

# No es misión imposible: 8 claves para navegar seguro en internet y evitar que roben tus datos

18/08/2024



Vivimos en una época donde internet nos atraviesa y es esencial para nuestras actividades diarias, tanto para trabajar, estudiar e incluso disfrutar de un rato libre.

Además, las **herramientas digitales** viven evolucionando a la vez que surgen modos más sofisticados para las **amenazas cibernéticas**.

Por más de que tomemos los recaudos necesarios y las medidas de ciberseguridad, siempre nos olvidamos de algo y los **hackers** están al acecho para robar nuestros datos. Por eso, es fundamental tener en cuenta **algunos consejos**.

# ¿Cómo mantenerse seguro en internet?: 8 claves para que no roben tus datos

Hay muchos pasos a seguir para **proteger la identidad online**. A continuación, las **8 opciones fáciles** de realizar y que no requieren de **conocimientos avanzados** en tecnología para quienes quieran cuidar su **privacidad de ataques digitales**:



✖ *Cómo prevenir cualquier ataque cibernético. Foto: Unsplash.*

## 1 – Usar conexiones seguras

Las **conexiones seguras** con aquellas que cifran la información entre tu dispositivo y el servidor web, es decir, las convierte en un **código imposible de leer para los atacantes**. De esta manera, protegen tu información sensible como tus **contraseñas** o los **datos de tu tarjeta de crédito**.

Se puede verificar de diferentes maneras:

- Buscar el símbolo de **candado** a la izquierda de la barra de direcciones: al hacer clic se podrá ver una explicación que verifique que la misma es una **conexión segura**.
- Que la URL empiece con «**https**»: la «s» significa «**secure**» y, por lo tanto, establece que la página utiliza el protocolo de seguridad correcto.
- Que tenga un **certificado de seguridad válido**: se puede visualizarse haciendo click en el candado.

## 2 – Usar contraseñas fuertes

Una contraseña fuerte es indispensable para proteger tus

datos, ya que será más difícil de vulnerar. Para asegurarte de que hayas elegido la correcta se recomienda utilizar de **más de 14 caracteres, que combinen mayúsculas y minúsculas, números y símbolos.**

**✘ Una contraseña fuerte es indispensable para proteger tus datos. Foto: Unsplash.**

Otro consejo útil es utilizar una **única para cada sitio web** y usar patrones aleatorios. Se pueden utilizar generadores para crear claves seguras y un administrador para almacenar todas las que tengas. Siempre es recomendable cambiar tus contraseñas cada 6 meses.

### **3 – Activar la autenticación multifactor (MFA)**

En muchos sitios web, cuando creás una cuenta, es posible activar algún tipo de autenticación multifactor (MFA). Esta es una manera de **agregar un paso extra durante los inicios de sesión** para asegurarse de que quien quiere ingresar al usuario es el dueño del mismo.

Las más conocidas son: las **huellas digitales o el reconocimiento facial**, los códigos de uso único enviados por **correo o por SMS** y el uso de apps autenticadoras como **Google Authenticator**.

### **4 – Mantener tus dispositivos actualizados**

Las actualizaciones de software son fundamentales para **mantener la seguridad** de nuestros equipos porque les permiten a los desarrolladores mejorar debilidades de nuestros sistemas operativos que pueden haber puesto nuestros datos en riesgo a medida que avanza la capacidad de los ciberdelincuentes.

❌ *Las actualizaciones de software son fundamentales para mantener la seguridad. Foto: Unsplash.*

## 5 – Leer los Términos de Privacidad

Puede parecer la tarea más aburrida y tediosa del mundo, pero con solo tomarse unos minutos para leer los términos de privacidad de los sitios web que visitamos y en los que creamos cuentas, uno puede **comprender el uso que estos hacen de nuestros datos.**

## 6 – Aprender a reconocer enlaces sospechosos

No siempre es evidente cuando un link puede contener **malware o ser un intento de phishing**, por eso es necesario conocer sus características y particularidades. De esta manera podemos asegurarnos de no brindar datos personales a actores malintencionados.

❌ *No ingresar a enlaces sospechosos. Foto Unsplash.*

Algunas maneras de reconocer enlaces sospechosos son:

- Si se trata de un correo, **verificar el remitente.**
- Si es una página web, asegurarse de que la URL comience con «**https**» y de que el dominio no presente irregularidades.
- Estar atento a **errores de ortografía** y mensajes con promesas demasiado buenas para ser ciertas.

## 7 – Cuidar qué y dónde posteamos

Es fundamental ser consciente de la información que compartimos sobre nosotros para **proteger nuestra identidad** y prevenir malos intercambios.

## 8 – Ser cuidadoso con quienes conversamos en línea

Evitar el **ciberacoso** y los **casos de grooming** es muy importante. En internet es muy fácil ocultar tu identidad y hay quienes usan este hecho a su favor para perjudicar a otros. Uno nunca puede saber al 100% si la gente que conoce en línea está diciendo la verdad sobre quién es y es por esto que hay que mantenerse alerta.

Se recomienda no interactuar en redes sociales con gente que no conozcas en la vida real y dar la **menor cantidad de información personal** posible.

Fuente: Canal 26