

Passwords **versus** passphrases

	PASSWORD	PASSPHRASE
What it is	Random characters	Random words
Easy to remember?	No	Much easier
Easy to type?	Slower, especially on phones	Easier
Best for	Accounts stored in a password manager	Your manager's master password, device login, Wi-Fi
Strength grows by	About 4.7 to 6.3 bits per character	About 12.9 bits per word

Both must be random. Use a generator. People are poor at making unpredictable choices.

Reading the **strength readout**

Weak

about 38 bits

Shown for about 38 and 39 bits in the video: 8 lowercase letters, 3 words.

Good

about 52 bits

Shown for about 52 bits: 4 random words.

Strong

75 bits and up

Shown from about 75 bits up: 16 lowercase letters, 6 words and more.

- Accounts in a manager: 16 or more random characters
- Master password: 6 or more random words
- Sites should allow 64 characters or more
- Sites should not force symbols or scheduled changes
- Sites should check against breached passwords

The tiers are the tool's own labels. Aim higher than the minimum for secrets that protect a lot.

CURRENT GUIDANCE

Based on NIST SP 800-63B-4 and EFF passphrase advice. See the guide.

Beyond the password

Unique for every account

Reuse lets one breach open many doors. A unique secret limits the damage.

A password manager

It remembers long random secrets for you, so you remember only one strong passphrase.

A second factor or a passkey

A stolen password is not enough on its own.

Check for breaches

Services like Have I Been Pwned show whether a password or email has leaked. Change it when a breach happens.

Where a generator runs matters. PrivacySafe Bot says it runs in your browser and sends nothing. Prefer tools you can inspect.

Your password plan

- ☐ Use a password manager
- ☐ Make every password unique
- ☐ Use 16 or more random characters for accounts
- ☐ Use a 6-word random passphrase for your manager and devices
- ☐ Turn on a second factor or passkeys
- ☐ Never build secrets from personal facts or patterns
- ☐ Check whether your accounts appear in known breaches
- ☐ Change a password after a breach, not on a schedule

DISCUSSION

Why do some sites still demand symbols and monthly changes? What would you change about their rules?

Where should a password generator run, on your device or on a server? What would you check before trusting one?