Practical Steps to Enhance Your Online Privacy

A Comprehensive Handout for Safer Digital Living

Introduction

In an increasingly connected world, our digital footprints are expanding faster than ever before. Every click, search, download, and interaction can add to a profile that companies, hackers, or even governments might compile about you. Protecting your online privacy is not just tech-savvy caution—it's an essential life skill. This handout provides a detailed guide to practical things you can do to stay safer and maintain your privacy online.

1. Use Strong, Unique Passwords

- Create complex passwords: Combine uppercase and lowercase letters, numbers, and special characters. Avoid predictable patterns such as "password123" or your birthdate.
- Use a different password for every account: This way, if one password is compromised, other accounts remain secure.
- Utilize a reputable password manager: These tools generate, store, and autofill strong passwords so you don’t have to remember each one.
- Update passwords regularly: Change your passwords periodically, especially for sensitive accounts like email, banking, and social media.

2. Enable Two-Factor Authentication (2FA)

- Add an extra layer of security: With 2FA, logging in requires your password and a second verification step, such as a code sent to your mobile device or generated by an authenticator app.
- Use 2FA wherever possible: Prioritize enabling this on your email, financial, and social accounts.
- Prefer authentication apps over SMS: Authenticator apps (like Google Authenticator, Authy) reduce the risk of SIM swapping attacks that can affect SMS codes.

3. Keep Software and Devices Updated

- Install updates promptly: Software updates patch vulnerabilities that hackers might exploit.
- Automate updates: Enable automatic updates for your operating system, browsers, antivirus, and other critical software.
- Don’t forget connected devices: Update firmware on routers, smart TVs, IoT devices, and other gadgets.

4. Be Cautious with Public Wi-Fi

- Avoid sensitive transactions: Don’t access banking or confidential information on public Wi-Fi networks.
- Use a VPN (Virtual Private Network): A VPN encrypts your internet traffic, making it harder for others on the same network to intercept your data.
- Forget the network after use: Don’t let your device automatically reconnect to public networks.

5. Control Your Social Media Exposure

- Review privacy settings: Adjust who can see your posts, photos, and personal info.
- Think before sharing: Avoid posting sensitive details (address, phone number, travel plans).
- Limit third-party app access: Revoke permissions for apps you no longer use that are linked to your social media profiles.
- Regularly audit your friend/follower lists: Remove contacts you do not know personally or no longer trust.

6. Browse the Web More Securely

- Use privacy-focused browsers: Options like Firefox, Brave, or Tor offer features to block tracking.
- Install browser extensions: Add-ons like uBlock Origin, Privacy Badger, or HTTPS Everywhere can enhance privacy.
- Clear cookies and cache regularly: This can reduce tracking and improve privacy.
- Use private browsing/incognito mode: This limits local storage of browsing history and cookies.

7. Manage Your Digital Footprint

- Google yourself: Search for your name regularly to see what information is publicly available.
- Request removal of unwanted content: Contact website admins or use official channels (like Google's removal tools) to take down sensitive data.
- Be wary of online quizzes and surveys: These can collect more personal information than you realize.
- Use disposable emails for signups: Create temporary emails for newsletters or services you don't fully trust. Proton Pass is a password manager that uses aliases for each login.

8. Secure Your Mobile Devices

- Set a strong screen lock: Use PINs, passwords, or biometrics like fingerprint or facial recognition.
- Limit app permissions: Go through your apps and disable access to your location, contacts, microphone, and camera unless absolutely necessary.
- Install apps only from trusted sources: Avoid downloading unofficial apps that might contain malware.
- Enable remote wipe: Make sure you can erase your device if lost or stolen.

9. Protect Your Email Accounts

- Beware of phishing: Don't click on suspicious links or attachments in emails, even if they look legitimate.
- Use email aliases: Create separate email addresses for different types of accounts (shopping, banking, personal, etc.).
- Enable security alerts: Turn on notifications for suspicious login attempts or password changes.
- Use an email provider that provides end-to-end encryption (i.e. Proton Mail).

10. Use encrypted communications

- Whenever possible, use applications that encrypt your data by default.
- End-to-end encryption is best because the app developers themselves cannot access your data.
- Signal is the gold standard when it comes to end-to-end encrypted text, voice, and video calls.

11. Back Up Your Data Securely

- Use encrypted backups: Whether you use an external hard drive or a cloud provider, encryption ensures your data remains private.
- Schedule regular backups: Automate backups to minimize data loss risks from hacks or hardware failure.

12. Be Aware of Data Brokers

- Opt out where possible: Many data brokers provide mechanisms for you to remove your information from their databases.
- Use privacy services: Consider dedicated services that help you monitor, manage, and remove your data from broker lists.

13. Educate Yourself and Others

- Stay informed: Keep up with current news about cyber threats and common scams.
- Teach family and friends: Share good privacy practices, especially with children and less tech-savvy relatives.
- Participate in privacy workshops and webinars: Take advantage of free resources provided by reputable organizations.

Conclusion

Enhancing your online privacy requires ongoing attention and proactive habits. While no single strategy guarantees complete anonymity, combining the steps outlined above can significantly reduce your exposure to privacy risks. By taking ownership of your digital safety, you not only protect your own information but contribute to a safer internet for everyone.