Sentrly — Google Account Security Checklist

Account-protection essentials, including 2FA, recovery options, and connected apps.

Accounts

- ■ Set up a password manager and start migrating logins to it.
  Reuse is the #1 reason small breaches become big ones. The manager removes the temptation.
- ■ Turn on two-factor authentication (TOTP or hardware key) for primary email.
  Email is the recovery account for almost everything else. Protect it first.
- ■ Add 2FA to financial accounts, password manager, and identity-provider logins (Google, Apple, Microsoft).
  These accounts have the largest blast radius if taken over.
- ■ Review and revoke third-party apps connected to Google / Microsoft / Apple / GitHub.
  Apps you authorized years ago may still have access to mailbox contents or files.
- ■ Search for your email at haveibeenpwned.com and rotate any reused passwords found.
  Knowing where you've been exposed lets you respond instead of guessing.

Devices

- ■ Enable full-disk encryption on every laptop and desktop.
  FileVault, BitLocker, LUKS — all built in, all free, all stop a stolen-laptop scenario cold.
- ■ Set a 6+ digit PIN or alphanumeric passcode on every phone.
  Biometrics are convenience; the PIN is what actually protects the encryption key.
- ■ Enable automatic OS updates and let them apply.
  Most exploits used in the wild target patched vulnerabilities.
- ■ Audit installed apps and browser extensions; remove anything you don't actively use.
  Each extension is code that can read pages you visit.

Browser & email

- ■ Use a privacy-respecting browser with built-in tracker blocking.
  Brave, Firefox with strict ETP, Safari, or LibreWolf — all reduce cross-site tracking.
- ■ Configure encrypted DNS (DoH) in your browser or OS.
  Stops your ISP and Wi-Fi network from reading every domain you visit.
- ■ Enable HTTPS-Only mode in your browser.
  Forces an upgrade to HTTPS or warns you before connecting over plaintext.
- ■ Move from SMS-based 2FA to TOTP or a hardware key for important accounts.
  SMS can be intercepted via SIM-swap. TOTP/keys can't be.

Data shared with services

- ■ Review privacy settings on each social network you use.
  Defaults are 'maximum visibility'. Tighten audience, hide email/phone, disable face-recognition where offered.

■ Disable ad personalization on Google, Meta, Microsoft, and Apple accounts.
Doesn't remove ads, but stops cross-site profiling on these large networks.

■ Request a data export from your top three services.
Knowing what they store is more useful than guessing.