human rights first

American ideals. Universal values.

How to Thwart Digital Surveillance

This guide covers some best practices for digital security, specifically to thwart surveillance of your communications and location. Remember, there is no perfect security -- someone with virtually unlimited time and money will likely eventually be able to overcome your security protocols. But the tougher you make their job, the less likely they will try, and the fewer resources they will have to target others. You can taken steps avoid being an easy target.

Things change constantly, with new ways to target people's information, and new ways to guard against those threats. It's important to stay up to date on the latest security practices to keep your systems protected from new attacks.

The most important things to remember:

1. Always keep your software updated. Updates of apps fix weak points in the tech's security.
2. Turn on and use two-factor authentication for access to your accounts.

Step 1: Start with a Clean Slate

1a. Create a new persona - there are a variety of open source tools for you to generate a random persona. See: https://backgroundchecks.org/justdeleteme/fake-identity-generator/ or https://www.fakenamegenerator.com/ or https://randomuser.me/

1b. Download a profile picture here: https://thispersondoesnotexist.com/ (Note: an experienced adversary may be on the lookout for artificially generated pictures like this)

1c. Associate your newly-created persona with new digital accounts: withdrawing cash → one-time use debit card → purchase burner phone → crypto wallet with burner email which you need a burner phone to create. (This may be impractical given the current banking situation, as always, understand what is possible before attempting)

For a guide see: https://theintercept.com/2020/06/15/protest-tech-safety-burner-phone/

For a guide see: https://www.dailydot.com/debug/how-to-create-digital-identity/

Step 2: Mask Your Location

A. Location (current and previous)
    a. Default phone settings
        i. Android: https://support.google.com/accounts/answer/3467281?hl=en

ii. Apple: https://support.apple.com/en-us/HT207092
iii. https://lifehacker.com/psa-your-phone-logs-everywhere-you-go-heres-how-to-t-1486085759

b. A Faraday bag / cage is a device that prevents signals coming from your phone that can track your location. We recommend keeping your phone and laptop in a Faraday bag when it is not in use. Wrapping your phone and laptops in tin/aluminum can help.
   i. Some potential options include: https://www.amazon.com/Mission-Darkness-Non-Window-Faraday-Laptops/dp/B01A7NDHZO/
   ii. https://www.amazon.com/Mission-Darkness-Non-Window-Faraday-Phones/dp/B01A7MACL2/

c. Unauthorized listening can be enabled by software. Use a tool like Mic Lock to prevent it.
   i. https://www.amazon.com/Mic-Lock-Microphone-Blocker-Pack-Surveillance/dp/B01LPQJGA2/

Step 3: Securing your Data and Communications

A. Local data - email, contacts, photos, videos, etc.
   d. Encrypt data to stop others seeing it.
      i. Turning on encryption for mobile phones
         1. iPhone - https://www.zdnet.com/article/how-to-turn-on-iphone-ipad-encryption-in-one-minute/
         2. Android - https://www.androidcentral.com/how-enable-encryption-android
      ii. Turning on encryption for laptops
         1. MacOS - https://support.apple.com/en-us/HT204837
         2. Windows - https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption
   e. Turn off biometrics entry (FaceID, fingerprint), and turn on passwords and passcodes
      i. This prevents physical forced entry of your biometrics to open your device
B. Keep Safe While Browsing Online
   a. TOR browser: https://www.torproject.org/
   b. Tails Operating System: operating system meant to run off of a USB drive, utilizes TOR protocol for web-browsing, somewhat complicated to get running but most secure
      i. https://tails.boum.org/about/index.en.html
   c. VPN - there are various Virtual Private Network options available for free which make it hard to trace your online activity back to you.

i. NordVPN, ExpressVPN, TunnelBear are all good options - TunnelBear currently offering free access up to the first 10GB transferred in Afghanistan
ii. ProtonVPN is another good system with free options
1. Also recently open sourced their systems: https://protonvpn.com/blog/open-source/
iii. OpenVPN - set up your own, requires a higher level of technical sophistication but security is reliant on the user as opposed to a third party: https://openvpn.net/
iv. Bottom line: find one that works and that is well rated by third party organizations

C. Internet access - when do you trust wifi and bluetooth?
a. Do not use or turn on wifi unless you are sure that the network you're joining is secure
b. Use a Faraday bag while in transit to protect your laptop and phone, or try wrapping your devices in tin/aluminum foil.

D. End-to-end encrypted (E2EE) chat and messaging
a. Many E2EE options are available: Signal, Telegram, WhatsApp are most robust
b. Is Telegram secure? Not by default -- ensure the secure chat function is turned on
c. Signal is more secure than WhatsApp due to its privacy policies. If using Whatsapp, download the latest version if possible, and enable one week of disappearing messages

E. Encrypted email - there are free, encrypted emails available, including
a. Protonmail (does not encrypt subject line) https://protonmail.com/
b. Tutanota (encrypts subject line) https://tutanota.com/
c. To encrypt attachments use Sendsafely https://www.sendsafely.com/
d. Gmail relatively secure

Step 4: Protect Yourself from Malware (for more information see: https://securityinabox.org/en/guide/malware)

a. Mobile
i. Phishing via SMS
1. Don't click on links from senders you don't know or recognize

e. Laptop
i. Phishing via email
1. Don't click on links from senders you don't know or recognize

f. Antivirus - free solutions (note: some sophisticated actors may be able to evade antivirus)
i. Sophos at home https://home.sophos.com/en-us.aspx
ii. Bitdefender https://www.bitdefender.com/
iii. Adaware https://www.adaware.com/

iv. AVG https://www.avg.com/en-us/homepage#mac

Step 5: Use Anonymous File Transfer

A. Check this list of online file storage services that do not require sign up and come with encryption for up to 30 days.

Other Suggested Reading:

https://securityinabox.org/en/

https://www.securityplanner.org/#/