Key

Symbol	Meaning
👍	Something everybody should do
🤔	Something worth doing, but will take some effort
😕	Impractical for most
🔐	Passwords App
⊕	Available via iCloud+

Comprehensive Privacy and Security Action Items

1. Account and Password Security

- □ 👍 🔐 Use strong, unique passwords (20-25 characters, mix of characters)
- □ 👍 🔐 Utilize a reputable password manager
- □ 👍 Implement Two-Factor Authentication (2FA)
- □ 👍 Be cautious with security questions
- □ 🤔 Regularly monitor accounts for unauthorized activity
- □ 🤔 Use a "security" birthday--not your real birthday--for identity verification

2. Device and Network Security

- □ 👍 Secure mobile devices with strong passcodes, encryption, and auto-lock
- □ 👍 Lock computers when not in use
- □ 👍 Use up-to-date antivirus and anti-malware protection
- □ 👍 Secure home Wi-Fi networks (strong passwords, WPA2/WPA3 encryption)
- □ 🤔 Disable WPS and update router firmware regularly
- □ 🤔 ⊕ Use MAC address filtering for network access control
- □ 👍 Be cautious when using public Wi-Fi
- □ 😕 Use a separate device for sensitive transactions
- □ 👍 Cover webcams when not in use
- □ 🤔 Regularly update firmware on all devices, including IoT
- □ 🤔 Disable unnecessary features on smart devices
- □ 🤔 Monitor network traffic for unusual patterns
- □ 🤔 Reboot IoT devices regularly to clear potential malware

3. Communication Security

- □ 👍 Use end-to-end encrypted messaging apps (e.g., Signal)
- □ 🤔 Encrypt emails using PGP, OpenPGP, or GPG
- □ 🤔 Be aware of metadata in communications
- □ 😕 Consider using burner phones for sensitive communications
- □ 🤔 Utilize secure VoIP options with strong encryption
- □ 🤔 ⊕ Use disposable email addresses for temporary communications

4. Online Privacy and Browsing

- □ 👍 Use private browsing mode and clear browser data regularly
- □ 🤔 ⊕ Disable location tracking in browsers
- □ 👍 Use privacy-focused search engines (e.g., DuckDuckGo)
- □ 🤔 Be cautious with cloud backups and syncing
- □ 🤔 Block third-party requests and manage cookies
- □ 👍 Use privacy-focused browser extensions (e.g., NoScript, Ghostery)
- □ 🤔 Start browsing sessions from neutral sites
- □ 🤔 ⊕ Regularly change MAC addresses
- □ 😕 Use virtual machines for enhanced browsing security
- □ 😕 Utilize the Tor browser for accessing the Dark Web
- □ 😕 Maintain a persistent Tor connection to avoid identifiable patterns

5. Anonymity and VPN Usage

- □ 👍 Use VPNs to mask IP addresses, especially on public Wi-Fi
- □ 😕 Utilize the Tor network for enhanced anonymity
- □ 🤔 Consider using anonymous remailers for email
- □ 😕 Create new anonymous accounts when necessary
- □ 🤔 Evaluate VPN providers carefully for privacy policies and security features
- □ 🤔 Use tools for location obfuscation (e.g., proxy servers, ProxyHam)

6. App and Software Management

- □ 🤔 Review and adjust app permissions regularly
- □ 🤔 Prefer open-source software for critical privacy tools
- □ 👍 Keep all software and operating systems updated
- □ 👍 Be skeptical of unverified security claims
- □ 👍 Avoid unnecessary toolbars and add-ons

7. Social Media and Online Presence

- □ 👍 Limit personal information sharing on social platforms
- □ 👍 Regularly review and adjust privacy settings
- □ 👍 Be cautious with photo sharing and metadata
- □ 🤔 Monitor your digital footprint and online presence
- □ 👍 Educate children about online privacy and monitor their activity
- □ 👍 Be wary of friend requests from strangers
- □ 🤔 Avoid linking real-world and online identities

8. Mobile Device Privacy

- □ 🤔 Manage location and connectivity settings (GPS, Bluetooth, Wi-Fi)
- □ 😕 Use airplane mode when not actively using wireless features
- □ 🤔 Regularly clear app data and review permissions
- □ 👍 Be cautious with mobile apps and their data access

9. Physical Security

- □ 👍 Protect against physical access to devices
- □ 👍 Be aware of surroundings when discussing sensitive matters
- □ 👍 Secure physical documents and storage devices
- □ 🤔 Use secure printing methods in shared environments
- □ 🤔 Be cautious of physical surveillance and eavesdropping

10. Data Management and Protection

- □ 👍 Regularly back up important data securely
- □ 🤔 Be aware of data retention policies of service providers
- □ 👍 Minimize sharing of personal information online
- □ 👍 Use encryption for sensitive files and communications
- □ 😕 Consider using Bitcoin for anonymous transactions (with proper precautions)
- □ 🤔 Securely wipe data from devices before selling or discarding

11. Workplace Privacy

- □ 👍 Lock devices when leaving your desk
- □ 🤔 Limit personal activities on work devices
- □ 👍 Use secure printing methods
- □ 👍 Be cautious with office cameras and microphones
- □ 👍 Secure videoconferencing systems

- □ 🤔 Remove metadata from documents before sharing externally
- □ 👍 Separate work and personal communications

12. IoT and Smart Home Security

- □ 🤔 Change default passwords on all IoT devices
- □ 😕 Disable unnecessary features on smart devices
- □ 👍 Physically secure devices to prevent tampering
- □ 🤔 Use strong authentication methods for smart home ecosystems
- □ 🤔 Avoid connecting sensitive devices to shared networks

13. Vehicle Privacy and Security

- □ 👍 Update vehicle software regularly
- □ 🤔 Limit telematics and remote features when not in use
- □ 👍 Clear infotainment system data before selling or returning a vehicle
- □ 👍 Be cautious with connected car features and data sharing

14. Travel Security

- □ 👍 Clean up sensitive data from devices before travel
- □ 🤔 Use whole-disk encryption and consider hidden encrypted folders
- □ 👍 Upload encrypted data to secure cloud services
- □ 👍 Be aware of local laws regarding device searches
- □ 👍 Avoid leaving devices unattended in hotel rooms
- □ 🤔 Use a VPN immediately upon connecting to hotel Wi-Fi

15. Education and Awareness

- □ 🤔 Stay informed about current privacy and security threats
- □ 🤔 Educate others about privacy and security best practices
- □ 🤔 Regularly review and update security measures
- □ 👍 Be aware of phishing attempts and social engineering tactics

16. Legal and Ethical Considerations

- □ 👍 Know your rights regarding privacy laws and regulations
- □ 👍 Advocate for stronger privacy protections
- □ 👍 Be aware of surveillance practices by companies and governments
- □ 👍 Use caution with intellectual property and sensitive information online

17. Incident Response

- □ 🤔 Have a plan for responding to potential security breaches or identity theft
- □ 🤔 Know how to report and address unauthorized access or data leaks
- □ 👍 Monitor accounts and credit reports for signs of compromise

18. Advanced Anonymity Techniques

- □ 👍 Use public Wi-Fi cautiously and with proper protection
- □ 🤔 ⊕ Create and maintain separate email accounts for different personas