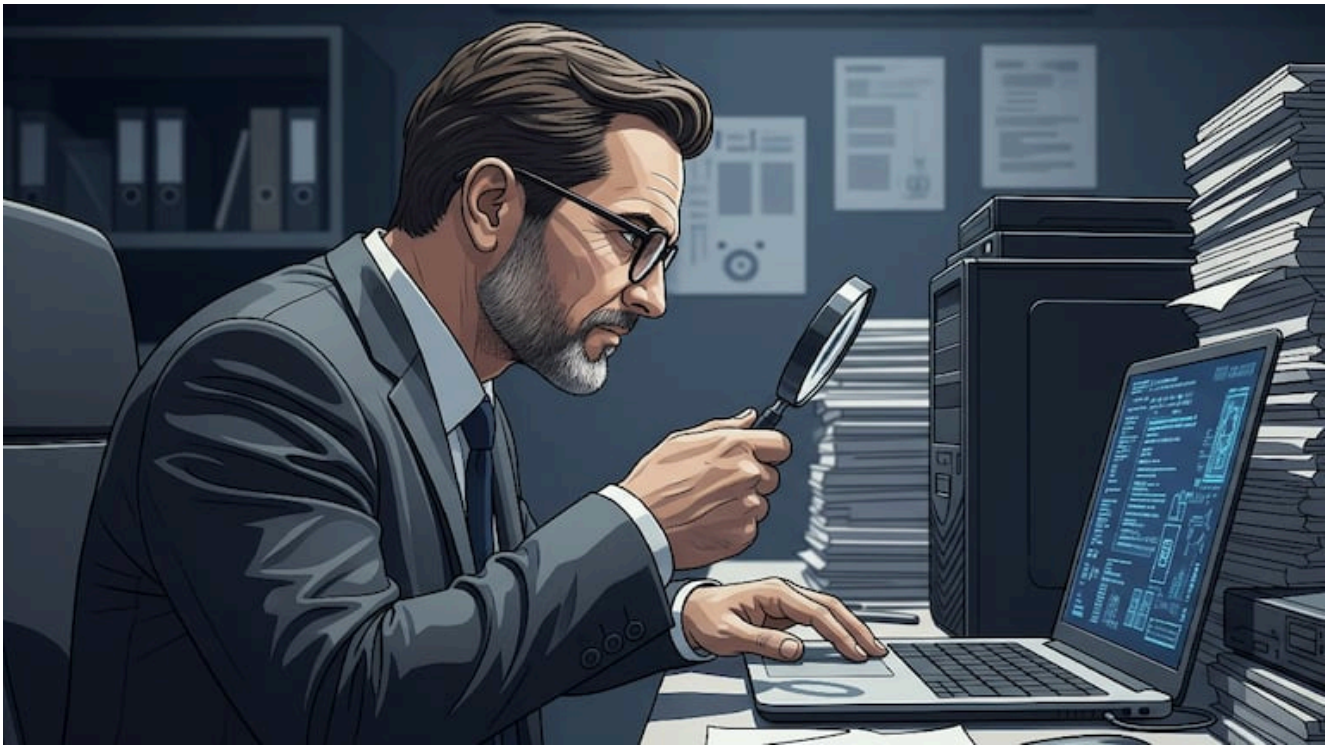
Las cuatro claves para identificar cuando un enlace es un virus o lleva a una estafa virtual

12/11/2025

Los enlaces maliciosos, que llevan a sitios fraudulentos y abren la puerta a virus y estafas, son uno de los principales focos de atención en el ámbito de la ciberseguridad.

Cada vez más, los ciberdelincuentes usan métodos sofisticados para engañar a los usuarios y convencerlos en que hagan clic y sigan estos enlaces; y de esa manera, acceder a información personal o empresarial desde correos, mensajes de redes sociales o sitios web falsos.

En este sentido, **reconocer un link sospechoso** antes de hacer clic es **fundamental** para protegerse de fraudes, **malware** y robo de datos.



Verificar la URL del link y buscar errores en la dirección son algunas importantes prácticas de ciberseguridad. (Imagen generada por GeminiAI).

El auge del comercio electrónico, las ofertas y descuentos online y el uso constante de servicios en la nube multiplicó los peligros asociados a enlaces peligrosos. **Un clic** en el link equivocado puede llevarte a activar una campaña de **phishing, la instalación de virus en tu dispositivo o un robo de identidad**.

Por eso, conocer **cómo distinguir un link falso** de uno genuino es una habilidad indispensable en estos días.

Cuatro claves para verificar que un enlace no es malicioso

1. Buscar errores, caracteres extraños y extensiones desconocidas

Antes de interactuar con un enlace, conviene revisar si contiene faltas de ortografía, **símbolos extraños o extensiones inusuales**. Estos detalles pueden indicar que la página fue creada para engañar al usuario o redirigirlo a contenido

malicioso.

2. Comprobar datos de contacto reales

Un sitio confiable suele incluir información verificable como dirección física, teléfono y correo corporativo. La ausencia de estos datos, o la presencia de información vaga, puede ser señal de un **portal falso** o peligroso.

Sus direcciones web y de redes sociales también están publicadas en sus páginas oficiales.

3. Desconfiá de mensajes no solicitados

Si recibís un email o mensaje directo con una empresa u organismo en el que no hiciste ningún reclamo ni trámite, **desconfiá**.

Los ciberdelincuentes suelen enviar **correos similares a los de compañías conocidas** en los que piden a los usuarios que sigan un enlace para completar información o solucionar algún inconveniente inexistente en la realidad. Lo mejor, en estos casos, es **contactar al remitente real por otros medios** (website oficial, redes, teléfono).

4. Si es urgente, es probable que sea falso

Si quien te envía el enlace te **insiste que hagas clic lo antes posible**, ya sea porque expira una supuesta oferta, o amenaza con la suspensión de un servicio o la implementación de una **multa**, lo más probable es que todo sea **mentira** y estén aprovechando una falsa urgencia para que la víctima caiga.

Una recomendación por fuera de la lista es que **nunca sigas enlaces que te lleven a instalar aplicaciones desconocidas.** Muchos ciberdelincuentes envían links de descarga a apps con la **excusa** de que con ella el usuario va a poder solucionar algún problema, ya sea de registro de datos o de servicio técnico, e incluso para acceder a alguna promoción.

Lo que hacen esas aplicaciones es **darle a la otra persona acceso remoto y total** al dispositivo en el que se instalan.

Como siempre, la sugerencia es, ante un enlace desconocido, detenerse a **pensar unos minutos y repasar las buenas prácticas de ciberseguridad**. La prevención es la mejor arma ante amenazas de este tipo.

Fuente: TN