Casi cinco meses después de que Google agregara soporte para claves de acceso a su navegador Chrome, la compañía comenzó a implementar la solución sin contraseña en las cuentas de Google en todas las plataformas.

Las claves de acceso, respaldadas por FIDO Alliance, son una forma más segura de iniciar sesión en aplicaciones y sitios web sin tener que utilizar una contraseña tradicional. Esto a su vez, se puede lograr simplemente desbloqueando la computadora o dispositivo móvil con los datos biométricos o un PIN local.

> *«Y, a diferencia de las contraseñas, las claves de acceso son resistentes a los ataques en línea como el phishing, lo que las hace más seguras qu cosas como los códigos SMS de un solo uso»,* dijo Google.

Las claves de acceso, una vez creadas, se almacenan de forma local en el dispositivo y no se comparten con ninguna otra parte. Esto también elimina la necesidad de configurar la autenticación de dos factores, ya que demuestra que *«tiene acceso a su dispositivo y no puede desbloquearlo».*

Los usuarios también tienen la opción de crear claves de acceso para cada dispositivo que usen para iniciar sesión en la cuenta de Google. Dicho esto, una clave de paso creada en el iPhone estará disponible en otros dispositivos si han iniciado sesión en la misma cuenta de iCloud.

Cabe mencionar que tanto el Administrador de contraseñas de Google como el Llavero de iCloud usan cifrado de extremo a extremo para mantener las claves de acceso privadas.

Además, los usuarios pueden iniciar sesión en un nuevo dispositivo o usar de forma temporal un dispositivo distinto seleccionando la opción *«usar una clave de paso de otro dispositivo»,* que después usa el bloqueo de pantalla y la proximidad del teléfono para aprobar un inicio de sesión único.

> *«Después, el dispositivo verifica que su teléfono está cerca mediante un pequeño mensaje anónimo de Bluetooth y establece una conexión cifrada de extremo a extremo con el teléfono a través de Internet»*, dijo la compañía.

> *«El teléfono usa esta conexión para entregar su firma de clave de acceso única, que requiere su aprobación y el paso biométrico o de bloqueo de pantalla en el teléfono. Ni la clave de acceso en sí ni la información de bloqueo de pantalla se envían al nuevo dispositivo».*

Aunque este puede ser el *«comienzo del fin de la contraseña*«, la compañía dijo que tiene la intención de seguir admitiendo los métodos de inicio de sesión existentes, como contraseñas y autenticación de dos factores, en el futuro previsible.

Google también recomienda que los usuarios no creen claves de acceso en dispositivos que se comparten con otros, una medida que podría socavar todas sus protecciones de seguridad.