

Password Security Checklist

Print this page or save it as a PDF to keep track of your security hygiene.

☐ **Use Unique Passwords for Every Account**

Never reuse passwords. If one site gets breached, criminals will try that same password across hundreds of other popular websites.

☐ **Enable Two-Factor Authentication (2FA)**

A strong password is your first line of defense. 2FA (using an authenticator app or hardware key) is your safety net if your password is ever compromised.

☐ **Use a Secure Password Manager**

You only need to remember one strong passphrase—the one that unlocks your password manager. Let the software handle the rest of your 100+ unique logins.

☐ **Use 16+ Characters or 4-Word Passphrases**

Instead of short complex passwords that are hard to remember, use long phrases composed of random words. Length provides more entropy than complexity.

☐ **Never Write Passwords on Sticky Notes**

Keep physical spaces clear of digital secrets. Storing passwords unencrypted on your desk or in spreadsheets defeats their purpose.

☐ **Regularly Check for Breaches**

Use services like HavelBeenPwned to monitor if your email or passwords have been exposed in third-party data breaches.

Brought to you by [PDFZora](#)