Cómo recuperarse de la exposición de contraseñas

Son muchas las formas en las que tu contraseña puede quedar expuesta a terceros no autorizados:

1. Es frecuente que, por comodidad, las contraseñas se "guarden" a la vista en documentos electrónicos o impresos. Si alguien roba el documento impreso o se pierde, o si alguien accede al documento electrónico, tu contraseña quedará expuesta.
2. Los ataques de phishing tratan de convencerte de que facilites tu contraseña voluntariamente en un sitio web que se hace con ella para ponerla a la venta o usarla. Si no detectas el ataque, tu contraseña quedará expuesta.
3. Tú, tu empleador o cualquier organización con la que interactúes digitalmente puede sufrir una vulneración.
4. Las tecnologías relacionadas con contraseñas, como los exploradores que recuerdan contraseñas, las extensiones de exploradores, los gestores de contraseñas o incluso los Llaveros de Apple pueden sufrir una vulneración.

Lo más probable es que descubras vulneraciones que pueden afectarte a través de medios de difusión digitales y tradicionales o directamente procedentes de la organización que es víctima de la vulneración, si está obligada a avisarte. También puedes adquirir algún servicio de supervisión de la web oscura para recibir avisos. Algunas herramientas y servicios gratuitos permiten que hagas comprobaciones personalmente o pueden avisarte de manera proactiva de que la vulneración te ha afectado; por ejemplo:

- ';--have i been pwned? permite buscar información sobre un gran número de vulneraciones para averiguar si tu dirección de correo electrónico está afectada.
- Apple puede enviar notificaciones a teléfonos iPhone (consulta la función Detectar contraseñas en peligro) y a usuarios del explorador Safari.
- Google puede enviar avisos a usuarios de Chrome y proporciona una herramienta de Revisión de contraseñas como recurso de seguimiento.

En este blog nos centramos en las vulneraciones que pueden ocurrir cuando una herramienta de gestión de contraseñas sufre un incidente de seguridad que expone datos de contraseñas de usuarios.

En agosto de 2022, LastPass, una popular herramienta de gestión de contraseñas, sufrió una vulneración de seguridad. Aunque la empresa garantiza a los usuarios que los gestores de contraseñas cifradas siguen siendo seguros, robaron parte del código fuente y la información técnica. Este incidente desató la preocupación de muchos usuarios, que empezaron a cuestionarse la seguridad de la plataforma.

Si utilizas una herramienta de gestión de contraseñas y estás planteándote cambiarla, esto es lo que necesitas saber:

Explicación de la vulneración

LastPass reconoce que la información robada en el primer incidente permitió a los atacantes acceder a volúmenes de datos almacenados que consideraban protegidos de forma adecuada, aumentando el riesgo de que cualquier contraseña asociada se viera en peligro. Aunque trataron de asegurar a los clientes que no se había accedido directamente a los datos de los usuarios, la vulneración resalta la importancia de proteger las contraseñas de la forma más segura posible.

Es interesante que comprendas la naturaleza de cualquier vulneración de tus términos. No dudes en contactar a tu proveedor actual a través de sus canales de atención al cliente para que te aclare cualquier duda que puedas tener.

Así que, ¿cuál debería ser el siguiente paso?

1. **Evaluar tus necesidades y tu tolerancia al riesgo:** busca gestores de contraseñas alternativos. Algunas de las opciones más populares son 1Password, Bitwarden o Dashlane, entre otras. Ten en cuenta características como la compatibilidad con múltiples dispositivos, las medidas de seguridad, la compatibilidad con la autenticación de doble factor o de múltiples factores, los procedimientos de recuperación de cuentas y la facilidad de uso. Y lo que es más importante, evalúa tu tolerancia al riesgo en diferentes tipos de cuentas.

   Ten en cuenta que estos solo son ejemplos; conviene evaluar los riesgos personalmente según las propias necesidades y tolerancia:

   - **Riesgo bajo:** las cuentas de redes sociales y los sitios de compras que no sueles usar y en los que no guardas datos de pago.
   - **Riesgo medio:** las direcciones de correo electrónico independientes que no se utilizan para inicio de sesión único o para gestionar servicios de alto riesgo.
   - **Riesgo alto:** cuentas bancarias, aplicaciones financieras, portales sanitarios, almacenamiento en la nube y otras cuentas que interactúen con tu vida financiera.
   - **Riesgo extremo:** cuentas usadas como apoyo de servicios de inicio de sesión único populares como tu Apple ID, Microsoft ID o Cuenta de Google.

2. **Priorizar según el riesgo:** prioriza acciones en tus cuentas críticas en función de tu evaluación de riesgos.

Enfoques de seguridad basados en el riesgo

- **Esencial (tanto si te vas a cambiar a una nueva herramienta como si no):**
  - Utiliza una contraseña segura para tu gestor de contraseñas y cámbiala con frecuencia.
  - Habilita el método de autenticación de múltiples factores más seguro posible para la herramienta en sí:
    - Entre los métodos menos seguros están el correo electrónico, los SMS o la verificación mediante llamada telefónica.
    - Los métodos más seguros incluyen el uso de aplicaciones o dispositivos de autenticación biométrica o de códigos de un solo uso, como Google Authenticator o Microsoft Authenticator.
    - Los métodos más seguros disponibles incluyen claves de acceso (passkeys) y certificados.
  - Si es posible, asegúrate de tener el control sobre las claves de cifrado.
  - Elimina todas las cookies y contraseñas de tu explorador.
- **Bueno:**
  - si vas a migrar a una nueva herramienta, sigue las instrucciones proporcionadas.
  - Utiliza la herramienta correspondiente para cambiar las contraseñas de tus cuentas.
  - Dado el caso, elimina cualquier archivo utilizado para exportar las contraseñas antiguas de tu herramienta de gestión de contraseñas anterior.
- **Mejor:**
  - Este enfoque añade una capa extra de seguridad.
  - si vas a migrar a una nueva herramienta, sigue las instrucciones proporcionadas.
  - Plantéate cambiar el ID de usuario o la dirección de correo electrónico asociada después de usar la herramienta correspondiente para crear contraseñas seguras para todas las cuentas de riesgo ALTO o EXTREMO.
  - Dado el caso, elimina cualquier archivo utilizado para exportar las contraseñas antiguas de tu herramienta de gestión de contraseñas anterior.
  - Platéate crear varios perfiles de explorador que no tengan plugins ni extensiones (excepto las necesarias para tu gestor de contraseñas) para poder utilizarlos como contenedores para el uso directo de tus cuentas de riesgo EXTREMO.
- **Óptimo:**
  - Este enfoque es más seguro, pero requiere una inversión de tiempo considerable.
  - si vas a migrar a una nueva herramienta, sigue las instrucciones proporcionadas.
  - En este caso deberías cambiar la contraseña de todas tus cuentas (independientemente del riesgo) utilizando la nueva herramienta, y modificar el ID de usuario y la dirección de correo electrónico asociados a CADA una de tus cuentas de riesgo ALTO y EXTREMO para que sean únicos.
  - Este enfoque crea credenciales de inicio de sesión aparte para tus cuentas más críticas, minimizando el impacto de una vulneración sobre cualquiera de ellas.

- El inconveniente de este enfoque es que es posible que no puedas utilizar servicios de inicio de sesión único de uso común para tus cuentas de máximo riesgo.
- Dado el caso, elimina cualquier archivo utilizado para exportar las contraseñas antiguas de tu herramienta de gestión de contraseñas anterior.
- Plantéate crear varios perfiles de explorador que no tengan plugins ni extensiones (excepto las necesarias para tu gestor de contraseñas) para poder utilizarlos como contenedores para el uso directo de tus cuentas de riesgo ALTO y EXTREMO.

Recuerda:

- Ten cuidado con los intentos de phishing.
- Nunca guardes tus contraseñas como texto sin cifrar ni en formato electrónico ni impreso.
- Elige contraseñas seguras y únicas para todas tus cuentas. Un gestor de contraseñas puede ayudarte a generar y guardar contraseñas de forma segura.
- Habilita el método de autenticación de múltiples factores más seguro disponible en todas partes.
- Y no te olvides de otros datos sensibles que puedas tener guardados en un gestor de contraseñas, como información financiera, de recuperación de cuentas o incluso datos de billeteras de criptomonedas. Si bien no hablamos de ello directamente en esta publicación de blog, tienes que realizar un análisis de riesgos para determinar qué medidas de recuperación conviene adoptar. Entre las acciones que debes plantearte, conviene incluir el cambio de los números de las cuentas financieras o de las tarjetas de crédito/débito, o la migración a una nueva billetera de criptomonedas.

La vulneración mencionada sirve como recordatorio de lo importante que es la vigilancia en ciberseguridad. Mediante la evaluación de tus necesidades y tu tolerancia al riesgo y su correcto tratamiento, puedes asegurarte de que tus cuentas en línea estén bien protegidas incluso contra los delincuentes más hábiles y decididos.