MOBILES REFERENCE DOCUMENT

Essential reference document for all workshops and activities related to mobiles.

Contents

Supporting resources and references

- Mobile Tools (Security in-a-box, Tactical Tech) https://securityinabox.org/en/mobile-tools
- Trainers' Curriculum: Mobile Safety (Level-Up)
  https://www.level-up.cc/leading-trainings/training-curriculum/mobile-phones
- Umbrella app for Android (Security First)
  https://play.google.com/store/apps/details?id=org.secfirst.umbrella&hl=en

1. Comparing phones

Each type of phone has a specific set of advantages and disadvantages. Below is a comparison of Android phones, iPhones, and Windows phones, and feature phones.

Android

(Note: Not all android versions are the same in terms of features and security.)

Benefits

- Open Source: The Android operating system is open source.
- An open source app store can be used: F-Droid.
- Good security tools are available: Psiphon, Panic button.

- Open source secure communication tools are available: Signal, Chatsecure.
- Tor: Can connect to the Tor network through tools Orbot and Orfox.
- Malware defence: Android has multiple layers of defence from malware.
- Lost and stolen phones: Device manager favailable to help with phone recovery.

Limitations

- Google's business model is based on the use of data.
- Malware: Despite defences, there is malware (eg Androrat).

iPhone

Benefits

- A strong screen lock can be enabled.
- Malware: There is less malware in the app store/iTunes than in the Play Store.
- Permissions are given separately for each app.
- Open source, encrypted communication tools available: Signal, Chatsecure, Surespot.
- Find my iPhone for lost and stolen phones.

Limitations

- Closed source.
- Not many security apps available, compared to Android.
- Default screen lock is only 4 digits.
- Encryption keys are stored on Apple servers.

Windows Phone

Limitations

- Closed source.
- No Security apps available.
- No encryption.

Feature phone

Limitations

- Usually no screen lock
- Closed Source
- No encryption

2. Criteria for a secure phone

If you're looking to buy a phone that you can make as secure as possible, here are some criteria to consider:

- Battery: The battery should be removable
- Updates: The phone's manufacturer should have a good history of pushing updates regularly.
- Operating System: Check the version - does it allow for encrypting the phone? (Older versions don't)
- Chip Set: The Media Tech Chip (MTK) set is the only chip that allows you to change the IMEI number. A list of devices with this chip can be found here: https://en.wikipedia.org/wiki/List_of_devices_using_Mediatek_SoCs

3. What is a mobile phone? A breakdown in 4 layers

The following notes are designed to supplement a set of Mobile Breakdown Cards.
These can be downloaded from here: https://myshadow.org/materials

Page 1: "Core"

- IMEI Baseband: The Baseband is what makes connection between the mobile phone provider and the mobile infrastructure possible. The IMEI is the unique number of the phone, and is connected to the baseband. In most countries it is illegal to change the IMEI number, and in fact on most mobile phones this is not even possible.
- Battery:Is the battery removable? This is the only way to really turn a mobile off.
- Central Processing Unit (CPU): More and more phones integrate the Baseband into the CPU, instead of keeping them separate. Integration means that the mobile phone provider could get access to the CPU and the CPU could have access to the mobile infrastructure (cell phone towers and location tracking).

Page 2: "Smart"

- GPS: There are three ways to determine the location of a mobile phone: Through the baseband, via cell towers (using triangulation to measure exact location); through GPS, via satellites; and through Wi-Fi.
- Wi-Fi: When Wi-Fi is switched on, your phone will broadcast known Wi-Fi networks, offering a history of the networks your mobile has connected to in the past. This could also be used to predict your future location.
- SIM Card: The SIM card holds your phone number. In many countries, you need to register for your phone number with your legal identity, either when you buy the SIM, or after a few weeks.
- Position sensors: Is the phone lying down or held upright? Is it accelerating? Moving in a specific direction? Position sensors can be used to interpret whether someone is moving, calling, texting, or sleeping.

Page 3: "Operating System"

- Built-in apps: These come with your phone and you can't delete them. New built-in apps can also be included in updates. For Android phones, built-in apps can come not only from Google, but also from the manufacturer (Sony, Samsung etc).

- Operating System: Each operating system is developed and owned by a different company (Android=Google / iOS=Apple / Windows=Microsoft), and has pros and cons from a privacy/security perspective.
- Third Party Apps: Apps you install voluntarily from third parties.
- App Store: Your operating system determines which app store you can use. *Android* comes with Google's *Play Store*, ***iPhone*** comes with Apple's *App Store*. Both stores need an email address to work. Note that if the email address you use is already associated with a credit card, your phone will by implication be tied to your financial transactions. Android users, however, are able to use an alternative App Store which is not tied to Google, called F-Droid, which does not require any user information.
- *Note: The above does not necessarily apply to a phone that has been rooted.*

Page 4: Data Traces

- Financial information: Most app stores are connected to a credit card, which is connected to a name and bank account.
- Email: Which email account is tied to tied to the app store? Your email provider will receive notification on every app that you buy or download. If you have an iPhone and you are using Gmail, you are in fact sharing information with both companies. Google is then also able to tie your App Store activity to your Google profile.
- Timestamps and frequency: Timestamps and frequency of contact can be used to analyse mobile data in bulk (using powerful computer programs), to reveal patterns of your networks, social relationships, location, and so on. For example, when you call someone: is the call happening during the day or at night? For how long? How often do you call this person? This can reveal whether they are a partner, friend, colleague or family.
- When all this information is combined with other data traces, and with the data traces of other people, the picture can become incredibly detailed.

4. How a mobile phone connects to the internet

How the internet works

EFF has a good interactive diagram showing the infrastructure of the internet
https://www.eff.org/pages/tor-and-https

The diagram also shows who can see what along the way, and shows how this changes when you connect to the internet via HTTPS or when you use Tor.

HTTP and HTTPS

- When you connect to a website, the connection between you and the website will use one of two protocols: HTTP (the default), or HTTPS.
- When you connect using HTTPS, this created an encrypted connection between the website and your mobile phone. This means that any data you send over the connection (emails, passwords and so on) is scrambled and can't be deciphered by anyone along the way.
- Without HTTPS, ie when a connection is made using just HTTP, our data, including any passwords, travels unencrypted across the web, and can be seen by third parties along the way.

- You can see your connection is using HTTPS by the green lock to the left of the URL. If the green lock is not there, your data is travelling in the clear.
- HTTPS is most consistently used in online banking, email, and shopping websites, though many other websites support it as well. Whether a website supports an HTTPS connection in the first place is up to the website owner, who needs to implement an HTTPS certificate.

HTTPS Everywhere

https://www.eff.org/https-everywhere

- *Android:* To force connections over HTTPS where the option exists (ie, where the website supports https), you can install a simple add-on in the Firefox browser called HTTPS Everywhere. This by default encrypts your connections to all websites that support HTTPS.
- *iPhone:* HTTPS Everywhere is not available for Firefox on iPhone.

Tor

https://www.torproject.org/

- Connecting to the internet via the Tor network allows users to hide their IP address (and therefore their geolocation), while simultaneously blocking trackers and enforcing HTTPS where available. This can provide a degree of anonymity online.
- Using Tor - legality & red flags: In some countries, use of Tor can raise a red flag, and is illegal in some countries. Depending on your own assessment of your risk Tor might not be a good option for you.
- "Tor is only used by criminals:" Tor is also used by activist, dissidents, and many other privacy-aware people.
- Installing Tor:
  - *Android:* To use Tor, Android users first need to install Orbot, which connects you to the Tor network, and then install the Orfox browser. Find out more on the Guardian Project website (creators of Orbot and Orfox) website: https://guardianproject.info
  - *iPhone:* Tor cannot be used on an iPhone.

5. Comparing Browsers for mobile

Android

(Note that all the browsers below can also be run over Orbot.)

Firefox for Android

Developed by Mozilla

Benefits

- Customisation: On Android, Firefox is the only browser where you can change the default privacy settings and install add-ons.

- Proven commitment to security, with highly-paid bug bounty programmes.
- SSL certificate revocation: handles this better than any other browser.
- Data protection is a key issue: corporate manifesto states, "individuals' security and privacy on the Internet are fundamental and must not be treated as optional."
- The source code is available (Firefox is the only browser that is fully open source).
- Non-profit: Firefox is developed by Mozilla, a non-profit organisation that produces free, quality software. This means that the browser is not being used as part of larger profit-making agenda.
- New Private Window": Easy-to-use browsing 'mode' that prevents Firefox from saving your browsing history, and offers some protection against trackers.

Limitations

- Security still not as high as Chrome.

Chrome for Android

Developed by Google

Benefits

- Security: Chrome is among the best browsers out there.
- Flash is built in and automatically updated, which means that vulnerabilities are kept to a minimum (note however that security studies of Chrome were funded by Google in 2011, and a lot has changed since then).
- "Incognito Mode": Easy-to-use browsing 'mode' that prevents Chrome from saving your browsing history.

Limitations

- Privacy: Google makes most of its money through advertising. For this they use information they collect through their services, including Chrome, to find out what you do, where you are, what you buy, etc.
- Default settings: On Android, users are not able to change these.
- Not open source.

Orfox for Android

Developed by The Guardian Project. Orfox requires prior installation of Orbot to function.

Benefits

- Privacy: Orfox by default runs over Tor, and therefor offers online anonymity (hides your IP address), and blocks online tracking.
- Circumvention: helps users circumvent online censorship.

Limitations

- You might not be able to use all online services.

iPhone

Safari for iPhone

Developed by Apple

Benefits

- Customisation: Safari is the only browser on iPhone where you can change the default privacy settings.

Firefox for iPhone

Developed by Mozilla

Benefits

- Proven commitment to security, with highly-paid bug bounty programmes.
- SSL certificate revocation: handles this better than any other browser.
- Data protection is a key issue: corporate manifesto states, "individuals' security and privacy on the Internet are fundamental and must not be treated as optional."
- The source code is available (Firefox is the only browser that is fully open source).
- Non-profit: Firefox is developed by Mozilla, a non-profit organisation that produces free, quality software. This means that the browser is not being used as part of larger profit-making agenda.
- New Private Window": Easy-to-use browsing 'mode' that prevents Firefox from saving your browsing history, and offers some protection against trackers.

Limitations

- Security still not as high as Chrome.
- No add-ons available - Firefox on iPhone is actually just the Safari browser wrapped into a Firefox shell.
- Default settings can't be changed on iPhone.

Chrome for iPhone

Developed by Google

Benefits

- Security: Chrome is among the best browsers out there.
- Flash is built in and automatically updated, which means that vulnerabilities are kept to a minimum (note however that security studies of Chrome were funded by Google in 2011,

and a lot has changed since then).

- "Incognito Mode": Easy-to-use browsing 'mode' that prevents Chrome from saving your browsing history.

Limitations

- Privacy: Google is an advertising company and makes the majority of its money through advertising. For this they use information they collect through their services, including Chrome, to find out what you do, where you are, what you buy, etc.
- Default settings can't be changed.
- Not open source.

6. Search Engines

Privacy-friendly alternatives to Google Search or Bing:

- DuckDuckGo - https://myshadow.org/duckduckgo
- Searx - https://myshadow.org/searx
- StartPage - https://myshadow.org/startpage

7. Encrypting your phone

While newer iPhones are encrypted by default as soon as you put a password on them, Android users need to encrypt their phones manually. Be aware that the process encrypting your phone requires a password; and if you forget this password, you will be locked out of your phone permanently. So, before encrypting:

- Back up the important data on your phone (Contact list, Photos, Videos, etc).
- Charge your phone so it doesn't break the encryption process.
- Use a strong password to encrypt the phone, and make sure that you can remember this password.

8. Location tracking

Location tracking works in three main ways:

- Wi-Fi: When you use the internet via Wi-Fi, your location can be tracked through your IP address.
- Mobile data: Your phone is constantly connecting to cell phone towers in the vicinity, each of which has a location. Triangulation allows your exact location to be pinpointed.
- GPS: Your phone's built-in GPS allows for accurate tracking (by either the US or Russia, depending on what type of GPS your phone has)

9. 'Find my phone' / 'Anti theft' apps

Should you use an app that could help you locate your phone if it got lost of stolen?

- *A 'find my phone' app can be used to:*
  - block the phone

- find the phone if it is lost
- make the phone ring or make a noise
- erase the data on the phone.

- *Whether you decide to use one of these apps will depend on your answers to the following questions:*
    - Is this solution actually useful to you? What is the risk of your phone being stolen
    - If your phone was stolen, what would the impact be?
    - Are you prepared to put in a bit of work initially? (downloading the app, registering the phone, learning how it works, testing it)
    - Do you trust the app developer with the data they will subsequently have access to?
- If you decide to install a 'find my phone' app, Avira (http://www.avira.com/) is recommended.

10. Apps

Though apps are "verified" by app store owners (Google or Apple), in reality this provides weak protection against what applications will do after being installed on your phone - some applications may, for example, copy and send out your address book. You can often, however, regain some control over what an app is allowed to do, and what other parts of your phone it has access to.

Necessary access

Sometimes certain access is required for the app to function - for example, many messenger apps (like Whatsapp and Signal) require access to your Contacts list. Whether or not you are comfortable with this app having this kind of permission should come into your decision about whether or not to use the app.

Permissions

- Check what kind of access your installed apps have to the following: Location, Contacts, Photos, Calender, Speakers, Microphone, Camera.
- Limit access permissions where possible. If an app requires you to give more access than you're comfortable with, consider deleting the app. Perhaps a better alternative exists, or perhaps you don't really need that app after all.

Overreach

Does your newsreader app have access to your contacts? Does the city navigation app you just downloaded want access to your photos? Why? Since these permissions are not central to the app's functioning, they can often be refused. If not, you should consider alternative applications which request more appropriate access and rights.

App Store / Play Store

Record of activity: Keep in mind that because installing an app requires being logged in to either the App Store or the Play Store, either Google or Apple have a record of what you've searched for in the store, and what you've downloaded and installed.

Alternative app stores

Android

- If you want to opt out of Google's Play Store, there are alternatives - for example F-Droid or the Guardian Project's app store, both of which only offer free and open source apps. In general, you should trust a site before you download any apps from it.

- To install tools from an app store other than Google Play, you need to configure your phone settings accordingly.

iPhone

- It is not possible to opt out of Apple's App Store.

How to verify that an app is legitimate

- Check the app's gpg signature. By default, Android requires all applications to be signed with a gpg signature. This can be used to identify the author of an application (i.e. verify its legitimacy), as well as establish trust relationships between applications with the same signature.
  Example: This is the signature of the Orbot app on F-Droid:
  https://f-droid.org/repo/org.torproject.android_15012316.apk.asc
- Do multiple downloads: One of the easiest ways to verify a signature is to download the app several times, from several locations, several computers, and several websites and then compare all signatures to make sure that they are all identical and belong to the same group of developers.
- Compare gpg signatures. This way of verifying is a bit more difficult. This guide can take you through it: https://www.gnupg.org/download/integrity_check.html
- *Chekey*, an app by the Guardian Project, can also help you verify apps:
  https://play.google.com/store/apps/details?id=info.guardianproject.checkey

11. Rooting / Jailbreaking your phone

Should you root your Android phone, or jailbreak your iPhone? The short answer is *Probably Not* :)

- *Rooting* means that you have root access to your device. It is like running programmes as an administrator in Windows PCs.
- Rooting also means unlocking your operating system, which allows you to remove any built-in apps, and to install an alternative operating system, or apps that are not approved by Google/Apple or the phone's manufacturer.
- *Note on legalities*: in some places, rooting/jailbreaking is illegal.
- Be aware that many rooting tools come from China, and a lot contain malware, so if you do decide to root your phone, it's important to use a tool that can be trusted, like Superuser, available from F-droid.
  https://f-droid.org/repository/browse/?fdcategory=Security&fdid=me.phh.superuser&fdpage=2

The good about rooting/jailbreaking

You can remove built-in apps that you don't use, to save space and battery.

- Permissions: If you are using Android 5 or below, you can install an application to control app permissions.
- Updates: You can install custom ROM to get the latest updates from Android, often delayed or blocked by the phone's manufacturer.
- Security: You gain full control over the privacy and security settings of the phone.

The bad about rooting/jailbreaking

- Risks: You risk making your smartphone permanently inoperable ('bricking' it, i.e. turning it into a 'brick').
- Voided Warranty: The manufacturer or mobile carrier warranty may be voided.
- No going back: The process may not be reversible.

Taking all of the above into account, if you do want to root your phone, these resources offer guidance:

- http://www.cyanogenmod.org
- https://wiki.cyanogenmod.org/w/P760_Info
- https://en.wikipedia.org/wiki/Replicant_(operating_system)

12. Checklist for Hands-On Sessions - *Android & iPhone*

Basics

1. Email address

Your phone always has a primary email address connected to it, which is also connected to your App Store / Play Store account. If you create a new email address just for your phone, this can limit social graphing and can help to compartmentalise your digital traces.

- *Android:* Android requires your email address to be a Gmail account; however creating a new email address that is only tied to your phone and Google Play account, and nothing else, makes it harder for Google to tie your different social networks together.
- *iPhone:* It's preferable not to use a gmail account.

2. Phone "name"

Change the name of your phone if necessary (from "Bob's Phone" to something less tied in with your identity). If someone scans the network, this is the name they will see.

3. Passwords

- Put a strong password on your phone.
- Create passwords for individual apps, where possible.
- Disable passwords from being visible

4. Encrypt the phone

See notes on Encryption in Section 7 of this document. While newer iPhones are encrypted by default as soon as you put a password on them, Android users need to encrypt their phones manually. It is not recommended to do this during a hands-on session, as participants might forget their password. However, you can show participants where they can do this at home, and remind them to back up important data, create a strong password, and make sure their phone is charged.

5. SIM card lock

Set this up.

6. Backup & Reset

Android:

- *Backup:* You have the option to *not* have your data backed up on Google servers.
- *Reset:* Additionally, under *Factory data reset*, you can reset your phone and erase all data from the phones' internal storage.

iPhone:

- *Backup:* You have the option to *not* have your data backed up on Apple's iCloud, or to only have *some* data backed up: Settings > iCloud > *Set permissions for each item you want to share with iCloud.* (Transferring photos from your phone to your computer can be done manually, by connecting the two devices with a cable).
- *Reset:* You can reset your phone and erase all its content under Settings > General > Reset.

7. Unique numbers

Know where to find the unique numbers of your phone (IMEI, SIM etc). These can be useful if your phone is stolen.

Connectivitiy & tracking

8. Wi-Fi

Turn off Wi-Fi when you're not using it. When Wi-Fi is on, it continuously broadcasts your Wi-Fi history to Wi-Fi networks in the vicinity.

9. Bluetooth

Turn off bluetooth when you're not using it.

10. Limit location tracking

- Turn off your phone and take out the battery if possible. If you want to be 100% sure, just leave your phone at home, or use a faraday bag/cage.
- Put the phone into flight-safe mode when you don't need to be connected.
- Change settings:

  Android:

  - Disable location tracking. (Note that this will disable some services, such as certain features in Google Maps.) Google Settings > Services > Location
  - Delete location history: Google Settings > Services > Location > Google Location History.

  iPhone:

  - Turn location services off: Settings > Privacy > Location Services > off

11. Opt out of profile-based advertising

Android: Google Settings > Services > Ads: enable *Opt out of interest-based ads*. This will instruct your apps not to use your advertising ID to build profiles or show you interest-based ads. You can subsequently reset your advertising ID by tapping *Reset advertising ID*.

iPhone: Settings > Privacy > Advertising > turn on *Limit Ad Tracking*

12. Choose and customise a browser

Compare the browsers available for your operating system and choose a default browser.

Android: Install and customise Firefox (*On Android, Firefox is the only browser where you can change the default privacy settings and install add-ons.):*

- Change the search engine
- Block pop-ups
- Enable Do Not Track
- Delete history and website data.
- Install HTTPS Everwhere

iPhone: Customise Safari (*Safari is the only browser for iPhone where you can change the default settings*: Settings > Safari):

- Change search engine
- Block pop-ups
- Do No Track
- Clear history and website data.
- The browser history is stored under Settings > Safari > advanced > Websitedata

13. Change the way you connect to the internet

Set up a VPN or Tor (Tor can only be used on Android).

Android: Install Orbot and Orfox

- To use Orfox, you first need to install Orbot. This enables you to connect to the Tor network. You can install both Orbot and Orfox directly from Google Play, F-droid or from the Guardian Project.
- Orbot: Hands-on Guide - https://securityinabox.org/en/guide/orbot/android
- Orfox and Orbot: More information - https://guardianproject.info/2015/06/30/orfox-aspiring-to-bring-tor-browser-to-android/

iPhone: Since Tor is not available for iPhone, for safer browsing it is recommended to set up a VPN and route traffic through this.

- Choose a VPN provider, for example *iPredator, RiseUp VPN,* or *Tunnelbear.*
- Set up the VPN on your phone: Settings > General > VPN > Add VPN Configuration --> add the configurations of the Selected VPN provider and the user account.
- To see if your VPN is on: Settings > see if VPN is turned on.

Security & Permissions

14. Install an antivirus

Avira is recommended (It will also allow you to locate your phone if lost).

15. Find my phone
Anti-virus Avira has this capability, or:

- *Android* users can download *Android Device Manager* from the Play Store
- *iPhone* users can use the phone's *Find My iPhone* app.

16. Check and limit app access/permissions
Android:

- On newer versions of Android you can set permissions per application. Consider restricting access to: location, contacts, photos, microphone, camera, calender
- *Note:* on older versions of Android you can only change the generic permission in the Google Settings sections on Android:

  Activity control: Google Settings > Account > Personal info & privacy > Activity controls > *turn the following OFF:*

  - YouTube Search History
  - YouTube Watch History
  - Google Location History.

iPhone:
You can check and manage app permissions in the settings:
Settings > Privacy > *restrict access per application for the following:*
location, contacts, photos, microphone, camera, calender

17. Enable installation of apps from Unknown Sources
Only possible on Android - this enables you to download apps from outside the Google Play Store.

18. Evaluate your apps

- Reduce: Do you use all the applications on your phone? Which ones can be deleted?
- Choose apps that respect your privacy. Look at the apps on your phone. Why did you choose to install these specific apps? Was it because your friends asked you? Was it an active choice? Discuss what makes an app more secure and better for your privacy (open source, use of encryption, who owns it, where is the company located, what data does it request permission to, does it provide the option of pseudonymous or anonymous use? Find more information on https://myshadow.org.

13. Checklist for Hands-on sessions - *Feature phones*

(A feature phone is a basic phone which doesn't have access to internet.)

- Set up a pin code, or if your phone allows for it, a longer password.
- Take the battery out to protect from location tracking and communication interception.

14. Strategies of Resistance: focus on Mobile Phones

MOBILES REFERENCE DOCUMENT

Below are mobile-specific examples that fall under four strategies of resistance for navigating the data environment. For full explanations of each framework, with more general examples, download the reference document "Strategies of Resistance" on myshadow.org/materials .

Reduce

- Turn off services when not in use (wifi, bluetooth, etc).
- Put phone in flight mode.
- Delete applications no longer in use.
- Change app permissions.

Compartmentalise

- Use different messenger apps for different social networks.
- Use different browsers for different things.
- Use a new email account as your primary email account (not your everyday email account).

Obfuscate

- Use a VPN, change the name on your phone.
- Put fake phone numbers in your phone.
- Leave your phone at home sometimes, to hide where you are going and to break the pattern of your daily routine.

Fortify

- Set up full disk encryption if it's not there automatically (encrypt your phone)
- Put a password on your phone.
- Put passwords on specific applications.
- Install a Find My iPhone Application.