Computer and Mobile Security

Your mobile device may be a significant vulnerability. There are several steps that you can take to help decrease the probability that you are being tracked, but you need to understand that there is absolutely no way to mitigate the risk entirely. Your risk is many times greater if you are using the same device that you left with. Whenever possible, get a new phone before leaving. Most large retailers will sell prepaid "burner" phones that won't have a connection to your old number. If that's not an option, you can have your phone moved to a new plan and perform a factory wipe to remove any unauthorized apps. Talk with the shelter or safe house about their phone policy.

There are a few steps that you can follow to help keep you safe. The following will work for both iOS and Android devices:

- Disable wifi, bluetooth, and location services anytime that you are not using them. These are some of the most common attack vectors.
- Do not remove your device from the faraday cage unless in a public place. You could compromise the location of the shelter which could not only endanger you, but your peers.
- Use the VPN that the shelter provided to you, and if this service is unavailable to you, it is okay to use a commercial service, but this will require research on your part. We recommend Private Internet Access (PIA).

Android

- Ensure that the storage on your device is encrypted, for devices running android 6.0 or greater this is done by default, for older devices you can do this by going to the security settings and enabling it. It will take a long time to do, but it is necessary.
- Download Signal and set it as your default messaging client. It can send both encrypted messages to other Signal users (Please try to convince everyone to use this, as it only increases your safety, especially those who you talk to frequently) and regular SMS messages.
- Download Brave and set it as your default browser

iOS

- Storage encryption should be enabled by default, assuming you have updated your device and it supports iOS 8 or greater

Your laptop is also a major potential threat vector. Reinstall windows if that's what you are using and you aren't comfortable with changing. It is possible that a bug was installed on your system. Try to create the windows installation media on a separate computer (preferably a public one) and do the re-installation offline. This should help protect you. If you are comfortable switching operating systems, it is highly advised that you switch to Linux.

Once you have a fresh operating system installed, you should immediately go to **https://Torproject.org** and install the tor browser bundle. From this point onwards, you should only connect to the internet through Tor

Use Technology Safely

There's a certain risk when using your phone or computer to search for resources or to communicate with your support system. But there's a few steps you can take to stay safe.

- Whenever you're searching for information that you don't want anyone to see, make sure to use private browsing mode. All major browsers have one.
- Be aware that your phone can be used to track you. Both android and iOS phones have apps or built in tools to find lost phones, and tracking apps are easy to find. Make sure to turn off your phone's GPS whenever you don't want your location to be found. Better yet, turn it off and remove the battery. Better still, get a new phone and new number as soon as you leave.
- Before using a computer- especially a public one- look for anything plugged into the back of the computer between the keyboard and the port. If there's anything there, it might be a keystroke logger. Use a different computer.
- Again, using private browsing mode, create a new email address that has no connection to your real identity. Use this address to store reminders to yourself, save pictures and important information, and document your escape plan.
- When you're done, type the following command into your start menu to clear your DNS cache: ipconfig /flushdns . Otherwise, the DNS record can show the sites you've visited, even in private browsing mode.
- Next, copy this into your run bar or computer browser: %appdata%\Macromedia\Flash Player\#SharedObjects . This will show any flash cookies that may reveal the pages you've visited. Delete only the ones you want to hide. To delete them without sending them to the recycle bin, highlight the entry(s) and press Shift+Delete at the same time.
- Clear only specific pages from your browser history- don't clear the entire history for the day. Here's how.

Useful tips

Operation: Safe Escape can send you a tool that allows you to search the web and communicate with others securely and without leaving a trace.

It's a simple thumb drive that you plug into your computer; when you reboot, you're in an entirely new operating system that doesn't keep track of anything you do. See how it works here.

We'll send a free copy with to a safe address of your choosing. Just let us know where to send it.