Hate passwords? You're in luck—Google is sidelining them

May 4 2023, by David Hamilton

A cursor moves over Google's search engine page, Aug. 28, 2018, in Portland, Ore. Good news for all the password-haters out there: Google has taken a big step toward making them an afterthought by adding “passkeys” as a more straightforward and secure way to log into its services. Credit: AP Photo/Don Ryan, File

Good news for all the password-haters out there: Google has taken a big

step toward making them an afterthought by adding "passkeys" as a more straightforward and secure way to log into its services.

Here's what you need to know:

What are passkeys?

Passkeys offer a safer alternative to passwords and texted confirmation codes. Users won't ever see them directly; instead, an online service like Gmail will use them to communicate directly with a trusted device such as your phone or computer to log you in.

All you'll have to do is verify your identity on the device using a PIN unlock code, biometrics such as your fingerprint or a face scan or a more sophisticated physical security dongle.

Google designed its passkeys to work with a variety of devices, so you can use them on iPhones, Macs and Windows computers as well as Google's own Android phones.

Why are passkeys necessary?

Thanks to clever hackers and human fallibility, passwords are just too easy to steal or defeat. And making them more complex just opens the door to users defeating themselves.

For starters, many people choose passwords they can remember—and easy-to-recall passwords are also easy to hack. For years, analysis of hacked password caches found that the most common password in use was "password123." A more recent study by the password manager NordPass found that it's now just "password." This isn't fooling anyone.

Passwords are also frequently compromised in security breaches.

Stronger passwords are more secure, but only if you choose ones that are unique, complex and non-obvious. And once you've settled on "erVex411$%" as your password, good luck remembering it.

In short, passwords put security and ease of use directly at odds. Software-based password managers, which can create and store complex passwords for you, are valuable tools that can improve security. But even password managers have a master password you need to protect, and that plunges you back into the swamp.

In addition to sidestepping all those problems, passkeys have one additional advantage over passwords. They're specific to particular websites, so scammer sites can't steal a passkey from a dating site and use it to raid your bank account.

How do i start using passkeys?

First step is to enable them for your Google account. On any trusted phone or computer, open the browser and sign into your Google account. Then visit the page g.co/passkeys and click the option to "start using passkeys." Voila! The passkey feature is now activated for that account.

If you're on an Apple device, you'll first be prompted to set up the Keychain app if you're not already using it; it securely stores passwords and now passkeys as well.

Next step is to create the actual passkeys that will connect your trusted device. If you're using an Android phone that's already logged into your Google account, you're most of the way there; Android phones are automatically ready to use passkeys, though you still have enable the function first.

On the same Google account page noted above, look for the "Create a

passkey" button. Pressing it will open a window and let you create a passkey either on your current device or on another device. There's no wrong choice; the system will simply notify you if that passkey already exists.

If you're on a PC that can't create a passkey, it will open a QR code that you can scan with the ordinary cameras on iPhones and Android devices. You may have to move the phone closer until the message "Set up passkey" appears on the image. Tap that and you're on your way.

And then what?

From that point on, signing into Google will only require you to enter your email address. If you've gotten passkeys set up properly, you'll simply get a message on your phone or other device asking you to for your fingerprint, your face or a PIN.

Of course, your password is still there. But if passkeys take off, odds are good you won't be needing it very much. You may even choose to delete it from your account someday.