Enhancing your Smartphone Security, Privacy and Anonymity

Michel NALLINO

Nice, France, 2025-09-20 - Revision 7

Disclaimer:

THERE IS NO WARRANTY FOR THE DOCUMENT CONTENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW.

THE COPYRIGHT HOLDER PROVIDES THE DOCUMENT CONTENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

THE ENTIRE RISK AS TO USE OF THE DOCUMENT CONTENT IS WITH YOU. SHOULD THE DOCUMENT CONTENT PROVE WRONG, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

Document Internal Links

1. Introduction

Smartphones have invaded our lives, to the point that they sometimes appear as absolutely necessary.

However, though practical, they are often perceived as "Spies in the pocket", to the point that some people refuse to use them.

The goal of this small guide is to show how to enhance your smartphone security, privacy, and anonymity, whatever the kind of your device, Android smartphone or Apple iPhone.

Some figures: There are today 8.6 billion smartphones used in the world, by 7.3 billion users. Android active smartphones are some 5.4 to 5.6 billions, and active iPhones are more than 1 billion.

2. Filtering DNS resolvers

Filtering DNS resolvers are a common tool to increase Android devices and iPhones security and Privacy.

So, this chapter is valid for both kind of devices, and the way to use them will be explained in the Android devices and iPhones dedicated chapters.

2.1) Cloudflare with malware block:

Primary server IPV4 address: 1.1.1.2

Secondary server IPV4 address: 1.0.0.2

Primary server IPV6 address: 2606:4700:4700::1112

Secondary server IPV6 address: 2606:4700:4700::1002

DNS over HTTPS: https://security.cloudflare-dns.com/dns-query

DNS over TLS: security.cloudflare-dns.com

2.2) Cloudflare with malware and adult content block:

Primary server IPV4 address: 1.1.1.3

Secondary server IPV4 address: 1.0.0.3

Primary server IPV6 address: 2606:4700:4700::1113

Secondary server IPV6 address: 2606:4700:4700::1003

DNS over HTTPS: https://family.cloudflare-dns.com/dns-query

DNS over TLS: family.cloudflare-dns.com

2.3) OpenDNS Family Shield:

Primary server IPV4 address: 208.67.222.123

Secondary server IPV4 address: 208.67.220.123

Primary server IPV6 address: 2620:119:35::123

Secondary server IPV6 address: 2620:119:53::123

DNS over HTTPS: https://doh.familyshield.opendns.com/dns-query

DNS over TLS: familyshield.opendns.com

NB: Cisco has stopped OpenDNS activities in France, effective on June 28, 2024. See:

https://support.opendns.com/hc/en-us/articles/27951404269204-OpenDNS-Service-Not-Available-To-Users-In-France-and-Portugal (service has been reactivated in Portugal).

2.4) Rethink configurable DNS resolver:

Rethink offers, for free at the moment, DNS resolver with filters that the user can configure.

There are two ways to do it:

* "advanced" configuration, https://rethinkdns.com/configure, you select the filters you want among more than 190 filters;

* "simple" configuration, from the former web page you click on "simple" button, and you select full categories of filters (Adult, Piracy, Gambling, Dating, Social Media, Security Full, Security Extra, Privacy Lite, Privacy Aggressive, Privacy Extreme);

In both cases, once your selection done, you get a DNS resolver name as DNS over TLS (DoT) or DNS over HTTPS (DoH).

Example: having selected from the simple configuration page "Security Full" and "Privacy Agressive", you get the following DNS resolver DoT name:

"1-6apx6ah77w4p7ug6snibagicimaqaaba.max.rethinkdns.com".

2.5) Mullvad DNS resolvers:

Mullvad has opened its DNS servers, used with Mullvad VPN, to everybody as a free service.

Hostnames and content blockers

The table below shows the different hostnames options and their content blockers. Refer to this when configuring the DNS with the instructions below.

Hostname	**Ads**	**Trackers**	**Malware**	**Adult**	**Gambling**	**Social media**
dns.mullvad.net						
adblock.dns.mullvad.net	✅	✅				
base.dns.mullvad.net	✅	✅	✅			

Hostname	Ads	Trackers	Malware	Adult	Gambling	Social media
extended.dns.mullvad.net	✅	✅	✅			✅
family.dns.mullvad.net	✅	✅	✅	✅	✅	
all.dns.mullvad.net	✅	✅	✅	✅	✅	✅

IP-addresses and ports

The table below shows the corresponding IPV4 and IPV6 addresses.

Hostname	IPV4 address	IPV6 address	DoH port	DoT port
dns.mullvad.net	194.242.2.2	2a07:e340::2	443	853
adblock.dns.mullvad.net	194.242.2.3	2a07:e340::3	443	853
base.dns.mullvad.net	194.242.2.4	2a07:e340::4	443	853
extended.dns.mullvad.net	194.242.2.5	2a07:e340::5	443	853
family.dns.mullvad.net	194.242.2.6	2a07:e340::6	443	853
all.dns.mullvad.net	194.242.2.9	2a07:e340::9	443	853

DNS over HTTPS:

https://dns.mullvad.net/dns-query

https://adblock.dns.mullvad.net/dns-query

https://base.dns.mullvad.net/dns-query

https://extended.dns.mullvad.net/dns-query

https://family.dns.mullvad.net/dns-query

https://all.dns.mullvad.net/dns-query

Mullvad DNS resolvers only use encrypted DoH or DoT, and not unencrypted DNS over UDP/53. The filters lists used by Mullvad DNS resolvers are available here: https://github.com/mullvad/dns-blocklists.

More on Mullvad DNS resolvers here: https://mullvad.net/en/help/dns-over-https-and-dns-over-tls.

2.6) Recursive DNS Resolvers, sovereign and GDPR-compliant, for EU citizens:

There are two initiatives of sovereign, GDPR-compliant, recursive DNS Resolver:

- "sovereign": servers are inside EU, and there is at least one server in each of the 27 EU countries,

- "GDPR-compliant": offering the best privacy protection to its users, in accordance with EU General Data Protection Regulation, see https://gdpr-info.eu/,

- "DNSSEC compatible": DNS answers are signed by the servers.

* EU founded DNS4EU, see https://www.joindns4.eu/. This DNS exists in five flavors:

Hostname	Ads	Trackers	Malware	Adult
unfiltered.joindns4.eu				
protective.joindns4.eu			✅	

Hostname	Ads	Trackers	Malware	Adult
noads.joindns4.eu	✅	✅	✅	
child.joindns4.eu			✅	✅
child-noads.joindns4.eu	✅	✅	✅	✅

Non filtering DNS:

Primary IPV4 DNS server: 86.54.11.100

Secondary IPV4 DNS server: 86.54.11.200

Primary IPV6 DNS server: 2a13:1001::86:54:11:100

Secondary IPV6 DNS server: 2a13:1001::86:54:11:200

DNS over HTTPS: https://unfiltered.joindns4.eu/dns-query

DNS over TLS: unfiltered.joindns4.eu

Protective resolution DNS:

This DNS is a hardened one, security oriented.

Primary IPV4 DNS server: 86.54.11.1

Secondary IPV4 DNS server: 86.54.11.201

Primary IPV6 DNS server: 2a13:1001::86:54:11:1

Secondary IPV6 DNS server: 2a13:1001::86:54:11:201

DNS over HTTPS: https://protective.joindns4.eu/dns-query

DNS over TLS: protective.joindns4.eu

Protective resolution with ad-blocking:

Primary IPV4 DNS server: 86.54.11.13

Secondary IPV4 DNS server: 86.54.11.213

Primary IPV6 DNS server: 2a13:1001::86:54:11:13

Secondary IPV6 DNS server: 2a13:1001::86:54:11:213

DNS over HTTPS: https://noads.joindns4.eu/dns-query

DNS over TLS: noads.joindns4.eu

Protective resolution with child protection:

Primary IPV4 DNS server: 86.54.11.12

Secondary IPV4 DNS server: 86.54.11.212

Primary IPV6 DNS server: 2a13:1001::86:54:11:12

Secondary IPV6 DNS server: 2a13:1001::86:54:11:212

DNS over HTTPS: https://child.joindns4.eu/dns-query

DNS over TLS: child.joindns4.eu

Protective resolution with child protection & ad-blocking:

Primary IPV4 DNS server: 86.54.11.11

Secondary IPV4 DNS server: 86.54.11.211

Primary IPV6 DNS server: 2a13:1001::86:54:11:11

Secondary IPV6 DNS server: 2a13:1001::86:54:11:211

DNS over HTTPS: https:/child-noads.joindns4.eu/dns-query/

DNS over TLS: child-noads.joindns4.eu

* Privately founded, DNS0.EU. This DNS exists in three flavors:

Non filtering DNS:

See https://www.dns0.eu

Primary IPV4 DNS server: 193.110.81.0

Secondary IPV4 DNS server: 185.253.5.0

Primary IPV6 DNS server: 2a0f:fc80::

Secondary IPV6 DNS server: 2a0f:fc81::

DNS over HTTPS: https://dns0.eu

DNS over TLS: dns0.eu

Zero filtering DNS:

This DNS is a hardened one, security oriented, using both human and heuristics filtering, see details at https://www.dns0.eu/zero

Primary IPV4 DNS server: 193.110.81.9

Secondary IPV4 DNS server: 185.253.5.9

Primary IPV6 DNS server: 2a0f:fc80::9

Secondary IPV6 DNS server: 2a0f:fc81::9

DNS over HTTPS: https://zero.dns0.eu

DNS over TLS: zero.dns0.eu

Kids filtering DNS:

This DNS protects kids against adult content, see details at https://www.dns0.eu/kids

Primary IPV4 DNS server: 193.110.81.1

Secondary IPV4 DNS server: 185.253.5.1

Primary IPV6 DNS server: 2a0f:fc80::1

Secondary IPV6 DNS server: 2a0f:fc81::1

DNS over HTTPS: https://kids.dns0.eu

DNS over TLS: kids.dns0.eu

3. Android devices

3.1) Introduction to Android

Android devices include an operating system with several layers:

- A Linux kernel, personalized for Android,

- A layer of Open Source Android, AOSP, see https://source.android.com/

- In most cases, a Google layer (with Google Play, Google Play Service, Google Assistant or Gemini, Android Auto, Google Chrome, Gmail, Google Maps etc.),

- Manufacturer specific drivers and settings,

- In some cases an extra manufacturer layer (example, Samsung) over Google one or partially replacing some Google applications,

- Applications from Google Play Store, or from alternative stores such as F-Droid, or installed from an apk file.

Android security is based on the use of SELinux (Security Enhanced Linux), that provides full isolation of applications in the strongest sandboxes. Some mechanisms allow sharing data and files between sandboxed applications.

Security weaknesses come mainly from the use of malware.

Malware are controlled by Google in its Play Store, and by Google Security on the device; risk to download and install malware is greater when using alternative store or when installing from an apk file.

It is recommended to shut down and restart periodically Android devices, to remove memory persisting malware.

As with any operating system, it is recommended to update it as frequently as possible (system and applications), for bugs and security fixes.

The main problem with Android is tracking: you are tracked by Google and by all the "free" (non-pay) applications installed on the device (and even by some pay ones).

Another problem is ads, being displayed so aggressively inside applications that they prevent their normal use.

3.2) Use of alternative distributions

Some users may install alternative distributions instead the one delivered with their Android smartphone, in order to be completely freed from Google.

It requires user skillfulness, and it is not available for all the devices.

Installing an alternative distribution is risky: it might induce smartphone bricking. This risk is canceled when user buys a smartphone with one of these distributions being installed.

Finally, without a Google account, Google cloud backup is not possible; user should set up another backing solution. Some users choose root rsync backup but, some applications such as Netflix will not work once the smartphone is rooted.

→ **For all those reasons, it is a niche use.**

Here are some alternative distributions:

Linux distributions:

* Ubuntu Touch

https://www.ubuntu-touch.io/

"A whole mobile operating system experience, that is yours".

Ubuntu Touch is a Linux operating system, dedicated to smartphones, totally replacing Android.

It is compatible with the following list of devices: https://devices.ubuntu-touch.io/. It is possible to get it preinstalled on some devices (Volla, Pine64 and FXP).

It uses its own applications. Some Android applications can be run on Ubuntu Touch using applications that allow to run containerized Android applications on Linux systems without the need for a complete Android operating system.

There are some 200,000 to 300,000 Ubuntu Touch users.

* Sailfish OS

https://sailfishos.org/

"Sailfish OS is a Linux-based European alternative to dominating mobile operating systems, and the only mobile OS offering an exclusive licensing model for local implementations".

It is compatible with the following devices: https://docs.sailfishos.org/Support/Supported_Devices/.

It uses its own applications store, Jolla Store.

There are some 80,000 to 120,000 users, mainly developers.

* PostmarketOS

https://postmarketos.org/

"PostmarketOS develops free and open-source software to extend the life of consumer electronics. By empowering people to have full control of their devices, we promote a healthier and more sustainable society".

It is compatible with the following devices: https://wiki.postmarketos.org/wiki/Devices.

There are some 1,000 users.

* Mobian

https://mobian-project.org/

"A Debian derivative for mobile devices".

It is compatible with the following devices: https://wiki.debian.org/Mobian/Devices, mainly Pine64 and OnePlus smartphones.

There are some 2,000 to 5,000 users.

* Plasma Mobile

https://plasma-mobile.org

"An ecosystem for telephones that respect privacy, free and secure software".

Plasma mobile can be installed on Linux distributions such as PostmarketOS or Mobian.

There are few users of Plasma Mobile, some 1,000, since it is a beginning project.

* PureOS

https://www.pureos.net/

"A fully-convergent, user-friendly, secure and freedom respecting OS for your daily usage. With PureOS, you are the only one in control of your digital life".

PureOS is officially compatible only with Librem 5 smartphone made by Purism.

There are some community projects to have it compatible with PinePhone and some Mobian on Nokia.

Purism has delivered some 20,000 Librem 5 with PureOS.

→ Globally, the alternative Linux distributions users on smartphones are some 300,000 to 450,000.

Android alternative distributions:

* /e/OS

https://e.foundation/e-os/

"/e/OS is a complete, fully "deGoogled", mobile ecosystem"

/e/OS is an open-source mobile operating system paired with carefully selected applications. They form a privacy-enabled internal system for your smartphone. And it is not just claims: open-source means auditable privacy. /e/OS has received academic recognition from researchers at the University of Edinburgh and Trinity College of Dublin.

/e/OS could have just focused on an OS, but apps and online services are crucial components of everyday experience, too.

These online services, including search engine, email platform, cloud storage and other online tools, create a unique privacy enhanced environment.

It is compatible with the following list of devices: https://doc.e.foundation/devices. Murena sells some smartphones with preinstalled /e/OS.

Applications are installed from App Lounge: the App Lounge is the second iteration of the application store embedded within /e/OS. It allows everyone to access millions of applications directly from their phone home screen.

It combines common Android apps, open source apps and even progressive web apps in one single repository. It is the only app store that does this today. You don't need to sign in to an account to download apps.

There are some 200,000 /e/OS users.

* LineageOS

https://lineageos.org/

"A free and open-source operating system for various devices, based on the Android mobile platform".

It is the successor of CyanogenMod.

It is compatible with the following list of devices: https://wiki.lineageos.org/devices/.

It includes a set of Open Source applications. Google applications are not bundled with LineageOS but can be downloaded separately.

There are some 1,800,000 LineageOS users.

* GrapheneOS

https://grapheneos.org/

"The private and secure mobile operating system with Android app compatibility. Developed as a non-profit open source project".

It is compatible with the following list of devices: https://grapheneos.org/faq#supported-devices, only some Google Pixel, because of GrapheneOS security hardware requirements.

GrapheneOS is a security hardened version of Android, Google free, with its own AppStore. Google Play Store can be optionally installed in a sandbox.

GrapheneOS probably provides the best compatibility with Google Play Store applications.

There are some 60,000 GrapheneOS users.

* CalyxOS and Pixel Experience are no longer maintained.

→ Globally, taking into account Calyxos and Pixel Experience users, there are some 2,600,000 alternative Android distributions users.

* Huawei

https://consumer.huawei.com

The case of Huawei is specific: Huawei sells Android smartphones, without any access to Google software.

Huawei smartphones do not have access to Google Play Store, or to any Google application, but to their own app store.

In a way, Huawei smartphone users are free from Google tracking, but it has just be replaced by Huawei one!

* XDA Developers

https://xdaforums.com/

On XDA Developers forums, you can find some customized ROMs for some Android devices.

3.3) Use of commercial Android devices

Most Android users use Android devices with the manufacturer provided operating system (Android 14, 15, 16…) and its tailoring.

However, user can set its commercial Android device up in order to enhance its security, privacy, and even have some anonymity.

* Protection against malware, ads and tracking

This part does also apply to Android smartphones with alternative Android distribution.

We are speaking here of malware on internet, not of the malware that you can install from stores. The best two filtering DNS resolvers, regarding malware protection are:

"zero.dns0.eu", it protects against phishing (it does not answer to requests for websites less than one month old, which is the case for most phishing websites with a small life duration) and protects against homograph attacks by filtering fraudulent websites with Cyrillic characters,

"protective.joindns4.eu" and other filtering DNS resolvers from the joindns4eu family, it includes a database of more than twenty million malevolent websites. This database is continuously updated, AI is used to analyze the websites behavior.

1st Method: use of a filtering DNS resolver and of DuckDuckGo browser.

Choose the filtering DNS resolver you want, see Filtering DNS resolvers, and enter its DoT name in the private DNS setting found in settings/internet and network.

Examples:

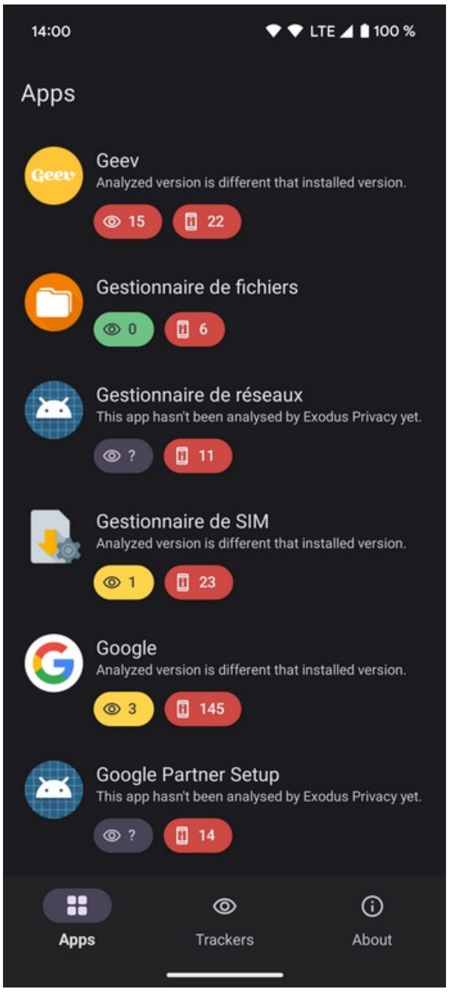
"zero.dns0.eu" for security enhanced dns0.eu resolver,

"1-6apx6ah77w4p7ug6snibagicimaqaaba.max.rethinkdns.com" for a rethink DNS resolver with "Security Full" and "Privacy Agressive" settings.

The filtering will be system-wide, for all the installed applications and the operating system.

Install DuckDuckGo browser from Play Store. DuckDuckGo browser is a bad browser (no extension, based on WebView and leaking the internal IP address through WebRTC leak), but we will use it just to add an extra tracking filtering layer over the applications installed on the device, using its App Tracking Protection. More: read https://duckduckgo.com/duckduckgo-help-pages/p-app-tracking-protection/what-is-app-tracking-protection.

App tracking is different from the usual tracking that occurs when using a browser; trackers are specific ones. You can install on your Android smartphone Exodus Privacy application; it will analyze the apps installed on your smartphone and download reports giving, for each app, the trackers used by the app and the list of authorizations requested by the app.



14:00 LTE 100 %

Apps

Geev
Analyzed version is different that installed version.
15 22

Gestionnaire de fichiers
0 6

Gestionnaire de réseaux
This app hasn't been analysed by Exodus Privacy yet.
? 11

Gestionnaire de SIM
Analyzed version is different that installed version.
1 23

Google
Analyzed version is different that installed version.
3 145

Google Partner Setup
This app hasn't been analysed by Exodus Privacy yet.
? 14

Coupling both filtering DNS resolver and DuckDuckGo App Tracking Protection can protect your Android Device against malware, ads and tracking.

2nd Method: use of Personal DNS filter

Personal DNS filter is an application that can be downloaded from Google Play Store and can be used on a standard non-rooted Android device.

It combines the use of the DNS resolver of your choice, using IPV4 or IPV6 addresses (this excludes rethink DNS resolver), with a set of filters, accepting two syntaxes: hosts files or DNS filters. You can choose one or several of the preexisting filters, or add a filter of your choice.

More: read https://www.zenz-solutions.de/personaldnsfilter-wp/.

I use "zero.dns0.eu"as filtering DNS resolver, with the following IP addresses:

193.110.81.0
185.253.5.0
2a0f:fc80::
2a0f:fc81::

Here are the filters lists I use (malware, ads, tracking and social networks):

Ads:
https://v.firebog.net/hosts/AdguardDNS.txt;
https://v.firebog.net/hosts/Easylist.txt;
https://raw.githubusercontent.com/lassekongo83/Frellwits-filter-lists/master/Frellwits-Swedish-Hosts-File.txt.
Malware:
https://raw.githubusercontent.com/greatis/Anti-WebMiner/master/hosts;
https://raw.githubusercontent.com/hoshsadiq/adblock-nocoin-list/master/hosts.txt;
https://malware-filter.gitlab.io/malware-filter/urlhaus-filter-hosts.txt;
https://urlhaus.abuse.ch/downloads/hostfile/;
https://raw.githubusercontent.com/FadeMind/hosts.extras/master/add.Spam/hosts;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/rpz/tif.mini.txt;
https://raw.githubusercontent.com/davidonzo/Threat-Intel/master/lists/latestdomains.piHole.txt.
Trackers:
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.amazon.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.apple.txt;
https://v.firebog.net/hosts/Easyprivacy.txt;
https://hostfiles.frogeye.fr/multiparty-trackers-hosts.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.huawei.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.winoffice.txt;
https://raw.githubusercontent.com/mullvad/dns-blocklists/refs/heads/main/files/tracker;
https://raw.githubusercontent.com/notracking/hosts-blocklists/master/hostnames.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.oppo-realme.txt;
https://gitlab.com/quidsup/notrack-blocklists/-/raw/master/trackers.hosts;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.tiktok.extended.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.vivo.txt;
https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/domains/native.xiaomi.txt.
Multiple filters kinds:
https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts;
https://big.oisd.nl/domainswild2;

https://raw.githubusercontent.com/hagezi/dns-blocklists/main/wildcard/pro-onlydomains.txt.

(Ads, Affiliate, Tracking, Metrics, Telemetry, Phishing, Malware, Scam, Fake, Crytojacking and other "Crap").

Social networks:
https://raw.githubusercontent.com/mullvad/dns-blocklists/refs/heads/main/files/social.
(NB: the use of this list will prevent the use of Facebook, Instagram etc., but will allow the use of WhatsApp).

With Personal DNS filter, no need of DuckDuckGo browser; moreover, it includes the possibility to whitelist some websites (included in the filters) that you would want to connect to, and to add manually some websites you would want to filter.

* Partial deGoogling
This doesn’t apply to Android smartphones with alternative Android distribution.
I have uninstalled or deactivated (when uninstalling is not possible) all the Google Applications that I do not use:

- Android Auto,
- Gemini,
- Gmail (replaced by Thunderbird),
- Google,
- Google Assistant,
- Google Chrome (replaced by Firefox),
- Google Docs (replaced by Collabora Office),
- Google Fit,
- Google Maps (can be accessed more privately with a browser),
- Google Meet (can be accessed more privately with a browser),
- Google News (can be accessed more privately with a browser),
- Google TV,
- Google Voice Recognition and Synthesis,
- Notes Keep,
- YouTube (can be accessed more privately with a browser),
- YouTube Music (replaced by VLC).

A zoom on Firefox:
Firefox for Android is my default browser, it replaces Google Chrome.
I have installed the following extensions:

- "Canvas Blocker", fingerprinting protection,
- "CSS Exfil Protection", privacy protection,
- "Dark Reader", it allows displaying web pages with white characters on black pages, just a question of taste,
- "DuckDuckGo Search and Tracker Protection", privacy protection, it installs DuckDuckGo search as home page, DuckDuckGo search engine by default and DuckDuckGo Privacy Essentials extension,
- "Privacy Badger", privacy protection,

- "Font Fingerprint Defender", fingerprinting protection,
- "uBlock Origin", one of the best ads, privacy and malware filter.

Note that not all Firefox extensions are available for Android version of Firefox. However, using the debug mode (type five times on Settings/About Firefox) allows installing any extension from a file.

Officially, "about:config" is not available in the Android version of Firefox; but it is there, just hidden! In the address bar type: "chrome://geckoview/content/config.xhtml" and the usual content of "about:config" is there! Bookmark it.

Make the following changes in "about:config":

- "browser.cache.disk.enable" set to "false", to disable disk caching,
- "webgl.enable-debug-renderer-info" set to "false", to prevent graphic driver to be exposed,
- "media.peerconnection.enabled" set to "false", to disable WebRTC leak,
- "javascript.options.baselinejit" set to "false", to disable javascript just in time compilation, it reduces javascript attack surface,
- "pdfjs.enableScripting" set to "false", to disable scripting in PDF,
- "network.IDN_show_punycode" set to "true", to be protected against IDN homograph attacks, URLs with non-Latin characters will be displayed as punycode.

You may want to install other browsers than Firefox:

- IronFox is a fork of Firefox, based on former Mull, it is a security hardened version of Firefox, through configuration preferences; it has Fission enabled, this means that all tabs are isolated and work in different processes (though this is enabled in Firefox desktop versions, it is not yet available on Firefox for Android version, but it is already enabled on IronFox). See:
https://gitlab.com/ironfox-oss/IronFox

- Cromite is a fork of Chromium, based on former Bromite, it is a privacy hardened version of Chromium, with its own filter capability, still offering full Chromium security. See:
https://github.com/uazo/cromite

Those browsers are not available from Google Play Store; to install them, you should first download and install F-Droid store, from https://f-droid.org/. Then,

- To install Ironfox, add the following repository to F-Droid:
https://gitlab.com/ironfox-oss/fdroid/-/raw/main/fdroid/repo
then, look for IronFox in F-Droid and install it.

- To install Cromite, add the following repository to F-Droid:
https://www.cromite.org/fdroid/repo/?fingerprint=49F37E74DEE483DCA2B991334FB5A0200787430D0B5F9A783DD5F13695E9517B
then, look for Cromite in F-Droid and install it.

Note that IronFox and Cromite are maintained by very small teams and could disappear without notice, as their predecessors did; check that they are updated regularly.

* Other precautions

- Enable localization, NFC, Bluetooth, Wi-Fi only when you need it,
- never connect to a public Wi-Fi spot,
- for each installed application, set its notifications, authorizations, battery use,

- use the "System Manager" application to set the "super energy economy mode", it will prevent most applications to work in the background,
- if the setting is available (Android 14 and later), disable 2G,
- when possible, prefer to use the browser than a dedicated app (example: connect to Facebook with Firefox, don’t use Facebook app),
- keep your system and applications updated.

* VPN

It is possible to use a VPN in Android devices. Once installed, the VPN connection can be set to permanent in Settings/Internet and Network.

Note that the use of a VPN prevents the use of DuckDuckGo Browser and of Personal DNS Filter; though they are not VPNs, they use the VPN setting of Android.

* Anonymity

Tor Browser is available from the Play Store; use the same settings as for Firefox, and do use the NoScript extension.

However, Tor Browser for Android, like Firefox for Android, does not use Fission and does not provide processes isolation. For more security, use Orbot and launch the browser you want, IronFox or Cromite, with Orbot VPN mode.

Several messaging applications offer anonymity and full End-to-End Encryption. Avoid WhatsApp (undisclosed source), Telegram (encrypted up to the servers, nobody knows what happens on the servers), prefer Signal or, in France, Olvid.

4. iPhones

4.1) Introduction to iPhones

iPhones are exclusively made by Apple; their operating system, iOS, is of the "undisclosed sources" kind, and all the applications are preinstalled by Apple or come from Apple AppStore.

EU has asked Apple to open its smartphones to alternatives stores, threatening Apple with hundreds millions dollars fees; Apple has finally accepted, and removed any difficulty to use an alternative store from iOS 18.6. Of course, the security of apps installed from an alternative store is no longer managed/guaranteed by Apple.

Security is so under the strict control of Apple. Few is known about security weaknesses. Apple has no rewards program for researchers finding security weaknesses, while an Israel company pays for that and makes programs able to attack iOS, programs sold at very high cost to governments. Overall security seems very good.

Applications are strongly isolated, to the point that they cannot share anything (if you want to use Apple Music and VLC to listen music, you need to copy your music within both the applications directories).

iOS has some protection against tracking, cross applications tracking is just a setting to select, and Safari, the web browser, does include some tracking protection.

Ads seem to be displayed less aggressively in applications than in Android versions of the applications.

4.2) Protection against malware, ads and tracking in iOS

There is only one method that works system-wide: the use of a filtering DNS resolver (see Filtering DNS resolvers).

There is no equivalent of Personal DNS filter for iOS, and DuckDuckGo Browser for iOS cannot work as a tracking protection for applications.

The best two filtering DNS resolvers, regarding malware protection are:
"zero.dns0.eu", it protects against phishing (it does not answer to requests for websites less than one month old, which is the case for most phishing websites with a small life duration) and protects against homograph attacks by filtering fraudulent websites with Cyrillic characters,

"protective.joindns4.eu" and other filtering DNS resolvers from the joindns4eu family, it includes a database of more than twenty million malevolent websites. This database is continuously updated, AI is used to analyze the websites behavior.

If you want to use a filtering DNS resolver with malware and ads filtering, you should use:

- one of the protective DNS4EU resolvers, "noads.joindns4.eu", "child.joindns4.eu" or "child-noads.joindns4.eu",

- one of the Mullvad filtering DNS resolvers, "base.dns.mullvad.net", "extended.dns.mullvad.net", "family.dns.mullvad.net", "all.dns.mullvad.net",
- a tailored version of rethink DNS resolver, example with "Security Full" and "Privacy Aggressive" settings "1-6apx6ah77w4p7ug6snibagicimaqaaba.max.rethinkdns.com".

In order to set DNS resolver in iOS devices, you need a DNS profile; such a DNS profile can be downloaded for DNS0.EU, DNS4EU and Mullvad DNS from their websites (see the links in Filtering DNS resolvers).

Rethink DNS does not offer such a facility. You can generate a DNS profile from Secure DNS profile creator, https://dns.notjakob.com/.

Once you have the profile you need, you import it in your iOS device (send it by mail), install it in General Settings/VPN and device management, and validate it; it will be active in the "Restrictions and Proxies" section.

Browser: there is no need to use any other browser than Safari; because of Apple restrictions, Firefox for iOS is very poor, based on webkit (the same rendering engine as Safari), and has no extension. The only interest is in Firefox Focus, that can be used as a browser with "quick forget" and anti-tracking features; moreover, it can act as a content blocker for Safari.

You can install uBlock Origin Lite extension for Safari; once installed, give it the necessary permissions, set the level of protection and select the lists of filters.

You can complete anti-tracking features using Firefox Focus, and use a free version of Adguard or Adblock Plus as extra content blocker.

4.3) Other precautions on iOS

- It is recommended to shut down and restart periodically iOS devices, to remove memory persisting malware,
- as with any operating system, it is recommended to update it as frequently as possible (system and applications), for bugs and security fixes,
- enable localization, Bluetooth and Wi-Fi only when you need it,
- never connect to a public Wi-Fi spot,
- for each installed application, set its notifications and authorizations,
- disable Siri, globally and in each application setting,
- use the energy economy mode permanently, it prevents background applications working,
- set the cross applications tracking prevention,
- when possible, prefer to use the browser than a dedicated app (example: connect to Facebook with Safari, don’t use Facebook app),
- keep your system (iOS version) and apps updated.

4.4) VPN on iOS

The use of a VPN is possible on iOS. See General Settings/VPN and device management.

4.5) Anonymity on iOS

Tor Browser is not available from the Play Store, but you can use Onion Browser or Orbot and Safari on iOS (with reduced confidentiality protection because of Apple restrictions, memory is limited to 50 MB and this prevents to find long paths in Tor network).
Several messaging applications offer anonymity and full End-to-End Encryption. Avoid WhatsApp (undisclosed source), Telegram (encrypted up to the servers, nobody knows what happens on the servers), prefer Signal or, in France, Olvido.