SECURE PASSWORD MANAGEMENT

Creating and managing strong, unique passwords is fundamental to personal cybersecurity. Here's a concise, actionable guide to help you protect your digital life:

1. Creating Strong Passwords

- **Length Matters:** Use at least 12–16 characters.
- **Complexity:** Mix uppercase, lowercase, numbers, and special symbols.
- **Avoid Personal Info:** Don't use names, birthdays, or common words.
- **No Dictionary Words:** Hackers use dictionary attacks; avoid real words or predictable patterns.
- **Passphrases:** Consider using a random phrase or sentence (e.g., *Blue!Monkey$Drinks7Tea*).

2. Ensuring Uniqueness

- **Never Reuse Passwords:** Every account should have its own unique password.
- **Why?** If one account is breached, reused passwords put all your accounts at risk.

3. Password Managers

- **Use a Password Manager:** Tools like Bitwarden, 1Password, Dashlane, or LastPass securely store and generate strong passwords.
- **Benefits:** You only need to remember one master password; the manager does the rest.
- **Auto-Fill:** Most managers can auto-fill passwords, reducing the risk of phishing.

4. Multi-Factor Authentication (MFA)

- **Always Enable MFA:** Adds a second layer of security (e.g., code from an app, SMS, or hardware key).

- **Authenticator Apps:** Use apps like Google Authenticator, Authy, or Microsoft Authenticator for better security than SMS.

5. Regularly Update Passwords

- **Change Passwords:** If you suspect a breach, change your password immediately.
- **Review Accounts:** Periodically review and update passwords, especially for sensitive accounts (email, banking, etc.).

6. Recognize and Avoid Risky Practices

- **Don't Write Down Passwords:** Especially not on sticky notes or in unsecured files.
- **Beware of Phishing:** Never enter passwords on suspicious sites or links.
- **Don't Share Passwords:** Even with people you trust.

7. Back Up Your Passwords Securely

- **Password Manager Backup:** Use the backup/export feature of your password manager and store the file securely (e.g., encrypted USB drive).
- **Master Password:** Memorize your master password and keep a secure, offline backup in case you forget.

8. Respond to Breaches

- **Monitor for Breaches:** Use services like Have I Been Pwned to check if your credentials have been exposed.
- **Act Quickly:** If notified of a breach, change your password for the affected account and any others where it was reused.

Quick Reference: Strong Password Example

- **Bad:** password123, John1990, qwerty!
- **Good:** *T!gerw1mming!*

SUMMARY CHECKLIST

- Use a unique, strong password for every account
- Store passwords in a reputable password manager
- Enable multi-factor authentication everywhere possible
- Never share or write down passwords in insecure places
- Regularly check for breaches and update passwords as needed

By following these best practices, you'll greatly reduce your risk of account compromise and keep your digital identity safe.