SEGURIDAD INFORMÁTICA PERSONAL

**La necesidad de utilizar contraseñas seguras en nuestros sitios web**

*La mayoría sabe de qué se trata cuando se habla de contraseñas, pero es tan importante conocer cómo usarlas de forma correcta.*

**Por Julián M. Zappia.  
Diplomatic Week.**

Según datos de Unicef, la juventud es la mayor impulsora de la conectividad a nivel mundial. Un 75% de los jóvenes de entre 15 y 24 años tenían conexión a Internet en 2022, en comparación con el 65% del resto de la población mundial.

Ese organismo internacional señaló que los niños también pasan más tiempo en línea que nunca y están accediendo a edades cada vez más tempranas ya que, según sus estimaciones, a nivel global un niño se conecta a internet por primera vez cada medio segundo.

Y en ese contexto, el peligro de hackeo se ha multiplicado. Según los datos de registro de autenticación de Microsoft Azure Active Directory de 2022, se producen 921 ataques de contraseña cada segundo, casi el doble en frecuencia respecto de los 12 meses anteriores.

Google, que trabaja en forma constante para proteger la seguridad de sus usuarios, y estudia detalladamente este tema, asegura que las contraseñas complicadas tientan a los usuarios a usarlas para más de una cuenta, lo cual es un error.

Según un estudio realizado en Estados Unidos, el 66% de las personas admite que usa la misma clave en varios sitios, lo que hace que todas esas cuentas sean vulnerables si alguna falla.

Es fácil suponer que en los demás países ocurre algo similar.

Pero las personas comienzan a preocuparse cada vez más por mantener sus contraseñas a resguardo. En 2020, las búsquedas de “qué tan fuerte es mi contraseña” aumentaron en un 300%.

Aun así, según Google, desafortunadamente, incluso las contraseñas más seguras, pueden verse comprometidas y utilizadas por un atacante.

De acuerdo con datos de Google Trends, durante 2022 el término “administrador de contraseñas” se convirtió en tendencia en el buscador: creció un 150% en la Argentina, respecto al año anterior.

Google dio a conocer el año pasado los resultados de un estudio acerca de cómo los padres y las madres en Argentina perciben la seguridad online de sus hijos, y de qué manera se modificaron los hábitos de uso de Internet en los hogares durante 2021.

La buena noticia es que el 82% de ellos admite haber mantenido charlas con sus hijos para ayudarlos con temas vinculados a la seguridad online. Incluso, el 60% de los chicos han recurrido a sus padres para notificar o resolver este tipo de problemas.

Sin embargo, aún persiste la preocupación asociada al grooming (22%), seguido por el contenido inapropiado (15%) y el cyberbullying (14,8%), entre otros peligros.

**Cómo crear contraseñas seguras.**

Los siguientes son tips de los especialistas que resultan imprescindibles a la hora de generar y mantener las contraseñas seguras:

1- Usar al menos ocho caracteres y una combinación de letras (mayúsculas y minúsculas), números y símbolos.

2- Utilizar una contraseña diferente para cada una de las cuentas personales.

3- No es recomendable usar una contraseña que sea fácil de adivinar, como un apodo, el nombre de la escuela, el equipo de fútbol preferido, una secuencia de números (123456), etc. Y nunca emplear la palabra “contraseña”.

4- No usar información personal (nombre, dirección, número de teléfono, número de documento de identidad, fechas de nacimiento, etc.).

5- Es fundamental cambiar la contraseña de inmediato si se tiene conocimiento o se cree que alguien más, aparte de un adulto de confianza, la conoce.

6- Proteger la cuenta con la verificación en dos pasos. Esto es un sistema de protección que dota de una capa adicional de seguridad a las cuentas y ayuda a proteger la información personal. Además de la contraseña añade un segundo paso para verificar nuestra identidad.

**Cómo ver las contraseñas guardadas en Android.**

Conocer cómo proteger nuestras contraseñas es un paso en la formación de una cultura digital para todos y en la creación de estrategias de protección ante los posibles riesgos que pueden surgir en los entornos digitales

**Mitos y verdades sobre las contraseñas.**

Para conocer un poco más sobre la seguridad de las claves personales hay algunas creencias falsas que es bueno repasar y rebatir.

1- Se dice muchas veces que no es seguro colocar en una contraseña en un único lugar, pero ahora la tecnología aplicada en herramientas como Google Password Manager (Administrador de contraseñas de Google) son claves para proteger nuestra información, ya que utiliza varias capas de seguridad para proteger toda la información incluso de los ataques más persistentes. En cada una de las plataformas en las que está integrado (dispositivos Android y Chrome en Android, Chrome OS, iOS, Linux, MacOS y Windows), la autenticación en el espacio de almacenamiento está protegida al iniciar sesión, en tránsito y en reposo.

2- También suele pensarse que la función autocompletar no es segura, pero la misma herramienta mencionada en el punto anterior impulsa el uso de la función de “autocompletar contraseñas” en aplicaciones nativas de Android y en cualquier lugar en el que se utilice el navegador web Chrome (incluidas las aplicaciones iOS). A diferencia de una contraseña memorizada, en la que se puede engañar a un usuario para que inicie sesión en una página engañosa, Chrome y Android realizan una coincidencia exacta en el nombre de dominio y, por lo tanto, es mucho menos probable que nos engañen.

Incluso las contraseñas más seguras, pueden verse comprometidas y utilizadas por un atacante. De acuerdo con datos de Google Trends, durante 2022 el término “administrador de contraseñas” se convirtió en tendencia en el buscador (Getty)

**Un futuro sin contraseñas.**

El próximo gran salto en la autenticación en línea es la evolución de las contraseñas a las claves de acceso.

Con el respaldo de la criptografía de clave pública, estas claves de acceso son más seguras que las contraseñas (son como una contraseña de mil letras almacenada en un hardware seguro) y más cómodas, ya que pueden ser incluso más sencillas que el autocompletado, ya que basta con pasar el dedo por un dispositivo biométrico para iniciar sesión en cualquier dispositivo.

Hace un año Apple, Google y Microsoft anunciaron que, en un esfuerzo conjunto para hacer que la web sea más segura y útil para todos, están ampliando el soporte para un estándar común de inicio de sesión sin contraseña creado por FIDO Alliance y el Consorcio World Wide Web.

La nueva capacidad permitirá que los sitios web y las aplicaciones ofrezcan inicios de sesión sin contraseña que sean consistentes, seguros y fáciles en todos los dispositivos y plataformas.

Las claves de acceso son un reemplazo más seguro para las contraseñas y otros factores de autenticación.

No se pueden reutilizar, no se filtran en las infracciones del servidor y protegen a los usuarios de los ataques de phishing. Son claves que pueden funcionar en diferentes sistemas operativos y tanto en sitios web como con aplicaciones.

La idea de los desarrolladores es que las claves de paso se usen para iniciar sesión en sitios y aplicaciones que las admitan y deberán autenticarse igual que cuando se desbloquea un dispositivo, con huella dactilar, código o reconocimiento facial.

Google informó que con la última versión de Chrome ya se están habilitando claves de acceso en Windows 11, macOS y Android.

Pero aun cuando el avance de la tecnología es rápido, dejar atrás por completo el uso de contraseñas todavía llevará tiempo.

Por lo tanto, las passwords seguirán formando parte de nuestro día a día y, aunque los inicios de sesión tienden a simplificarse, la transición a un mundo sin contraseñas no será inmediata.