx o cualquier otra empresa de envío.

PARA MÁS INFORMACIÓN CONTÁCTANOS EN NUESTRAS REDES SOCIALES

IMAGENTI

IMG