Password Security Checklist

Checklist · From Reused Passwords To Bulletproof — The 30-Minute Routine.

Run through this once and your password situation is fixed for years. Five sections, no jargon, all actions you can do today.

Pick & Install A Password Manager (10 Min)

- Choose one: Bitwarden Free, 1Password, Proton Pass, or Apple/Google Keychain (if all-in on one ecosystem).
- Install on your primary phone.
- Install on your primary laptop / desktop.
- Install the browser extension on every browser you use.
- Set up the master password — long, memorable, never reused anywhere else. Write it on paper, store in a safe.

Migrate Existing Passwords (15 Min)

- Use the 'Import' tool — most managers can pull passwords from your browser automatically.
- Sort by 'Reused' or 'Weak' password report — fix the top 5 highest-priority accounts (email, bank, brokerage).
- For each fix: log into the site, change password, let the manager generate and save the new one.
- Aim for 16+ characters, fully random, unique per account.
- Set yourself a target of fixing 3 reused passwords per week until the report is clean.

Enable MFA Across The Board (10 Min)

- Email — authenticator app, NOT SMS.
- Bank and brokerage — authenticator app, NOT SMS.
- Password manager itself — secondary MFA.
- Primary social account — Authenticator or Security Key.
- Cloud storage (Google Drive, iCloud, Dropbox) — authenticator app.
- Save every recovery code in your password manager's Secure Notes section.

Recovery & Backup

- Print recovery codes for at least the email and password manager. Store in a fire safe.
- Set up a trusted-contact / emergency-access feature in your password manager.
- Note an out-of-band restore plan (paper backup of master password + recovery email).
- Test the restore plan once a year — pretend you've lost your phone and walk through recovery.

Maintenance

- Run the password manager's breach scan (Watchtower, Reports) monthly.
- If a service you use is breached, rotate that password and any others that resembled it.
- Audit Tier 1 accounts (email, bank, brokerage, PM, cloud) every 6 months.
- Delete accounts you no longer use — fewer accounts = smaller attack surface.