Contraseñas:
Aumente su seguridad

Aunque casi todo el mundo ha oído hablar de los aspectos básicos de la seguridad de las contraseñas (utilizar una contraseña segura, no utilizar la misma contraseña en distintos sitios, etc.), muchos de nosotros hacemos caso omiso de esos consejos porque nos parecen demasiado complicados, o simplemente porque no tenemos tiempo. Sin embargo, las contraseñas son una parte importante de la seguridad en el trabajo y en nuestra vida personal y además, sirven como primera línea de defensa para proteger nuestra información y datos delicados. La gran mayoría de los incidentes de piratería informática y filtraciones de datos se deben a contraseñas débiles o robadas (en inglés). A continuación le ofrecemos algunos consejos clave para aumentar la seguridad de sus contraseñas.

Antes de empezar: Priorice la seguridad

Es importante reconocer que para muchas personas sobrevivientes, utilizar contraseñas seguras no es suficiente y actualizarlas incluso puede ser peligroso. Si una persona agresora vigila regularmente los dispositivos y las cuentas, puede saber que se ha cambiado una contraseña y ella puede tener la capacidad para cambiarla. Además, las personas agresoras pueden coaccionar u obligar a las personas sobrevivientes a compartir sus contraseñas.

No hay una forma "correcta" de responder a un incidente, solamente hay maneras que se ajustan o no a su situación. Lo que funciona para otra persona puede no funcionar o no ser seguro para usted. Siempre dé prioridad a la seguridad y confíe en sus instintos. Hacer cambios suele alertar a la otra persona. Puede que le obligue a desbloquear su teléfono o a compartir sus contraseñas. La persona puede volverse más agresiva. En algunas situaciones, hacer cambios también podría borrar algo que podría

usarse como evidencia. Estas medidas de seguridad podrían resultarle útiles:

- Utilice un dispositivo más seguro. Si cree que alguien está vigilando su teléfono o sus cuentas, utilice un dispositivo diferente (tal como una computadora de la biblioteca o el teléfono de una amistad) y una cuenta a la que esa persona no tenga acceso (y a la que tampoco haya tenido acceso en el pasado).
- Obtenga más información. Enfrentarse a la violencia, los malos tratos y el acoso puede ser difícil y peligroso. Las personas intercesoras pueden ayudarle a encontrar opciones y recursos locales y a crear un plan para su seguridad. Puede ponerse en contacto al teléfono de ayuda nacional para que le remitan a recursos locales.

¿Qué es lo que hace que una contraseña sea segura?

Concéntrese en la longitud. Las mejores contraseñas tienen al menos entre 12 y 15 caracteres y pueden contener letras, números y símbolos. Puede parecer mucho, pero recuerde: lo importante es la longitud. *Siempre y cuando la contraseña sea lo suficientemente larga*, las letras minúsculas son útiles mezclándolas con números y símbolos. Puede simplificarla creando una frase corta que le resulte fácil de recordar, como veranoesmiestaciónfavorita. Asegúrese de no utilizar frases que otros puedan adivinar o predecir. Para reforzar la contraseña aún más o si un sitio web lo requiere, puede agregar números y símbolos: Veran0e$miestacionfavorita.

Cambie la contraseña. Utilice contraseñas distintas para las cuentas que contengan información delicada o que le identifiquen personalmente. Nunca se insistirá lo suficiente en la importancia de este consejo. Si usted usa la misma contraseña para todas estas cuentas, una vez que una de ellas

haya sido descifrada, TODAS sus cuentas serán vulnerables. Del mismo modo que usted usa llaves distintas para proteger lugares distintos, debe usar contraseñas distintas para proteger cuentas importantes.

Gestores de contraseñas

Los gestores de contraseñas recuerdan sus contraseñas de forma segura para que usted no tenga que hacerlo. La mayoría de nosotros evitamos utilizar contraseñas distintas para cuentas diferentes porque es demasiado difícil recordarlas todas, y sabemos que escribirlas no es seguro. Por suerte, los gestores de contraseñas, que son herramientas que almacenan y protegen las contraseñas, como los bancos almacenan y protegen el dinero, pueden ayudarle. Estas herramientas también pueden crear contraseñas increíblemente difíciles de descifrar. Todas sus contraseñas (tanto si las ha creado usted como si lo ha hecho el gestor de contraseñas por usted) se guardan en una caja fuerte encriptada, que sólo puede abrirse con una contraseña principal. La contraseña principal debe ser la más larga y única que usted haya creado y el gestor de contraseñas no debe almacenarla.

Si está considerando esta opción, hay algunos factores que debe tener en cuenta a la hora de elegir un gestor de contraseñas. Dos cosas iniciales importantes que hay que averiguar son:

- ¿La compañía puede ver sus contraseñas almacenadas?
- ¿La compañía ve o almacena su contraseña maestra?

Las opciones más seguras serán las que respondan con un **no** a estas dos preguntas.

He aquí otros factores para tener en cuenta:

Clave comparada o contraseña

En lugar de, o además de, una contraseña principal, algunos gestores de contraseñas -y algunos sitios web- ofrecen la opción de utilizar una clave de autenticación sin contraseña, a menudo denominada (dependiendo de la empresa) Passkey (Clave de acceso) o Secret Key (Clave Secreta) (en inglés). Una clave es una información almacenada en el propio dispositivo que indica a un sitio web o a una aplicación que ese dispositivo tiene permiso para acceder a información protegida. No se sube a Internet, por lo que si roban los datos de la empresa gestora de contraseñas, o alguien obtiene su contraseña por algún otro medio, el ladrón seguirá sin poder leer su información. Esto puede hacer que una clave sin contraseña sea una opción útil para las personas que controlan sus propios dispositivos. Las claves de acceso, que son un tipo específico de clave sin contraseña que cumple ciertas normas, se tratan con más detalle en la sección Autenticación multifactorial de este recurso.

Gestores de contraseñas para otras cuentas

Algunos navegadores (como Firefox) y cuentas que se utilizan para otros fines (como Google) tienen la opción de utilizar gestores de contraseñas integrados. Aunque pueden resultar prácticos, también conllevan el riesgo de que alguien que acceda a su cuenta pueda robar sus contraseñas, ya que la seguridad de las contraseñas sólo es tan buena como la seguridad de su cuenta de Google, de Microsoft, de Firefox o de cualquier otra opción integrada que utilice. Por este motivo, suele ser más seguro utilizar un gestor de contraseñas independiente que sólo sea un gestor de contraseñas, como 1Password o LastPass.

Autenticación multifactorial

Utilice la autenticación de dos factores o multifactorial. Esto significa que en lugar de introducir sólo una contraseña para acceder a su cuenta, tendrá que introducir también un segundo dato. Suele encontrar esta opción en la

configuración de la cuenta o en la configuración de seguridad del servicio en línea.

Hay una gran variedad de opciones para la autenticación multifactorial o de dos factores, y se dividen en dos categorías distintas: "algo que tengo" o "algo que soy". Actualmente, la mayoría de los servicios utilizan el tipo "algo que tengo". Funciona así: tras introducir su contraseña, la empresa le envía inmediatamente un código corto a algo que tiene: una cuenta de correo electrónico, un mensaje de texto o una llamada de voz a su teléfono, o una app que tenga instalada en su dispositivo. A continuación, introduce ese código en el sitio web y, ¡voilá! - ya puede acceder a su cuenta. Se confirma que usted es quien dice ser, porque ha verificado que tiene la cuenta de correo electrónico, el teléfono móvil, etc. que previamente usted había conectado o vinculado a esa cuenta.

Como ocurre con tantas otras cuestiones relacionadas con la privacidad digital y la ciberseguridad, no hay una única respuesta que sea la "mejor"; ¡depende del tipo de riesgos que más le preocupen a usted!

Autenticación de hardware

Para las personas a las que les preocupa que sus dispositivos estén vigilados o en peligro y, por tanto, no están seguras de introducir "algo que tengo" en sus dispositivos que podría llegar a manos de una persona agresora, una opción interesante es un autenticador de hardware, como una YubiKey (en inglés), un pequeño objeto que puede conectar a un dispositivo como prueba de que usted es quien dice ser. Puede responder a un cuestionario (en inglés) para determinar qué tipo funcionaría mejor para usted.

Este puede ser un método excelente para proteger sus cuentas y dispositivos que no requiere utilizar información que ya está en sus

dispositivos. Sin embargo, si le preocupa no poder evitar que una persona agresora descubra el autenticador de hardware y se lo quite, puede que esta no sea la opción adecuada para usted.

Autenticación biométrica

Cada vez más plataformas tienen la opción de utilizar la forma de autenticación "algo que soy": una huella dactilar o su cara, por ejemplo. Tradicionalmente, estos métodos de autenticación se han considerado "más seguros" que los de "algo que tengo". Sin embargo, hasta ahora, las autoridades no tienen las mismas restricciones para forzar el acceso a través de la biometría (en inglés) que para forzar el acceso a través de contraseñas. Y a diferencia de lo que ocurre con las contraseñas, si los datos de "algo que soy" se ven comprometidos, no es fácil cambiarlos.

Claves de acceso

Una clave de acceso o passkey (en inglés) es un tipo de clave de autenticación sin contraseña, de la que ya hablamos brevemente en la sección de gestores de contraseñas. Las passkeys son un proyecto conjunto de Google, Apple y Microsoft para reducir la necesidad de contraseñas, y cumplen ciertos estándares de diseño. Las Passkeys se almacenan en sus dispositivos -nunca tiene que recordarlas y los operadores de sitios web o aplicaciones nunca las ven- y usted la utiliza en combinación con el método de seguridad de su dispositivo (por ejemplo, biometría como FaceID o TouchID, una contraseña, un PIN) para iniciar sesión en aplicaciones, sitios web y otros servicios que las admitan.

Las claves de acceso o passkeys pueden ser una gran opción para aumentar la privacidad y la seguridad de muchas personas, incluidas muchas personas sobrevivientes. Sin embargo, *si* una persona agresora tiene acceso físico a uno de sus dispositivos y tiene la capacidad de iniciar sesión en ese

dispositivo – por ejemplo, porque conoce la contraseña de inicio de sesión de su computadora portátil o podría coaccionarle u obligarle a abrir el dispositivo con la huella del pulgar o la cara – esta puede no ser la opción adecuada para usted, ya que podría llevar a la persona agresora a acceder no solo a ese dispositivo, sino también a otros dispositivos de la misma empresa que usted posea, (por ejemplo, otros dispositivos Apple).

Inicio de sesión único

Muchos sitios web le ofrecen la posibilidad de utilizar sus credenciales de redes sociales o de correo electrónico para iniciar sesión en su sitio web o crear una cuenta (como utilizar su cuenta de Facebook o Google para crear una cuenta o iniciar sesión en LinkedIn, TikTok, un sitio de compras, etc.). Esto se llama inicio de sesión único y usted debería tener cuidado con ello.

Aunque puede ser útil porque significa una cuenta menos para la que tiene que recordar un nombre de usuario y una contraseña, su uso conlleva una serie de posibles riesgos. Si decide hacerlo, es probable que esté dando a Facebook, Google, etc. acceso a más información sobre usted de la que ya tienen, y además, estaría compartiendo información de su cuenta de redes sociales con el nuevo sitio o servicio.

Un último riesgo para tener en cuenta es que si su cuenta de redes sociales o de correo electrónico se ve comprometida ya sea por un pirata informático o por una persona agresora, significa que las otras cuentas para las que ha utilizado esas credenciales de inicio de sesión también están comprometidas.

La manera en la que alguna persona puede conocer sus contraseñas y cuándo cambiarlas

Hay varias formas de que alguien pueda conocer sus contraseñas:

- Pueden aparecer en *filtraciones de datos*, en las que alguien copia o roba información, como la base de datos de nombres de usuario y contraseñas de un sitio web. Puede verificar en qué filtraciones ha aparecido una dirección de correo electrónico o un número de teléfono concretos en HaveIBeenPwned (en inglés), que puede ayudarle a averiguar qué contraseñas necesitas cambiar.
- Es posible que un miembro de la familia o una pareja sentimental o sexual actual o anterior las conozca, ya sea por haberlas compartido con consentimiento, por haberlas vigilado sin consentimiento o por haberlas adivinado (si se trata de una contraseña fácil). El taller de Cornell llamado Clinic to End Tech Abuse tiene una guía útil para "desconectarse" de una expareja (en inglés) (o familiar) en la que, entre otros muchos temas, se abordan las contraseñas.
- Puede que alguien le haya engañado para que le dé una o varias de sus contraseñas. Muchos piratas informáticos utilizan estrategias para engañar a la gente y conseguir que les facilite sus contraseñas (*ingeniería social*). Una forma habitual de hacerlo es llamando por teléfono y haciéndose pasar por un representante de algún lugar del que usted sea cliente y convenciéndole de que les proporcione información privada. Otra forma es enviar un correo electrónico simulando ser de un sitio web, servicio, amigo o colega, y dándole un enlace a un sitio web para que lo siga (*phishing*). Cuando usted hace clic en ese enlace, le dirigen a un sitio web falso en el que le piden información privada, o el enlace lanza malware a su computadora.

Si usted cree que alguien conoce su contraseña, cámbiela desde un dispositivo que no esté vigilado por esa persona para evitar que siga accediendo a su cuenta, por ejemplo, use una computadora de la biblioteca. Pero si su cuenta no se ha visto comprometida y ha creado una contraseña segura siguiendo las pautas anteriores, no es necesario que la cambie a menudo. Si una persona agresora intenta coaccionarle para que

comparta sus contraseñas o le amenaza, puede solicitar ayuda y apoyo a una persona de confianza o a una persona intercesora.

Otros consejos sobre seguridad de contraseñas

- Utilice la estrategia para crear sus preguntas y respuestas secretas. Alguien que le conozca (o alguien que sepa buscar en Google) podrá adivinar a qué instituto asistió o cuál es su color favorito. No hay ninguna norma que le obligue a ser sincero cuando responda a esas preguntas secretas, así que invente cosas que recordará pero que nadie más pueda adivinar.
- Puede crear una cuenta de correo electrónico distinta para iniciar sesión en cuentas en línea o hacer compras, y utilice la opción de pago invitado cuando sea posible. Puede crear una cuenta de correo electrónico alternativa para las cuentas en línea y las compras, esto puede ayudarle a proteger su privacidad y dificultar que una persona agresora, acosadora u hostigadora descubra o ponga en peligro sus cuentas. También puede ayudarle a reducir el correo spam en su bandeja de entrada de correo electrónico real.
- Recuerde que debe desconectarse. A menos que cierre activamente la sesión de una cuenta o dispositivo, puede permanecer abierta indefinidamente, permitiendo a otros un fácil acceso. Aunque es cómodo no tener que iniciar sesión cada vez en nuestros propios dispositivos, es importante sopesar esa comodidad con el riesgo de lo que podría ocurrir si nuestro dispositivo cae en las manos equivocadas. Adquirir el hábito de cerrar sesión en nuestros propios dispositivos también hace que sea menos probable que permanezcamos conectados accidentalmente a nuestras cuentas en computadoras y dispositivos que no son nuestros.

  Si le preocupa haber iniciado sesión en una cuenta por error, algunos

servicios en línea como Facebook y Gmail (en inglés) le permiten ver los lugares en los que ha iniciado sesión y le dan la opción de cerrar la sesión de forma remota. Si utiliza una aplicación en un dispositivo inteligente que no le permite desconectarse, quizá deba plantearse eliminar la aplicación o la cuenta. Es una molestia adicional, pero sopesa la delicadeza de la información de esa cuenta y el riesgo de que otra persona tenga acceso a ella.

 Apoyado por US DOJ-OVW Subvención #15JOVW-21-GK-02216-MUMU. Las opiniones, resultados y conclusiones o recomendaciones expresadas son de los autores y no representan necesariamente los puntos de vista del Departamento de Justicia de los Estados Unidos. Actualizamos nuestros materiales con frecuencia. Visite TechSafety.org para obtener la última versión de este y otros materiales.