# Cybersecurity Checklist

A practical security hygiene checklist for individuals and small businesses.

## Secure your accounts

- [ ] Use a unique, strong password for every account.
  Aim for long passphrases of 12 or more characters.
- [ ] Install a reputable password manager to generate and store passwords.
- [ ] Turn on multi-factor authentication everywhere it is offered.
  Prefer an authenticator app or security key over SMS codes.
- [ ] Change any passwords you have reused across multiple sites.
- [ ] Review and remove old accounts and apps you no longer use.
- [ ] Check whether your email appears in known data breaches and update affected passwords.

## Protect your devices

- [ ] Enable automatic updates for your operating system and apps.
- [ ] Set a screen lock with a PIN, password or biometric on every device.
- [ ] Turn on full-disk encryption such as BitLocker or FileVault.
- [ ] Install reputable antivirus or rely on built-in protection, and keep it updated.
- [ ] Enable a firewall on each computer.
- [ ] Only install apps from official stores or trusted sources.
- [ ] Set up remote find-and-wipe in case a device is lost or stolen.

## Secure your home network

- [ ] Change the default admin password on your router.
- [ ] Use WPA3 or WPA2 encryption for your Wi-Fi network.
- [ ] Set a strong, unique Wi-Fi password and update it periodically.
- [ ] Keep your router firmware up to date.
- [ ] Create a separate guest network for visitors and smart-home devices.
- [ ] Disable remote management and unused features on the router.

## Back up your data

- [ ] Identify the files and accounts you cannot afford to lose.
- [ ] Follow the 3-2-1 rule: three copies, two media types, one offsite.
  An offsite or cloud copy protects against theft, fire and ransomware.
- [ ] Schedule automatic backups so you don't rely on memory.
- [ ] Encrypt sensitive backups, especially on external drives.
- [ ] Test a restore to confirm your backups actually work.
- [ ] Keep at least one backup disconnected to survive ransomware.

## Recognize and avoid scams

- [ ] Pause before clicking links or attachments in unexpected messages.
- [ ] Verify urgent requests for money or credentials through a separate channel.
- [ ] Hover over links to check the real destination before clicking.
- [ ] Never share one-time codes, passwords or recovery keys with anyone.
- [ ] Be cautious with public Wi-Fi and avoid logging into sensitive accounts on it.

- [ ] Report suspected phishing to your provider or IT contact.

### Plan for the worst

- [ ] Know how to reset passwords and lock accounts quickly if compromised.
- [ ] Keep account recovery information current, such as backup email and phone.
- [ ] Store recovery codes for MFA in a safe, separate location.
- [ ] Keep a short list of who to contact if a device or account is breached.
- [ ] Review your security settings at least twice a year.