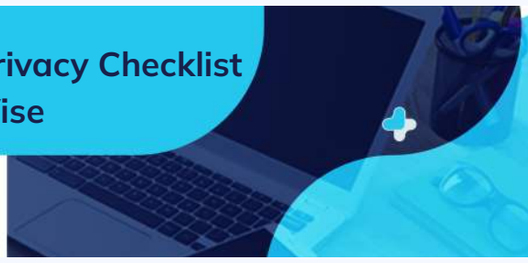
Digital Privacy Checklist by TechVise



your guide
in tech world

Technology doesn't have to complicate our lives
but simplify it once showcased the right way.

AI and Sensitive Data

- [ ] Never input ID numbers, financial details, or medical information into public AI platforms.
- [ ] Read the privacy policies of any AI tool you use for work before submitting sensitive data.
- [ ] Use a VPN when interacting with AI tools to mask your IP address and jurisdiction.

Passwords and Authentication

- [ ] Install a password manager such as Proton Pass and store all credentials inside it.
- [ ] Replace every reused password with a unique, randomly generated strong password.
- [ ] Enable two factor authentication or multi factor authentication on every account that supports it.
- [ ] Use Authy or Proton Pass as your authenticator app so codes are backed up and transferable across devices.
- [ ] Remove saved passwords from your browser on any shared or work device.

Network Security

- [ ] Always connect to a VPN before using public Wi-Fi.
- [ ] Enable your VPN's kill switch so unprotected connections are blocked automatically.
- [ ] Set up your VPN at the router level to protect every device on your home network.

Email, Messaging and Identity

- [ ] Use email aliases for signups to services you do not fully trust.
- [ ] Move sensitive professional communication to Proton Mail for end-to-end encrypted email.
- [ ] Keep work and personal email accounts completely separate.
- [ ] Use Signal for sensitive conversations. Know whether your messenger encrypts by default before trusting it with anything important.

Browser and Search

- [ ] Install uBlock Origin and Privacy Badger on your browser.
- [ ] Disable third-party cookies in your browser privacy settings.
- [ ] Switch your default search engine to a private alternative that does not track queries.
- [ ] Enable HTTPS-only mode in your browser settings.

Device and App Permissions

- [ ] Audit app permissions on your device every three months and revoke what is unnecessary.
- [ ] Delete apps you no longer use.
- [ ] Check app privacy labels before installing anything new.
- [ ] Enable parental controls on any device used by children in your household.

Device Security and Physical Habits

- [ ] Set every device to lock automatically and require authentication to unlock.
- [ ] Enable remote wipe on all your devices before you need it, not after.
- [ ] Keep your operating system, browser, and apps updated. Treat pending updates as a security priority.
- [ ] Before purchasing any connected device, check its data practices. Change default passwords immediately after setup.

Social Media

- [ ] Restrict your social media profiles to minimum public visibility in privacy settings.
- [ ] Disable automatic geotagging on your camera and be deliberate about any location data attached to posts.
- [ ] Apply the same privacy standards to other people's information that you would want applied to your own before posting photos or screenshots of others.
- [ ] Never post images containing visible ID documents, boarding passes, bank cards, or addresses.

Cloud and Files

- [ ] Move sensitive files to Proton Drive or encrypt them before uploading to any standard cloud provider.
- [ ] Wipe devices fully before disposal and confirm data deletion when closing cloud accounts.

Breach Monitoring

- [ ] Set up breach monitoring so you are alerted the moment your personal data appears in a compromised dataset.
- [ ] Periodically review which services hold your data, close inactive accounts, and submit deletion requests where possible.