



everyday identity

10 Essential 'Be Safe' Authentication Checklist

1. Use Strong, Unique Passwords

☐

Create passwords that are at least 12 characters long, incorporating a mix of letters, numbers, and symbols. Avoid using easily guessable information like dictionary words, names, or common phrases.

2. Avoid Password Reuse

☐

Ensure each of your online accounts has a distinct password. Reusing passwords increases the risk of multiple accounts being compromised if one password is exposed.

3. Use a Secure Password Manager

☐

Employ a reputable password manager to generate, store, and autofill your login credentials securely. This helps in managing complex passwords without the need to remember each one.

4. Enable Two-Factor Authentication (2FA)

☐

Activate 2FA on your accounts to add an extra layer of security. This typically involves a second verification step, such as a code from an authenticator app, in addition to your password.

5. Secure Backup Codes

☐

When setting up 2FA, securely store the provided backup codes. These codes can help you regain account access if your primary 2FA method becomes unavailable.

6. Be Cautious with Password Sharing

☐

Avoid sharing your passwords. If sharing access is necessary, use features within password managers designed for secure password sharing.

7. Sign Up for Breach Alerts

☐

Register with services like "Have I Been Pwned" to receive notifications if your email addresses are found in data breaches, allowing you to take prompt action.

8. Avoid Saving Passwords in Browsers

☐

Refrain from using your web browser's password-saving feature, as it may not be as secure as dedicated password managers.

9. Use Caution on Public or Shared Devices

☐

Avoid logging into sensitive accounts on devices that aren't yours or are shared, as they may be compromised or have malware installed.

10. Be Wary of Security Questions

☐

Provide fictitious answers to security questions to prevent unauthorized access, and store these answers securely in your password manager.