The Bare Minimum

PAUSE – an IT security guide

Timber

May, 2026

Contents

1 Introduction

There are *a lot* of IT security guides out there. However, almost all of them have one thing in common: They're incredibly outdated. This is because the world of computers and phones, and thus of IT security, is evolving so quickly, that basically as soon as an IT security guide is released, it's already out of date.

However, I believe there's some common ground, the *bare minimum* that's recommended that doesn't change quickly. This is not enough for everyone and depending on the threats your facing, you should definitely do further research. But I believe that *everyone* should implement the following five recommendations – and convince friends and family to do the same.

To aid your memory, I arranged the recommendations to build the acronym *PAUSE* (use a **P**assword manager, use an **A**d blocker, regularly install **U**pdates, use **S**ignal and **E**ncrypt your data). You really should PAUSE everything you're doing (especially with computers / phones) and implement those five recommendations first.

Who am I to talk about this? Good question and please, don't blindly trust me. Use your head to check if the recommendations make sense and do further research if you're unsure. Good places are for example esc-it[1] or EFF.[2] Such places are also the sources for my knowledge on the topic, in addition to my experience working as a software engineer and my own tinkering.

Some things in this guide are simplified, but I always attempt to simplify without decreasing the security.

[1] https://esc-it.org/en/
[2] https://ssd.eff.org/

2 *P*: Use a password manager

Everyone knows they should use secure passwords (and different ones for each account), but most people don't use secure passwords anyways. Be it because it's hard to remember different randomly generated passwords for each service or because it's annoying to enter them manually.

Both problems get solved with a password manager: You only have to remember one password (in addition perhaps to your encryption password; see chapter 6) which unlocks your password database, containing all your other passwords. It's a bit of work changing the passwords on all your accounts to an automatically generated one that's stored in your password manager, but once you did the work you'll never want to go back. It's more convenient *and* way more secure.

There's different options for password managers, the most notable ones being KeePass[1] and Bitwarden[2]. KeePass doesn't automatically synchronise the database between different devices, so while it's open source and a bit safer than Bitwarden, Bitwarden is definitely the more convenient option. Both can be used for free.

For KeePass I recommend KeePassXC[3] on your computer and KeePassDX[4] on your phone. You can synchronise the database for example with Syncthing[5], but that's a bit more advanced and not the *bare minimum* anymore.

Bitwarden also has apps and browser plugins and should be quite intuitive to set up.

[1] https://keepass.info/
[2] https://bitwarden.com/go/start-free/
[3] https://keepassxc.org/
[4] https://www.keepassdx.com/
[5] https://syncthing.net/

3 *A*: Use an ad blocker

Using an ad blocker is not only a way to get rid of annoying ads, it also increases your security and privacy in the internet. Security because some ads are malicious and privacy because some ads track you. Whilst the increase of security is not huge (not only ads can serve malicious content), I definitely find it worth it because it also increases the usability of the internet significantly.

On your **computer** you can install the extension uBlock Origin[1]. It's available both for Firefox and Chrome (for Chrome only in the *lite* version though) and blocks ads and trackers very reliably.

On your **phone** you can either also install uBlock Origin (if you use Firefox mobile), or set up a specific *DNS* server. This sounds scarier than it is and also blocks most ads and trackers. You can change the DNS server in your phone settings to block ads in all apps. There's various options for ad blocking DNS servers, I like DNS Forge[2].

For **iOS** you can download the profile (e.g. from DNS Forge[3]), open the settings app, tap on `Profile Downloaded` and then on `Install`.

For **Android** go to your settings, then to `Network & Internet` and then `Private DNS`. Select `Private DNS provider hostname` and enter e.g.
`dnsforge.de` if you want to use DNS Forge.

[1] https://ublockorigin.com/
[2] https://dnsforge.de/
[3] https://dnsforge.de/dnsforge-dot.mobileconfig

4 *U*: Regularly install updates

You should regularly install (security) updates. This is because often security vulnerabilities get fixed in updates and then publicised. So if you don't install the update, there's basically a manual online on how to hack your device / system / app.

For regularly installing updates you should enable automatic updates wherever possible. This applies to your apps / installed software as well as for your operating system itself (so for example your Android / Linux / Windows etc.). If there are no more updates available because your device is too old, you should consider getting a new device (as annoying and sad as it is out of a climate justice perspective) or (if you're more advanced) installing LineageOS on your Android phone or Linux on your Windows computer. This is not the *bare minimum* anymore though.

5 *S*: Use Signal

If you communicate with others, this communication should be securely encrypted. If it isn't encrypted it's possible to eavesdrop your private communication. If it's not *end to end* encrypted, the operator of the service might still eavesdrop your communication. To communicate end to end encrypted it almost always makes sense to use Signal.

All you need to do to use Signal is download it from your app store and go through the steps of signing up. It's just as easy as using WhatsApp.

Of course to use Signal your contacts also need to use Signal. So this is also a great opportunity to convince your friends and family to use Signal as well.

5.1 Why Signal?

There are a few other options that come to mind:

- **Telegram**: Telegram is not (end to end) encrypted by default. That means that Telegram can read all your messages. Signal is always end to end encrypted.
- **WhatsApp**: WhatsApp uses Signals algorithm and thus uses strong encryption. However it's not open source, so you can't know if WhatsApp has a back door through which it still reads your messages. Signal is open source.
- **Mails**: While you can (end to end) encrypt mails, it is tricky to do so. And even if you manage, it's still way less secure than Signal: If your private key ever gets leaked, all your mails can get decrypted. This is not the case with Signal (keyword *perfect forward secrecy*).

- **Phone calls**: Phone calls outside of an app like Signal aren't encrypted. Thus if the wire is tapped, adversaries can listen in. Calls in Signal are encrypted.
- **Something else**: There are other options (like *Matrix* or *Briar*) but they rarely make sense since they're way harder to use. In specific use cases also something like *Mattermost* might make sense, but the default should always be Signal.

5.2 Understanding Phishing

While Signal itself is very secure, your security can be compromised if you get tricked into giving adversaries access to your account. This process is called *Phishing*. Signal itself has a great FAQ[1] on the topic, but the most important take away is: **Signal support never contacts users directly**. Especially not to ask for verification codes, recovery keys, or payment details. If you receive a message on Signal stating to be from the Signal support or similar, *this is a phishing attack*. Do not reply and instead report and block the account.

[1] https://support.signal.org/hc/en-us/articles/9932566320410-Staying-Safe-from-Phishing-Scams-and-Impersonation

6 *E*: Encrypt your data

All the data stored on your devices (so called data *at rest*) should be encrypted. So for example if you save a picture on your phone, this picture is data at rest. It should thus be encrypted.

Why? Because otherwise adversaries can access your data even if the device is locked. Often it's as easy as plugging your storage drive into another computer.

Data is most typically at rest on our computers and on our phones. Additional places include external drives and cloud services, but this goes beyond the *bare minimum*.

Generally it's crucial to understand that your data is only really encrypted **when your device is powered off**. This is because your encryption key is stored on your device as long as it's powered on, so that you don't have to constantly enter it. That means that you need to turn your device off completely (locking it is not enough) for the encryption to take effect.

The encryption password should be automatically generated (e.g. with your password manager (see chapter 2) or the Bitwarden online tool[1]), contain lower- and uppercase letters and numbers and it should be at least 8 characters long. Ideally it's 12 characters or longer, but that's beyond the *bare minimum*. Even better is a passphrase with 6 or more words (also automatically generated, e.g. on Bitwardens website), but this also takes more time to enter (but has the advantage of being easier to remember).

6.1 On your phone

Android If you use Android and your phone runs Android 10 or newer (this is the case for at least all phones released in 2019 or later), it is automatically encrypted. That applies to 99% of all

[1] https://bitwarden.com/password-generator/#password-generator

Android devices. If you're Android version is older, you can check your settings if there's an encryption option nevertheless.

iOS If you use **iOS** it's even more likely your phone is already encrypted: iPhones are automatically encrypted since iOS 8. So if you updated your iPhone at least once since 2014, it should be encrypted.

Both for iOS and Android the encryption key (i.e. the password used for encrypting your data) is the normal code / password you use to unlock your phone. If you have a biometric unlocking method (so your fingerprint or face), you always *also* have a password as second method. This password is then your encryption password. Remember the password requirements from above.

6.2 On your computer

Linux If you use Linux you should activate encryption (ideally *full disk encryption*) while installing the operating system. If you didn't do this, you can still encrypt your `/home` folder, but it's not trivial – see for example this howtogeek guide[2]. Activating full disk encryption (meaning that all the files are encrypted, not just the ones in `/home`) after installing is very hard; it's probably easier to just reinstall Linux.

If you just encrypt your `/home` folder your encryption key is your normal device password and the `/home` folder gets decrypted automatically once you log in. If you encrypt your whole disk you can chose a separate encryption password and have to enter it while your device is booting.

[2] https://www.howtogeek.com/116032/how-to-encrypt-your-home-folder-after-installing-ubuntu/

Windows If you use an up to date Windows you can set up the encryption by following these steps:[3]

1. Sign in to Windows with an administrator account
2. In the Settings app on your Windows device, select `Privacy security` > `Device encryption`
   Note: If Device encryption doesn't appear, it's either unavailable on your device, or you might be signed in with a standard user account.
3. Use the toggle button to turn Device Encryption `On`
4. Your normal Windows password is now also your encryption password; you probably won't notice any difference

If this is not available for your computer, you might still be able to encrypt your device with BitLocker – see for example here.[4] Using BitLocker directly also has the advantage that your encryption key doesn't get uploaded ("backed up") by Microsoft, which might be undesirable. But again, this goes beyond the *bare minimum*.

Mac If you use a Mac, chances are it's already encrypted. Either way you should check and otherwise activate it by following these steps:[5]

1. On your Mac, choose Apple menu > `System Settings`, click `Privacy & Security` in the sidebar, then click `FileVault`. (You may need to scroll down.)
2. Turn on FileVault. You might be asked to enter your password.
3. Choose how to unlock your disk and reset your login password if you forget it:

[3] https://support.microsoft.com/en-us/windows/device-encryption-in-windows-cf7e2b6f-3e70-4882-9532-18633605b7df

[4] https://support.microsoft.com/en-us/windows/bitlocker-drive-encryption-76b92ac9-1040-48d6-9f5f-d14b3c5fa178

[5] https://support.apple.com/en-gb/guide/mac-help/mh11785/mac

- *iCloud account*: Click “Allow my iCloud account to unlock my disk” if you already use iCloud. Click “Set up my iCloud account to reset my password” if you don’t already use iCloud.
- *Recovery key*: Click “Create a recovery key and do not use my iCloud account”. Write down the recovery key and keep it in a safe place.

The encryption password should be the normal password used to unlock the computer.

7 Final thoughts

As already mentioned, this is just the *bare minimum*; there's a lot more you can do. If you implement those steps, you're on a great way to defend yourself against a lot of untargeted attacks. If you suspect that someone is trying to attack you personally (meaning that they target you directly), especially if it's a state level actor, you'll need to do a lot more (or less, the safest way is always to not use digital technologies at all). I would start by reading about threat modelling[1] and finding solutions to the specific threats your facing; this is not the *bare minimum* anymore though.

Also remember that your IT security significantly depends on the IT security of your contacts: If the phone of your friend you chatted with gets compromised, the messages are leaked even if you took great security precautions. So talk about it with your friends and family, convince them to also implement those five steps and point them to this resource you're reading.

[1] https://ssd.eff.org/module/your-security-plan