Google Is Rolling Out Password-Killing Technology to All Its Accounts

Description

Google this week said it is rolling out an update for its users that it describes as “the beginning of the end of the password.”

Known as “passkeys,” the tech giant wrote that “passkeys for Google Accounts are available” starting this week. Google also suggested that passwords may eventually be phased out for its products, including Gmail and YouTube.

“Of course, like any new beginning, the change to passkeys will take time. That’s why passwords and 2SV will still work for Google Accounts. We look forward to helping people, and others in the industry, take this next leap to make signing in easier and safer with Google,” the company wrote in a post.

The company said that the passkey technology will allow billions of Google users to sign into its websites and apps the same way they unlock a device. That’s through a fingerprint, face scan, or a device PIN that can verify their identity.

Services such as Docusign, Kayak, PayPal, Shopify, and Yahoo! Japan have already deployed the technology. Google has claimed that the keys are more secure than passwords and resist cyberattacks such as phishing or brute force attacks.

Google account holders can set up passkeys for their Google accounts by logging in to g.co/passkeys and following the company’s instructions. Business service Google Workspace accounts will “soon” get the option to enable passkeys for users, the company said.

Earlier this year, Apple, too, announced it would be switching to passkeys and will eventually remove passwords in general.

Criticism

One security researcher, Anthony Lawrence, noted that proclamations of a “password-free future” may be overblown and won’t happen for years to come. He also noted that because of the technology

involved in passkeys, websites will have to retain existing passwords.

“There is a true issue. Websites are going to retain existing passwords. They will have to, because it will be decades before every user will have the hardware and software necessary,” he wrote. “But let’s say you do have a new device and upon your next login, the website asks you to switch to passkeys. Will they destroy your old password? No, they can’t because having one capable device doesn’t mean all your devices are capable. Software may allow the use of your phone as the authentication for all of your devices, but they’d still need updated software that knows how to use the phone.”

He and others have noted that another major potential disadvantage to using passkeys is if a user loses the secondary device they use to get access to their accounts.

A separate “issue does not seem like it’s going to be fixed any time soon, and that’s that passkeys sync via your operating system ecosystem, not via a browser, which represents a major regression over the way passwords work,” according to Ars Technica. “Today if I add a password to Chrome on Windows, that password will instantly be available everywhere I have Chrome installed, like an Android phone, a MacBook, an iPhone, a Chromebook, etc., but passkeys don’t work like that.”

by Jack Phillips

Category

1. Freedom-Free speech-Resitance & H-rights
2. Main
3. NWO-Deep State-Dictatorship-Tyrrany
4. Science-Tech-AI-Medical & Gen. Research

Date Created
05/09/2023