

This guide aims to be a concise overview on information security for anyone in emancipatory struggles against structures of power. It represents assembled knowledge and best practices from personal experience, conversations with hackers and fellow activists, hacker conferences, and university courses on computer security and cryptography. Nonetheless, the best security is sharing skills with trusted people.

# ***AN ACTIVIST'S GUIDE TO INFORMATION SECURITY***



*Text originally published by the **Anarchist Black Cross - Dresden** in October 2016.  
Layout and minor typographical edits by **Sprout Distro** in November 2016.*



*For more zines and pamphlets, visit [www.sproutdistro.com](http://www.sproutdistro.com)*

This guide aims to be a concise overview on information security for anyone in emancipatory struggles against structures of power. It represents assembled knowledge and best practices from personal experience, conversations with hackers and fellow activists, hacker conferences, and university courses on computer security and cryptography. Nonetheless, the best security is sharing skills with trusted people.

If you have any corrections, questions or additions, please contact us at [abcd@riseup.net](mailto:abcd@riseup.net)

## Introduction

Technological progress has made it next to impossible to defend against a sufficiently powerful attacker (see [this](#)<sup>1</sup> for a scary example). Fortunately, most of us don't have the NSA hard on our heels, and local authorities are usually limited in their possibilities. The trick is to be sufficiently careful while staying functional.

This guide tries to point out the possibilities and their trade-offs. It is split into the following sections:

- **Security Culture** introduces the social side of things
- **Physical security** describes securing physical access to information
- **Traditional communication** is about the pre-Internet kind
- **Digital base security** discusses building a digital base to communicate from
- **Internet services** points out problems with and alternatives to common Internet communications services

## Security Culture

- **The need to know principle:** share information only with those who need it.
- Establish a culture where people realize when not to ask curious questions and don't take offense when information is not shared with them.
- It is not necessary to know who is in which group and participated in which action – don't brag about it and stop others if they do. You can't accidentally reveal something you don't know.

- Do not keep unnecessary information (e.g. meeting minutes) and keep your house clean of incriminating material (also: do not make pictures on action, not even pixelated ones<sup>2</sup>).
- Do not connect pseudonyms with their public information (e.g., if possible, do not store people’s activist email addresses with their name or group).
- Don’t let paranoia paralyze you: try to keep a realistic assessment of the threat model and don’t suspect people to be snitches just because they don’t conform to subcultural stereotypes.

## Physical Security

While few of our homes can successfully resist a police raid, measures can be taken to fend off fascist thugs or rouge state agents.

**Obscurity:** It can be useful to live at a place not registered as your official address, and without obvious subcultural symbols on the outside. Still, be prepared for sufficiently motivated forces of darkness to find and attack your home.

**Passive defense:** Protecting a home from the evils on the outside necessarily means forming an in-group. A reasonable front door and handpicked distribution of keys go a long way. Barred ground level and basement windows and anti-splinter films on the glass offer additional reinforcement.

**Active defense:** An alarm horn and a lighting system on the outside may mainly help against physical attacks, but they can also buy valuable time in case of a police raid.

**Process:** Have a short guide on dealing with police raids and your lawyers’ (mobile) numbers on the inside of the front door and next to the landline phone.

In some jurisdictions, having people’s private rooms marked with their name may help to argue against a search when it is only against one person. However, it obviously also reveals the inhabitants’ names to visitors and does only point out the existing legal situation to police who often ignore it anyway.

39. <https://wiki.immerda.ch/index.php/immerda:GnuPGIntroduction>
40. <https://ssd.eff.org/en/module/how-use-pgp-linux>
41. <https://ssd.eff.org/en/module/how-use-pgp-windows>
42. <https://ssd.eff.org/en/module/how-use-pgp-mac-os-x>
43. <http://schleuder2.nadir.org/>
44. <https://wiki.immerda.ch/index.php/immerda:NewSchleuderList>
45. [https://en.wikipedia.org/wiki/Skype\\_security#Eavesdropping\\_by\\_design](https://en.wikipedia.org/wiki/Skype_security#Eavesdropping_by_design)
46. <http://news.softpedia.com/news/ss7-attack-leaves-whatsapp-and-telegram-encryption-useless-503894.shtml>
47. <https://whispersystems.org/blog/contact-discovery/>
48. <https://unhandledexpression.com/2013/12/17/telegram-stand-back-we-know-maths/>
49. <https://news.ycombinator.com/item?id=6915194>
50. <https://whispersystems.org/>
51. [https://en.wikipedia.org/wiki/Signal\\_%28software%29#Metadata](https://en.wikipedia.org/wiki/Signal_%28software%29#Metadata)
52. <https://moxie.org/blog/we-should-all-have-something-to-hide/>
53. <https://moxie.org/stories.html>
54. <https://github.com/LibreSignal/LibreSignal/issues/37#issuecomment-217211165>
55. <https://yawnbox.com/index.php/2015/03/14/create-an-anonymous-textsecure-and-redphone-phone-number/>
56. <https://news.ycombinator.com/item?id=10500188>
57. [https://github.com/microg/android\\_packages\\_apps\\_GmsCore/](https://github.com/microg/android_packages_apps_GmsCore/)
58. <https://o9i.de/2015/10/23/howto-gmscore.html>
59. <http://www.einfachjabber.de/>
60. <https://ssd.eff.org/en/module/how-use-otr-linux>
61. [https://en.wikipedia.org/wiki/Comparison\\_of\\_VoIP\\_software](https://en.wikipedia.org/wiki/Comparison_of_VoIP_software)
62. <https://tox.chat/>
63. <https://jitsi.org/>
64. <https://ring.cx/en>
65. <https://wire.com/>
66. <https://wire.com/privacy/>
67. <https://palava.tv/>
68. <https://meet.jit.si/>
69. [https://en.wikipedia.org/wiki/Intel\\_Active\\_Management\\_Technology](https://en.wikipedia.org/wiki/Intel_Active_Management_Technology)
70. <https://mjpg59.dreamwidth.org/33981.html>
71. <https://libreboot.org/>
72. <http://mjpg59.livejournal.com/91123.html>
73. See Endnote “A” above.
74. <https://bits-please.blogspot.de/2016/06/extracting-qualcomms-keymaster-keys.html>
75. <http://blog.hansenpartnership.com/owning-your-windows-8-uefi-platform/>
76. <http://kroah.com/log/blog/2013/09/02/booting-a-self-signed-linux-kernel/>

## Links Mentioned in the Text

1. <https://www.cs.tau.ac.il/~etromer/mobilesc/>
2. <https://www.wired.com/2016/09/machine-learning-can-identify-pixelated-faces-researchers-show/>
3. [https://en.wikipedia.org/wiki/Lawful\\_interception](https://en.wikipedia.org/wiki/Lawful_interception)
4. <https://ferrancasanovas.wordpress.com/cracking-and-sniffing-gsm-with-rtl-sdr-concept/>
5. [https://en.wikipedia.org/wiki/Cell\\_site#Range](https://en.wikipedia.org/wiki/Cell_site#Range)
6. <http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz>
7. [https://de.wikipedia.org/wiki/GSM-Ortung#cite\\_note-3GPP43059-3](https://de.wikipedia.org/wiki/GSM-Ortung#cite_note-3GPP43059-3)
8. <https://en.wikipedia.org/wiki/U-TDOA>
9. [https://en.wikipedia.org/wiki/Short\\_Message\\_Service#Silent\\_SMS](https://en.wikipedia.org/wiki/Short_Message_Service#Silent_SMS)
10. <https://en.wikipedia.org/wiki/IMSI-catcher>
11. <https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector/wiki/Unmasked-Spies>
12. <http://www.cnet.com/news/fbi-taps-cell-phone-mic-as-eavesdropping-tool/>
13. [http://www.osnews.com/story/27416/The\\_second\\_operating\\_system\\_hiding\\_in\\_every\\_mobile\\_phone](http://www.osnews.com/story/27416/The_second_operating_system_hiding_in_every_mobile_phone)
14. <http://www.wthr.com/article/tapping-your-cell-phone>
15. <http://www.replicant.us/>
16. See Endnote “A” above.
17. <http://www.pcworld.com/article/2953052/security/most-android-phones-can-be-hacked-with-a-simple-mms-message-or-multimedia-file.html>
18. <http://www.linuxmint.com/>
19. <http://www.ubuntu.com/desktop>
20. <http://www.debian.org/>
21. <https://help.ubuntu.com/community/Installation/FromUSBStickQuick>
22. <https://www.youtube.com/watch?v=XKI024wUTUw>
23. <https://www.grc.com/misc/truecrypt/truecrypt.htm>
24. <https://launchpad.net/%7Estefansundin/+archive/ubuntu/truecrypt>
25. <https://veracrypt.codeplex.com/releases>
26. <https://veracrypt.codeplex.com/wikipage?title=Beginner%27s%20Tutorial>
27. See Endnote “B” above.
28. <https://www.engadget.com/2016/03/28/apple-s-encryption-battle-with-the-fbi-is-over-for-now/>
29. <http://www.howtogeek.com/141953/how-to-encrypt-your-android-phone-and-why-you-might-want-to/>
30. See Endnote “C” above.
31. <http://fusion.net/story/325231/google-deletes-dennis-cooper-blog/>
32. <https://www.systemli.org/en/friends.html>
33. <https://help.riseup.net/en/security/resources/radical-servers>
34. <https://riseup.net/en/better-web-browsing>
35. <https://www.torproject.org/>
36. <https://abcdd.org/en/english-security-guide/FIXME>
37. <https://ssd.eff.org/en/module/how-use-tor-windows>
38. <https://ssd.eff.org/en/module/how-use-tor-mac-os-x>

## Traditional Communication

With a reasonably safe home, let’s relax and see what our comrades were up to, shall we?

### Face to Face Communication

Modern technology enables the surveillance of the spoken word from far away and even microphone-unfriendly places such as swimming pools and concert halls can theoretically be surveyed with modern noise-canceling technology. However, taking a walk is still a fairly secure way of communication, when it is reasonably unlikely that hidden microphones are placed in clothes and accessories (that means no mobile phones, too!). If more security is needed, one can resort to writing on paper in a sight-protected place (e.g. under a blanket).

Closed rooms can be monitored even more easily, thus sensitive meetings in established autonomous centers, alternative house projects, lefty bars and the like are strongly discouraged!

### Letters

Hopefully you already figured that relying on the confidentiality of snail mail is a gamble at best. Code words are a last refuge for the imprisoned and desperate, but history has shown that relying on a secret method (e.g. swapping letters) alone to hide information is easily broken.

### (Mobile) Phones

Most importantly, all information (calls, texts, mobile Internet) exchanged via the (mobile) phone network should be considered captured by state agencies and potentially other enemies. They use ETSI wiretapping interfaces mandatory in all mobile network equipment sold in the EU (and thus available everywhere) ([source](#)<sup>3</sup>), but on top of that, other motivated actors can capture data in a local cell with a few hundred Euros worth of equipment ([source](#)<sup>4</sup>).

### Phones Themselves are Identifiable!

The second most important thing to know is that mobile phones have a unique IMEI number, that identifies it in the mobile network. Normally the information about your IMEI is registered in operator network together with SIM card, that means when you put a new SIM card into your old phone, it can be easily linked to your old SIM card. So for a safe phone, both SIM cards and phones need to be acquired and swapped in a way that does not link them to any other information, i.e. by buying phones with cash and getting pre-registered SIM cards or registering

them anonymously in the network, for example via TOR (see below).

## Location Tracking

To work, mobile phones regularly contact the *base station* they are booked into, which locates the phone within a minimum of about 400m from the cell tower in urban areas ([source](#)<sup>5</sup>). This information is routinely stored by mobile carriers and therefore available without prior targeted surveillance ([source](#)<sup>6</sup>). For users of centralized location services (like Google Maps), the police may be able to obtain extremely accurate long time location profiles from the provider ([source](#)<sup>7</sup>).

With targeted surveillance, triangulation and querying data from the phone can locate it down to 50m ([source](#)<sup>8</sup>), or even 5m with a GPS-equipped phone ([source](#)<sup>7</sup>). To get a more time-accurate location profile, state agencies may use so-called stealth pings / silent SMS to make a mobile phone contact its base station more often ([source](#)<sup>9</sup>).

As a last resort, police can use so-called *IMSI-catchers* which pretend to be the strongest network cell available, and then record what phones book into them, potentially even recording calls and text messages ([source](#)<sup>10</sup>, [some real-world examples](#)<sup>11</sup>).

Police have been known to use geodata on all kinds of incidents and extended cell phone surveillance of 10s of people on the most ridiculous accusations, or even deploying IMSI-catchers on sit-ins against fascist marches, so the technical possibilities are not to be taken lightly.

## Room Surveillance / “Silent Calls”

Much controversy exists as to whether it is possible to tap mobile microphones even when no calls are going on. [This](#)<sup>12</sup> article hints the FBI has done it, while [this](#)<sup>13</sup> research hints it would be built-in functionality. Our *guess* is that this at maximum used against high profile targets, because if any hicksville cop shop was able to use that, the evidence of it would be better known by now. Besides sneaky network attacks, smartphones have been surveyed by malicious apps ([source](#)<sup>14</sup>).

Open source mobile OSes (like *Replicant*<sup>15</sup> for Android devices) offer no protection against those attacks, because there is usually a direct connection from the microphone to the (always closed source, as to comply with regulations) baseband firmware and it can not reliably be powered off. To make matters worse, mobile phones without SIM card might still pre-register to the strongest network (for emergency services), and there is no way to check if “offline/airplane mode” is actually what it promises to be.

To err on the side of caution, it is advisable to leave your phone at home when

- have meetings in inconspicuous locations without mobile phones
- put Linux on your computer and encrypt your data, learn to use PGP for inter-group email and build a network of Jabber contacts with verified OTR encryption for ad hoc chats
- learn to use TOR safely
- share skills, teach each other and don't panic

## Endnotes

A) Technical background: most Intel-based computers run a software that can control the system remotely in parallel to the normal Operating System ([AMT](#)<sup>69</sup>), which can be “disabled” in the manufacturer’s firmware but that is closed source, and modern Intel Processors only boot with signed firmware ([Intel Boot Guard](#)<sup>70</sup>), so you will never be able to use alternative firmware like [Libreboot](#)<sup>71</sup>, and even if you could, there would still be [things in your computer that you do not have the source code for](#)<sup>72</sup>.

B) [This security analysis](#)<sup>74</sup> illustrates quite well that even without any malicious intent, mobile devices as commonly used are just not very secure.

C) The only way to prevent this to sign the unencrypted data and let some trusted part check the signature. This can either be done using a TPM, or more readily by using SecureBoot and trusting your manufacturer’s firmware (which is what modern Linux distributions do). Some pointers: [1](#)<sup>75</sup>, [2](#)<sup>76</sup>

exists as a pretty okay encryption method. However, some caveats apply:

1. The fact that two people are communicating is not concealed, therefore use pseudonyms not linked to other activities.
2. OTR commonly uses an authentication system based on things only the other person knows. It is important to make use of it to be sure you're actually talking to the right person. Otherwise if the dark side manages to intimidate your Jabber provider they could pose as your friend/comrade.
3. Files sent via Jabber are not encrypted with OTR.
4. Audio and video chats in Jabber clients are not encrypted by default.

[einfachJabber.de](http://einfachJabber.de)<sup>59</sup> has an elaborate German introduction and guides for all kinds of devices and operating systems. English language tutorials can be found at the EFF's Surveillance Self-Defence guide ([Linux](#)<sup>60</sup>, [Mac OS](#)<sup>38</sup>, [Windows](#)<sup>37</sup>).

## Voice / Videochat

There are several solutions that are Open Source software, available for multiple computing platforms and offer end to end encryption of audio and video ([overview](#)<sup>61</sup>). If you can live with the disadvantages, [Signal](#)<sup>50</sup> seems to be the most practical solution for mobile platforms.

On laptop/desktop computers, if you can get it to work, **Tox**<sup>62</sup> is a pretty amazing, high security and low effort alternative. More traditionally, **Jitsi**<sup>63</sup> enables encrypted calls via either a *SIP* or better yet, a Jabber/XMPP (see above) account. **Ring**<sup>64</sup> seems to be another promising alternative (that we haven't tried yet), and **Wire**<sup>65</sup>, while also centralized, seems to offer an alternative to Signal that does not need phone numbers or Google services and makes some bold [privacy claims](#)<sup>66</sup>.

A more ad-hoc method involves a technology called *WebRTC* just requires a modern web browser like Firefox or Chrome, with the caveat of trusting some central web site to not be malicious (and the connection to that network not to be manipulated). **pavala.tv**<sup>67</sup> and **meet.jit.si**<sup>68</sup> are two open source based web services for that.

## Wrapping it up

If this has gotten your head spinning, here is the bottom line.

*TL;DR:*

- do actions with people you trust, be honest with them but don't gossip and brag and don't keep more information than necessary
- separate your activist and your bourgeois life's Internet identities as much as possible

visiting a sensitive meeting, or at least take out your phone's battery a good couple of km from the meeting point, because the attendants, (cell tower) location, time and duration of a sensitive meeting can easily be spotted by 30 people switching off their phones simultaneously. Especially when meeting with small groups in densely populated areas, it might be as good to simply put the powered on mobiles in a location outside hearing distance (the fridge two rooms away, for instance).

It should be noted that mobile phones transmit power status (idle, running) during operation and send goodbye messages to the network when powered off properly (so that creates a different pattern than just ripping out the battery).

## Digital Base Security

Traditional means of communication don't feel so good anymore, so what about the Internet? First we need to find a secure device that we can use it with. When it is about information, security is classically divided into integrity, confidentiality and availability. Let's see what they mean.

### Chose your Computing Device (integrity)

*None of today's common devices are completely under your control.* Laptops and desktop computers come with obscure low level software ("*firmware*") that is controlled by the manufacturer. ([A](#))

The same is true for tablets; and smartphones are even worse, because they are always also controlled from the mobile network ([source](#)<sup>13</sup>). On top of that, smartphones are complex computers which often are not treated to security updates by their manufacturers, making them an easy target for attacks ([source](#)<sup>17</sup>). Moreover, they are designed to collect crazy amounts of information on people by default – information that is more often than not readily available to state agencies with or without request.

Therefore **the use of smartphones for activist work is strongly discouraged**, as even the security of alternative Internet services like Jabber/XMPP is greatly diminished on the vast majority of mobile devices.

But don't despair, running as much *Free and Open Source Software* as possible on your computer gives you a good deal of control back. With proprietary software like Microsoft Windows or Apple's Mac OS, chances are they will support law enforcement in their effort to "fight crime" and break into your computer. With

Linux or any other open alternative, the program code is exposed to a whole community, making it much harder to mess with.

There are many different bundles of the Linux core with various open source software called *distributions*, of which we recommend two specifically:

- *Linux Mint*<sup>18</sup> offers one of the most painless ways to get an open system with many probably familiar software like Firefox, VLC player, LibreOffice etc. They offer different *Editions* of which *XFCE* is a simple, fast desktop that still runs well on old computers and *Cinnamon* is a bit more fancy.
- *Ubuntu Linux*<sup>19</sup> is the base for Linux Mint and a company effort to build a user friendly version of Linux. It is itself based on one of the oldest community distributions, *Debian*<sup>20</sup>. While the company behind it decides its direction, it still has a very strong community around it.
- *Installation*: Make sure to save all your important data on some *external* medium (hard drive or stick) and get support from a computer geek if you can. It is usually possible to install Linux next to Windows, but **expect the installation to overwrite everything**. To get you started [here is a guide to install Ubuntu from a USB drive](#)<sup>21</sup> that should also work with Linux Mint if you just download their files, [and here is a video how to to install Linux Mint](#)<sup>22</sup> But first read the next paragraph...

## Storage Encryption (confidentiality)

Encrypt your computer! All further advices for software and communication means are not safe if your computer is not safe.

**The encryption is intended against offline attacks only, if the police captures your computer unlocked, they will just copy your data.** A screen lock or suspend mode with a decent password is better than nothing, but the device should be powered down whenever possible.

**So if the police knocks your door, first run to your computer and press the power button until it switches off.**

There are three major ways to encrypt your data:

### Encrypt your Home Folder

*Use this if unsure*: only your personal data gets encrypted (including Firefox Bookmarks etc.), but the rest is not.

In order to figure out who of your contacts uses the same application, the apps generally require uploading information on *all* of them to their servers ([source](#)<sup>47</sup>), but they do so in various degrees from grabbing the whole address book to just uploading an obscured form of the phone numbers. **The privacy implications of this for activist are huge, because one person uploading an anonymous number with the person's real name will ruin their effort.**

**WHATSAPP** is by far the most successful mobile messenger to date, and recently they too claim to support “end to end” encryption (everything is encrypted between you and the people you talk to). However, because the source code to their programs is not open, there is no way to check if there is a secret master key for law enforcement. Even if there is not, they can still disclose who you are communicating with and when.

Basically the same holds for **THREEMA**, as their software is not Open Source either.

**TELEGRAM** has convinced many boasting with their altruism. They *do* provide the source code of their client, but their encryption is outdated techniques from the 70ies ([source](#)<sup>48</sup>), needs to be enabled manually and does not work for group chats. On the other hand, they *do* go all inclusive when they just grab your address book, unlike others not just number but with names ([source](#)<sup>49</sup>).

Now, **SIGNAL**<sup>50</sup>. They are *a lot* more privacy minded than the rest of the phone number based messenger crowd. Whilst they still technically get to see all the patterns of communication (but not the content) ([source](#)<sup>51</sup>), at least their founder comes from a more trustworthy background ([source](#)<sup>52</sup>; and he has some pretty funny [stories](#)<sup>53</sup>, too). Still, the system is centralized and while the clients are Open Source, they maintain tight control over their network. Signal is only available on Android with Google Services / Google Play and iOS and Signal's inventor actively asks alternative software to leave the network ([source](#)<sup>54</sup>). People find elaborate ways to get around the need for a phone number ([guide](#)<sup>55</sup>) and make Signal work without Google Services ([1](#)<sup>56</sup>, [2](#)<sup>57</sup>, [3](#)<sup>58</sup>). Altogether this makes Signal a good choice for people who use Google-enabled Android or Apple smartphones anyway, but better tools exist for people who need more security than mobile platforms provide.

## Jabber / XMPP

Enter **Jabber / XMPP**. *Finally, you made it!* **This is what we currently recommend for sensitive real-time communication.**

Similarly to email, people from many different service providers (see the alternative tech collectives above) can talk to each other. Also similarly to email, per default Jabber offers only very weak encryption. For actual messages, *OTR*



## Email

Email is like postcards, assume it is read by transport providers and state agencies. PGP is a way to encrypt (wrap your postcard) email contents, but be aware that the email subject and the fact who is communicating when, with whom and from which computer, are not concealed.

Immerda.ch has is a nice German introduction into how PGP works [here](#)<sup>39</sup>. PGP depends on *keys* (special files that are protected with a password) that, like physical keys, should restrict access to information. Therefore PGP's security depends on a safe key exchange; so make sure you got the right key, e.g. by getting it in person from the recipient.

The Electronic Frontier Foundation's Surveillance Self-Defence guide has a pretty good howto for using PGP ([Linux](#)<sup>40</sup>, [Windows](#)<sup>41</sup>, [Mac OS X](#)<sup>42</sup>).

## Mailing Lists

Now if PGP encrypts messages between two people, what about mailing lists? If there is just a small group, people can exchange PGP *public* keys and then everybody can encrypt their message so that every recipient can read it. Unfortunately, this gets messy quickly if new people join the list. Therefore, people came up with a solution that is not as secure, but better than nothing:

*Schleuder*<sup>43</sup> is a mailing list software that gets its own PGP pair. Everybody then encrypts email to Schleuder's mailing list key and Schleuder decrypts the message, and encrypts and sends it to each list member separately. Of course the downside is that whoever is running Schleuder could get hold of Schleuder's PGP private key and read the encrypted messages. Yet, as Schleuder is a complex beast, it is recommended to use it from a tech collective you trust, like for example [Immerda.ch](#)<sup>44</sup>.

## Messengers / Chat

TL;DR: don't use the rest and skip down to **Jabber** below

**SKYPE** has a reputation for being encrypted, however they have publicly stated their ability and willingness to hand out information to law enforcement, which they do in required cases. All your written text are stored on the servers of Skype and can be accessed by police ([source](#)<sup>45</sup>).

For quite awhile, mobile messenger apps based on phone numbers have been gaining popularity. If you consider using any "secure" messenger on a mobile device, be [reminded](#)<sup>46</sup> that communication through the mobile network is vulnerable to eavesdropping and manipulation.

### *Advantages:*

- The computer pretty much works as normal and your personal files are still very safe.

### *Disadvantages:*

- You should use a long user password, which you will need to type each time the screen is locked
- It is possible to manipulate your programs (e.g. Firefox, GPG) so they reveal your passwords etc.
- How to: during Linux installation, select "Encrypt my home folder" when creating your user

## Encrypt the Whole System

This means that only a tiny part of your hard drive remains unencrypted and everything else – your programs, etc. – is.

### *Advantages:*

- It makes it harder e.g. to put a bad version of Firefox or GPG on your computer
- You can use one long strong password just for starting the computer and a shorter for your screen lock

### *Disadvantages:*

- You need to start the computer, put in the password and then wait for it to come up
- You need to remember two passwords, and the disk encryption password is harder to change
- How to: during Linux installation, at *Installation type* select "Encrypt the new (Linux Mint/Ubuntu) installation for security"

## Use an Encrypted Container

An external drive or a very big file ("container") is encrypted and you need to unlock / put files in and out / lock the encryption separately

### Advantages:

- Can be used to transfer files between encrypted computers
- Can be used on external hard drives
- Can be used on Windows and Mac OS
- Can be used as additional secure place that is normally closed on an already encrypted Linux
- Has special features to so that a fake password can show fake files, if you are forced to give a password

### Disadvantages:

- All kinds of temporary files from LibreOffice, Thunderbird email, Firefox surfing profiles etc. are not encrypted
- Needs to be opened and closed separately

How to: get [Truecrypt](#)<sup>23</sup> ([Linux install](#)<sup>24</sup>) or [Veracrypt](#)<sup>25</sup> and follow the [howto](#)<sup>26</sup>

## Android and iOS

While mobile platforms are still not recommended for sensitive data (**B**), some protection is better than none, and turning on encryption for your personal data will at slow down the cops (but remember [FBI vs. Apple](#)<sup>28</sup> and especially their general cooperation).

- [Howto for Android](#)<sup>29</sup>

## Limitations

Your password prompt must come from somewhere and so there's always unencrypted data on your device, data that can be messed with (e.g. replacing your Linux' password prompt with one that sends the password to the police). This can be made harder with some tricks (**C**), but remember that the most realistic scenario is a simple police raid.

## Backup your Data (availability)

If it comes to a police raid (or a simple break-in), an oh-so-amazingly encrypted device will still be taken by the police. To take some of the pressure off yourself, **regularly** stash encrypted copies of your data outside your home, ideally with people that are not relatives nor active in the same groups.

While we are at it, even public data should not be trusted to IT corporations, as they might just [delete](#)<sup>31</sup> or accidentally lose it.

# Internet Services

So by now we can use a well-secured Laptop behind our locked door to write lengthy security guides, but how do we actually talk to people in a secure way?

Besides the technical aspects below, using alternative service providers offers an additional degree of protection, such as storing data encrypted and refusing to cooperate with the police. A list of alternative tech collectives can be found [here](#)<sup>32</sup> and even more [here](#)<sup>33</sup>.

## A word about Web Browsers

Web browsers like Mozilla Firefox or Google Chrome are complex monsters and a lot of web sites out there track their visitors. The Riseup Collective has a compact [guide](#)<sup>34</sup> how to use a browser more securely.

## Anonymity

The whole point of the Internet is to connect two computers, like yours with... say *Youtube*. Now for the cat videos to find their way back to you, obviously the computers on the way (*routers*) need to know the Internet address of your connection. The trouble is that if any computer on the way is surveyed by the state or you access an evil web site like e.g. that of the police, they could track that Internet address back to your physical place, or connect it with other online activity you were doing (like accessing your web mail). There are two ways to avoid this, which for additional security should ideally be combined with each other:

**The first** is simply to use public wifi in places where there are no surveillance cameras. Unfortunately, your computer's wifi has a unique *MAC* address. It can be changed with software in case the wifi stores them (some corporate portals will, to tell if you already acknowledge the Terms of Service, or used up your hour of free Internet), but for a start just also use method number two:

**The second** method is to use a software called *TOR*<sup>35</sup>, or *The Onion Router*. In a nutshell, it works by sending your data in 3 layers of encryption (hence the "onion") over three computers (*TOR nodes*), where the first knows your Internet address and the second node to contact (but not the destination), the second knows nothing (only which the third node will be), and the third node knows the destination, but not the origin. There are some subtleties to use it securely so best follow the guides ([Linux](#)<sup>36</sup>, [Windows](#)<sup>37</sup>, [Mac OS X](#)<sup>38</sup>) and strictly only use the TOR Browser when doing anything sensitive.