Digital Safety Checklist

Protect Yourself Online in Just 5 Minutes!

This checklist contains 10 essential steps to help you secure your digital life. Each item includes simple actions you can take today to build your digital armor.

Step 1: Strengthen Your Passwords

☐ Use passwords that are at least **12 characters long**, including letters, numbers, and symbols.
☐ Create **unique passwords** for each account—never reuse the same one.
☐ Store passwords securely using a **password manager** (e.g., Bitwarden, Dashlane).
☐ Avoid using personal details like names, birthdays, or “123456.”

Step 2: Enable Two-Factor Authentication (2FA)

☐ Activate **2FA** on critical accounts, such as email, banking, and social media.
☐ Use an **authenticator app** (e.g., Google Authenticator, Authy) for stronger protection than SMS codes.
☐ Back up recovery codes in a safe place for emergencies.

Step 3: Lock Down Your Social Media Privacy

☐ Review and update privacy settings on platforms like Facebook, Instagram, and LinkedIn.
☐ Limit who can see your posts, profile information, and friend lists.
☐ Avoid sharing sensitive details like your phone number, address, location, or vacation plans.
☐ Remove suspicious or inactive accounts from your followers.

Step 4: Beware of Suspicious Links and Emails

☐ Never click on links in unsolicited emails or messages.
☐ Check sender email addresses for typos or mismatched domains.
☐ Verify unexpected requests by contacting the sender directly through official channels.
☐ Install a browser extension like **uBlock Origin** to block malicious ads.

Step 5: Keep Devices and Software Updated

☐ Enable **automatic updates** for your operating system, browser, and apps.
☐ Regularly update your antivirus software and run scans.
☐ Delete unused apps and browser extensions to minimize vulnerabilities.
☐ Restart devices weekly to ensure updates are applied.

Step 6: Use Secure Wi-Fi Networks

☐ Avoid public Wi-Fi for sensitive activities like banking.
☐ Use a **Virtual Private Network (VPN)** when accessing public Wi-Fi.
☐ Secure your home Wi-Fi with a strong, unique password.

Step 7: Regularly Check for Data Breaches

☐ Visit **haveibeenpwned.com** to check if your accounts have been exposed in breaches.
☐ Change passwords immediately for any compromised accounts.
☐ Set up breach alerts to get real-time notifications.

Step 8: Back Up Important Data

☐ Use cloud services or external drives to back up critical files.
☐ Enable automatic backups to protect against accidental data loss.
☐ Test your backups periodically to ensure they work as intended.

Step 9: Monitor Your Financial Activity

☐ Set up alerts for transactions on banking apps and credit cards.
☐ Review account statements regularly for suspicious charges.
☐ Report unauthorized transactions immediately to your bank or card provider.

Step 10: Educate Yourself and Your Family

☐ Share this checklist with friends and family to help them stay secure.
☐ Stay informed about the latest cybersecurity threats and best practices.
☐ Visit https://randallthomastech.com for more security tips and actionable information
☐ Follow trusted resources like the **Electronic Frontier Foundation (EFF)** or **The Hacker News** for updates.

How to Use This Checklist

- Print it out and check items off as you complete them.
- Share it with others to promote digital safety.
- Use it quarterly to maintain strong security practices.