Accounts & Passwords

Creating Unique Passwords

Give every important account its own password, then turn on login codes.

About 30 minutes to start

Steps checked October 11, 2026

By Jason Phillips, Founder

General information, not professional advice. You decide which steps fit your situation.

The short answer

Give your email, your bank and your phone carrier each a long password used nowhere else, keep your passwords in a password manager or a password book kept somewhere safe at home, and turn on a second sign-in step. Start with those three accounts, because they can reset almost everything else.

What you will need

- Your phone
- A password manager, or a notebook kept somewhere safe
- About 30 minutes for the first three accounts

Why one password should

never open every door

When a website you use is breached, and websites are breached all the time, your email and password can end up on a list. Criminals run that list against thousands of other sites automatically to see where else it works. If you reuse a password, one leak becomes a key to everything that shares it.

The fix is simple and it works: every account that matters gets its own password, and none of them share pieces with the others. If your bank password is unique, a breach at a shopping site can never touch it.

Decide where your passwords will live

Nobody can remember thirty unique passwords, so the real question is where they live. There are two honest options, and both are far better than reusing a password.

- **A password manager.** An app that creates strong passwords, remembers them and fills them in for you. You remember one strong main password. iPhones, Android phones and most web browsers now include one, and there are well-known independent ones too. If you are comfortable with an app, this is the path we recommend.
- **A password book.** A small notebook where you write each site and its password, kept in a private place at home, where you would keep your passport, not in your bag or by the computer. There is no shame in it. A notebook in a drawer beats a reused password every time.

How to build a password worth writing down

Length matters more than symbols. A simple formula works well: four random, unrelated words, plus a short code for the site.

The formula

Four random words plus a short site code. For example, "Blue Ocean Desk Apple" for your bank becomes **BlueOceanDeskApple-Bank**. Long enough to be very hard to guess, simple enough to write down and read back. Choose your own words, and use different words for every account.

Start with the critical three

You do not have to fix every account tonight. Start with the three that control everything else, then work outward.

1. **Your primary email.** It can reset the password on almost everything else. Give it a brand-new password used nowhere else.
2. **Your bank and money accounts.** Give each its own new password.
3. **Your phone carrier account.** So no one can take over your number. Then lock your phone number too.
4. **Break every shared password.** Make sure those three share no words or pieces with any other login.
5. **Replace the leftovers.** A router, smart device or account still on its factory or default password gets a new one. Default passwords are public knowledge.
6. **Make sure someone can find them.** Whether it is a manager or a book, make sure one person you trust knows how to reach it in an emergency.

Add a second lock

A password is something you know. A second sign-in step is something you have, usually your phone. With it turned on, someone who steals your password is still stopped at the door. It is the

highest-value ten minutes in this guide.

Not all second steps are equally strong. Here they are, best first:

Option	How it works	Our take
Passkey or security key	Your phone, computer or a small physical key confirms it is you, often with your face or fingerprint. There is no code to steal.	Best, where offered
Authenticator app	A free app shows a fresh six-digit code every 30 seconds, made on your device.	Very good
Email code	A code sent to your email.	Good, if your email has its own strong lock
Text message code	A code sent by text.	Better than nothing; use it only when nothing else is offered

Turning on your first one

1. Sign in to your email or bank and open its security settings. Look for "Security," "Sign-in and security" or "Login and security."
2. Choose to turn on two-step verification, also called two-factor authentication or login codes.
3. Pick a passkey or an authenticator app if it is offered. If not, choose email over text message.
4. Follow the prompts. For an authenticator app, you will scan a square code with the app.

The step people skip, and regret

Most services offer one-time backup codes during setup. Save them. Do not screenshot them into your photos or email them to yourself. Write them down and keep them with your password book, or in your password manager. They are your spare key if you lose your phone.

Check your work

- [ ] Your passwords live in a password manager or a password book kept somewhere safe.
- [ ] Your email, bank and phone carrier each have a password used nowhere else.
- [ ] No default passwords are left on your router or devices.
- [ ] Your email has a second sign-in step turned on.
- [ ] Your backup codes are saved somewhere safe.
- [ ] Someone you trust knows how to reach your passwords in an emergency.

About this guide

General information to help you make safer choices online, not legal, financial, tax or professional security advice. You decide which steps fit your situation. No tool or checklist can prevent every kind of fraud or identity theft; these steps lower your risk but cannot remove it. Companies named here reflect our independent view and are not paid endorsements. Caveo is not affiliated with any agency or company named here. Steps checked against official sources on October 11, 2026; corrections to hello@joincaveo.com. Terms and Privacy Policy.