Google propone un futuro sin contraseñas: consejos para una navegación más segura

06/05/2022

En el **Día Mundial de la Contraseña, Google** cuenta cómo está trabajando para **lograr que sus productos no necesiten claves de acceso para ingresar** y, a su vez, acerca técnicas para realizar una revisión de seguridad en todas las cuentas y dispositivos.

De acuerdo a un **estudio realizado por Google** e **Ipsos** sobre los **hábitos en el uso de contraseñas**, casi el **20% de las personas todavía eligen palabras comunes** como **“Contraseña”**, o combinaciones simples como “**abc123”** y **“123456”**. En el **Día Mundial de la Contraseña**, que se celebra el **5 de mayo**, **Google** anuncia que se ha convertido en la primera empresa de plataformas de dispositivos en unirse a la **FIDO**

Alliance, un organismo de la industria de estándares abiertos formado para **resolver problemas de contraseñas y phishing.**

Durante el **próximo año**, las principales plataformas de dispositivos móviles se han comprometido a d**esarrollar soporte para los estándares de inicio de sesión sin contraseña de FIDO**, y **Google** planea implementarlo en **Android y Chrome**, facilitando los inicios de sesión entre dispositivos, **sitios web y aplicaciones sin importar la plataforma y sin la necesidad de ingresar una contraseña.**

¿Cómo funcionará el futuro sin contraseñas?
Cuando el usuario inicie sesión en un sitio web o aplicación en su teléfono, podrá hacerlo únicamente desbloqueandolo. Ninguna cuenta necesitará una contraseña de ingreso. En su lugar, el teléfono almacenará una credencial de **FIDO** llamada clave de acceso, que se utiliza para desbloquear cualquier cuenta online. La clave de acceso hace que iniciar sesión sea más seguro, ya que se basa en la criptografía de clave pública y sólo se muestra en la cuenta cuando se desbloquea el teléfono. Para iniciar sesión en un sitio web desde una computadora, sólo hará falta tener un teléfono cerca y desbloquearlo para acceder. **¿Qué ocurre si se perdiera el teléfono celular?** Las claves de acceso se sincronizarán de forma segura con el nuevo dispositivo desde la copia de seguridad en la nube.

“El soporte extendido de **FIDO** que estamos anunciando hoy hará posible que los sitios web implementen las experiencias de claves de acceso. Cuando este soporte esté disponible a lo largo de toda la industria en 2022 y 2023, dispondremos de Internet para un futuro sin contraseñas”, dijo **Sampath Srinivas, Director de Gestión de Producto, Autenticación Segura en Google.** Y agregó: “Mientras tanto, las contraseñas seguirán siendo parte de nuestras vidas, y **desde Google seguiremos dedicados a hacer que los inicios de sesión convencionales sean más seguros y fáciles** a través de nuestros productos existentes y la innovación continua”.

Uso de password. Foto: Google.

Consejos para una limpieza digital

Google acerca algunas recomendaciones para que las personas se mantengan seguras en línea a través de herramientas que les dan control y elección sobre sus privacidad. Como primer paso, la compañía sugiere realizar una verificación de seguridad rápida y proteger las cuentas de Google en el momento. Algunas otras recomendaciones son:

Utilizar la verificación en dos pasos (V2P): este método requiere una segunda forma de verificación para acceder a la cuenta además de la contraseña, que podría ser un código enviado directamente al teléfono, una clave de seguridad, etc. Si alguien que no es el propietario de la cuenta intenta acceder, necesitará, además de la contraseña, una segunda forma de verificación. Para configurar la verificación en dos pasos en la cuenta de Google, hay que ingresar a "Mi cuenta" en Google y hacer clic en «Verificación en dos pasos».

Administrador de contraseñas: protege automáticamente las contraseñas de los usuarios. Dentro del administrador, se encuentra disponible la Verificación de contraseña, una funcionalidad que, con un solo clic, indica si alguna de las contraseñas es débil, si la han usado en múltiples sitios o si descubre que ha estado expuesta (por ejemplo, por una filtración por parte de terceros). Más info sobre la Verificación de contraseña acá.

Revisión de contraseña (Security Checkup): es una función integrada al administrador de contraseñas que verifica la fortaleza y seguridad de todas las contraseñas guardadas, indica si han sido comprometidas y brinda recomendaciones personalizadas y útiles cuando es necesario. Ayuda a mantener la cuenta de Google segura al detectar y responder de manera proactiva a las amenazas de seguridad. Por ejemplo, restablece de manera automática la contraseña en la cuenta de Google si cree que ha estado expuesta en un robo de información. Más

info, aquí.

Copia de seguridad: en cualquier momento los usuarios pueden acceder a “Descargá tus datos” y hacer una copia de toda su información en Google. Incluso pueden hacer una copia de su información y, si lo prefieren, abandonar Google y usar sus datos con un servicio diferente.

Agregar computadoras o teléfonos móviles de confianza: Si el usuario no desea ingresar un código de verificación en dos pasos ni usar la Llave de seguridad cada vez que accede a su cuenta de Google, puede establecer su computadora o dispositivo móvil como de confianza. No es necesario ingresar un código de verificación cada vez que se quiera acceder a una computadora o dispositivo de confianza. Acá más información.

Recuperar la cuenta si el teléfono fue robado/extraviado: en caso de que ocurra esta situación, el usuario deberá salir de su cuenta en el dispositivo que ya no usa. Para recuperar la cuenta, deberá seguir los siguientes pasos: 1) Acceder a la Cuenta de Google, 2) presionar “No tengo mi teléfono” y 3) elegir una de las opciones disponibles y realizar los pasos que aparecen en pantalla. En caso de que no aparezca ninguna, lo recomendable es intentar acceder desde una computadora que se utilice con frecuencia. Más información en este enlace.

Cómo acceder a una cuenta en caso de que se solicite un código por mensaje de texto y no se cuente con un teléfono: siempre es importante tener un método de validación y que el mismo esté actualizado, pero en caso de no tenerlo, lo recomendable es ingresar al formulario de recuperación de cuentas. Facilita mucho la recuperación accediendo desde un equipo y ubicación con el que se suele conectar a dicha cuenta.

Fuente: Diario 26