

Phishing: Cómo Proteger tus Datos y Mantenerte Seguro en la Era Digital



Phishing: Cómo Proteger tus Datos y Mantenerte Seguro en la Era Digital

En la era digital, internet nos ofrece infinitas oportunidades para conectarnos, aprender y realizar diversas actividades en línea. Sin embargo, también nos enfrentamos a riesgos cibernéticos, uno de los más comunes y peligrosos es el phishing. Aunque su nombre suena complicado, en realidad es algo que puede afectar a cualquiera, incluso a aquellos que no estamos muy familiarizados con la tecnología. En este artículo, te explicaremos qué es el phishing y te brindaremos consejos prácticos para proteger tus datos y mantener la seguridad mientras navegas por la web.

¿Qué es el Phishing?

Imagina recibir un correo electrónico que aparenta ser de tu banco o de una tienda en línea conocida, solicitándolo que hagas clic en un enlace o que ingreses tus datos personales. En realidad, este tipo de correos pueden ser trampas elaboradas por estafadores para obtener información confidencial como contraseñas, números de tarjetas de crédito o datos personales. Esto es lo que se conoce como “phishing”

(la pesca), un tipo de estafa cibernética en la que los delincuentes se hacen pasar por entidades legítimas para engañarnos.

Ejemplos Comunes de Phishing:

1. Correos Electrónicos Engañosos: Los estafadores envían correos electrónicos que parecen legítimos, pero en realidad son falsificaciones. Estos mensajes a menudo incluyen enlaces maliciosos o archivos adjuntos que pueden llevarnos a sitios web falsos o infectar nuestros dispositivos con malware.
2. Sitios Web Falsos: Los ciberdelincuentes crean sitios web que se ven exactamente iguales a los de empresas o servicios populares. Estos sitios buscan que ingresemos nuestros datos personales, los cuales luego son robados y utilizados con fines fraudulentos.
3. Llamadas Telefónicas Fraudulentas: Los estafadores pueden llamarnos haciéndose pasar por representantes de empresas o instituciones y solicitar información personal o financiera. Es importante estar alerta y no proporcionar datos confidenciales a menos que estemos seguros de la legitimidad de la llamada.

Consejos para Protegerte del Phishing:

1. Sé cauteloso con los correos electrónicos: Si recibes un correo electrónico inesperado o sospechoso, evita hacer clic en enlaces o descargar archivos adjuntos. Verifica el remitente y fíjate si hay errores de ortografía o gramática en el mensaje, ya que esto podría ser una señal de alerta.
2. Verifica la autenticidad de los Sitios Web: Antes de ingresar información personal en un sitio web, asegúrate de que la dirección comience con “https://” y que haya un candado en la barra de direcciones. Si tienes dudas, visita el sitio web oficial de la empresa o servicio en cuestión para evitar caer en trampas.
3. No Reveles Información Personal por Teléfono: Si recibes una llamada inesperada solicitando información confidencial, no la proporciones de inmediato. Cuelga y busca el número oficial de la empresa para verificar la autenticidad de la llamada.

4. Mantén tus Dispositivos Actualizados: Asegúrate de tener siempre las últimas actualizaciones de software en tus dispositivos, ya que esto puede ayudar a protegerte contra vulnerabilidades explotadas por los estafadores.

El phishing puede parecer intimidante, pero con un poco de conocimiento y precaución, podemos proteger nuestros datos y mantenernos seguros en línea. Al ser conscientes de las señales de alarma y seguir los consejos prácticos que hemos compartido, podemos disfrutar de una experiencia en internet más segura y sin preocupaciones. Recuerda, la seguridad en línea es responsabilidad de todos, ¡así que protege tus datos y navega con confianza!

<https://youtu.be/FRodJr4RxQU>

Ahora bien, ya que leyó y vió el video sobre el Phishing, podrás practicar con Google y gratuitamente. [Denle “click” aquí para acceder al quiz de practica de Google.](#)