

Personal Cybersecurity Checklist

Protecting your digital life from cyber threats

- 1 Install a password manager and generate unique 16+ character passwords for every account.
- 2 Enable two-factor authentication on email, banking, cloud storage, and social media accounts.
- 3 Use an authenticator app like Authy or Google Authenticator for 2FA instead of SMS.
- 4 Enable automatic updates on all devices: Windows, macOS, iOS, Android, and browsers.
- 5 Set up cloud backup with version history and test restore functionality twice yearly.
- 6 Hover over links and check sender addresses before clicking emails that trigger urgency.
- 7 Review and restrict privacy settings on Google, Facebook, Instagram, Amazon, and LinkedIn accounts.
- 8 Install free browser extensions like Privacy Badger and uBlock Origin to block trackers.
- 9 Consider a hardware security key like Yubikey for high-risk accounts like email and banking.
- 10 Unplug external backup drives after completing backups to prevent ransomware encryption.
- 11 Use legitimate email providers with strong spam filters like Gmail, Outlook, or ProtonMail.

Read the full article: <https://privacylabpro.com/blog/personal-cybersecurity-checklist/>

privacylabpro.com