Accounts and Passwords

Make accounts that are hard to break into, and keep them yours.

Weak ✗

`sunshine1`

Strong ✓

`river lamp ocean button cactus paper`



Two-step login
Code from an app

What an account is

An account is a username or email address plus a password. Websites, apps and computers use accounts to know it is you.

Make a strong password

A longer password is harder to guess. Use at least 16 characters, make them random, and use a different password for every account. Six random words work well, picked by chance and not from your own life. Avoid names, birthdays and pet names. If one site leaks a password you reused, every account that shares it is open.

Keep track of them

A password manager stores them so you only remember one strong password. KeePassXC is free, open source, and keeps your passwords in a file on your own computer. Ask us if you want help setting it up.

Add a second step

Two-step login, also called multi-factor or 2FA, asks for a code after your password. An authenticator app makes a new code every 30 seconds and is safer than a code sent by text. Aegis (Android) and 2FAS (iPhone and Android) are free and open source. A text code is still better than none. Keep the backup codes somewhere safe.

Protect your email first

Email can reset your other accounts, so give it your strongest password and two-step login.

Never share codes

No real company, bank or helper will ask for your password or the code sent to you. Anyone who does is trying to get into your account.

Names and recovery

Most sites let you use a name you choose. Banks and government sites usually need your legal name. Set up a recovery email or phone now, so Forgot password works when you need it.

Sources: CISA Secure Our World (cisa.gov/secureourworld); EFF Surveillance Self-Defense (ssd.eff.org). Last checked November 2026. Is something unclear or out of date? Use the contact form on our website and choose Guide feedback.