Contraseñas: 5 errores comunes que deberías evitar

Reutilizar contraseñas o el uso de contraseñas fáciles de adivinar son solo dos de los errores más comunes que podrías estar cometiendo a la hora de proteger tus cuentas.

Escribir una contraseña para acceder a una de las decenas de servicios que utilizamos se ha convertido en una parte tan cotidiana de nuestras vidas que rara vez pensamos en ello. A menudo procuramos que nuestras contraseñas sean simples y fáciles de recordar para poder pasar rápidamente por el proceso de iniciar sesión y continuar con lo que importa. Este es uno de los muchos errores que cometemos cuando se trata de algo en lo que confiamos para asegurar una parte de nuestra identidad digital.

Pero como hoy es el Día Mundial de la Contraseña, es una gran ocasión que ahora para pensar en los 5 errores más comunes que cometen los usuarios cuando se trata de contraseñas.

1. Reutilizar las contraseñas

Uno de los errores más frecuentes es, sin lugar a dudas, la reutilización de contraseñas (https://www.welivesecurity.com/la-es/2018/05/03/por-que-es-tan-riesgoso-reutilizar-tu-contrasena/). El problema a menudo comienza con la creación de la contraseña en sí. La mayoría de las veces las personas se preocupan por crear contraseñas que sean fáciles de recordar, lo que generalmente significa que son cortas y simples, aunque ahora la mayoría de los servicios tienen requisitos para ingresar una contraseña y exigen una longitud mínima y la inclusión de algunos caracteres que le aportan un poco más de complejidad.

Una vez que hayamos memorizado la contraseña y nos registremos en un nuevo servicio, y luego en otro, y otro, no queremos tener que recordar una contraseña para cada uno de estos servicios. Por eso, muchos usuarios deciden reutilizar la contraseña que han logrado guardar en su memoria. Según una encuesta realizada por Google (http://services.google.com/fh/files/blogs/google_security_infographic.p el 52% reutiliza la misma contraseña en varias de sus cuentas, mientras que un sorprendente 13% usa la misma contraseña para todas sus cuentas. Sustituir letras por números o minúsculas por mayúsculas y viceversa también se considera una reutilización de la contraseña, aunque algunos podrían opinar que es una ligera mejora.

El problema más grave con la reutilización de contraseñas es que los usuarios quedan expuestos a lo que se conoce como credential stuffing (https://www.welivesecurity.com/2019/04/10/credential-stuffing-attacks-login/). ¿Qué es esto? Se trata de un ataque que busca tomar el control de las cuentas de los usuarios y para ello utiliza bots que intentan iniciar sesión utilizando credenciales de acceso que fueron filtradas en brechas de datos antiguas que sufrieron otros sitios; hasta que logran dar con la combinación correcta de un nuevo sitio en el cual se utilizaron las mismas credenciales de acceso que se filtraron. Por lo tanto, diversificar las contraseñas es lo mejor.

2. Crear contraseñas simples

(https://www.welivesecurity.com/la-es/) (https://www.eset.com)

Como ya hemos mencionado, muchos de los problemas comienzan cuando se crean las contraseñas. Las contraseñas simples suelen ser las más utilizadas. Es posible que haya visto la película “Acusado sin razón” (en España titulada “¡Vaya un fugitivo!”), donde Leslie Nielsen intenta vulnerar una computadora adivinando las credenciales de inicio de sesión, que simplemente resultaron ser Inicio de sesión y Contraseña.

Si crees que en la vida real las personas son más cuidadosas con la elección de sus contraseñas, lamentablemente estarías equivocado. Todos los años se publica una lista de las peores contraseñas (https://www.welivesecurity.com/la-es/2019/12/17/peores-contrasenas-2019/) que demuestra que cuando se trata de contraseñas, las personas toman decisiones altamente cuestionables, con “12345” y “password” entre las cinco contraseñas más utilizadas.

Además de patrones simples y palabras obvias, un error frecuente que puede estar cometiendo al crear contraseñas es utilizar datos personales como parte de las estas, lo que las convierte en fáciles de adivinar o de encontrar. Seis de cada diez adultos en los Estados Unidos (https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf) han incorporado un nombre (el de ellos, el de su cónyuge, el de sus hijos o su mascota) o una fecha de cumpleaños a sus contraseñas.

Lo ideal es utilizar como contraseña una frase (https://www.welivesecurity.com/la-es/2016/05/06/crear-contrasena-fuerte-un-minuto/). El doble factor de autenticación

(https://www.welivesecurity.com/la-es/2019/05/21/doble-factor-autenticacion-solucion-seguridad-mas-efectiva/) (2FA, por sus siglas en inglés) también debe activarse cuando sea posible, ya que agrega una capa de seguridad adicional contra varios tipos de ataques que intentan revelar credenciales de inicio de sesión.

3. Almacenar las contraseñas en texto plano

Otro error frecuente es escribir nuestras contraseñas. Esto se presenta de dos formas: contraseñas anotadas en papel o notas adhesivas, o guardadas en hojas de cálculo o documentos de texto en nuestra computadora o teléfono. En el primero de los casos: a menos que el actor malicioso desee sumar a sus antecedentes el ingreso por la fuerza a un domicilio, no hay forma de que acceda a las mismas.

Quizás te interese: Cómo saber si la contraseña que utilizas fue filtrada en una brecha (https://www.welivesecurity.com/la-es/2019/02/01/como-saber-si-la-contrasena-que-utilizo-fue-filtrada-en-una-brecha/)

Eso no quiere decir que debas escribirlas en un papel o simplemente dejarlas a la vista. En todo caso las anotaciones deberían ser más bien pistas que ayuden a recordarlas, y deberían almacenarse en un lugar protegido de los ojos curiosos. En caso de almacenar las claves en alguno de sus dispositivos, estará expuesto a una serie de desafíos. Si un atacante obtiene acceso a su dispositivo y hurga en él, tendrá acceso, con poco o ningún esfuerzo, a una gran cantidad de datos confidenciales, incluidas las contraseñas almacenadas en texto plano.

Alternativamente, si su dispositivo se ve comprometido por un malware que copia sus datos y los envía a un servidor remoto, un actor malicioso podría acceder a todas sus cuentas antes de que tenga la oportunidad de darse cuenta. En algunos casos podrá incluso examinar al detalle su dispositivo para ver si pueden encontrar datos explotables en él, incluido el archivo que contiene las contraseñas. Por lo tanto, queda claro que almacenar contraseñas en texto plano en cualquier dispositivo conectado es una mala idea.

4. Compartir contraseñas

Si bien compartir es un acto de generosidad, no se recomienda hacerlo con las contraseñas. Aunque algunos no opinan lo mismo, como el 43% de los participantes de una encuesta en Estados Unidos que admitió haber compartido sus contraseñas con otra persona. Entre ellas contraseñas para servicios de streaming, cuentas de correo electrónico, cuentas de redes sociales e incluso para acceder a cuentas para realizar compras en línea. Más de la mitad de los encuestados dijo haber compartido su contraseña con sus seres queridos. Si bien compartir la contraseña para acceder a una cuenta de un servicio de streaming es un fenómeno generalizado, es menos peligroso que el resto de las opciones mencionadas.

Una vez que comparte su contraseña con otra persona, la seguridad de su cuenta queda endeble, ya que ha perdido su control. No puede estar seguro de cómo la otra persona manipulará la clave y si la compartirá con otra persona. Mucho depende de cómo compartió la contraseña: ¿la escribió en su cuenta y la guardó? ¿O tal vez la envió por correo electrónico o mediante una aplicación de mensajería instantánea en forma de texto sin formato? Si esta última opción fuera el caso, usted

está a merced de su discreción y debe esperar que sus dispositivos se mantengan protegidos, ya que en la sección anterior hemos discutido las implicaciones de guardar una contraseña en forma de texto sin formato.

(https://www.welivesecurity.com/la-es/)

Otra cosa que es importante recordar es que si compartió su contraseña en cualquier plataforma de comunicación que use, las personas con las que la compartió pueden causar estragos en sus relaciones, ya sea de negocios o personales, ya que ahora pueden iniciar sesión con su identidad. Si compartió las credenciales para cualquiera de las plataformas de compra en línea que utiliza y los métodos de pago están guardados, entonces la parte con la que compartió puede usar esta información para realizar una transacción. Incluso si la persona con la que comparte sus credenciales es su cónyuge, no es aconsejable mantener todos los huevos en una misma canasta.

5. Cambiar las contraseñas periódicamente (sin pensarlo demasiado)

Algunas organizaciones obligan a los usuarios a cambiar sus contraseñas cada dos o tres meses "por razones de seguridad". Pero, contrariamente a la creencia popular, cambiar su contraseña regularmente, sin evidencia de que su contraseña haya sido filtrada en una brecha, no hace que su cuenta sea más segura.

La profesora de ciencias de la computación de Carnegie Mellon, Lorrie Cranor, dice (https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes) que existen estudios que demuestran que cuando las personas se ven obligadas a cambiar sus contraseñas con frecuencia, no piensan

demasiado en ello. Además, investigadores de la Universidad de Carolina del Norte (http://people.scs.carleton.ca/~paulv/papers/expiration-authorcopy.pdf) (UNC) descubrieron que los usuarios se inclinarían hacia la creación de contraseñas que siguieran patrones predecibles que denominaron “transformaciones”. El profesor Cranor enumera algunos ejemplos de estas transformaciones: “por ejemplo, incrementar un número, sustituir una letra por un símbolo similar (por ejemplo, cambiar una S por $), agregar o eliminar un carácter especial (por ejemplo, pasar de tres signos de exclamación al final de una contraseña a dos), o cambiar el orden de los dígitos o caracteres especiales (por ejemplo, mover los números al principio en lugar del final)”. Luego añadió que escuchó de casos en los que los usuarios incluían el mes y, en algunas ocasiones, el año del cambio de contraseña como una solución fácil para recordar estos cambios frecuentes.

Esto hace que sea bastante fácil para los atacantes hacer su trabajo, ya que, como los investigadores de UNC demostraron, una vez que los cibercriminales conocen una contraseña pueden adivinar estas transformaciones con poco esfuerzo. También vale la pena señalar que una vez que los ciberdelincuentes obtienen acceso a su dispositivo, pueden instalar un keylogger que les permitirá realizar un seguimiento de sus contraseñas cada vez que las cambie. Por supuesto, si tiene una solución de seguridad instalada en su dispositivo, hay muchas más posibilidades de que el keylogger sea detectado y desactivado.

Conclusión

Crear una contraseña que cumpla con todas las condiciones mencionadas en este artículo puede parecer una tarea desalentadora, pero hay varias formas de hacerlo sin que se convierta en una tarea tan compleja. Como mencionamos anteriormente, crear una frase como

contraseña es preferible a una contraseña simple, y agregar una capa adicional de seguridad activando el doble factor de autenticación en cada servicio que esté disponible debería ser la norma. Si le resulta tedioso recordar todas las contraseñas únicas que ha creado, entonces un administrador de contraseñas podría ser la respuesta a sus necesidades: de esa manera, tendrá que recordar solo una contraseña, pero asegúrese de que sea una que siga las pautas que hemos mencionado en esta publicación.

Amer Owaida **(https://www.welivesecurity.com/la-es/author/aowaida/) 7 May 2020 - 11:30AM**

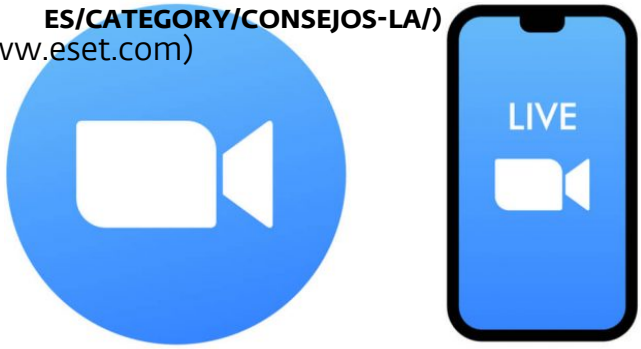
Newsletter

Correo electrónico... **Enviar**

Artículos similares

(ht /www.eset.com)
es/

CONSEJOS (HTTPS://WWW.WELIVESECURITY.COM/LA-ES/CATEGORY/CONSEJOS-LA/)



(https://www.welivesecurity.com/la-es/2020/05/07/que-hacer-contrasena-filtro-brecha-seguridad/)

Qué hacer si tu contraseña se filtró en una brecha de seguridad (https://www.welivesecurity.com/la-es/2020/05/07/que-hacer-contrasena-filtro-brecha-seguridad/)

(https://www.welivesecurity.com/la-es/2020/04/14/seguridad-zoom-como-configurarla-manera-correcta/)

Seguridad en Zoom: cómo configurarla de manera correcta (https://www.welivesecurity.com/la-es/2020/04/14/seguridad-zoom-como-configurarla-manera-correcta/)

Discusión

What do you think?

0 Responses

Upvote Funny Love Surprised Angry Sad

0 Comments WeLiveSecurity.com Disqus' Privacy Policy 1 Login

Recommend Tweet Share Sort by Best

Start the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

Be the first to comment.

Subscribe Add Disqus to your siteAdd DisqusAdd Do Not Sell My Data

welivesecurity™ BY eset®

(https://www.welivesecurity.com/la-es/) (https://www.eset.com)

Inicio (/la-es)

Acerca de (https://www.welivesecurity.com/la-es/acerca-de/)

Contáctanos (https://www.welivesecurity.com/la-es/contactanos/)

Investigaciones (https://www.welivesecurity.com/la-es/category/investigaciones/)

Tutoriales (https://www.welivesecurity.com/la-es/category/tutoriales/)

Mapa del Sitio (https://www.welivesecurity.com/la-es/mapa-del-sitio/)

Categorías (https://www.welivesecurity.com/la-es/categorias-2/)

(https://www.welivesecurity.com/la-es/) (https://www.eset.com)

Nuestros Expertos (https://www.welivesecurity.com/la-es/nuestros-expertos/)

RSS (https://www.welivesecurity.com/la-es/configurar-rss/)

ESET (https://eset.com)

Noticias (https://www.welivesecurity.com/la-es/news-widget-generator-la-es/)

Política de Privacidad (https://www.welivesecurity.com/la-es/politica-de-privacidad/)

Información Legal (https://www.welivesecurity.com/la-es/informacion-legal/)