Google rolls out passkey technology in ‘beginning of the end’ for passwords

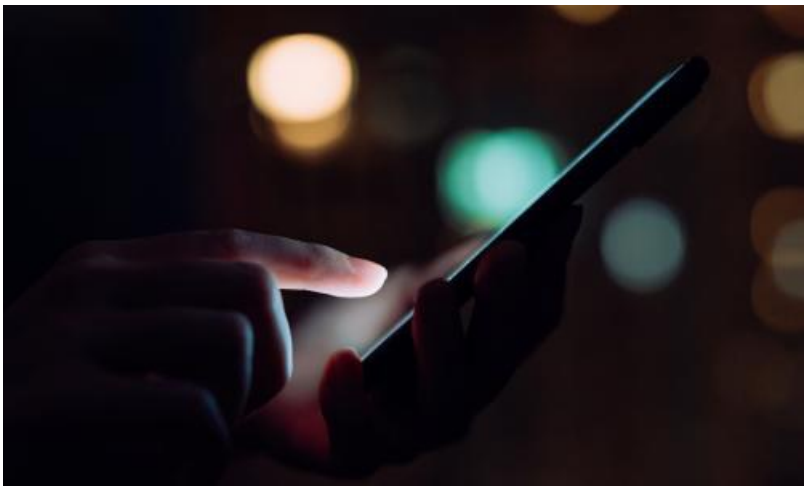
Publication Date: 2023-05-04

Author: Josh Taylor

Section: Technology

Tags: Google, Cybercrime, Internet, Apple, Microsoft, news

Article URL: https://www.theguardian.com/technology/2023/may/04/google-rolls-out-passkey-technology-in-beginning-of-the-end-for-passwords



Google is moving one step closer to ditching passwords, rolling out its passkey technology to Google accounts from Thursday. The passkey is designed to replace passwords entirely by allowing authentication with fingerprint ID, facial ID or pin on the phone or device you use for authentication. Apple has begun using the technology in iOS16 and the latest MacOS release, and Microsoft has been using it through the Authenticator app. Users can create a passkey for each device they use, or the operating system or app used to manage the passkeys can be shared between the devices. A cryptographic private key is stored on the device, and there is a corresponding public key uploaded to Google. When a user signs in, the device must solve a unique challenge using the private key to generate a signature. The signature is then verified using the public key to allow a person to access their account. All Google sees out of the transaction is the signature generated, and the public key. Google has said this will prevent people using phishing, SIM-swap and other methods to obtain passwords and bypass authentication methods – because the private key and the biometrics used are never shared. Google said the rolling out of the passkey technology – to mark World Password Day – signified “the beginning of the end” for passwords for Google accounts. The technology is still in early stages, and it will be a while before there is mass adoption across apps and websites. Google will still let people use passwords in circumstances where they do not have the passkey-enabled device available, but over time the company said it would pay closer attention to accounts using passwords for signs of compromise. Each passkey is unique to each service a person uses, too, meaning that there’s no risk of one compromised account compromising every other account using a passkey. If a user wants to temporarily share their passkey to a new device, they can get a one-time share by scanning a QR code or by using AirDrop for Apple devices. It uses Bluetooth to determine that the device is actually in proximity to the new device. If a user loses their device with the passkey, they can revoke access immediately in account settings. The technology has been developed as part of the Fido (Fast Identity Online) alliance with Apple, Google and Microsoft leading the charge. Ebay, Docusign, PayPal and a number of other businesses are already using passkey. While there may be a time when passkey spells the end of passwords and password managers, 1Password – one of the leading password manager apps – has welcomed the move from the tech giants. The 1Password chief executive, Jeff Shiner, said the move by Google would allow 1.5 billion people in the world to try passkeys but in order to secure wider adoption, passkeys needed to allow users to easily switch between ecosystems such as iOS or Android. “As we actively work with other Fido alliance leaders to eliminate passwords, we’ll inevitably remove one of phishers’ biggest rewards – credentials,” he said. “This is a tipping point for passkeys and making the online world safe.” For companies that use

Google for work accounts, the administrators in those businesses will soon be able to enable those users to use passkeys to sign in.