Qué es el “spoofing” y cómo puede afectar tu identidad digital

27/03/2026

El término **spoofing** designa la suplantación digital en la que un delincuente se hace pasar por una institución o una persona de confianza para engañar y obtener datos sensibles. Esta técnica, cada vez más habitual, busca que la víctima entregue desde claves de acceso hasta información bancaria o permita instalar software malicioso.

Qué es el “spoofing” y cómo puede afectar tu identidad digital

Entre las modalidades más conocidas están el phishing —correos que imitan a empresas—, el smishing, que abusa de SMS para redirigir usuarios, y el pharming, que reproduce sitios oficiales para robar credenciales. Los atacantes suelen generar sensación de urgencia para que la persona actúe rápido y escriba sus datos en plataformas controladas por el

estafador.

Existen variantes más complejas que falsean números telefónicos, manipulan direcciones IP, alteran sistemas DNS o incluso presentan información biométrica y ubicación GPS para dar apariencia de legitimidad. Ese arsenal tecnológico dificulta distinguir un mensaje real de uno fraudulento, por lo que conviene advertir señales atípicas antes de responder.

Cómo protegerse del “spoofing”

La defensa principal contra el **spoofing** pasa por un escepticismo organizado: ante llamados que pidan claves o pagos, cortar la comunicación y comunicarse por canales oficiales. Nadie serio solicita datos confidenciales por correo o SMS. Si recibe un enlace sospechoso, mejor escribir la dirección manualmente en el navegador y confirmar que la URL sea la del sitio oficial.

También conviene desconfiar de mensajes que presionan por pagos inmediatos o amenazas, y revisar la redacción del remitente: los ciberdelincuentes a menudo no replican el tono habitual de un conocido o empresa. Ante dudas, llamar al número oficial o usar canales de atención verificados; no responder ni compartir capturas con información sensible.

Las consecuencias del **spoofing** pueden ser graves: desde vaciados de cuentas hasta accesos no autorizados a correos y redes sociales, y la instalación de malware que compromete todos los datos del equipo. Por eso resulta clave mantener actualizado el sistema operativo y activar la autenticación de dos factores en servicios críticos.

Fuente: La 100