El jueves, Google anunció que más de 400 millones de cuentas de Google están utilizando claves de acceso, autenticando a los usuarios en más de mil millones de ocasiones en los últimos dos años.

> Según un comunicado de Heather Adkins, vicepresidenta de ingeniería de seguridad en Google, *«Las claves de acceso son simples de utilizar y resistentes al phishing, ya que solo requieren una huella dactilar, un escaneo facial o un PIN, lo que las hace un 50% más rápidas que las contraseñas».*

El gigante de la búsqueda señala que las claves de acceso se están utilizando más frecuentemente para autenticar en las cuentas de Google que las formas tradicionales de autenticación de dos factores, como los códigos de un solo uso (OTPs) por SMS o basados en aplicaciones.

Además, la empresa anunció que está ampliando la Protección de Cuentas Cruzadas, que alerta sobre eventos sospechosos con aplicaciones y servicios de terceros conectados a la cuenta de Google de un usuario, para incluir más aplicaciones y servicios.

Se espera que Google también apoye el uso de claves de acceso para usuarios de alto riesgo como parte de su Programa de Protección Avanzada (APP), diseñado para proteger a personas de ataques dirigidos debido a su perfil y actividad. Esto incluye a trabajadores de campañas y candidatos, periodistas y activistas de derechos humanos, entre otros.

Anteriormente, el APP requería el uso de llaves de seguridad de hardware como segundo factor, pero ahora permitirá la inscripción con cualquier clave de acceso junto con las llaves de seguridad de hardware, o su uso como único medio de autenticación.

Google introdujo las claves de acceso en Chrome en diciembre de 2022 y desde entonces ha implementado la solución de autenticación sin contraseña en todas las cuentas de Google en todas las plataformas de forma predeterminada.

1Password, Amazon, Apple, Dashlane, Docusign, eBay, Kayak, Microsoft, PayPal, Shopify, Uber y WhatsApp son algunas de las otras empresas importantes que han adoptado claves de acceso.

Este desarrollo se produce el mismo día en que Microsoft, que integró claves de acceso en Windows 11 en septiembre de 2023, anunció sus planes para admitir el estándar de autenticación para cuentas de consumidores utilizando biometría o PIN de dispositivo en plataformas de Windows, Google y Apple.

Las claves de acceso funcionan mediante la creación de un par de claves criptográficas, una privada que se almacena en el dispositivo y una pública que se comparte con la aplicación o sitio web para la que se utilizará la clave de acceso.

> Vasu Jakkal de Microsoft explicó: *«Debido a que esta combinación única de claves solo funciona en el sitio web o aplicación para el que se creó, no es posible ser engañado para iniciar sesión en un sitio malicioso similar».*

Las claves de acceso también pueden ser almacenadas en soluciones de gestión de contraseñas de terceros, como 1Password y Dashlane, ofreciendo a los usuarios más control sobre su almacenamiento más allá de Google Password Manager, iCloud Keychain y Windows.

> Los gerentes de producto de Google, Sriram Karra y Christiaan Brand, destacaron que *«Las claves de acceso pueden actuar simultáneamente como primer y segundo factor de autenticación». «Al crear una clave de acceso en tu llave de seguridad, puedes evitar la entrada de tu contraseña. Esto reemplaza tu contraseña almacenada en la nube con el PIN que utilizaste para desbloquear tu llave de seguridad, mejorando así la seguridad del usuario».*

Sin embargo, algunos plantean preocupaciones de que las claves de acceso estén siendo utilizadas por las empresas para *«atrapar a los usuarios y audiencias en una plataforma»* y que *«los intereses corporativos estén primando sobre una buena experiencia de usuario».*

> William Brown, un ingeniero de software involucrado en el desarrollo de webauthn-rs, comentó: *«¿Qué mejor manera de fomentar el encarcelamiento a largo plazo de los usuarios que bloquear todas sus credenciales en tu plataforma, y aún mejor, credenciales que no se pueden extraer ni exportar de ninguna manera?».*