



Source:

Dirección de Comunicación Institucional

La protección de los datos personales es un tema de vital importancia.

Debido al crecimiento del acceso a Internet (sobre todo por la pandemia de COVID-19) y el aumento del horarios pasados navegando en la red, ha ocurrido un incremento considerable de hackers e incidentes a internautas desprevenidos, al no conocer medidas de seguridad.

Aquí le brindamos 5 consejos que evitarán incidentes de ciberseguridad.

### **1. Elegir contraseñas seguras**

Entre más compleja sea la contraseña, más difícil será de adivinar y se evitará el robo de datos personales. Siempre que se vaya a elegir una contraseña, se recomienda combinar mayúsculas, minúsculas, símbolos y números.

No se debe utilizar la misma contraseña en todas las cuentas, ni incluir números de teléfono, fechas de nacimiento o aniversarios.

Una vez elegida la contraseña, no debe ser compartida.

### **2. Tener cuidado con la información compartida en redes sociales**

Configurar la privacidad de cada una de las cuentas para que la información no pueda ser vista por cualquier persona y nunca publicar datos personales (dirección, teléfono o imágenes de la zona donde vive) son medidas claves para evitar el robo de identidad y de su información personal.

### **3. Revisar la configuración de privacidad**

Es importante aprender a configurar adecuadamente las opciones de privacidad de los perfil en las redes y activar los límites en cada una de ellas. Muchas aplicaciones las suelen tener desactivadas por defecto. De esta forma, sólo tendrán acceso a los datos las personas que el usuario establezca, reduciendo el riesgo de ser utilizados con fines malintencionados.

### **4. Brindar datos personales sólo en sitios de confianza**

Muchas páginas piden datos personales. Antes de dárselos es importante asegurarse que no sea un sitio web falso y corroborar qué datos necesitan y para qué los van a utilizar.

Además, revisar que la web que le solicita la información cuente con la dirección HTTPS (aparece en el navegador) esto significa que inicia con el protocolo SSL (Secure Sockets Layer), es decir, permite que los datos que comparta viajen por un canal cifrado.

### **5. No confiar en desconocidos**

Una de las principales formas de robo de datos es el envío de archivos, formularios y solicitudes de contacto a través de perfiles y cuentas falsas.

Lo más recomendable es no abrir archivos de dudosa procedencia ni aceptar solicitudes de personas desconocidas en redes sociales, que pudieran ser perfiles falsos.

Al recibir una solicitud de amistad, asegúrese de poder comprobar la veracidad de la cuenta o usuario (que tenga fotos, recuerdos y sugerencias que demuestren antigüedad de la cuenta o amigos en común).

---