Los siete errores más comunes al navegar por internet que ponen en riesgo tu privacidad y datos personales

10/10/2025

La privacidad en internet es cada vez más difícil de proteger. Con millones de personas conectadas todo el día a través de sus celulares, computadoras o televisores inteligentes, la cantidad de datos personales que circulan por la red no deja de crecer.

Y aunque los ciberataques son cada vez más sofisticados, muchas veces somos los propios usuarios quienes, por descuido o desconocimiento, dejamos la puerta abierta a hackers, estafadores y aplicaciones que rastrean nuestra actividad on line.

¿Cuántas veces hiciste **click en un enlace desconocido solo por curiosidad**? ¿O descargaste una aplicación de un sitio web que

te pareció atractiva? Estas prácticas, tan comunes como peligrosas, pueden terminar exponiendo tu **información sensible**, desde fotos, ubicaciones y conversaciones, hasta **contraseñas**, claves bancarias y números de tarjetas.

Las trampas de phishing son una de las principales causas de robos de información o instalación de malware. (Imagen: GeminiAI)

Estos son las siete prácticas que exponen nuestra privacidad en internet

- **1. Hacer click en enlaces desconocidos y no solicitados (phishing)**

Las trampas de phishing son una de las principales causas de robos de información o instalación de malware. Muchos atacantes envían **correos o mensajes con diversas excusas** (técnicas de **ingeniería social**) que incluyen enlaces que parecen legítimos, pero conducen a **sitios maliciosos**

ideados para capturar credenciales o datos bancarios.

Suelen presentarse en forma de notificaciones falsas de falta de pago, deudas, paquetes detenidos en aduana, activaciones o actualizaciones de claves de PAMI o servicios de streaming, etc.

- **2. Usar contraseñas débiles o repetidas**

Usar la misma clave en múltiples servicios o elegir contraseñas simples **facilita que un solo robo comprometa varias cuentas.** Por ese motivo, siempre se recomienda crear combinaciones únicas para cada perfil, que contengan mayúsculas y números.

- **3. Conectarse a Wi-Fi pública sin protección**

Las redes abiertas, sobre todo en cafés, aeropuertos o transporte público, te permiten conectarte a internet cuando te quedás sin datos. Pero también dan la posibilidad a terceros para que **intercepten tus datos**.

Si vas a conectarte a una **Wi-Fi** pública, no navegues en sitios que incluyan información sensible, como tu *homebanking* o billeteras digitales.

- **4. Ignorar actualizaciones de software y navegador**

No instalar las actualizaciones de app, sistema operativo y programas deja tu dispositivo **vulnerable frente a ataques que explotan fallas conocidas**. La mayoría de los ciberataques actuales aprovechan vulnerabilidades que ya tienen un parche disponible, por lo que es **vital aceptar y descargar los *updates***oficiales.

- **5. No activar la verificación en dos pasos (2FA)**

Muchas cuentas y perfiles importantes, como el email, **WhatsApp**, servicios financieros o redes sociales, se protegen con una capa adicional si activás la autenticación doble (2FA). Es una barrera **muy efectiva** incluso si alguien descubre tu contraseña.

- **6. Otorgar permisos excesivos o innecesarios a apps**

Instalar una app y permitirle acceso a cámara, micrófono, contactos o ubicación, cuando no hace falta, expone tu privacidad. Algunas apps aparentemente inofensivas solicitan **permisos sin relación con su funcionalidad y pueden vender esos datos a terceros.**

Por ese motivo en conveniente revisar y limitar los permisos al instalarlas o desde los ajustes en tu dispositivo.

- **7. Compartir en exceso detalles personales en redes**

Publicar en redes sociales **datos personales** como dirección, cumpleaños, rutinas o fotos, como las que se ve el colegio al que van tus hijos o los lugares donde hacen actividades, **expone tu identidad y la de tu familia y facilita ataques o robos de identidad.** Es clave revisar qué compartís y ajustar las opciones de privacidad en cada plataforma.

Fuente: TN