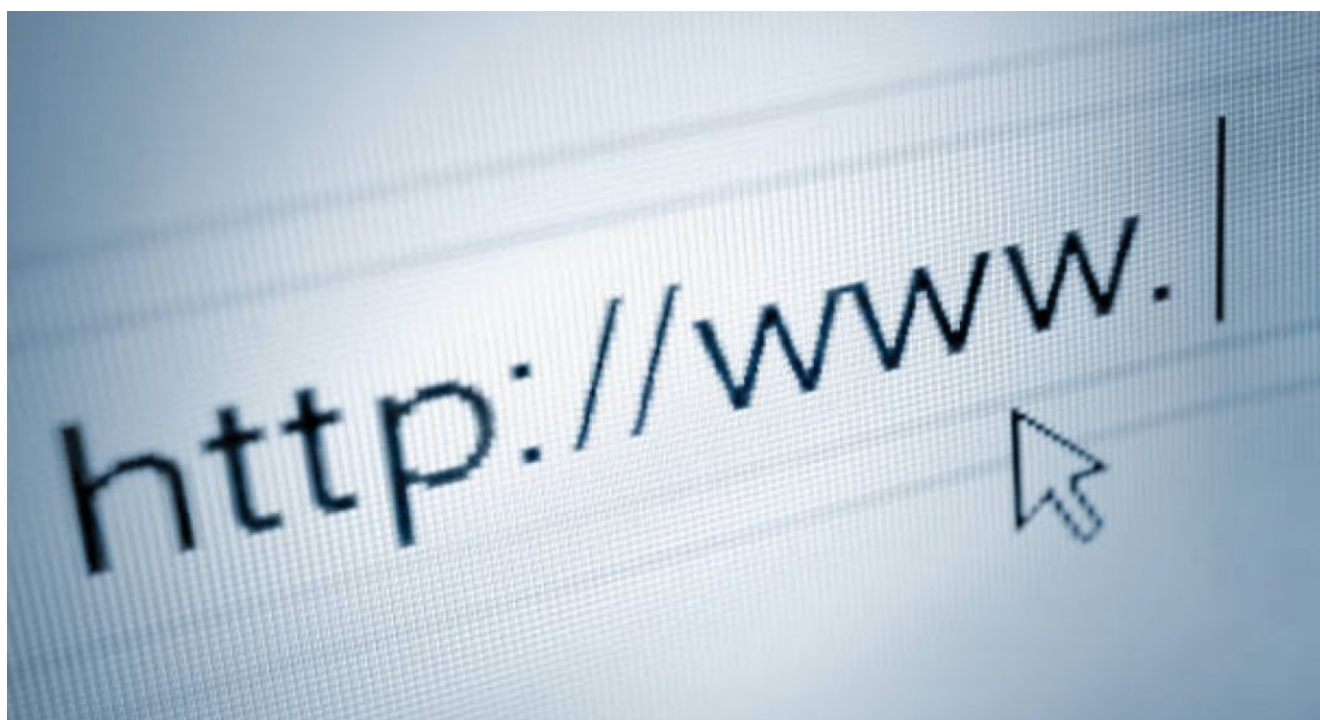


Guía práctica para evitar estafas: cómo protegerse del phishing y las URL falsas en internet

29/03/2024



En la era digital, la **seguridad informática** se convirtió en una prioridad para millones de usuarios en todo el mundo. Entre las amenazas más comunes se encuentran el **phishing** y las **URL falsas**, tácticas utilizadas por cibercriminales para engañar a las personas y obtener información confidencial.

Un reciente informe presentado por **Google** reveló que, a pesar de los esfuerzos para combatir el phishing, aún se detectan millones de **intentos de estafas** diariamente. Es por ello, que resulta importante tomar medidas proactivas y efectivas para protegerse al navegar por la web.

✘ **Hacker, ciberataque. Foto: Unsplash.**

¿Cómo puedo verificar la autenticidad de una URL?

Una de las primeras acciones que los usuarios pueden tomar es examinar detenidamente la **estructura de una URL** antes de interactuar con ella. Las **URL's legítimas** suelen tener un **patrón claro y coherente**, mientras que las falsas pueden contener errores ortográficos o utilizar caracteres especiales para imitar a las auténticas.

Otro indicador clave de seguridad es el **protocolo HTTPS**. Al buscar el prefijo «**https://**» en la dirección web, los usuarios pueden verificar que la conexión con la página es segura y cifrada. Si este protocolo está ausente, es recomendable proceder con precaución.

 **Google, tecnología, página web. Foto: Unsplash.**

Además, es fundamental verificar el **certificado de seguridad** del sitio haciendo click en el icono de candado que aparece junto a la URL en la barra de direcciones. Los sitios legítimos suelen tener un certificado válido emitido por una autoridad reconocida, lo que brinda mayor confianza al usuario.

Evitar hacer clic en enlaces directos de **correos electrónicos o mensajes sospechosos** también es una medida preventiva de las más importantes. En su lugar, se recomienda acceder directamente a la página oficial ingresando la URL en la barra de direcciones o realizando una búsqueda segura en un motor confiable.

Existen herramientas y servicios online diseñados específicamente para verificar la **autenticidad de las URL's**. Estas herramientas pueden analizar la seguridad de un enlace antes de que el usuario acceda a él, proporcionando una **capa adicional de protección** contra estafas y phishing.

❌ **Los «hackers» utilizan varias técnicas como el «phishing» o «ransomware». Foto: Unsplash.**

Es crucial estar alerta a las señales de alerta en el **contenido de la página**, como ofertas demasiado buenas para ser reales, solicitudes de información personal o financiera, y una cantidad excesiva de anuncios. Estos elementos podrían indicar la presencia de una **URL falsa**.

Acceder a una **URL falsa** puede tener consecuencias graves, incluyendo la exposición a **phishing**, la instalación de **malware** en el dispositivo del usuario, el riesgo de **ransomware** y el **fraude financiero** directo. Por lo tanto, es fundamental tomar medidas preventivas y verificar siempre la autenticidad de una URL antes de interactuar con ella.

En ese sentido, los expertos expresan que la seguridad es **responsabilidad de todos los usuarios**. Al adoptar hábitos seguros de navegación y verificar la autenticidad los sitios web, se podrán evitar estafas y se ayudará a contribuir a un entorno digital más seguro y confiable.

Fuente: Canal 26