FORTRA
Terranova Security | Microsoft Security

Siete maneras de protegerte del phishing

El phishing es una estafa en la que los delincuentes intentan obtener información o acceso a través de engaños y trucos. Los estafadores se harán pasar por una empresa o persona de confianza, o pueden disfrazar su malware en algo que parezca inocente con la esperanza de que lo instales en tu sistema.

Ataques de phishing comunes

Inyección de contenido

Este tipo de ataque de phishing inyecta un sitio web familiar, como una página de inicio de sesión de correo electrónico o un portal de banca online, con intenciones malintencionadas. Puede incluir un enlace, un formulario o una ventana emergente que dirija a los usuarios a un sitio web secundario, donde se les pide que introduzcan información confidencial.

Manipulación de enlaces

A veces, una estafa de phishing puede adoptar la forma de un enlace malicioso que parece provenir de una fuente de confianza, como grandes empresas y marcas famosas. Si se hace clic en el enlace, se lleva a los usuarios a un sitio web falso, donde se les pide que introduzcan la información de la cuenta.

Correo electrónico

Con mucho, la táctica más común de esta lista, un correo electrónico de phishing puede llegar a tu correo electrónico personal o profesional. Este correo electrónico puede incluir instrucciones que debes seguir, un enlace web en el que debes hacer clic o un archivo adjunto que debes abrir.

"Man-in-the-middle"

Los ataques de phishing «man-in-the-middle» se producen cuando un ciberdelincuente engaña a dos personas para que se envíen información mutuamente. El estafador puede enviar solicitudes falsas o alterar los datos que envía y recibe cada parte.

Spear phishing

El spear phishing, una forma más avanzada de phishing, se dirige a personas concretas en vez de a objetivos aleatorios.

Caer en un ataque de phishing puede provocar la filtración de información confidencial, redes infectadas, demandas financieras, datos corruptos o algo peor, por lo que te explicamos cómo evitar que esto suceda:

1

Inspecciona la dirección de correo electrónico del remitente. ¿Todo está en orden? Un carácter fuera de lugar o una ortografía inusual podrían indicar que se trata de un correo electrónico falso.

2

Desconfía de los correos electrónicos con saludos genéricos («Estimado cliente», por ejemplo) que te piden que actúes con urgencia.

3

Busca información de contacto del remitente verificable. Si tienes dudas, no respondas. Crea un nuevo correo electrónico para responder.

4

No envíes nunca información confidencial por correo electrónico. Si debes transmitir información privada, utiliza el teléfono.

5

Piénsatelo dos veces antes de hacer clic en enlaces inesperados, especialmente si te piden que inicies sesión en tu cuenta. Para estar a salvo, inicia sesión desde el sitio web oficial.

6

Evita abrir archivos adjuntos de correo electrónico de remitentes desconocidos o amigos que no suelen enviarte archivos adjuntos.

7

Instala un filtro de phishing para tus aplicaciones de correo electrónico y habilita el filtro de spam en tus cuentas de correo electrónico.

Explora más temas de concienciación sobre ciberseguridad y oportunidades de formación en https://aka.ms/cybersecurity-awareness.

FORTRA
Terranova Security | Microsoft Security