# Full Cyber Safety Checklist

## Passwords & Accounts

• Use different passwords for email, banking, cloud storage, and other important accounts.
• Update weak or reused passwords, aiming for 12+ characters each time.
• Avoid predictable patterns like Summer2025! or Password123.
• Gradually upgrade older passwords over time, starting with the most sensitive accounts.
• Consider using a password manager to keep everything organized and secure.

## Multi-Factor Authentication (MFA)

• Turn on MFA/2FA for email accounts, especially the one used for password resets.
• Enable MFA for bank and financial accounts whenever it's offered.
• Turn on MFA for cloud storage and document accounts that hold sensitive files.
• Store backup codes somewhere safe but accessible if you lose your phone.

## Email & Phishing Defense

• Pause before clicking any link in an email or text—especially if it feels urgent.
• Verify urgent messages by going directly to the official website or app instead of using the link.
• Be careful with unexpected attachments, especially from unknown senders.
• Watch for common red flags: odd sender address, spelling mistakes, strange links, or unusual requests.
• When in doubt, do not reply or click—contact the company through their official support page.

## Devices (Phone, Laptop, Tablet)

• Use a PIN, password, or biometric lock on all devices.
• Turn on auto-lock so devices lock themselves after a short idle time.
• Keep your operating system and apps updated to the latest versions.
• Avoid installing apps or software from unknown sources.
• Back up important files and photos so you can recover them if something goes wrong.

## Browsing & Wi■Fi

• Be cautious on public Wi■Fi; avoid logging into banking or other sensitive accounts when possible.
• Look for HTTPS and a valid padlock icon before entering sensitive information on websites.
• Use a strong, unique password for your home Wi■Fi network.

• Log out of sensitive accounts on shared or public computers.

## Money, Credit & Fraud

• Review your bank and card transactions regularly for anything unfamiliar.
• Know how to quickly contact your bank or card issuer if you spot a problem.
• Turn on transaction or login alerts if your bank offers them.
• Learn about placing fraud alerts or a credit freeze if you suspect identity theft.

## Monthly or Quarterly Tune-Up

• Review which devices and apps have access to your important accounts.
• Remove old apps, browser extensions, or services you no longer use.
• Check whether your email addresses appear in known breach databases.
• Review basic safety habits with family members or coworkers.

## Optional tools that can help (affiliate links)

• Password manager – NordPass: https://go.nordpass.io/aff_c?offer_id=488&aff;_id=136229&url;_id=9356
• Malware scan & cleanup – Malwarebytes: https://www.jdoqocy.com/click-101600442-15734534
• VPN for safer Wi■Fi – NordVPN: https://go.nordvpn.net/aff_c?offer_id=15&aff;_id=136229&url;_id=902
• Breach & data leak alerts – Surfshark Alert: https://get.surfshark.net/aff_c?offer_id=1420&aff;_id=42859

Disclosure: These are affiliate links. If you choose to sign up through them, EmailBreachGuard may earn a small commission at no extra cost to you.