Versión con letra grande
Versión en audio
(Audio disponible únicamente en inglés)

Google

Llaves de acceso: Un gran paso hacia un futuro sin contraseñas

Debido al dramático aumento de ciberataques auspiciados por el estado y las personas malintencionadas en internet, ahora más que nunca nos concentramos en proteger a la gente, a los negocios y gobiernos: compartimos nuestra experiencia, empoderamos a la sociedad y trabajamos incesantemente para mejorar la tecnología de vanguardia de ciberseguridad con el fin de ayudar a crear un mundo más seguro para todos los usuarios.

Hoy en día las contraseñas son esenciales para la seguridad en internet, sin embargo, las amenazas, como los ataques de phishing continúan aumentando. Desde hace tiempo Google ha reconocido esos problemas y ha recomendado el uso de herramientas de autenticación como la verificación en 2 pasos (2SV), el Administrador de contraseñas de Google, las llaves de seguridad y ahora las llaves de acceso.

Desafío

Por más de 60 años se han utilizado las contraseñas en las computadoras, pero, en la actualidad, las contraseñas simplemente ya no son tan efectivas para mantener la seguridad de los datos de los usuarios y de las organizaciones. Los ataques de phishing cada vez son más frecuentes y sofisticados, ya que toman ventaja de la vulnerabilidad de la seguridad de las contraseñas. Por ejemplo:

- Más del 60% de las violaciones de la seguridad de los datos en 2021 implicaron el robo de credenciales o los ataques de phishing.[1]
- Las violaciones de la seguridad de los datos causadas por ataques de phishing conllevaron a una pérdida promedio de $4.91 millones para las organizaciones en el año 2022.[2]
- Los ataques de phishing aumentaron un 61% en 2022, con un alcance de 255 millones de personas en un período de seis meses.[3]

La verificación en 2 pasos/autenticación en 2 fases (2SV/2FA) ayuda, pero puede representar una inconveniencia y ser demandante para los usuarios y, aun así, no protegen por completo contra aquellos ataques de phishing y ataques dirigidos, como los “intercambios de tarjetas SIM” (SIM swapping) para realizar la verificación de tarjeta SMS.

Solución

Al asociarnos con FIDO Alliance, habilitamos la compatibilidad de las llaves de acceso, una alternativa más sencilla y segura a las contraseñas, que ofrece tecnología resistente a los ataques de phishing para millones de personas en todo el mundo. Con las llaves de acceso, no necesitarás contraseñas, lo que ofrecerá una experiencia más sencilla y segura de iniciar tus sesiones, ya sea a través de las huellas digitales, el escaneo facial o el bloqueo de pantalla.

Desde principios del año 2023, las llaves de acceso han estado disponibles para las cuentas personales de Google al igual que para los 9 millones de usuarios de Google Workspace, y también para sitios web de terceros y las aplicaciones en Chrome y Android.

La manera más sencilla y rápida de iniciar sesión

Las llaves de acceso son 4 veces más sencillas de usar, gracias a que no es necesario recordarlas ni ingresarlas. Simplemente utilizas tu huella digital, realizas un escaneo facial, o usas tu bloqueo de pantalla para iniciar sesión en todos tus dispositivos y plataformas.[4]

Seguridad de vanguardia para tus cuentas

Las llaves de acceso brindan una protección más robusta contra las amenazas cibernéticas como los ataques de phishing. Además, como están almacenadas en tu dispositivo personal, no es posible adivinarlas ni reutilizarlas, ayudándote a mantener segura tu información contra cualquier ataque.

Privacidad totalmente tuya

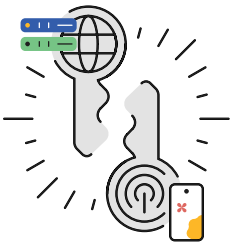
Tu llave de acceso se mantiene privada en tu dispositivo personal y jamás será compartida con Google ni con ningún socio externo. Simplemente utilizas tu huella digital, realizas un escaneo facial, o usas tu bloqueo de pantalla para verificar que eres tú quien está utilizando tu llave privada.

Más seguridad con Google

Versión con letra grande
Versión en audio
(Audio disponible únicamente en inglés)

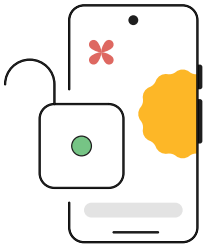
Google

En detalle

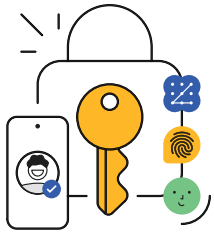


Las llaves de acceso se componen de dos partes: una llave pública en el servidor del sitio web al que ingresas y una llave privada correspondiente en tus dispositivos.

Cuando inicias sesión, el sitio web verifica que tu llave pública coincida con tu llave privada.



Para verificar que las llaves coinciden, simplemente se te pedirá que desbloquees tu dispositivo.



Al ingresar a tu cuenta, tu llave privada y datos biométricos permanecerán seguros en tu dispositivo y jamás serán compartidos.

Posibilitamos un ecosistema más seguro

Introdujimos las llaves de acceso a las empresas y los gobiernos

Las llaves de acceso brindan una seguridad significativa y numerosas ventajas de usabilidad para los usuarios. Y nos complace ser el primer proveedor importante de la nube pública en ofrecer dicha tecnología a nuestros clientes, desde pequeñas a grandes empresas hasta escuelas y gobiernos.

Una alianza a favor de una experiencia en internet más segura y sin contraseñas

Nos hemos asociado con diversas marcas para facilitar llaves de acceso en todas las plataformas de Chrome y Android, lo que proveerá inicios de sesión más sencillos y seguros para sus usuarios. Innumerables socios de todas las industrias, como el comercio electrónico, la tecnología financiera, el sector turístico y otros, ya se unieron a nosotros en esta nueva travesía sin contraseñas, tales como 1Password, Adobe, Dashlane, DocuSign, Kayak, Mercari, PayPal y Yahoo! Japón.

Nuestra travesía sin contraseñas

Las llaves de acceso definitivamente nos acercan a ese futuro sin contraseñas que hemos estado trazando durante más de una década.

2008 — Lanzamos el Administrador de contraseñas de Google para inicios de sesión más sencillas y seguras.

2011 — Posibilitamos la verificación en 2 pasos (2SV) para las cuentas de Google.

2012 — Presentamos la llave de seguridad resistente a los ataques de phishing para el personal de Google.

2013 — Nos unimos a FIDO Alliance con el fin de implementar normas abiertas para un mundo sin contraseñas.

2014 — Aumentamos la cantidad de llaves de seguridad resistentes a los ataques de phishing para todos los usuarios.

2017 — Presentamos el Programa de Protección Avanzada (APP) para los usuarios de alto riesgo.

2019 — Extendimos el soporte de FIDO en Android para brindar reautorización sin contraseñas en los sitios web.

2023 — Habilitamos las llaves de acceso para las cuentas de Google, los clientes de Google Workspace y los socios externos en Chrome y Android.

Aunque las contraseñas seguirán siendo parte de nuestra vida cotidiana hasta que completemos la transición a las llaves de acceso, estamos comprometidos a ayudar a los usuarios, y a otros en la industria, a que den este gran paso con el fin de lograr que los inicios de sesión sean más sencillos y seguros con Google.

Fuentes: 1 – Reporte de investigación de la violación de la seguridad de los datos de Verizon 2022 | 2 – Reporte de pérdidas por violación de la seguridad de los datos de IBM 2023 | 3 – Reporte cibernético de CNBC | 4 – Blog de seguridad de Google, mayo de 2023

Más seguridad con Google

Descubre cómo Google ayuda a mantener la seguridad en internet. Visita g.co/safety