NOVIEMBRE 2024

NEWSLETTER

1 Phishing, cómo reconocerlos y cómo evitar caer en ellos

El phishing es una de las amenazas cibernéticas más comunes y efectivas, utilizando tácticas de ingeniería social para engañar a las víctimas y obtener información confidencial. A continuación, exploramos cómo reconocer estos ataques y las mejores prácticas para evitarlos, basándonos en información de empresas líderes en ciberseguridad como Sophos, Fortinet, IBM, Dell Technologies y Bitdefender.

¿Qué es el Phishing?

El phishing es un tipo de fraude en línea donde los atacantes se hacen pasar por entidades confiables para engañar a las personas y hacer que revelen información sensible, como credenciales de inicio de sesión y datos financieros. Este tipo de ataque se realiza principalmente a través de correos electrónicos, mensajes de texto (smishing) y llamadas telefónicas (vishing).

Cómo reconocer un ataque de Phishing

- **Enlaces y Archivos Adjuntos Sospechosos:** Los correos electrónicos de phishing a menudo contienen enlaces que parecen legítimos, pero redirigen a sitios web maliciosos. También pueden incluir archivos adjuntos diseñados para infectar dispositivos con malware.
- **Mensajes Urgentes o Amenazantes:** Los atacantes suelen crear un sentido de urgencia o miedo, indicando que hay un problema con tu cuenta que necesita ser resuelto inmediatamente.
- **Errores Gramaticales y Ortográficos:** Muchos correos de phishing contienen errores gramaticales y ortográficos, lo cual puede ser una señal de alerta.
- **Direcciones de Correo Electrónico Falsas:** Verifica siempre la dirección de correo electrónico del remitente. Los atacantes a menudo utilizan direcciones que imitan a las de empresas legítimas.

Cómo evitar caer en un ataque de Phishing

Educación y concienciación: La formación continua sobre ciberseguridad es crucial. Programas como Sophos Phish Threat ayudan a los empleados a reconocer y responder adecuadamente a los intentos de phishing.

Tecnología de seguridad: Utiliza soluciones de seguridad avanzadas que incluyan filtros de correo electrónico y análisis de enlaces en tiempo real. Sophos Email Security, por ejemplo, revisa los enlaces antes de que lleguen a la bandeja de entrada y nuevamente cuando se hace clic en ellos.

Autenticación Multifactor (MFA): Implementar MFA añade una capa adicional de seguridad, haciendo más difícil para los atacantes acceder a las cuentas incluso si obtienen las credenciales.

Actualizaciones y Parches: Mantén todos los sistemas y software actualizados para protegerte contra vulnerabilidades conocidas.

Verificación de fuentes: Siempre verifica la autenticidad de los mensajes antes de proporcionar cualquier información. Contacta directamente a la empresa a través de canales oficiales si tienes dudas.

Conclusión

El phishing sigue siendo una amenaza significativa debido a su capacidad para evolucionar y adaptarse. Sin embargo, con la combinación adecuada de educación, tecnología y prácticas de seguridad, es posible protegerse eficazmente contra estos ataques. Mantente alerta y siempre verifica la autenticidad de los mensajes que recibes.

admmarketing@buromc.com