COMPUTER GURU – *by Don Benjamin*

Passkeys

This is the second in a three-part series on modern sign-in security. Last month's issue explained how to create better passwords. September's article will suggest ways to safely store your passwords. Today's topic is "passkeys."

Passkeys are a newer and safer way to sign in to websites and apps. Instead of entering your username and password to authenticate yourself, passkeys use:

- Something unique to you – like your fingerprint or face – that identify you, and
- Something you own – a device such as your phone, tablet, or computer to store your passkeys.

To use a passkey instead of a username and password:

- The website you're logging into must accept passkeys. Google, Microsoft, and Apple iCloud all accept passkeys. Your bank and investment broker may also accept passkeys.
- Your device must require that you authenticate who you are. Facial or fingerprint recognition, called biometric authentication, are convenient and very difficult to fake.[1]

Setting up a passkey:

- When you navigate to the website, look for an option to set up a passkey.
- When you select that option, your browser creates two digital keys. One key is public that is sent to website's server on the internet. The other key is private that stays on your device. These two keys work with each other.
- The website also proves to your browser that it's a legitimate site.

How passkeys work:

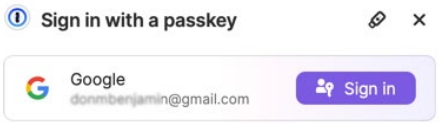
- When you sign in, the website uses your public key to encrypt a secure, digital challenge that is sent back to your device.
- Your device confirms that it's really you using your fingerprint, face, or PIN.
- Your device then uses your private key to encrypt a secure response that proves your identity.

Passkeys are secure because:

- There are no passwords to steal, and if someone finds your device, they don't know your passcode or PIN, and don't possess your face or fingerprint.
- Your private keys (one for each website) are encrypted and only exist on your device.
- Your public key can only be used by a legitimate website. Even if a hacker acquires your public key, he can't fool your device because he doesn't control the website that's associated with that public key.

NERD ALERT

NOTE: This is one of the Guru's nerdier articles. You may want your slide rule and pocket protector handy.



I can sign in to Google with a passkey that uses my fingerprint on my MacBook for authentication.

If you need help with your computer, just click "Tech Help" at the bottom of our website's home page or request help from our tech team at: **https://engage.cmaprinceton.org/tech-help**.

---

1 You can also use the device's PIN or password, but I think facial recognition using the device's camera or fingerprint reader are more convenient.