Filtraciones de datos

Obtenga información sobre qué hacer si es parte de una filtración de datos.

1. ¿Qué es una filtración de datos?

Una filtración de datos es una violación de seguridad en la que un usuario no autorizado copia o roba información confidencial, privada o personal.

Los actores maliciosos pueden obtener información para venderla en la Internet oscura o hacer estafas y fraudes de suplantación de identidad. Estos son algunos elementos que los actores maliciosos intentan robar durante una filtración de identidad:

- Contraseñas
- Correos electrónicos
- Información financiera
- Información personal, como su número de Seguro Social o dirección

Las filtraciones de datos son cada vez más habituales y pueden ser difíciles de evitar. No se sienta mal si le ocurre a usted. Hay medidas que puede tomar para proteger sus datos y abordar una filtración de datos.

2. Protección contra filtraciones de datos

Planifique proteger su información con antelación evaluando la seguridad de sus datos personales. Las prácticas recomendadas de privacidad en línea pueden ser una buena forma de asegurar su información y evitar que esté comprometida. Utilice el espacio en las próximas dos páginas para anotar cómo se siente con respecto a las siguientes áreas y si hay áreas que mejorar.

Solidez y singularidad de sus contraseñas:

Uso de todas las herramientas y técnicas disponibles de autenticación multifactor:

Uso de un administrador de contraseñas (recuerde que hay versiones gratuitas):

Monitoreo rutinario de cuentas: ¿controla servicios de forma habitual, como haveibeenpwned.com, para ver si su información estuvo comprometida en una filtración? Diseñe un plan sobre cómo podría abordar esto en el futuro:

Minimización de datos: ¿comparte solo lo necesario, en línea y en espacios físicos, como las tiendas? Describa su enfoque hacia los datos:

3. ¿Fui víctima de un hackeo?

Verifique lo siguiente para determinar si fue víctima de un hackeo:

- Notificación del sitio hackeado.
- Noticias (los hackeos importantes suelen aparecer en fuentes principales de noticias).
- Actividad sospechosa en la cuenta, como correos electrónicos de restablecimiento de contraseña que usted no solicitó.
- La cuenta aparece cuando busca sus cuentas en https://haveibeenpwned.com/

4. Pasos a seguir en caso de ser víctima de un hackeo

Inmediatamente después del hackeo:

- Determine qué información fue robada.
- Cambie su contraseña.
- Cierre las cuentas según sea necesario, en particular, las cuentas de tarjetas de crédito comprometidas.
- Notifique a sus amigos o contactos si su correo electrónico o redes sociales sufrieron un hackeo.

Con el tiempo:

- Esté atento a los fraudes de suplantación de identidad.
- Implemente una seguridad de contraseñas más sólida.
- Implemente la autenticación multifactor.
- Preste atención a los informes de crédito y la actividad de su cuenta.

¿Qué más podría recomendar?