Filtración masiva de datos 2024 -- ¿Que debo hacer ahora?

(traducido por Google)

Antecedentes: Hace unos días se anunció otra filtración masiva de datos, que afectó a más de 3 MIL MILLONES de registros. Los datos pirateados incluyen nombres, direcciones, números de teléfono, fechas de nacimiento, números de seguro social y similares actuales y pasados. Con esta información, los ciberdelincuentes pueden fácilmente hacerse pasar por otra persona y abrir cuentas financieras, robando efectivamente identidades y activos (dinero y otros).

Nota: Ha habido MUCHAS violaciones de datos en 2024, ésta es solo la más reciente.

¿Qué puedes hacer?

Los expertos recomiendan una variedad de acciones. Los enumeraré aquí y luego brindaré instrucciones sobre cómo hacer cada uno.

1. Verifique si su información personal se incluyó en la violación de datos más reciente.

2. Verifique sus informes de crédito para ver si ha habido alguna actividad inusual.

3. Coloque alertas de fraude en sus informes de crédito para recibir alertas si alguien accede a ellos.

4. Congele sus informes crediticios para que nadie más pueda acceder a ellos.

5. Agregue otras medidas de seguridad a sus registros financieros, si aún no lo ha hecho.

6. Si ya ha ocurrido un robo de identidad, comuníquese con su institución financiera, sus acreedores y la policía.

7. Explora otros recursos.

Mas tarde se explica cómo realizar cada una de estas tareas. No son difíciles, pero pueden llevar mucho tiempo, ya que hay tres agencias de informes crediticios independientes (Equifax, Experian, y TransUnion) y es necesario contactarlas para cada uno de estos pasos. No basta con ponerse en contacto con uno de ellos.

Verifique si su información personal se incluyó en la violación de datos más reciente.

Para determinar si su información personal se incluyó en la violación de datos más reciente, haga lo siguiente:

1. Acceda a https://npd.pentester.com/.

2. En los campos en la parte superior de la página, escriba su apellido, nombre y año de nacimiento. También puede elegir su estado en el menú desplegable; sin embargo, el Estado no es absolutamente necesario.

3. Cuando termine, haga clic en **Buscar**. La pantalla se actualizará y mostrará los registros de datos que coincidan con sus criterios de búsqueda.

4. Desplácese según sea necesario, buscando sus propios registros. Tenga en cuenta que es posible que tenga más de un registro, especialmente si ha tenido diferentes números de teléfono o direcciones.

5. Repita el proceso para todos los miembros de su familia, ¡tanto vivos como fallecidos!

Tenga en cuenta que esta búsqueda es sólo para la violación de datos más reciente. Si tu nombre no aparece aquí, ¡eso no significa que tus datos no estén en riesgo! Por lo tanto, se recomienda encarecidamente que continúe realizando los demás pasos a continuación.

También tenga en cuenta que si desea proteger la identidad de una persona fallecida, el proceso es un poco diferente. Consulte https://lifelock.norton.com/learn/identity-theft-resources/identity-theft-ghost-stories para obtener una buena explicación de qué hacer en ese caso.

Consulte sus informes de crédito para ver si ha habido alguna actividad inusual.

Cada año, tiene derecho a recibir un informe crediticio gratuito de cada una de las tres agencias de informes.

Para solicitar fácilmente estos informes anuales gratuitos, haga lo siguiente:

1. Acceda a http://www.annualcreditreport.com/.

2. Haga clic en el botón **Solicite sus informes de crédito gratuitos**.

3. Siga las instrucciones en pantalla.

Recuerde solicitar informes de las tres agencias de crédito: Equifax, Experian, y TransUnion.

4. Después de recibir los informes, revíselos para ver si hay entradas inusuales o desconocidas. Si es así, eso podría ser un indicador de que sus cuentas ya han sido comprometidas.

Tenga en cuenta que, si bien esta es una verificación realmente buena, solo puede solicitar estos informes de forma gratuita una vez al año. Eso no es suficiente para seguir el ritmo de los ciberdelincuentes.

Coloque alertas de fraude en sus informes de crédito para recibir alertas si alguien accede a ellos.

No voy a dedicar mucho tiempo a esta sección. Aunque las alertas son buenas (y gratuitas), y hasta que esta última infracción podría haber sido todo lo que necesitaba hacer, con la infracción masiva de la semana pasada, congelar los informes es la acción recomendada actualmente.

Sin embargo, si aún desea colocar las alertas, los pasos son similares a congelar. (Los detalles sobre las congelaciones estarán en la siguiente sección). En resumen, se comunicaría con cada agencia de crédito y solicitaría una alerta de fraude.

Aquí encontrará información de contacto para colocar alertas de fraude en sus informes de crédito:

- Equifax-https://www.equifax.com/, 800-525-6285
- Experian: https://www.experian.com/, 888-397-3742
- TransUnion: https://www.transunion.com/, 800-680-7289

Tenga en cuenta que cada una de las agencias de crédito también tiene muchos servicios pagos y probablemente habrá muchos anuncios sobre ellos, pero puede omitir esos anuncios si lo único que desea son alertas o congelaciones.

Congele sus informes de crédito para que nadie más pueda acceder a ellos.

Esta es la acción recomendada ahora. Si bien puede ocasionar pasos adicionales si abre una nueva tarjeta de crédito o cuenta bancaria, establece una nueva hipoteca o préstamo para automóvil, o realiza otras transacciones financieras, ese inconveniente es extremadamente menor en comparación con lo que podría tener que hacer si alguien roba su crédito y arruina todo lo que quizás ya haya trabajado duro para obtener.

Básicamente, cuando congela su crédito, eso significa que nadie puede realizar una verificación de crédito sobre usted; las agencias de crédito rechazarán la solicitud y, por lo tanto, se rechazará su solicitud de nuevo crédito. Sin embargo, puede planificar con anticipación y descongelar temporalmente su crédito (solo por el tiempo suficiente para que se procese la verificación de crédito) y luego restablecer el congelamiento. El proceso de congelar/descongelar/volver a congelar es simple; sin embargo, causa pasos adicionales e inconvenientes de su parte. Sin embargo, como se indicó anteriormente, es un inconveniente mucho menor que si alguien comienza a hacerse pasar por usted y abre crédito a su nombre, ¡y acumula facturas altísimas!

Estos son los pasos básicos para congelar su crédito. Tenga en cuenta que sus pantallas pueden variar ligeramente según cómo acceda a ellas.

Tenga en cuenta que, como en muchas de las secciones anteriores, debe repetir el proceso para cada una de las tres agencias de crédito.

1. Acceda a los sitios web de los burós de crédito o comuníquese con ellos por teléfono. Aquí está la información de contacto:

• Equifax: https://www.equifax.com/personal/credit-report-services/credit-freeze/, 888-298-0045

• Experian: https://www.experian.com/freeze/center.html, 888-397-3742

• TransUnion: https://www.transunion.com/credit-freeze, 800-916-8800

2. Siga las instrucciones en la pantalla o en el teléfono.

En mi experiencia, tuve que configurar cuentas (con nombres de usuario y contraseñas) para cada buró de crédito. Algunos requirieron validación adicional (como autenticación de dos factores, donde enviaron códigos de confirmación a mi teléfono celular) y otros requirieron que respondiera una serie de preguntas de opción múltiple relacionadas con el crédito para demostrar mi identidad. Las preguntas relacionadas con el crédito pueden incluir cosas como:

• ¿Cuál de estos autos has tenido alguna vez?

• ¿En cuál de estas direcciones has vivido?

• En 1999, ¿dónde obtuvo un préstamo para automóvil?

• ¿Qué compañía hipotecaria utilizó para su primera vivienda?

• ¿Alguna vez ha tenido una tarjeta de crédito con alguna de estas compañías?

Y cosas similares.

Después de congelar su crédito, recibirá un aviso de confirmación, junto con instrucciones para descongelar su crédito, ya sea de forma permanente (no recomendado) o temporal (útil cuando solicita algún crédito nuevo).

Recuerde congelar no solo sus informes crediticios, sino también los de los demás miembros de su familia.

Agregue otras medidas de seguridad a sus registros financieros, si aún no lo ha hecho.

Esta sección describe varias otras acciones de seguridad que debe tomar, si aún no lo ha hecho. Nuevamente, algunos de ellos causarán algunos inconvenientes, pero esos inconvenientes son menores en comparación con las posibles consecuencias de no realizarlos.

1. Agregue autenticación de dos factores a todas sus cuentas médicas y financieras. Esto significa que cuando inicie sesión en una cuenta (como el sitio web de su banco, sus registros de MyChart, sus proveedores de tarjetas de crédito y similares), tendrá que hacer más que simplemente escribir su nombre y contraseña. Por lo general, después de escribir su nombre y contraseña, aparecerá una pantalla para confirmar aún más su identidad enviando un código al número de teléfono celular o dirección de correo electrónico que figura en sus registros. Cuando reciba este código, podrá escribirlo en la pantalla de inicio de sesión y luego continuar con sus transacciones. Este proceso agrega otra capa de seguridad a sus cuentas.

Tenga en cuenta que puede hacer esto con muchos tipos de cuentas. Los más importantes son financieros y médicos, pero normalmente, si una cuenta ofrece esta función, se recomienda continuar y configurarla.

2. Cambie periódicamente sus contraseñas y PIN de todas sus cuentas médicas y financieras. Recuerde utilizar contraseñas únicas y difíciles de adivinar, no utilizar palabras comunes ni contraseñas que se compartan con otras cuentas.

3. Si está disponible en su institución financiera (banco o cooperativa de crédito), puede configurar alertas que le notifiquen cuando ocurren tipos específicos de transacciones. Al configurar estas alertas, puede monitorear más fácilmente la actividad para asegurarse de que no ocurra nada inusual o no autorizado.

4. Revise periódicamente su información de contacto en sus instituciones financieras, proveedores médicos y proveedores de crédito para asegurarse de que todo esté correcto.

5. Tenga cuidado con las estafas, el phishing y otros intentos de obtener información personal que puedan llegar por correo electrónico, mensaje de texto o teléfono.

Si ya ha ocurrido un robo de identidad, comuníquese con su institución financiera, sus acreedores y la policía.

Las secciones anteriores han hablado sobre cómo prevenir el robo de identidad, centrándose en congelar sus informes crediticios. Sin embargo, si ya ha sufrido un robo de identidad, asegúrese de hacer lo siguiente de inmediato:

• Notifique a su(s) institución(es) financiera(s).

• Notifique a todos sus acreedores.

• Notificar a la policía.

Para obtener una buena lista de verificación, consulte https://www.wellsfargo.com/assets/pdf/personal/privacy-security/fraud/identity-theft-kit.pdf. Aunque está dirigido principalmente a los clientes de Wells Fargo, todavía hay mucha buena información general en sus consejos.

Otros recursos

• Información sobre otras grandes violaciones de datos en 2024: https://www.komando.com/news/security/biggest-data-breaches-of-2024-so-far/

• Información adicional sobre la violación de datos de NPD: https://ktla.com/news/data-breach-may-have-exposed-private-info-of-billions-of-people-lawsuit-says/

• Recursos de la Comisión Federal de Comercio relacionados con el robo de identidad: https://www.ftc.gov/news-events/topics/identity-theft

• Guía de Wells Fargo para detectar estafas comunes: https://www.wellsfargo.com/privacy-security/fraud/bank-scams/

Conclusión

Espero que estas pautas y recursos sean útiles para proteger el crédito y la identidad que tanto le costó ganar y los de los miembros de su familia. Recuerde el viejo dicho, "más vale prevenir que curar".

Escrito por Diana Nelson Haase, 19 agosto 2024