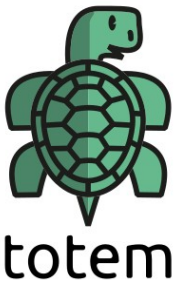
Totem's Desk Research course

Tip Sheet - TP_DR_EN



Mobile phone security tip-sheet

Mobile phone are convenient, but they can also be dangerous. They can be a valuable source of information about you, your sources and your investigations. These tips put you on the path to better mobile investigations. Use them are a starting point to better secure your mobile phone.

1. Compartmentalization

You're only human, and you want to be able to use your personal phone like the rest of us. For very sensitive investigations, consider starting with a clean slate, a clean mobile phone. Use a separate mobile phone for each of your sensitive investigations.

The rest of this tip-sheet considers especially your mobile phone for sensitive investigations!

2. Use a genuine operating system

Make sure you buy your phone from a trusted source and in its original packaging. Don't replace the operating system with a jail-broken version. Always use a genuine operating system for a more secure mobile phone. Keep your operating system up-to-date.

3. Passcodes and biometrics

Protect your mobile phone with a passcode and consider the use of biometrics. Fingerprint and facial recognition may put your phone at additional risk because you can be compelled to hand-over biometrics to law enforcement. In many cases it's advisable not to use biometrics to unlock your phone.

4. Telephone and mobile internet

Your telephone and internet connections are only as strong as the weakest link. How well do you trust your mobile phone operator? Consider using Skype, WhatsApp Voice calls or Signal instead of a telephone call. Replace SMS with WhatsApp and Signal messages. Use a VPN to better protect your internet communication, also on your mobile phone.

5. Don’t use WiFi in untrusted locations

You may not trust your mobile phone operator, but you should trust open and public WiFi even less. Rely on your mobile internet connection when you’re not at home or at work. Never connect to an public WiFi network, especially if the WiFi network offers no password protection.

6. Installing apps

Install apps sparingly and only download apps from reputable sources. Strange or suspicious apps are the primary source of mobile surveillance so it pays to be very scrupulous when choosing favourite apps. At Totem, we only use apps when we need them at least every one or two days. For everything else, just use your mobile browsers. Keep your apps up-to-date at all times.

7. App permissions

Does that local weather app really need access to your contact list or the camera and microphone on your mobile phone? Of course not! We’ve gotten so used to apps over-asking for permission to access our entirely life history, that we click “allow” just out of convenience. Open the settings on your phone and review the permissions for each and every app on your phone as your earliest convenience.

8. Disk encryption

Many newer mobile phone offer disk encryption out-of-the-box. Try to find out if your phone encrypts the data is contains. Switch this feature on, if possible, when that’s not already the case. If your phone doesn’t offer disk encryption then consider replacing it with a model that does.