Google anunció hoy sus planes para implementar soporte para inicios de sesión sin contraseña en Android y el navegador web Chrome, para permitir a los usuarios iniciar sesión sin problemas y de forma segura en distintos dispositivos y sitios web, independientemente de la plataforma.

> *«Esto simplificará los inicios de sesión en dispositivos, sitios web y aplicaciones sin importar la plataforma, sin la necesidad de una sola contraseña»,* dijo Google.

También se espera que Apple y Microsoft amplíen el soporte a los sistemas operativos iOS, macOS y Windows, así como a los navegadores web Safari y Edge.

El sistema común de inicio de sesión Fast IDentity Online (FIDO), elimina las contraseñas por completo y muestra un mensaje que le pide al usuario que desbloquee el teléfono cuando inicia sesión en un sitio web o una aplicación.

Esto es posible gracias al almacenamiento de una credencial FIDO protegida criptográficamente llamada clave de acceso en el teléfono que se utiliza para iniciar sesión en la cuenta en línea después de desbloquear el dispositivo.

> *«Una vez que haya hecho esto, no necesitará su teléfono nuevamente y podrá iniciar sesión simplemente desbloqueando su computadora»,* dijo Google.

> *«Incluso si pierde su teléfono, sus claves de acceso se sincronizarán de forma segura con su nuevo teléfono desde la copia de seguridad en la nube, lo que le permitirá continuar justo donde lo dejó su dispositivo anterior».*

Se espera que las nuevas capacidades de inicio de sesión sin contraseña estén disponibles en las plataformas de Apple, Google y Microsoft en el transcurso del siguiente año.

> *«Los usuarios iniciarán sesión a través de la misma acción que realizan varias veces al día para desbloquear sus dispositivos, como una simple verificación de su huella digital o rostro, o un PIN del dispositivo»,* dijo la alianza FIDO.

> *«Este nuevo enfoque que protege contra el phishing y el inicio de sesión será radicalmente más seguro en comparación con las contraseñas y las tecnologías multifactor heredadas, como los códigos de acceso de un solo uso enviados por SMS».*

En cierto modo, el método puede verse como una extensión de sus propias indicaciones de Google para iniciar sesión en cuentas protegidas con autenticación de dos factores (también conocida como verificación en dos pasos).

El desarrollo se produce cuando la plataforma de alojamiento de código GitHub anunció que *«requerirá que todos los usuarios que aportan código en GitHub.com habiliten una o más formas de autenticación de dos factores (2FA) para fines de 2023»*, con el fin de evitar ataques de apropiación de cuentas.