



Person of Non-Interest

[Home \(https://beaponi.com/\)](https://beaponi.com/) > [Learn \(https://beaponi.com/learn\)](https://beaponi.com/learn) > How to create a strong password

How to create a strong password

The short version: long, unique, and saved in a password manager.

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

Think someone has your password right now? Change it on that account first, then on any other account where you used the same password. Then [turn on two-step verification \(https://beaponi.com/learn/two-step-verification\)](https://beaponi.com/learn/two-step-verification). If someone may have had remote access to your computer, follow [those steps first \(https://beaponi.com/help-with-a-scam\)](https://beaponi.com/help-with-a-scam) and change your passwords from a different device you trust.

What makes a password strong

1. **Long.** At least 16 characters. Longer is stronger. Length matters more than anything else.
2. **Random.** Use either a random mix of letters, numbers, and symbols, or a passphrase: four or more random, unrelated words, like lantern-marble-orbit-cactus. (Don't use that one. It's on the internet now.)
3. **Unique.** Use a different password for every account. If one site leaks your password, the others stay safe.

Why: criminals try leaked passwords on other sites automatically. A long, unique password stops one leak from turning into many break-ins.

What matters less than you think

- **Swapping letters for symbols** (like P@ssw0rd) doesn't make a short password strong. Length does far more.
- **Changing a strong password on a schedule** isn't necessary. Change it when it may have been exposed, such as after a data breach, a scam, or if you shared it.

U.S. government password guidance (NIST) tells websites not to force mixes of character types or regular password changes, and to let you use a password manager.

Let a password manager do the work

Nobody can remember dozens of long, random passwords, and you shouldn't try. A password manager is an app that:

- creates strong passwords for you,
- remembers them, and fills them in when you sign in, and
- warns you about passwords that are weak or used more than once.

Your phone or web browser may already include one (which one is right for you? (<https://beaponi.com/learn/password-managers>)). Whichever you choose, protect it with a strong passphrase and turn on two-step verification for it.

Start small: give your email and your bank their own new, strong passwords today. Do the rest over time.

Even better: passkeys

Some accounts let you sign in with a **passkey** instead of a password. A passkey uses your phone or computer's screen lock (your face, fingerprint, or PIN) to sign you in. There's no password to type, so there's no password to steal or trick you into giving away. If an account offers a passkey, it's worth turning on. What are passkeys? → (<https://beaponi.com/learn/passkeys>)

Official how-tos: About passkeys (<https://support.apple.com/en-us/102195>) (Apple) · Sign in with a passkey (<https://support.google.com/accounts/answer/13548313>) (Google)

Next step

A strong password is the first lock. Two-step verification (<https://beaponi.com/learn/two-step-verification>) is the second, and it protects you even if a password leaks.

Common questions

Is it okay to keep my passwords in a file or a note on my computer? It's better not to. CISA points out we don't want to save strong passwords in a file on a computer. A password manager is the safer way to keep track of them.

Is a passphrase as strong as a random password? A long passphrase is a strong choice. CISA lists both random characters and passphrases as good options, and NIST describes a passphrase as generally longer than a password for added security. Aim for at least 16 characters either way.

Should I let my phone or browser save my passwords? That's a good, free way to start. Apple Passwords and Google Password Manager can create strong passwords, save them, and fill them in for you. See Which

password manager is right for you? (<https://beaponi.com/learn/password-managers>)

Sources

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

- Use Strong Passwords (<https://www.cisa.gov/secure-our-world/use-strong-passwords>) (CISA)
- Digital Identity Guidelines: Authentication, SP 800-63B-4 (<https://pages.nist.gov/800-63-4/sp800-63b.html>) (NIST)
- About the security of passkeys (<https://support.apple.com/en-us/102195>) (Apple) · Sign in with a passkey instead of a password (<https://support.google.com/accounts/answer/13548313>) (Google)

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