



Person of Non-Interest

[Home \(https://beaponi.com/\)](https://beaponi.com/) > [Learn \(https://beaponi.com/learn\)](https://beaponi.com/learn) > What are passkeys?

What are passkeys?

A simpler, safer way to sign in, with no password to remember.

Last reviewed October 18, 2026 · [See the sources](#)

The short version

A **passkey** replaces your password. Instead of typing a password, you sign in the same way you unlock your phone or computer: with your **face, your fingerprint, or your screen lock PIN**.

There's no password to type, so there's no password for a scammer to steal, guess, or trick you into giving away.

How it works, in plain words

When you create a passkey for an account, your device makes a matched pair of digital keys:

- **One key stays on your device and stays secret.** It never gets sent to the website.
- **The other key goes to the website.** It isn't secret, and it's useless on its own.

When you sign in, the website checks that your device has the matching secret key. You prove it's you by unlocking your device. **Your face or fingerprint never leaves your device.** The website never sees it.

Why passkeys are safer than passwords

- **They can't be phished** (<https://beaponi.com/learn/glossary#phishing>). A passkey only works on the real website it was made for, so a fake look-alike page can't trick it out of you. U.S. cybersecurity guidance (CISA) calls this kind of sign-in the "gold standard."
- **A break-in at the website doesn't expose them.** The website only stores the public key, which can't be used to sign in as you.
- **They can't be reused or guessed.** Each passkey is unique to one account, and there's nothing to guess.
- **They can't be shared or written down**, even by accident.

One important thing to know

Passkeys protect you against many common password attacks, but they're only as safe as the device that holds them and your account's recovery options.

Anyone who can unlock your phone or computer may be able to use your passkeys. So:

- Use a **strong screen lock** on your phone: a PIN of at least six digits, or a password (see [step 7 of the Starter Checklist \(https://beaponi.com/checklist#doors\)](https://beaponi.com/checklist#doors)).
- **Don't share your phone's unlock code** with anyone you wouldn't trust with your accounts.

A safety note. If someone in your home knows your phone's PIN and you don't feel safe with them, a passkey gives them access too. Make a safety plan first. Support is available, for example from the National Domestic Violence Hotline at [thehotline.org \(https://www.thehotline.org\)](https://www.thehotline.org).

How to start using passkeys

1. **Watch for the offer.** Many sites and apps now ask, "Create a passkey?" when you sign in. You can say yes.
2. **Or turn it on yourself.** Look in the account's **Security** settings for **Passkeys**.
3. **Unlock your device to confirm**, with your face, fingerprint, or PIN. That's it.

Start with your email account, for example your Google or Apple account, because it's the key to everything else.

Official how-tos: [Sign in with a passkey instead of a password \(https://support.google.com/accounts/answer/13548313\)](https://support.google.com/accounts/answer/13548313) (Google) · [About the security of passkeys \(https://support.apple.com/en-us/102195\)](https://support.apple.com/en-us/102195) (Apple)

Common questions

Do I still need my password? For now, usually yes. Many accounts keep your password as a backup, so keep it strong and saved in a password manager. See [How to create a strong password \(https://beaponi.com/learn/strong-passwords\)](https://beaponi.com/learn/strong-passwords).

What if I lose my phone? On Apple devices, passkeys are saved in iCloud Keychain, so they're on your other Apple devices too. Whatever you use, keep your account's recovery options up to date, such as a backup phone number or recovery email, so you can always get back in.

Can I sign in on a computer with a passkey saved on my phone? Often, yes. With Google, for example, you choose to use your passkey on the computer, a QR code appears, and you scan it with your phone. You can also create a passkey on each device you use.

Is a passkey the same as two-step verification? It does the job of both your password and a second step at once. If an account offers a passkey, it's the strongest choice. See [How to turn on two-step verification \(https://beaponi.com/learn/two-step-verification\)](https://beaponi.com/learn/two-step-verification).

Sources

Checked on October 18, 2026. Next review: by October 2027.

- [Passkeys \(https://fidoalliance.org/passkeys/\)](https://fidoalliance.org/passkeys/) (FIDO Alliance, the group behind the passkey standard)
- [About the security of passkeys \(https://support.apple.com/en-us/102195\)](https://support.apple.com/en-us/102195) (Apple)
- [Sign in with a passkey instead of a password \(https://support.google.com/accounts/answer/13548313\)](https://support.google.com/accounts/answer/13548313) (Google)
- [Implementing Phishing-Resistant MFA \(https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf\)](https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf) (CISA fact sheet, PDF)

From beaponi.com/learn/passkeys · Last reviewed October 18, 2026 · General education, not professional advice.