DIGITAL SECURITY PROTOCOL

a basic safety guide for everyone

internationalistcommune.com

Digital Security Protocol

a basic safety guide for everyone

internationalistcommune.com

Digital Security Informative Protocol

We use our phones, tablets or smartphones as well as our computers and our cameras every day. Therefore, our security when using them is a very important topic we have to confront ourselves with. Especially for people who organize and fight against the capitalist system, security and self-defense are essential topics that should equally be taken into consideration on the digital level. With the use of such devices on a daily basis we can become vulnerable to the state or to anybody who would want to harm us. When we receive a call, when we use the internet, when we send messages, we leave digital traces the enemy can then use against us. **This protocol is intended to present the main threats and propose solutions with resources to adapt and protect yourself in good ways.**

Digital Security for what?

In the topic of digital security, it is important to ask a few questions so that we can understand the reason why certain steps have to be taken for our protection and what impact they have. This way we can prevent to become either paranoid or an easy target to the enemy. The following questions are therefor important for us.

Why is it important to take care of our security?

Protecting yourself, your devices, phone and computers means at the same time protecting your comrades, your collective or your organisation. Cyber security is not an individual issue and we are responsible not only for our security but those of our comrades as well.

What information do I want to protect?

My identity, my research on the Internet, my activity on social networks, in general my location or my presence in a certain place, my communications, information channels, internet publications...

From whom I want to protect myself, from which enemies?

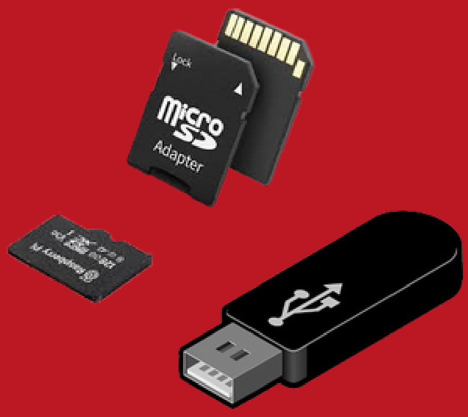
Unknown people, state intelligence services, other states, bankers, hackers, judicial police services, thieves, my mobile operator or my internet service provider, etc. ...

What types of attack?

When the enemy has direct access after having seized my phone by search, when the enemy is looking for me on the Internet, when an enemy tries to hack my computer, when my enemy asks for information from my telephone operator etc. ...

We want to understand all this better. So let's start with the usable traces that we leave on our devices (telephone/computer) and then we can have a look at those during our internet connections. For this reason, we will look at how we leave traces on computers and what kind of operating systems (software that manages a computer's hardware and applications) there are and how they are different from each other in matters of security and use. We will do the same for phones and we will have a look at the reasons on why and how to use VPN (Virtual Private Network). We will understand what kinds of attacks by the enemy there are and how we can protect ourselves against them as well. This means we will also present ways of secure use and good practices for the devices that we work with on a daily basis, to you.

Computers



<u>On computers we leave usable traces when:</u>

- We stock files (videos/photos/sounds/documents …) on a hard drive (internal or external), on USB keys, and on SD Cards

- We connect to the Internet to go to websites, use connected applications (messaging, emails, gaming applications and digital media applications like Instagram etc.), download files (photo/video/sound/document, etc.)

Operating Systems

An Operating System plays a very important role. It is responsible for making all the parts of the computer like memory, processor, storage work together. Also the Operating System translates the computer language into a language that we can understand. A computer without an operating system is useless. Softwares can be understood as a facilitator to carry a task in the computer. So for example, if you need to send a message, you can install a application that send messages. The software is this application. The term software is used to differentiate it from the hardware-i.e., the physical components of a computer system.

There are different operating systems, not all of them have the same features. Some of these operating systems are open source operating systems. This means that it is developed collaboratively and open for anyone to use it, change and distribute it.

- Windows:

Windows is an operating system developed by the company Microsoft, which collaborates with state services around the world. It can be useful for using private content creation software (like Adobe Photo-shop, Adobe Premiere, Sony Vegas Pro, etc.). But it is impossible to know how the computer data is processed by the company. It is not Open-Source, it does not provide its algorithms, its sources and does not allow the hard drive to be secured, it is quite easy to break the password and to break into your data. As a capitalist company, it can sell information of its users to states (such as Turkey) in exchange for making its services accessible in these countries.

- macOS:

It is an operating system developed by the company Apple Inc. As well as Windows it is impossible to know how your computer data is processed by the company. But it is as well useful for using private content creation software (Adobe Photo-shop, Adobe Premiere, Sony Vegas Pro, etc.). It does not provide its algorithms (its sources) and does not allow the hard drive to be secured. It is difficult to break the password and to break into your data. Apple states that they don't sell personal data to third parties. As anti-capitalist forces we still have to take precautions and should not believe any of these companies.

- Linux:

It is an open source operating system that has several available versions (for example Debian, Ubuntu, etc).

It was developed by Linus Torvalds and is based on Unix operating Systems.

It is not compatible for using private content creation software (Adobe Photo-shop, Adobe Premiere, Sony Vegas Pro ...). But there are all kinds of open source applications for Linux that can be used for private content creation as an alternative and any other works like communication etc. in a secure and private way available. All algorithms (its sources) are accessible in lines and regularly checked by people around the world. It is possible to securely encrypt the hard drive, and any other storage system. With a strong password, it is (very) difficult to break into your computer. That means that it is very expensive in time and energy, and therefore in money for an enemy who wants to take your data. In addition, many applications useful for data cleansing and navigation (detailed later) are pre-installed. It is the most effective of systems to avoid malware and viruses. For these reasons, it is recommended to use them instead of Windows/MacOS.

Find out more:
https://ubuntu.com/download/desktop
https://www.linux.org/pages/download/

- TAILS (The Amnesic Incognito Live System):

TAILS was developed to ensure a high level of safety and anonymity when browsing the Internet and filing storage. This is a live system. This means you can install it on a USB key or SD Card, and use it on all computers (but not on Macbooks), without using the original computer system (Windows/ Linux...). Therefore you leave no traces unless you want to do so. Its amnesiac (it looses all memory) function allows you to keep nothing on the computer. It connects to the internet by the TorBrowser. It is recommended by most Whistle Blowers (a person revealing information about activity within an organization) and was financed by the Tor Project (https://www.torproject.org/). Based on a Linux structure, with a good pass sentence, it is (very) difficult to break the password.

You will find the TAILS documentation and instructions for installation here: https://tails.net/

Phones

On a phone/ tablet, we leave usable traces when:

- We communicate by SMS/Call (via a telephone operator)
- We take photos/videos/sounds
- Location applications are used
- We stock files (videos/photos/documents) on the phone or mini SD Card
- We connect to the internet to go to websites, use connected applications (messaging, emails, etc.), download files (photo/video/sound/document ...)

Different phone operating systems exist, not all of them allow the same possibilities:

- iOS:

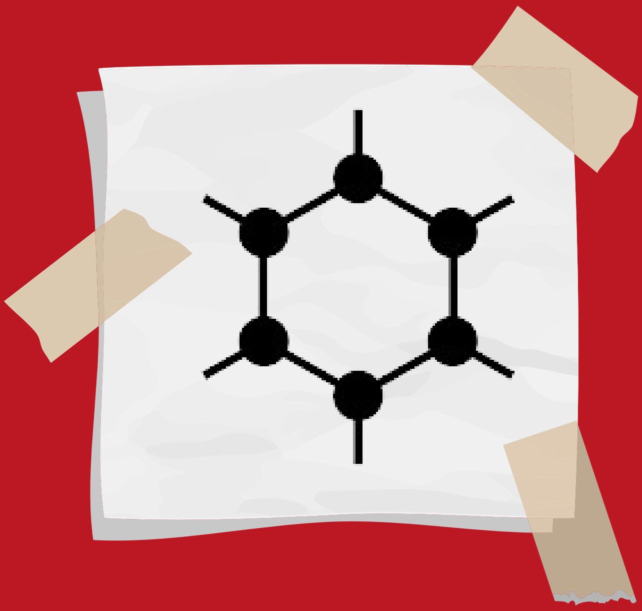
It is a mobile operating system for iPhone developed by Apple Inc. It is impossible to know how the telephone data is processed by the company.

- Android:

It is an open source mobile operating system used on most telephones (Samsung, Huawei, Redmi, etc.). It does not offer good security against hacking. It is impossible to know how the phone data is processed.

- GrapheneOS:

It is an open source mobile operating system that only supports Google Pixel Phones. It is recommended to use new Pixel series, since older Pixels series are not supported anymore by GrapheneOS. This operating system is replacing the original operating system. It allows you to avoid Google's surveillance and encrypt the contents of your phone using an system developed by comrades. It is compatible with most android applications and serves open source alternatives as well. It was developed as a non-profit alternative project.

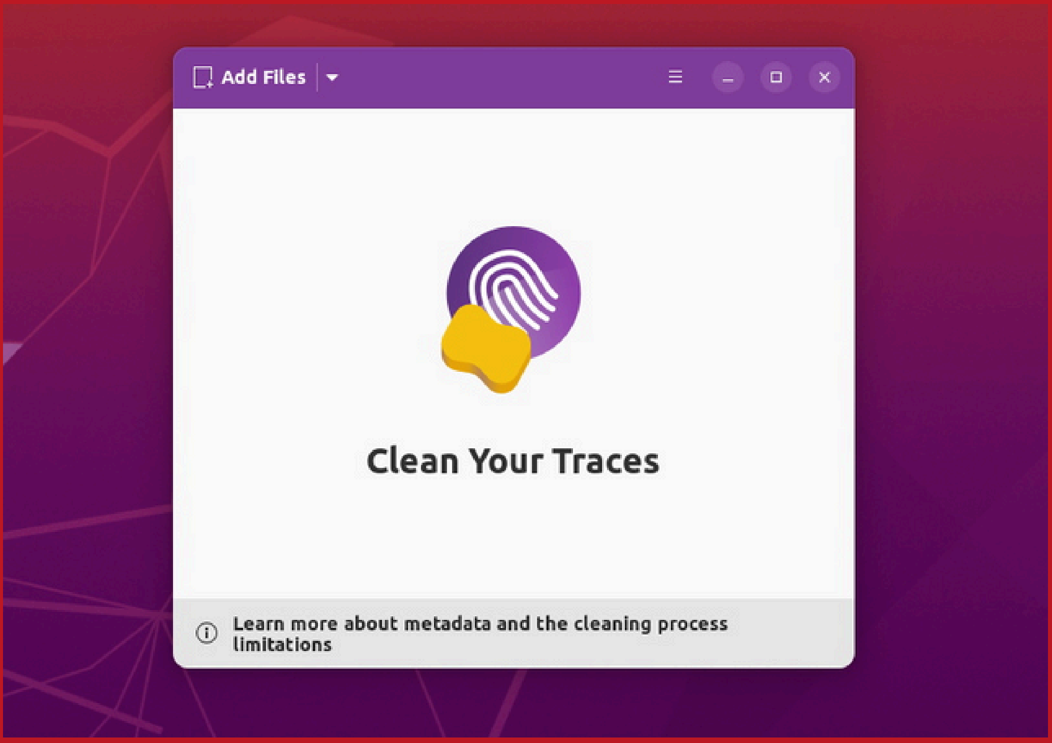


Because of the privacy and security it provides it makes exploitation of the most common sources of vulnerabilities substantially more difficult. It improves the security of both the operating system and the apps running on it.

GrapheneOS adds various settings for features like the network permission, sensors permission (Microphone, Camera etc.), restrictions when the device is locked (USB-C/pogo pins, camera, quick tiles settings, etc.) along with more complex user-facing privacy and security features. It is recommended to install GrapheneOS for the secure use of phones.

About Storage

Each file (video, photo, pdf etc.) contains metadata which is information on its creation date, modification, size, camera, format, application used to create and modify it. Geo-location is also metadata. It is the process of determining the physical location of a device using technologies like GPS, Wi-Fi, or cellular networks. It provides information about where a device is located, often expressed in coordinates or a physical address. It is recommended to check your device to make it difficult to access its content. There is the constant danger to spread metadata by e-mail/ SMS/ social networks. It is desirable to remove them, especially in the event of publication on the Internet or sharing (by message or email). There is the Metadata Cleaner application on Tails/ Debian/ Linux or, on phone, the Image Pipe application.



Clean Your Traces

Learn more about metadata and the cleaning process limitations

1. How to prevent your information from being spread when using the internet?

When using the Internet, a lot of information circulates and is saved for several years. The information vary from which website we visit, from which phone, which Wi-Fi network, which internet connection sharing etc. Some solutions exist to reduce spying and identification while browsing the internet.

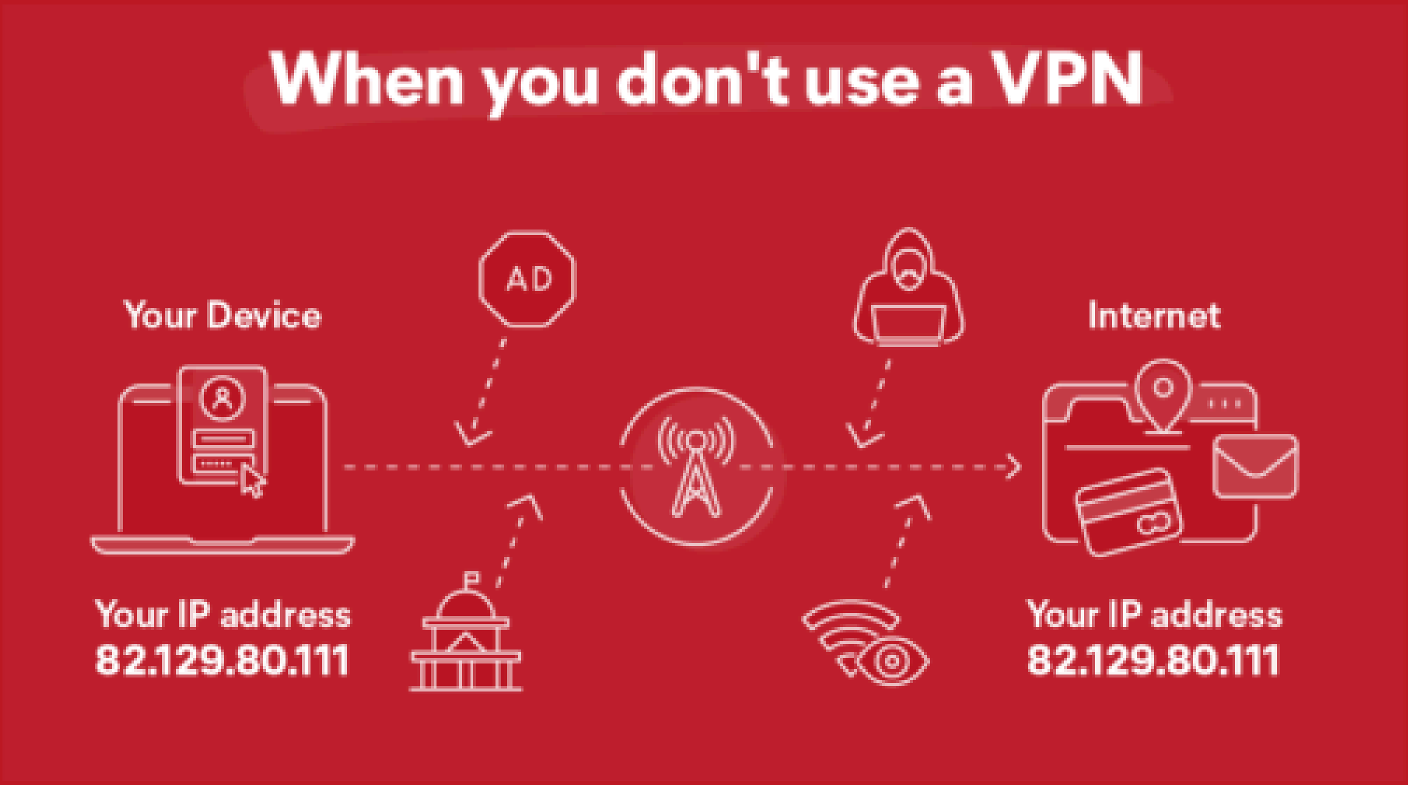
VPN

The VPN's (Virtual Private Network) role is to hide the location of your connection, and also to ensure that your information is better protected. VPN establishes a secure and reliable connection overlaying an insecure network, protecting your online activity, location, and identity.

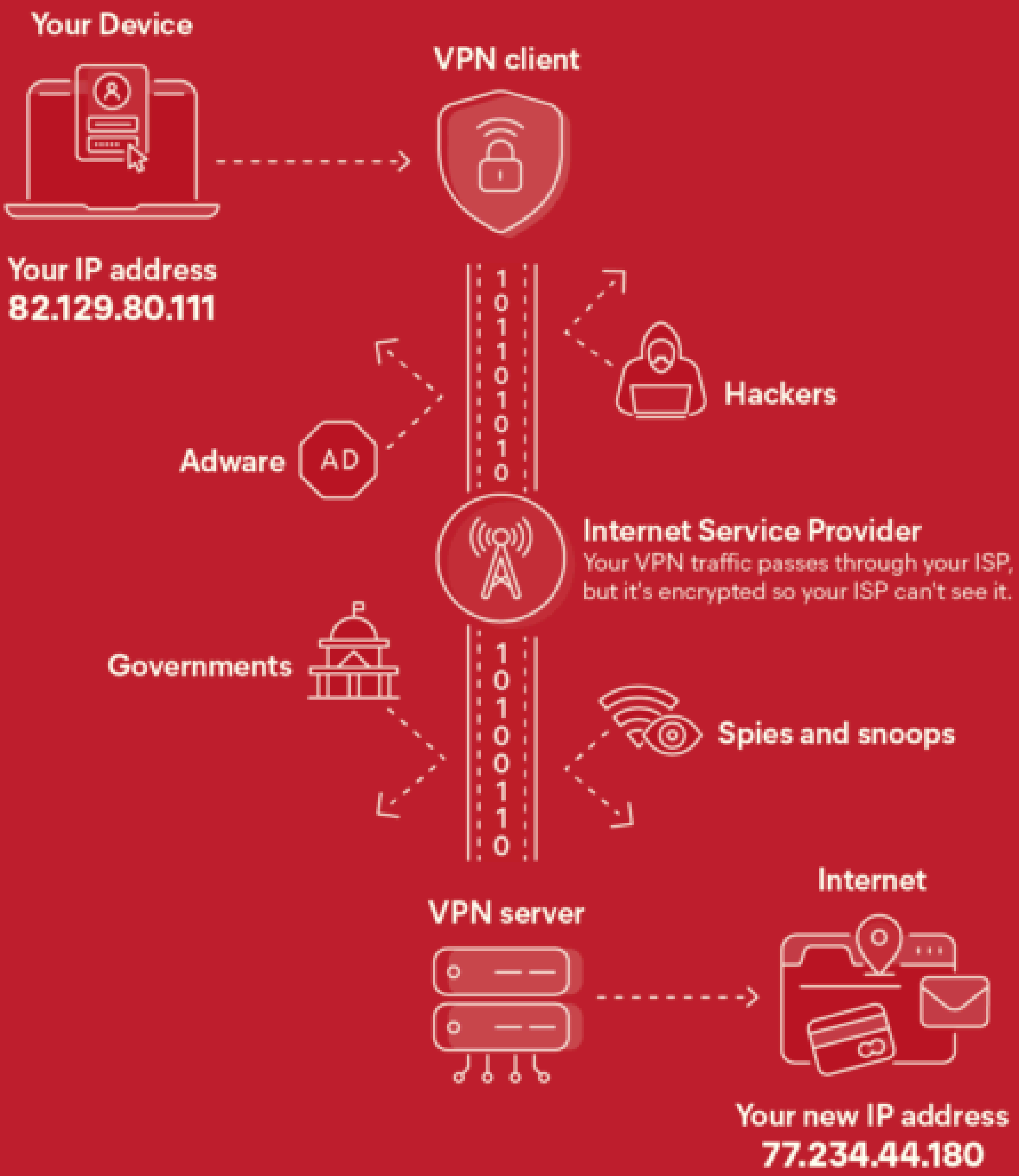
How does this work?
When you connect to the internet, every connection has an assigned address, for example, if you are connected to the internet at home, this connection has an address, a code, anyone who connects will be identified as present at that address. This address is called IP adress. This is the danger, if the enemy knows what your device is and if he is spying on you, your real location will be easily identified, when you connect to a network without using a VPN, exposing your location and that this is a place of comrades.

The VPN's function is to change this address, and also to hide the information that is sent, making the enemy's work practically impossible. The VPN will place your information in a box protected by a key, if the enemy tries to intercept your information through digital espionage, they will not be able to open this box.

There are some VPN providers you don’t have to pay for and that are completely anonymous like the RiseUp VPN which can be installed on any device. The RiseUp VPN is not compatible with iOS apple devices. The Proton mail VPN works without paying as well on iOS but requires mail log-in on some devices. Some other providers which are secure, like Mullvad, PIA etc, have to be paid for but are good and secure as well.



When you use a VPN



Your Device

VPN client

Your IP address
82.129.80.111

1011101010

Hackers

Adware

AD

Internet Service Provider
Your VPN traffic passes through your ISP, but it's encrypted so your ISP can't see it.

Governments

1010001110

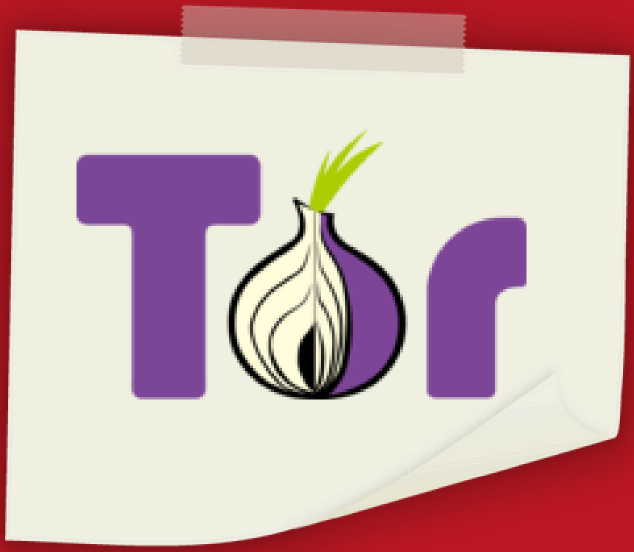
Spies and snoops

Internet

VPN server

Your new IP address
77.234.44.180

Tor Browser



The TOR Browser is the best solution to do research, watch videos or publish on the internet in a secure and simple way. There is no navigation history, no password recording and it allows you to hide from the Internet operator and the websites visited, the identity of the user. It uses several relay points which allow you to anonymize our connections and our work. It is available on all phones and computers.

https://www.torproject.org/

2. What to protect from?

It is difficult to verify whether or not a component of a phone has been physically modified and/or corrupted by enemies. Around us we have thousands of electronic devices such as telephones, computers, etc. Much more than that, most of our communications go through the same devices. This makes it even more necessary to use it safely and consciously to defend yourself from online threats. Online threats are sets of practices and techniques to invade devices, spy, collect and alter data. To counter this, digital security are techniques and practices that make the use of technology safer.

Types of Attacks

Malware

"Malware" is any kind of software designed to harm a computer. Malware can steal sensitive information from your computer, gradually slow down your computer, or even send fake emails from your email account without your knowledge.

Here are some common types of malware you might have heard about:

- **Virus:** A harmful computer program that can copy itself and infect a computer.
- **Worm:** A malicious computer program that sends copies of itself to other computers via a network.
- **Spyware:** Malware which collects information from people without their knowledge.
- **Adware:** Software that automatically plays, displays, or downloads advertisements on a computer.
- **Trojan horse:** A destructive program that pretends to be a useful application, but harms your computer or steals your information after it is installed.

How malware spreads:

- Downloading programs from the Internet that secretly contain malware
- Visiting a website infected with malware
- Clicking a fake error message or pop-up window that starts a malware download
- Opening an email attachment that contains malware
- trough USB drives and hard-disks

There are a lot of different ways that malware can spread, but that does not mean you are powerless to stop it. Now that you know what malware is and what it can do, let's go over some practical steps you can take to protect yourself.

How to prevent malware:

- Keep your computer and software updated
- Do not connect USB-Flashes that are not reliable
- Use Linux → for better security, malware usually only works on Windows
- Think twice before clicking links or downloading anything

Phishing

Used to steal information, including logins, access, data. Executed mainly via email, messages and phone calls.

How to defend yourself:

- Check whether the origin of the email message is trustworthy.
- Check if it has suspicious website addresses.
- If possible, always check the reliability of the message with the person who sent it.

“Man in the Middle Attack”

When the enemy connects to our networks, they can spy on the information that a device sends via internet. This attack can be carried out by malware, through unsafe network or by agents on the ground and thus obtain sensitive information.

How to protect yourself:

- Avoiding WiFi connections that aren’t password protected.
- Paying attention to browser notifications reporting a website as being unsecured.
- Immediately logging out of a secure application when it’s not in use.
- Not using public networks (e.g. coffee shops, hotels) when conducting sensitive transactions.
- Use TOR as internet navigator.

3. Cyber War

With the development of all these technologies, it became clear that states would use these tools and techniques to attack, spy and collect information. Other states such as the USA, Russia, Ukraine, Israel and Iran are also increasingly becoming more professional in carrying out attacks. NATO has increasingly been carrying out attacks and training in this area.

This we can see very much in the example of the Stuxnet malware. **Stuxnet is a malicious computer worm** first uncovered in 2010, and believed to have been in development since at least 2005. **Stuxnet targets control systems on computers and software** and is believed to be responsible for causing substantial damage to the Iranian nuclear program. Although neither the US nor Isreal have openly admitted responsibility, multiple independent news organizations claim Stuxnet to be a cyberworm built by the two countries collaboratively. Stuxnet functions by targeting machines using the Windows operating system and networks, then seeking out Siemens Step7 software which is the programm used in the nuclear program. Stuxnet reportedly compromised Iranian control systems, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart. Stuxnet reportedly destroyed almost one-fifth of Iran's nuclear centrifuges. Targeting industrial control systems, the worm infected over 200,000 computers and caused 1,000 machines to physically degrade.

This is not so far from our reality. **France created malware to spy on files, information, locations, especially in Syria**. To this day we see this virus infecting devices and circulating in our institutions. Here the **Babar malware** is a good example which was leaked by the whistle blower Edward Snowden. The spyware Babar is capable of logging keystrokes, clipboard logging, taking screenshots and even logging audio conversations through Skype and Yahoo. It can inject codes into running processes and steal files. It also uses a Tor network to communicate secretly. This spyware surely is a espionage tool and could have been used for various political reasons.

Turkey, despite many weaknesses, has plans to become a powerhouse in attacks and digital espionage. In terms of digital espionage, there is currently a law that in order for Google, Meta (Facebook, Whatsapp, Instagram) to operate within their territory, these companies must provide any data they request such as location, messages, access to their photos, etc., as well as almost any account on digital media platforms requested by them. Especially before attacks and operations by the state usually digital media such as Meta block accounts that share political content as a method of censorship.
For example: Before attacks by the Turkish state on Rojava start to happen usually accounts on digital media platforms like Instagram, Twitter etc. that could mobilize against these attacks get blocked and closed.

The action capabilities of digital intelligence services are mainly used for domestic surveillance and espionage against their political adversaries, using surveillance programs from powers such as Israel. Furthermore, spying on telephone services in other countries such as Armenia, Greece, Israel and Syria has already been proven. The Turkish state's intelligence organization MIT also states that it is working on digital security, satellites and signal interception around the world.

In this reality, we have to become aware of our use of technologies, especially with our enemy specializing, we also need to become professional, become aware and prepare for a war that has already become real. **This war needs to follow our principles of Revolutionary People's War**, as an unprotected person, a person who is not careful, could endanger dozens of comrades. We have to make this topic a common theme for all of us and the entire society. We all have to **work together to protect our identities, our locations, our messages and information.**

4. Camera and Microphone Security

If the enemy wants to take advantage of you by camera and microphone surveillance, they have to hack into your device. Nearly all hacks are caused by malware. **Opening unknown email attachments, downloading from unknown sources and visiting untrustworthy websites are how about 98% of malware ends up on our devices**. Once the malware is installed, your computer or phone is totally open to hackers. Simply avoiding malware and making sure your antivirus software is turned on and up to date can prevent this. But **once the malware is installed on your computer, the enemy is able to have access to your microphone and camera.**

Most computers have in-built microphones and cameras. The same applies for phones. Therefore, it is recommended to **cover all the camras on your devices.** Since especially the built in cameras and microphones are directly connected to the internet, they are very easily hacked. In this case,the enemy can easily take over the camera functionality and turn it on or off as they wish, as well as disable the LED light to avoid detection. Of course it is possible to block all permission and access to the microphone and the camera as well. In most cases, software protection is more convenient than physical – but not always as reliable. There are numerous softwares with access to this function. Especially GrapheneOS is giving this option for the device from the beginning and as well the ability to always check if microphone and camera access is given or not.

Even if covering your camera with tape does not prevent someone from listening through the microphone, it is still a good protection for your anonymity. Sure, it will thwart video surveillance, but the sound from the microphone can still be taken. Modern laptops often have several mics to enhance sound quality, and taping over them all will be difficult. In some models, built-in microphones are disabled when you connect an external one. A life hack for them is to plug a dummy into the microphone jack (or the universal jack for mics and headphones). Your laptop will think that an external mic is connected and turn off all its built-in ones. Because in most cases, software protection is more convenient than physical – but not always as reliable. We always have to be careful when we speak to not expose any information to the enemy while we are near to our devices.

5. How to communicate securely

The Signal Application

To communicate securely, it is good to know if the company which develops the application of the messaging service collaborates with the police, states, whether it sells data etc. or not. There are several applications which are not secure, such as Whatsapp, but some applications for communication provide encryption. Of course, by time better applications will be developed or there is always the possibility that the applications used will be taken over by the enemy. Therefore, it is in general recommended to be careful in the matter of communication on any devices to not expose information on these platforms and applications.

To communicate by messages/calls, **SIGNAL application provides very high communication encryption against hackers**. It is available on all phones and also on computers. It is possible to configure ephemeral messages and several options for more security.

As we mentioned previously, **the use of applications such as Whatsapp is not safe, in addition to providing information to the Turkish state, Whatsapp has very weak security against attacks**, it is very easy to discover information through spying technologies.

Another very dangerous aspect of Whatsapp is that all messages, even deleted ones, are stored in Whatsapp files. If the Turkish State requests your messages, rentals, number information, all your information will be passed on. In this case, not even using a VPN would be a complete solution, as only your informationwould be protected, but all messages and photos would still be shared even several months after sending.

In addition to that, TAILS is providing many options for encrypted communication. This way, many of the communication can be done by the services that are available on it. This can improve our privacy online.

Tails includes:

- Tor Browser with uBlock, a secure browser and an ad-blocker
- Thunderbird, for encrypted emails
- KeePassXC, to create and store strong passwords
- OnionShare, to share files, websites, and chat rooms over Tor
- Metadata Cleaner, to remove metadata from files

6. Practical Advices

- **Use different passwords** depending on the accounts and applications. The strength of a password is its length, we even speak of pass-sentence for more security. Using special characters does no longer improve the strength of an identifier. It is recommended to design a password of several random words for an identifier or a computer, and a 12-character password for a phone.

- **Use secure applications** recommended by comrades. Install Apps from trusted sources. Such apps undergo security checks, reducing the risk of malicious activities related to the microphone or other sensitive features.

- **Do not answer to messages of unknown or strange contacts** and don't open links that are send to you possibly by these, because these aim to get your location

- **Keep the location (GPS) deactivated**, with the best practice being to leave your cell phone always in airplane mode. The airplane mode can be turned on while the Wi-Fi connection is operating.

- **Do not travel with your cell phone turned on**, if possible remove the Sim Card before traveling to other locations, this also prevents your location from being deciphered via satellite.

- Organize the purchase of **safety packaging that cuts the signal** (like a **Faraday Bag**). This prevents any signal from being sent from your cell phone, making it the best option for travel and transportation.

- **Do not send messages with your name, location,** where you are, where you are going. Messages, especially on Whatsapp, can be intercepted and used by the enemy's intelligence.

- **Use an anti-virus\anti-malware solution**. It is an essential software or service that protects computer systems from malicious software. These programs do this by detecting possible malware threats, blocking threats before they access the system, and eliminating existing threats so they won't cause further damage to the system. For this, there are several software that you can download on your devices. That applies for all kinds of devices like computers, phones of every operating system and even phones with GrapheneOS.

- **Keep your device updated.** Ensure that your device is running the latest available operating system and security patches. Regular updates often include bug fixes and security enhancements that address potential vulnerabilities. Not to update to ensure security is a common thought or a false belief. It is better to update to ensure the security of a device that has internet access.

Conclusion

With this small digital security protocol we wanted to share some basic information on how to protect yourself on a digital level, with you. Since cyber attacks are increasing and the use of digital communications and platform become more and more present, it is important for us to know how we can use these in a secure way and how to maintain protected or prevent any attacks by the state or other enemies on us. Since we are the anti-capitalist part of society that wages a struggle against this system we have to always remind ourselves that we can become targets of such attacks. Therefore, taking our security serious is a very important matter that is essential for all us in everyday life.

internationalistcommune.com