POWERED BY
Terranova Security | Microsoft Security

Siete formas de protegerse de la suplantación de identidad (phishing)

El phishing es una estafa en la que los delincuentes intentan obtener información o acceso mediante el engaño y las artimañas. 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 instale en su sistema.

Ataques de phishing comunes

Inyección de contenido

Este tipo de ataque de phishing inyecta un sitio web conocido, como una página de inicio de sesión de correo electrónico o un portal de banca en línea, con intenciones maliciosas. Esto puede incluir un vínculo, un formulario o una ventana emergente que dirige a los usuarios a un sitio web secundario, donde se les pide que ingresen información confidencial.

Manipulación de vínculos

Una estafa de phishing puede venir a veces en forma de un vínculo malintencionado que parece provenir de una fuente de confianza, como empresas grandes o marcas famosas. Si se hace clic en el vínculo, este lleva a los usuarios a un sitio web falso, donde se les pide que ingresen la información de la cuenta.

Correo electrónico

La táctica más común de esta lista, un correo electrónico de phishing puede llegar a su dirección de correo electrónico personal o profesional. Este correo electrónico puede incluir instrucciones que hay que seguir, un vínculo web en el que hay que hacer clic o un archivo adjunto que hay que abrir.

Ataque de intermediario

Los ataques de intermediario ocurren cuando un ciberdelincuente engaña a dos personas para que envíen información entre sí. El estafador puede enviar solicitudes falsas o alterar los datos que cada parte envía y recibe.

Phishing dirigido

Una forma más avanzada de phishing, el phishing de objetivo definido está dirigido a personas específicas en lugar de a objetivos aleatorios.

Caer en un ataque de phishing puede conducir a la filtración de información confidencial, redes infectadas, demandas financieras, datos corruptos, o algo peor, así que aquí presentamos la forma de evitar que eso suceda:

1

Inspeccione la dirección de correo electrónico del remitente. ¿Está todo en orden? Un carácter mal colocado o una ortografía inusual podrían indicar una falsificación.

2

Desconfíe de los correos electrónicos con saludos genéricos ("Estimado cliente", por ejemplo) que le piden que actúe con urgencia.

3

Busque información de contacto verificable del remitente. Si tiene dudas, no responda el mensaje. En cambio, comience un correo electrónico nuevo para responder.

4

Nunca envíe información confidencial por correo electrónico. Si debe transmitir información privada, use el teléfono.

5

Piénselo dos veces antes de hacer clic en vínculos inesperados, especialmente si lo dirigen a iniciar sesión en su cuenta. Para estar seguro, inicie sesión desde el sitio web oficial.

6

Evite abrir archivos adjuntos de correo electrónico de remitentes desconocidos o amigos que normalmente no le envían archivos adjuntos.

7

Instale un filtro de phishing para sus aplicaciones de correo electrónico y habilite el filtro de correo no deseado en sus cuentas de correo electrónico.

Explore más temas de sensibilización sobre la ciberseguridad y oportunidades de capacitación en https://aka.ms/cybersecurity-awareness.

POWERED BY
Terranova Security | Microsoft Security