Email Security Checklist

Checklist · The Keystone Account — Every Other Login Resets Through Here.

If your email gets hacked, every other account is at risk. This checklist hardens the single most important account you own. 20 minutes.

Authentication

- ■ Password is 16+ characters, fully random, unique to this account.
- ■ Password is stored only in your password manager — NEVER on a sticky note or text file.
- ■ MFA enabled via authenticator app (Authy / 2FAS / Google Auth) — NOT via SMS.
- ■ Recovery codes printed and stored in a fire safe.
- ■ Recovery email is set to a different account that you also control.
- ■ Recovery phone number is your own — not a shared family number.

Active Sessions Audit

- ■ Reviewed 'Active sessions' / 'Where you're logged in' (Gmail: Security → Devices).
- ■ Signed out of every device I don't currently use.
- ■ Reviewed login history — flagged any unrecognised location.
- ■ Set up login notifications — email me if a new device signs in.

Third-Party App Access

- ■ Reviewed 'Apps with access to your account' (Google: Security → Third-party access).
- ■ Removed any app I don't currently use.
- ■ Removed any app I don't recognise.
- ■ Limited remaining apps to minimum permissions needed.

Email Routing & Forwarding

- ■ Checked 'Forwarding and POP/IMAP' — no unknown forwarding rules set.
- ■ No unknown filters that auto-archive or auto-delete (a hijacker's classic move).
- ■ Vacation responder / auto-reply is OFF unless I'm actually away.
- ■ Reply-to address matches my actual email — no hijacked reply routing.

Inbox Hygiene

- ■ Spam filter set to high.
- ■ External email warning enabled (banner on emails from outside my organisation).
- ■ Phishing report function familiar — I know how to use Gmail/Outlook 'Report Phishing.'

- Sensitive emails (tax docs, financial statements) periodically deleted or archived offline.

Account Recovery Plan

- I know how to recover this account if I lose access (recovery codes path).
- A trusted family member knows my account's recovery process exists (without seeing the secrets).
- If this is a Gmail account, I've added it to my Google 'Inactive Account Manager' for after I die.