

Locks and Keys

Passwords, passphrases, passcodes, two-factor, and signing in with Google

Most of the confusion here comes from mixing up three different things. Here is what each word actually means.

THE WORDS, IN PLAIN ENGLISH

Password	A secret you type. Short ones are broken by computers guessing billions per second — not by a person sitting there typing.
Passphrase	A password made of several ordinary words: sunset-kettle-yarn-14. Longer than a password, easier to remember, far harder to break.
PIN or Passcode	A short number that unlocks a device in your hand. Safe despite being short, because the device locks up after a few wrong tries.
Saved passwords	Passwords your web browser or phone remembers and fills in for you, protected by your device login.
Password manager	A separate app that holds all your passwords behind one master passphrase — and makes strong new ones for you.
Two-factor (2FA, MFA, TFA)	A second proof after your password: a code, a tap, or a fingerprint. A thief who has your password is stopped right here.
Authenticator app	An app on your phone showing 6-digit codes that change every 30 seconds. Free, and it works with no signal.
Passkey	A password replacement. Your device proves it is you with your face, fingerprint, or PIN. Nothing to type, nothing to steal.
Sign in with Google	Using an account you already have to open the door to a new site, instead of creating yet another password.

THREE WAYS TO PROVE WHO YOU ARE

Something you **KNOW** — a password, passphrase, or PIN.

Something you **HAVE** — your phone, a code, a plastic key.

Something you **ARE** — your face or your fingerprint.

THE ONE IDEA THAT MATTERS MOST

Using the same password in two places is a bigger risk than having a short one. When a company is breached, criminals take the whole list of addresses and passwords and try each pair at banks and shopping sites. They are not guessing yours — they already have it, and are checking where else it works.

Length beats complexity. Uniqueness beats both.

BUILDING A PASSPHRASE YOU WILL ACTUALLY REMEMBER

- **The recipe:** Four unrelated words plus a number. Picture them in one odd scene and it sticks: brass-otter-canyon-77.
- **Never use:** Your name, birthday, pets, street, spouse, grandchildren, or favorite team. Any of that can be read off Facebook in about a minute.
- **Memorize only two:** your email password, and the master passphrase for your password manager. It remembers the other hundred.
- **Guard your email hardest:** Password resets for every other account you own get sent there. Whoever controls your email controls everything else.

THREE HABITS YOU CAN SAFELY RETIRE

- **Changing passwords every 90 days.** The government's own standards body dropped that advice. Forced changes only push people toward Spring2024, then Summer2024. Change one when there is a reason.
- **Cramming in symbols and numbers.** P@ssw0rd! is among the first things a cracking program tries. Substituting symbols for letters is a pattern, and machines know every pattern. Length is what defeats them.
- **Never writing anything down.** That rule came from an era when the risk sat at the next desk. Today it is a stranger overseas. A notebook in a drawer beats one password used everywhere.

ONE QUESTION, EVERY TIME, BEFORE YOU TYPE A PASSWORD

Did I come to this page on my own — or did something send me here?

A link in an email or a text is the most common way passwords are stolen, and the fake page looks perfect because it was copied from the real one. Close it and type the address yourself.

WHERE SHOULD YOU KEEP THEM? AN HONEST COMPARISON

Option	What it gives you	What it costs you
Written on paper at home	Free. Nobody can hack it. Far better than reusing one password everywhere.	No help on your phone away from home. Keep it with your important papers, not taped to the monitor.
Saved in your browser or phone	Free, already there, fills in automatically. Fine for most people.	Anyone who can unlock your computer can read them. May not follow you between Apple and Windows.
Password manager app	Strongest. One passphrase, every device. Warns you about reused or breached passwords.	A setup evening, and some cost money. Bitwarden is free; Apple and Google each have one built in.

SECOND LOCKS, WEAKEST TO STRONGEST

Type	How strong	Notes
Password alone	No second lock at all	If the password leaks, the account is open. This is where most accounts still sit today.
1. Text message code	Weakest — still far better than nothing	Use it when it is the only choice offered. A determined thief can talk your phone company into moving your number.
2. Emailed code	Only as strong as your email account	Fine for low-stakes sites. Never rely on it for the email account itself.
3. Authenticator app	Strong, free, works offline	Google Authenticator, Microsoft Authenticator, or Duo. The sweet spot for most people.
4. Passkey or security key	Strongest — cannot be tricked out of you	A fake website cannot capture it, because it only works on the real one.

Turn it on in this order: email first, then your bank, then anything holding your money or your identity. Ten minutes spent on your email account buys more safety than everything else in this handout combined.

"SIGN IN WITH GOOGLE" — IS IT SAFE?

Usually yes, and often safer than inventing another password. The site never sees your Google password. Google vouches for you and passes along your name and email — one fewer password sitting on a small company's server.

- **If you ever lose that Google account:** Everything attached to it goes too. Protect it with an authenticator app or a passkey first.
- **Check the address bar:** The common theft is a fake pop-up asking for your Google password. The real one says accounts.google.com.
- **Read what it asks for:** Sharing your email address is normal. Contacts, photos, or calendar is not — decline, and sign-in still works.

PASSKEYS: THE THING REPLACING ALL OF THIS

A passkey lives on your phone or computer and unlocks with your face, fingerprint, or PIN. Nothing to remember, nothing to type, nothing a scammer can talk out of you. Google, Apple, Microsoft, Amazon, PayPal and many banks already offer them. **When a site offers you a passkey, say yes.** Your password stays as a backup, so there is nothing to lose.

THREE QUESTIONS WE GET EVERY TIME

- **Is it really safe to let my browser remember passwords?** Yes, for most people. Far safer than reusing one password, and they are locked behind your device login.
- **What if I lose the phone with my authenticator app?** This is why setup gives you backup codes. Print them and keep them with your important papers.
- **Do I have to pay for a password manager?** No. Bitwarden is free, and Apple and Google both include one at no cost with devices you already own.

TRY IT TONIGHT — about fifteen minutes

1. Change your email password to a four-word passphrase you have never used anywhere else.
2. In that same email account, open Settings → Security and turn on two-factor authentication.
3. Write the new passphrase and its backup codes on paper, with your important documents.