Mobile devices

Note: As operating systems of mobile devices undergo a lot of changes over time and the manufacturers often apply substantial modifications it is possible that certain settings cannot be found on your device or have a different name.

For beginners [Android & iOS]

Setup a screen lock:

- Mobile devices often get lost or stolen. To protect the data on your device you should setup a PIN code or password to prevent unwanted access. Especially swipe and pattern locks don't provide good protection and are easily circumvented. Locks based on biometric data are not recommended either, as biometric information such as your fingerprints and your iris are surprisingly easy to steal and to reproduce but hard to change.

Deactivate connections when you not using them:

- Activated Wi-Fi, GPS and Bluetooth connections reveal your location and may enable third-parties to track you. Try to activate them only when needed.

Limit or deactivate synchronization:

- Your calendar, contacts, Wi-Fi passwords and more are often synced by default with the servers of Google and Apple. You do not have to share such sensitive data with those companies.
  - Android: Deactivate or configure specific accounts in ***Settings*** → ***Accounts***.
  - iOS: Exclude apps from iCloud synchronization in ***Settings*** → ****your account name**** → **iCloud**.

Double-check your apps:

- Many apps ask for more permissions than they really need to provide basic functionalities. Pay attention on to what permissions are being requested when installing or updating apps. A flashlight app doesn't need a connection the internet, a media player doesn't require access to your contacts. Privacy friendly alternatives are often available (see "List of recommended apps available in F-Droid [Android]").
- Apps often spy on their users – and it even happens while they are not in active use. Try to pass on apps that don't provide you with important functionalities or that are known for privacy breaches.
- [Android only] The service **Exodus Privacy** allows you to check apps for third-party trackers and the amount of required permissions: https://reports.exodus-privacy.eu.org/. It is also available as an app via Play Store and F-Droid.

Customize and restrict app settings:

- Android:
  - Restrict app permissions in ***Settings*** → ***Apps & notifications***.
  - Customize your Google settings in the App **Google Settings** or by accessing ***Settings*** → ***Google***.

- iOS: Restrict app permissions in ***Settings*** → ***Privacy***.

Encrypted chats (alternatives to WhatsApp, Telegram etc.):

- Alternatives to messaging apps such as WhatsApp and Telegram are **Signal** and **Wire**. Both use a trusted end-to-end encryption algorithm to protect message content and calls, do not store your message logs on cloud servers and are free software.
  - **Signal:** https://signal.org/, APK download (Android): https://signal.org/android/apk/
  - **Wire:** https://wire.com/, APK download (Android): https://wire.com/en/download/

For advanced users [Android & iOS]

Activate device encryption:

- In order to keep your data save in case you lose your device you should activate the device encryption.
  - Android: ***Settings*** → ***Security & location*** → ***Encryption & credentials*** → ***Encrypt phone***. On device startup you will now be required to provide your PIN/password/ pattern etc. to decrypt your storage.

    WARNING: If you use an older Android version you will be unable to change your password/PIN etc. unless you do a factory reset.
  - iOS: Starting with version 8 encryption is enabled by default.

Chats via XMPP

- Decentralized chats based on the XMPP protocol can be protected by end-to-end encryption. You are free to register on one of many servers and still communicate with users from other servers. Multiple clients are available for Android and iOS:
  - Android: Conversations (Legacy) / Pix-Art Messenger – https://conversations.im/ / https://jabber.pix-art.de/
  - iOS: ChatSecure / Monal – https://chatsecure.org/ / https://monal.im/
- Read more about XMPP:
  - https://xmpp.org/about/
  - https://en.wikipedia.org/wiki/XMPP
  - List of XMPP servers: https://list.jabber.at/

Email encryption via OpenPGP [Android]:

- It is possible to send, receive and read OpenPGP encrypted emails on your phone. On Android you can use the email client apps K-9 Mail or FairEmail in conjunction with the OpenPGP app OpenKeychain.

Diasble or uninstall Google apps [Android]:

- By accessing ***Settings*** → ***Apps*** you can disable or uninstall unneeded preinstalled apps. Be aware that the removal of certain Google apps can restrict certain system functions or make other apps unusable. As long you want to keep using the Play Store you should keep the Play Services installed, as many apps from the Play Store depend on them.

Install the free software repository F-Droid [Android]:

- F-Droid is a repository that exclusively hosts free software and can be used a replacement for the Google Play Store. Most apps found in F-Droid respect your privacy by a much a higher degree than many apps from the Play Store. It can be installed next to the Play Store. Apps installed via F-Droid usually cannot be updated by the Play Store and vice-versa. If you don't want to use the F-Droid app you can also install all apps manually by downloading the APK files from the F-Droid website. Be aware though that most apps won't provide update notifications and depend on F-Droid or manual updating.
  - Offficial website: https://f-droid.org/

List of recommended apps available in F-Droid [Android]:

For many proprietary apps and preinstalled Google services there are free software replacements and alternatives available that pay more respect to your privacy:

- **Amaze:** A file manager with many functions.
- **andOTP:** App for two-factor authentication (2FA).
- **AntennaPod:** Podcast downloader and player.
- **AnySoftKeyboard:** Customizable keyboard alternative without excessive permissions.
- **Aurora Store:** Access the Google Play Store without Play Services. Currently broken. :(
- **Blokada:** System-wide blocking of ads and tracking via VPN interface.
- **DAVx^5:** Sync contacts, tasks and calendars via CalDAV/CardDAV.
- **Editor:** Simple text editor.
- **Etar:** Replacement for the Google Calendar.
- **Exodus Privacy:** Check installed apps for privacy issues.
- **FairEmail:** Email client with material based interface.
- **Feeder:** RSS/Atom feed reader.
- **Fennec F-Droid:** The popular Mozilla Firefox web browser.
- **ICSx^5:** Subscribe to iCalendar/.ics files.
- **LibreOffice Viewer:** Viewer for office file formats.
- **K-9 Mail:** Powerful email client.
- **KeePassDroid:** Password manager compatible with KeePassX.
- **MuPDF viewer:** PDF viewer.
- **Net Monitor:** Lists active network connections of apps and services.
- **NetGuard:** Firewall app to manage in- and outgoing connections.
- **NewPipe:** YouTube client supporting audio and video downloads.
- **Offline Calendar:** Create calendars without online accounts.
- **Open Camera:** Powerful camera app.
- **OpenKeychain:** OpenPGP and key management.
- **OsmAnd+:** Map and navigation app, that works offline.
- **QuickDic:** Dictionary supporting many languages.
- **RadioDroid:** Browse and listen to internet radio stations.
- **SecScanQR:** QR code scanner and generator.
- **Shattered Pixel Dungeon:** A well made dungeon crawler game.

- **Simple Gallery Pro:** Photo/video gallery app.
- **Tor Browser:** Browse the web anonymously via the Tor network; based on Firefox.
- **Transportr:** Find public transport connections.
- **Vanilla Music:** Slim audio player.
- **VLC:** Well known video- and audio player, that can handle many formats.
- **WiFi Automatic:** (De)Activate Wi-Fi connections under certain conditions.
- **Wikipedia:** Official Wikipedia app.

More alternatives to proprietary apps and services can be found here:

- https://prism-break.org/en/categories/android/
- https://www.cryptoparty.in/learn/tools#android

For pros [Android]

Install a Custom ROM:

Preinstalled versions of Android often include major changes of the manufacturer, spy on the users or limit the customizability of the system. Google apps and services are mostly tightly integrated into the system. The only option to avoid Google entirely on your device is to gain root access to remove all unwanted software components or install a Custom ROM. Be aware that you are likely to lose your manufacturer's warranty by doing so. On the plus side you will likely be getting regular system updates again and be able to enjoy additional features. Usually it is also pretty simple to gain root access in Custom ROMs. The LineageOS wiki lists instructions how to install a Custom ROM for many devices: https://wiki.lineageos.org/

WARNING: We are unable to help you with the installation of Custom ROMs during this workshop and cannot be held responsible data loss, damage to your device etc. if you should still decide to install one.

- **LineageOS**: The successor of the once widely used CyanogenMod is a modified Android variant and is developed and supported by a large community. Many devices are officially supported, for many more unofficial builds are available. https://lineageos.org/
- **/e/:** /e/ is a pretty new fork of LineageOS and tries to replace many of the Google apps and services with free software apps and services based on their own infrastructure. **https://e.foundation**
- **Replicant**: Replicant an entirely free operating system based on Android. Unlike LineageOS it replaces proprietary drivers by Google or by the manufacturer with free replacements. Because of this Replicant is only available for a few old devices. https://replicant.us/