Password Safety Checklist

Based on NIST SP 800-63B Digital Identity Guidelines - the gold standard for password security.

KEY How to use: Go through each item with your family. Check off what you already do well. The items you haven't checked are your action items. Aim to complete all items within 30 days.

SECTION 1: PASSWORD STRENGTH

NIST SP 800-63B (2023 update) recommends prioritizing password LENGTH over complexity. A long passphrase is easier to remember and harder to crack than a short complex password.

- ☐ All important passwords are at least 12 characters long. (Longer = stronger. Target 16+ characters for critical accounts.)
- ☐ Critical account passwords use passphrases - 4 or more random words strung together (example: 'coral-lamp-basket-seven'). These are both strong and memorable.
- ☐ No passwords contain your name, family members' names, birthdays, pet names, or obvious personal information.
- ☐ No passwords use common words, number sequences (12345), or keyboard patterns (qwerty, asdfgh).
- ☐ No passwords contain the name of the service or website they are for (example: using 'Facebook2024' for Facebook).

SECTION 2: PASSWORD UNIQUENESS

Reusing passwords is the #1 cause of account breaches. When one service is compromised, attackers try the same password on every other service (credential stuffing).

- ☐ Your email account has a unique password used NOWHERE else. (Email controls password resets for everything else - it is your master account.)
- ☐ Your banking and financial accounts each have unique passwords not shared with any other account.
- ☐ Social media accounts (Instagram, TikTok, Facebook, etc.) each have unique passwords.
- ☐ No two accounts share the same password.

SECTION 3: PASSWORD MANAGEMENT

With unique passwords for every account, you need a system to remember them. A reputable password manager is the most secure and practical solution.

- ☐ A reputable password manager is in use (recommended: Bitwarden - free, open source, highly audited; alternatives: 1Password, Dashlane).
- ☐ Passwords are NOT written on sticky notes, in plain text files, or in a notes app that is not encrypted.
- ☐ Passwords are NOT shared via text message, email, or social media (even with trusted people - these channels can be compromised).
- ☐ The master password for your password manager is strong (20+ characters), unique, and memorized - not stored anywhere digitally.

(c) ComputerLeap | computerleap.org | Free to share for educational purposes

- [ ] Passwords are updated immediately if you suspect a breach or receive a breach notification.

SECTION 4: MULTI-FACTOR AUTHENTICATION (MFA/2FA)

Multi-factor authentication adds a second verification step - even if someone steals your password, they cannot access your account without also having your phone. NIST strongly recommends MFA for all important accounts.

- [ ] MFA is enabled on your email account (This is the single most important MFA to enable).
- [ ] MFA is enabled on all banking and financial accounts.
- [ ] MFA is enabled on all social media accounts (Instagram, TikTok, Facebook, Snapchat, etc.).
- [ ] MFA is enabled on cloud storage (Google Drive, iCloud, Dropbox).
- [ ] An authenticator app (Authy or Google Authenticator) is used instead of SMS when available - authenticator apps are significantly more secure than text message codes.
- [ ] MFA backup codes are saved in a secure offline location.

SECTION 5: BREACH MONITORING

Data breaches are common - billions of passwords have been exposed over the past decade. You may not know your password was compromised until damage is done.

- [ ] Email addresses have been checked at haveibeenpwned.com - a free, trusted tool that tracks known data breaches.
- [ ] If any email address appeared in a breach, all passwords associated with that email have been changed.
- [ ] A password manager with breach monitoring (most reputable ones include this feature) is alerting you to compromised passwords.
- [ ] A calendar reminder has been set to check haveibeenpwned.com every 6 months.

SECTION 6: FAMILY & CHILDREN'S ACCOUNTS

- [ ] Children's online accounts use strong, unique passwords - not simple passwords because 'they're just kids' accounts.'
- [ ] Children know never to share their password with friends, even best friends.
- [ ] School-issued account passwords (Google Workspace for Education, etc.) follow the same safety rules.
- [ ] Children know to tell a parent immediately if they think their password was shared or discovered by someone else.

TIP Quick Win: Enable MFA on your email RIGHT NOW. It takes 5 minutes and is the single most impactful security improvement most families can make today.

RECOMMENDED TOOLS

- haveibeenpwned.com - Free breach notification service by Troy Hunt (security researcher)
- Bitwarden (bitwarden.com) - Free, open-source, independently audited password manager
- Authy (authy.com) - Free authenticator app with cloud backup
- NIST SP 800-63B - Official NIST password guidelines (csrc.nist.gov/publications/detail/sp/800-63b/final)