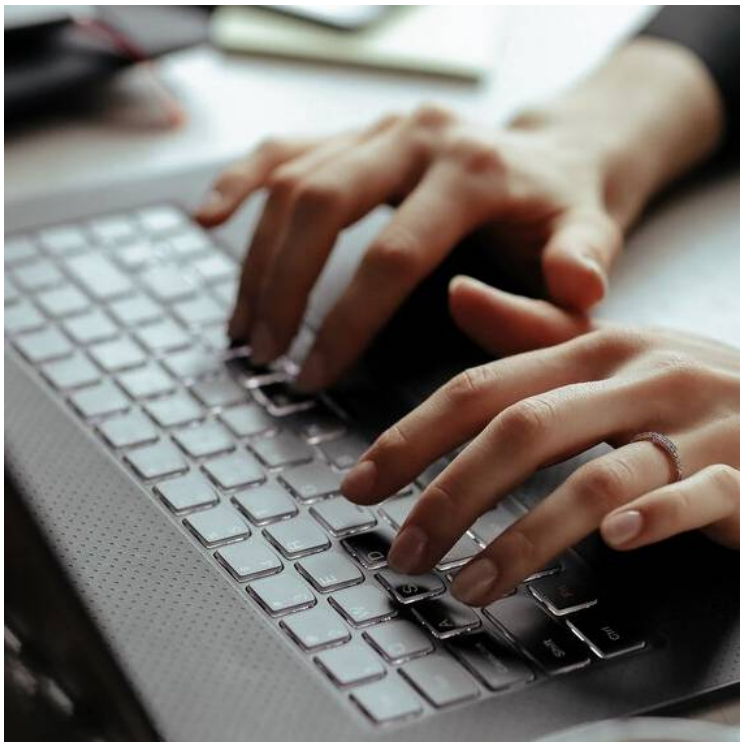
08/01/2025

Así es la nueva modalidad de estafa que te vacía la cuenta bancaria con un solo clic

Conocida como typosquatting, está poniendo en riesgo el dinero de miles de usuarios en todo el mundo



En la era digital, la tecnología ha transformado la vida cotidiana, ofreciendo una conectividad sin precedentes y facilidades como compras online, servicios de streaming y comunicación instantánea. Sin embargo, junto con estas comodidades, también ha surgido una creciente amenaza: los ciberataques. Entre estas prácticas fraudulentas, una nueva modalidad de estafa, conocida como typosquatting, está poniendo en riesgo las cuentas bancarias de miles de usuarios en todo el mundo.

¿Qué es el typosquatting?

El typosquatting es una **técnica de ingeniería social que explota los errores de escritura al teclear manualmente direcciones web**.

Los ciberdelincuentes registran dominios que son casi idénticos a los de sitios populares, pero con ligeras alteraciones, como letras añadidas, faltantes o reemplazadas.

Por ejemplo, en lugar de ingresar “amazon.com”, un usuario podría cometer un error y teclear “amazom.com”. Esta pequeña diferencia podría dirigirlo a un sitio malicioso que imita perfectamente al original, con el propósito de robar información confidencial como nombres de usuario, contraseñas y datos de tarjetas de crédito.

Cómo funciona esta estafa

Los sitios web fraudulentos diseñados por los atacantes suelen replicar cuidadosamente el diseño de las páginas auténticas, incluyendo logotipos y estilos corporativos. Esto hace que **el usuario no sospeche que está frente a una imitación**. Una vez que la persona interactúa con el sitio, como ingresando sus credenciales o detalles financieros, los estafadores obtienen acceso directo a su información personal.

Además del daño a las víctimas, este tipo de fraude también perjudica a las marcas, ya que pueden dañar su reputación y generar desconfianza entre sus clientes.

¿Cómo protegerse del typosquatting?

La prevención es clave para evitar caer en este tipo de estafas. Aquí hay algunas recomendaciones de los expertos en ciberseguridad:

- **Revisar cuidadosamente las URL:** antes de ingresar datos sensibles en un sitio web, asegúrate de que la dirección sea correcta. Presta atención a pequeños cambios como letras adicionales, faltantes o dominios inusuales.
- **Usar marcadores o motores de búsqueda:** en lugar de escribir manualmente las direcciones web, guarda los sitios confiables como favoritos o utilízalos a través de motores de búsqueda.
- **Evitar enlaces en correos electrónicos o mensajes:** si recibes un enlace, especialmente en mensajes no solicitados, verifica su autenticidad antes de hacer clic.
- **Habilitar medidas de seguridad adicionales:** configura la autenticación de dos factores (2FA) en tus cuentas para agregar una capa adicional de protección.

Dominios falsos comunes en typosquatting

- goooogle.co
- gogle.com
- amazom.com
- faceboook.com
- micorosft.com
- google.login.com

Estos dominios están diseñados específicamente para engañar a los usuarios y dirigirlos a sitios maliciosos.

Fuente: https://www.larazon.es/

LINK DE LA NOTICIA