



FREE GUIDE · PRIVACY ACTION NETWORK

Your first five privacy *wins*.

Five changes that make a real difference. About an hour,
free tools, and no technical skills needed.

- A password manager that remembers everything for you
- Two-factor sign-in on the accounts that matter
- A browser that blocks trackers
- Phone permissions you actually chose
- One old account gone for good

Five wins, about an hour.

Each win has its own page: why it matters, the steps, and a check to tell you it's done. Do them in order if you can. The first two protect everything else.

WIN	TIME	WHAT IT PROTECTS
1 · A password manager	15 min	Every account you have
2 · Two-factor sign-in	10 min	Your most important accounts, even if a password leaks
3 · A privacy-respecting browser	5 min	What websites and trackers learn about you
4 · Phone permissions	10 min	What apps can see: location, microphone, contacts, photos
5 · One old account closed	20 min	The details sitting in accounts you no longer use

You'll need

Your phone, your computer, the password for your email account, and about an hour. You don't need to do it all at once.

If a menu looks different

Apps rename their settings often. If a step doesn't match your screen, type the setting's name into the settings search box.

1

WIN ONE

15 MINUTES

Get a password manager.

Why it matters. When a website is breached, criminals try the leaked email and password on other sites. If you've reused that password, one leak becomes many. A password manager creates a different, strong password for every account and remembers them all, so the only one you need to remember is its own.

- 1 **Install Bitwarden** on your computer and your phone, from bitwarden.com or your app store, and create an account. It's free, open source and independently audited.
- 2 **Choose a master password** you'll remember but nobody could guess: four or five random, unrelated words. Avoid famous phrases, song lyrics or anything about you. Write it on paper and keep it somewhere safe at home. If you forget it, nobody can reset it for you.
- 3 **Add the Bitwarden extension to your browser**, so it can fill in passwords for you.
- 4 **Bring your saved passwords across.** In your browser's password settings, choose *Export passwords*. Then, in the Bitwarden web app, go to *Tools → Import data*. **Delete the exported file straight away:** it holds every password in plain text.
- 5 **Change the passwords on your most important accounts**, using Bitwarden's generator. Email first, because it can reset everything else, then banking, then social media and work.

Prefer nothing in the cloud? KeePassXC keeps your passwords in an encrypted file on your own computer, with no account and no company in between. It takes more looking after: the backups, and keeping your phone and computer in step, are yours to do. Either one is far better than reusing passwords.

Done when

- ☐ Bitwarden is on your phone and your computer
- ☐ Your email and your bank have new, unique passwords
- ☐ The exported password file is deleted

Keep going over the next week: update a few more accounts each day, starting with any that used your old passwords.

Turn on two-factor sign-in.

Why it matters. A password on its own can leak. Two-factor sign-in (often called 2FA) asks for a second proof, such as a code from an app on your phone, so a stolen password isn't enough to get in.

- 1 **Install an authenticator app:** Aegis (Android) or Ente Auth (iPhone and Android). Both are free and open source.
- 2 **Start with your email.** In its security settings, find *two-step verification* or *two-factor authentication* and choose *Authenticator app*. For Google, that's myaccount.google.com → Security.
- 3 **Scan the QR code** with your authenticator app, then type in the six-digit code it shows.
- 4 **Save the backup codes in Bitwarden**, in a secure note for that account. They get you back in if your phone is lost.
- 5 **Repeat** for Bitwarden itself, your bank (many banks use their own app for this), and your social media accounts. Write Bitwarden's own recovery code on paper and keep it with your master password: it's no use inside a vault you can't open.

Text message or app? An app is safer. Text codes can be stolen by a scammer who moves your phone number to their own SIM card. And if an account offers a *passkey*, that's stronger still: nothing to type, nothing to steal.

Done when

- ☐ Your email, Bitwarden and your bank ask for a second step
- ☐ Backup codes are saved in Bitwarden, and Bitwarden's own recovery code is on paper

3

WIN THREE 5 MINUTES

Switch to a browser that blocks trackers.

Why it matters. Most websites carry trackers that follow you from site to site and build a picture of your interests. Firefox and Brave block many of them by default, and with one add-on, Firefox blocks most of the rest.

Option A • Firefox

- 1 Download it from **mozilla.org** and make it your default browser.
- 2 In *Settings* → *Privacy & Security*, choose *Strict* tracking protection and turn on *HTTPS-Only Mode*.
- 3 Add **uBlock Origin** from addons.mozilla.org.
- 4 In the same settings, untick the options that send technical and interaction data to Mozilla.

Option B • Brave

- 1 Download it from **brave.com** and make it your default browser.
- 2 In *Settings* → *Shields*, set tracker and ad blocking to *Aggressive*.
- 3 In *Settings* → *Privacy and security*, switch off product analytics and the daily usage ping.

Then, in either browser

- Change the default search engine to **DuckDuckGo** or **Startpage**.
- Import your bookmarks from your old browser. Once everything works, stop using the old one. Edge can't be removed from Windows, but it can sit unused.

Done when

- ☐ The new browser is your default
- ☐ Tracking protection is on and your search engine is changed
- ☐ Your bookmarks came across

4

WIN FOUR 10 MINUTES

Take back your phone's permissions.

Why it matters. Apps often ask for more than they need, and it's easy to tap Allow to get on with your day. A torch app has no reason to see your contacts; a game doesn't need your microphone. Taking back what you didn't mean to give takes minutes.

iPhone

- 1 Open *Settings* → *Privacy & Security*.
- 2 *Location Services*: set each app to *While Using* or *Never*, and turn off *Precise Location* for apps that don't need it.
- 3 Check *Microphone*, *Camera*, *Contacts* and *Photos*. Switch off anything that surprises you.
- 4 *Tracking*: turn off *Allow Apps to Request to Track*.

Android

- 1 Open *Settings* and search for *Permission manager*.
- 2 *Location*: prefer *Allow only while using the app*. Remove *Allow all the time* unless there's a real need.
- 3 Check *Microphone*, *Camera*, *Contacts*, *Phone* and *SMS*. Remove anything that surprises you.
- 4 *Settings* → *Google* → *Ads*: choose *Delete advertising ID*.

Red flags. A torch, calculator or wallpaper app that wants your contacts, microphone or location. A "free VPN" that wants to read your texts. If an app wants access it has no business having, delete the app.

Done when

- ☐ No app has location "all the time" unless it truly needs it
- ☐ Ad tracking is off
- ☐ Apps you don't use are deleted

Close one account you don't use.

Why it matters. Every account you've forgotten about still holds your details, and can still be breached. Closing the ones you don't use shrinks what's out there about you. Pick one: an old social media account, a shopping site you used once, an email address you no longer check.

- 1 **Save anything you want to keep.** Most services have a "download your data" option.
- 2 **Find the delete option,** not "deactivate", which keeps your data. **JustDeleteMe** (justdeleteme.xyz) lists direct links for hundreds of services.
- 3 **Don't sign back in.** Some services wait before deleting, and signing in cancels it. Facebook, for example, waits 30 days.
- 4 **Tidy up:** delete the app from your phone, and the account from Bitwarden once it's gone.

WHERE	WHERE TO FIND IT
Facebook & Instagram	Accounts Centre → Personal details → Account ownership and control → Deactivation or deletion
X (Twitter)	Settings → Your account → Deactivate your account (deleted after 30 days)
TikTok	Profile → menu → Settings and privacy → Account → Deactivate or delete account

Can't close it yet? Lock it down instead: make it private, remove your phone number and old posts, and delete the app.

Done when

- ☐ At least one unused account is deleted, or scheduled for deletion
- ☐ Its app is gone from your phone

DONE

That's five real wins.

The Privacy Action Network framework looks at your digital life in nine layers. In about an hour, you've made solid progress on three of them.

YOU CHANGED	LAYER
Passwords and two-factor sign-in	7 · Identity & authentication
Your browser and search engine	5 · Applications, browsing & services
Phone permissions and ad tracking	2 · Operating systems
An old account closed	7 · Identity & authentication

Keep it going: one change a week

- Move a family or friends' group chat to **Signal**.
- Change your home router's admin password from the one it came with.
- Keep a second copy of your photos somewhere you control.
- When you're ready, move your email to a private provider such as Proton Mail.

Want a hand?

If you'd like help with any of this, or a full privacy check-up of your devices and accounts with the fixes put in order, I can do it with you: remotely wherever you are, or on-site in Gippsland.

privacyaction.network/services

General information, not advice for your specific situation. Menus and features change; if something looks different, search for the setting's name. Checked September 2026.