everyday identity

10 Essential 'Be Safe' Web Browsing Checklist

1. Use a Privacy-Respecting Browser ☐

Opt for browsers like Brave or DuckDuckGo that prioritize user privacy and offer robust security features.

2. Verify HTTPS Encryption ☐

Always check for the lock icon in the address bar, indicating a secure HTTPS connection, before entering sensitive information on a website.

3. Enable Two-Factor Authentication (2FA) ☐

Add an extra layer of security to your online accounts by enabling 2FA, which requires a second form of verification beyond just a password, especially for banking and credit card sites.

4. Use a Reputable VPN ☐

Protect your real IP address and encrypt your internet traffic by using a trustworthy, paid Virtual Private Network (VPN) service. Even when home.

5. Install a Firewall Application ☐

Monitor and block unwanted internet access by certain applications to safeguard against remote access attacks and privacy breaches.

6. Be Cautious with Email Links and Attachments ☐

Avoid clicking on suspicious links or downloading attachments from unknown sources to prevent phishing attacks and malware infections.

7. Regularly Update Software ☐

Keep your browser, operating system, and all software up to date to patch security vulnerabilities and protect against exploits.

8. Use Strong, Unique Passwords ☐

Create complex passwords for each of your accounts and avoid reusing them across different sites.

9. Utilize a Secure Password Manager ☐

Manage and store your passwords securely using a reputable password manager, reducing the risk of password theft.

10. Be Mindful of Social Media Sharing ☐

Limit the personal information you share on social media platforms to reduce the risk of identity theft and social engineering attacks.