¿QUÉ ES EL SPEAR PHISHING?

El spear phishing es una técnica de phishing dirigido en la que los atacantes personalizan sus correos electrónicos o mensajes para engañar a una persona o a un grupo específico, con el objetivo de robar información confidencial, como credenciales de acceso, datos financieros o información empresarial sensible.

A diferencia del phishing general, que se envía a una amplia audiencia sin personalización, el spear phishing está muy enfocado en una víctima concreta. Los atacantes recogen información detallada sobre la persona o el objetivo a través de investigaciones en línea (por ejemplo, redes sociales, sitios web, y fuentes públicas) para hacer que el mensaje parezca legítimo y convincente. Esto aumenta significativamente las probabilidades de éxito.

Características clave del spear phishing:

- ❖ Personalización: Los mensajes de spear phishing están diseñados para parecer legítimos y provienen de fuentes de confianza, como colegas, jefes, amigos o empresas con las que la víctima tiene relación.
- ❖ Objetivo específico: El ataque está dirigido a una persona o a un grupo en particular, en lugar de ser masivo, como el phishing tradicional.
- ❖ Manipulación psicológica: Los atacantes utilizan tácticas psicológicas (como urgencia, miedo o autoridad) para inducir a la víctima a hacer clic en un enlace malicioso o proporcionar información personal.
- ❖ Investigación previa: Los atacantes suelen estudiar a la víctima y sus contactos para hacer que el ataque sea más persuasivo y creíble.

Ejemplos comunes de spear phishing:

- ➢ Un correo electrónico aparentemente enviado por un jefe o compañero de trabajo, solicitando información confidencial o la transferencia de dinero, que en realidad es un intento de fraude.
- ➢ Un mensaje que aparenta provenir de una entidad financiera que solicita la actualización de los detalles de la cuenta, con el objetivo de robar las credenciales bancarias.
- ➢ Cuentas de redes sociales hackeadas que envían mensajes a contactos de la víctima solicitando dinero o datos personales.

Cómo prevenir el spear phishing:

Verificación:

Siempre verificar la autenticidad de los correos electrónicos o solicitudes de información, incluso si parecen provenir de fuentes confiables.

Cuidado con los enlaces:

No hacer clic en enlaces sospechosos ni descargar archivos adjuntos de correos electrónicos no verificados.

Educación:

Formación continua sobre las técnicas de ingeniería social y phishing para estar alertas a posibles ataques.

Autenticación de dos factores (2FA):

Activar la autenticación de dos factores para agregar una capa extra de seguridad a las cuentas sensibles.

El spear phishing es particularmente peligroso debido a su alto grado de personalización y la confianza que genera en la víctima, lo que lo hace más difícil de detectar.