
Privacy please

Welcome to new brave world, they say. Brave one is not the people; it is the firms. They are so brave that, they make you pay to infiltrate to your very personal life and sell it.

Someone was watching you. Now **EVERYONE** is watching you.

Whatever you do, never accept anything closed-source code. Why? Because **you have no idea** what that program / hardware does. Let me give you some examples.

- Once upon a time when I was abroad, I forgot my phone in front of the TV. It was an iPhone, and the screen was closed. There was no application running. I did not have any Google or Facebook based application. Only Instagram for that time and Facebook have not bought it yet. And there were some Spanish commercials on TV. I don't even know a word in Spanish.

5 minutes later, I am on my computer, opened Facebook, and there was a Spanish commercial right in front of me.

- Similar thing happened to my friend, he and his girlfriend saw a cockroach in their house and talked about how to get rid of it. Then immediately an advert about it on their Instagram page.

- I am sure that happened to you too, you just think about buying a nice coat, and there you go, you see that advert about coat in Instagram.

- (OR) You realize that Google's results are not the same with other people's results.

I can give you at least one hundred examples like that, just from my personal life. These technologies are **NOT** for the end user. They start telling you that they make your life easier, because they know what you are going to search by making a profile about you.

BUT the thing is this is not the point, because these firms do **NOT** care about you. They will never care about you. They only care about the people who pays them, everything, every single technological improvement is about money. They don't help you; they direct you! They tell you to get that nice pair of shoes that you deserve! They will tell you, if you smell nice you will get that woman of your dreams.

You might think, what is the harm? Like if the weather is getting cold, and I don't have a coat, I would love to see my options, and they help me, right? **No! Why?**

This phenomenon started after WWII. At first all the cities were demolished, there were no car, no clothes nothing. So, they built a lot of factories, a lot of quality products, and after some time, everybody had a house, nice clothes, everyone was happy, so there was no need for factories. I mean you have plates, nice ones, so why would you buy another one?

Then advertisement got a revolution, they stopped selling products, they started selling lifestyle. Some cabriolet cars with a cool dude driving and all the nice girls looking at him. This is what they started to sell, lifestyle.

From that moment, focus was/is/will never be the consumer. It is the money they have, that is it. So, they have taken all of the measurements to do that, and governments got their piece from that. With this they could control people a lot easier, they could track them a lot easier. Let me show you an amazing magic trick:

https://www.youtube.com/watch?v=43Mw-f6vIbo

Just watch this! Look at how these creative people are just devastated. They have no idea! And they are supposed to be the creative, open-minded ones. See? You are not making your own decisions; they are making it for you! THAT is the problem. This is not a magic trick; **this is the reality**. This is the **MATRIX**.

Do you really think these BIG companies pay $150k to shit tons of engineers just to make you comfortable googling some girls or looking at memes all day? If you think they do these for free, think again. Now think how you are paying for these services. **I KNOW!**

On the other hand, why open source? Easy, you will know what that software does! Even if it is a keylogger you will know exactly what it logs and whom it sends them to, but of course as it is open source, no one will do that. That is the idea.

Open source is the single most important thing about security and privacy. The idea is not only about the software, but also about the hardware. But I will get into that in the later in detail.

Part 1: The Easy One

This part is the most basic one, as every single one of us use browsers to **GET INTO** the internet.

What is internet? I mean how does that works?

First there are so called servers, what are they? They are exactly like your computer. Mainboard, CPU, GPU, hard drive.

And these computers are connected to internet.

They have an IP address, and domain names bound to IPs.

So, when you write that domain name on a browser you just get into that server, meaning that computer.

I guess you get where I am getting at right? The thing you call internet means someone else's computer!

This is same for cloud storage; you think you are saving your files to a cloud which is military grade encrypted. Right?

Lies, nothing else, they have access to everything you do on the net. It is their hard disk, and they all have backdoor to get whatever they want whenever they want. This is not limited to what you have on the internet, but we will get there.

Do you remember FBI was forcing Apple to give them a backdoor, and Apple was saying no. If it was not tragic, it would have been comedy. FBI **NEVER** had to have that backdoor, they could go into any phone they want at that time. And they didn't even need that, it was a message, they can read the messages just from the server, they did not even need that phone. BUT of course, they had to show people Apple is the good guy. There are millions of cases if they can get into the phone they can solve the crime, but they were talking about one single case, why? To make Apple more famous. And almost every single person still thinks iPhone is safe and private. **LOL**. Do they even care about crimes? Hell no! Who cares about the criminals? One person is killed, and people go crazy, but armies kill millions no one bats an eye. USA was in Middle East for years `**for peace**` and killed millions. What kind of peace is that? It was all money.

This is the part we need to understand, **NOTHING** they say, do is correct or honest.

So, what is the solution? Is there any solution? Or are you condemned to use this software / hardware?

Of course, there are, the ultimate protection will be just smash your laptop, your phone, and never go outside. EASY!

NOW the hard part is how to get private and secure while still being online. Here are some basic tips to get your journey start.

- Never ever use software from **BIG** corporations.

- Use open source, community driven software.

- Never trust any corporation to ensure your security or privacy. Instead trust the community of volunteers.

- Use different browsers for different kind of work. You can divide this stuff into **personal, banking-trading, stupid stuff** for starters.

- Use **Linux**. There are a lot of different distros, you can choose the most basic one with windows like interface. And trust me it is not as hard as people talk about it (Like **Fedora**, just search for the images, it's really like Mac OS and Windows). It will not take more than 30 minutes to get used to it. If you are expert, I would suggest using **Tails** or **Qubes**. - I am using Qubes -

- NEVER EVER click on a link someone sends. It might be from your brother, but his account might be compromised, you will never know.

- You must disable most of the tracking features of the browser.

- Use **Firefox**. You can use https://ffprofile.com/ to create a nice profile to get you started.

- You should use **uBlock** add-on. Enable **HTTPS** in the settings.

- If you are not going to use any accounts or sync, you can use **Tor Browser**, which is already optimized Firefox with a kind of a feature which tries to hide your trails..

- Generally, I would not suggest any VPN, as using VPN you trust its provider as all your online activity passes through their servers. So, it is important who gets your data and what they do with it. But there are couple of ones which are strict with their privacy. **Mullvad, ProtonVPN, IVPN**.

- If you must log into a website, do not click links, just write it yourself. Why? There might be a letter change which really looks like the original one. For example, you might be logging into **gmeil.com** instead of **gmail.com**, and you might not even recognize the difference, then in just a second your mail account is gone, and when they search your account with a simple bot, they will not a lot of websites that you used this mail to register and steal these accounts as well. This takes like 3-4 minutes tops. There were a lot of instances peoples steam account got hacked by this method. People see a nice trade offer in their mail, when you click the link, which is like staam.com/trade …, you log in, and all gone. **RIP**

And trust me, this is the easiest to prevent, just don't click on another person's links. Mostly if it is so good to be true, it is not true. You are not lucky; you are about to get wrecked.

- Use 2fa password. When they steal your cookies, this won't make any difference, but at least you will be protected from keyloggers and brute force attacks. For this I will only suggest 2 open-source ones: **Ravio OTP** and **FreeOTP**. Use them extensively, for every single account you have.

- Do not use any google service. No mail, no search engine, nothing. Never even log into your account with your laptop.

- Instead start using other safe mails: **Protonmail** is a good one. It has free and paid plans; you can choose whichever you want.

- For the search engine, you can use, **Startpage, DuckDuckGo.**

- Do not use gdrive, Dropbox, OneDrive or whatever the **BIG** companies give you. They are all free right? No it is not, you are the real product, **they sell you**. Instead use, Mega.nz for file sharing, it also has cloud drive. Or **NextCloud** as self-hosting cloud server. I will explain how to set up your own Nextcloud server with Raspberry Pie cheap and convenient in the *Pro Level info pdf*.*

Tip: I don't use any cloud service on my laptop, which is mostly used for trading, banking, and sometimes reading. For that computer I have **signal** app installed. I can send myself notes, links, docs. You can also use it like that. It is an amazing service, and if you stop using **WhatsApp** and use **signal** instead, that would be even better. Wait, no, use SIGNAL! And make **everyone** use it. If they want to message you, tell them to use **SIGNAL**. Easy.

- Disable wireless and Bluetooth. They are **ALSO** harmful for your brain anyway. Just use ethernet cable. Yes, for your phone too. And try using DNS. If you don't use your ISP will get every single request you make. The one I will suggest and maybe make a guide on it is **pie-hole**, or at least use NextDNS.

Part 2: Choosing hardware

Again, open source is the IDEA!

When you purchase a computer and connect it to internet, everything in your computer is connected to other people's computers. It is from your Operating system to your BIOS, your CPU to your graphics card, even your mouse!

At the basic level, let's say you have bought a gaming keyboard, and you have latest hardware/software, which is windows 10 now (I won't talk about win11 as it is not even stable yet) And in a second you will see a notification that that keyboard wants to connect to internet and install a software / and your profiles. However, if you are not on the net, it won`t ask.

There are a lot of problems with the software used even before installing BIOS. And these backdoors are hard to use, yet almost impossible to fix. Operating systems tries their best to cover them, but at the end of the day, how secure they are to talk about security, and privacy. One example can be Intel Management Engine and AMD Platform Security Processor. These are exactly small operating systems on your CPU running if this CPU has power. These systems have full access to your computer and internet. And these can be accessed by an adversary to de-anonymize you.

These has caused big problems in the past. And a lot of software accused of being backdoor into any system like EFF and Libreboot – which is why I don't suggest Librem -.

For AMD Laptops you can disable this feature in BIOS. For Intel there is no straightforward way to disable it, there are some scripts on the net. This is our best bet right now. So, in this case I would recommend AMD laptops over Intel ones.

Mobile:

Let's continue with your phone. Any closed software is a problem. Ditch iOS and Android. In some extreme cases you might need one for your bank apps, or some apps might be extremely essential for you. I might understand that, so if this is the case, buy a cheap one, and use that phone without SIM just for these needs. I am sure you can do whatever you want from the browser or laptop, but this is the extreme measurements.

Lemme tell you what your mobile device has about you, you need to see the truth before making and effort to solve it:

- Records of what you say anytime. (Hello Siri!)

- Records of your location, constantly, even when you turn them off. And if you use Wi-Fi, your exact movement. Explanation below.

- Always records other devices around you. So they know who is your friend, and who you are working with.

- Your health data. Your steps, screen time.

- All your network locations – Wi-Fi spots.

- All your pictures, videos, notes.

- Records of all your accounts, including e-mail, social media, financial accounts.

And all of this information is stored indefinitely, mostly unencrypted.

HOWEVER, most of you do not only use mobile phone, but also use, smart watch, smart speaker, smart transportation, smart … bulshit.

Now **THINK** what they know about you.

You might guess how they use this information about you. Let me give you some examples and this is only the tip of the iceberg.

- Law enforcement agencies can get your network activities.

- They can track how you write. How many times you mistype. How you use your mouse and how it reflects your psychological unique behavior.

- Marketing.

- They can change your feelings and mood.

- They can make you suffer!

Feeling paranoid already? **Good.**

What about **hardware**? What are you going to use?

- OK, first, we will have Pixel phone. I have tried 2 and 3, both are same, but I am against to pay premium for a phone. It is just a fucking phone, not a car. So, buy **Pixel 2**.

- Install **GrapheneOS**. It has all closed OS code running in a HAL sandbox and the system is extremely hardened and backed by a great hardware. Use this without SIM, and you are done.

- Unlike other android phones, Pixel has verified boot which is kind of one of the most important hardware security features.

- Disable Wi-Fi and Bluetooth. Geo-location is not only done by triangulation of the antennas. It is also done by Wi-Fi and Bluetooth devices around you. Operating systems makers like Apple and Google already has a list of most Wi-Fi access points. And if your phone is open, it will passively scan access points around you and geo-locate your location all the time.

This feature can provide them exact location of a person even the Wi-Fi is off. And this can be accessed by them or third parties for tracking.

Also, a side note, this is not what Wi-Fi can only do. With the recent developed tech, someone can track your exact movement just based on radio interference. Thus, at this point best bet is to disable Wi-Fi all together.

Even worse, some devices can be tacked even when they are offline. Therefore, you might see in some movies, that person always remove the battery. These devices are iPhones and iPads, Samsung Phones, MacBooks, and most probably many more. These devices constantly broadcast their identity to nearby devices using Bluetooth Low-Energy. So, it might not be connected to any internet, but your location is still there.

Laptop:

When you search for secure laptop over a search engine, you will see couple of choices.

First one is **Librem**. Don't get it. They run libreboot which run on binary blob that I would never suggest.

They say there is a hardware block to speaker/cam. It does not even matter, I will tell you the reason soon with Qubes.

Second one you will see is **Nitrokey**. They are good. Only problem is they have all your recovery keys. I really don't get it, why they would keep it?

Then there is **Insurgo**, they might have seen Nitrokey, and asked the same question. They have a good reownership feature which is an automated process that runs on your first boot. And you change all the recovery keys by yourself, and just for you. It has Nitrokey dongle with it, and your laptop will not boot without it. Your hard drive is encrypted, so it will ask for its password as well.

So, at the end: Do not get any consumer / gaming laptops. Try to get Business Grade Laptops. Thinkpad from Lenovo is my favorite. My personal computer is Lenovo X230 with IPS screen.

After you get the laptop of your dreams, first thing without even connecting to internet is changing some BIOS settings.

- Disable Bluetooth completely.

- Disable Webcam and Microphone and Biometrics.

- Use BIOS password.

- Enable HDD/SDD password.

- Disable Secure Boot if you are going to use Qubes OS.

Then you will be using **Qubes OS**. Which is the most amazing Operating System I have ever used. And trust me I have used almost all versions of all Operating Systems. I have other recommendations for all the OS in the Pro pdf, they all can be modified to a level.

So, what is special about Qubes?

- First, it is a **Linux** based on **Xen**, open source.

- It blocks almost all hardware; you cannot use GPU with it. It only runs on CPU, so you cannot use hardware acceleration with Firefox let's say. It blocks USB, microphone, camera. So as in Librem you don't need to disconnect them physically.

- It only runs of Qubes – which is their name for Virtual Machines.

- At default it gives you couple of premade virtual machines, basically they are different computers which has no relation with each other. How do you use it? For example, I have created some Qubes: **personal**, **trade**, **vault**.

Personal is for daily activities. Mail, Discord, Telegram (**WR**), watching videos, saving pdfs to read later, listening to music.

Trade is only for trade. It has Firefox and nothing else. It has all the settings to make it Firefox invincible. It has bookmark links to the banks I do use. It has **Metamask** and this is all. I only open this VM when I am about to trade. I also use ledger hardware wallet connected to Metamask. So even when my browser gets hacked or I click on a link that I should not click, nothing will happen.

Vault has **Keepassxc**, and my important files in it. It doesn't have any connection to internet.

So, without any physical hack, it is impossible to hack this computer. Even when someone gets my laptop, then they must get pass Nitrokey security, encrypt the hardware, then get pass OS password. When they do these, they can use my personal Qube, which has nothing personal in it. They need to open other Qubes and know their passwords, and USB to make a trade.

This is enough for security, now it is about privacy. As Intel ME is disabled, as this OS doesn't use GPU driver, as this Qubes OS doesn't let any Qube to even use microphone or cam, or USB without my permission, everything is under control. And If I want, I can set Qubes's internet to Tor network. So, It is not only perfectly safe for me, but also completely anonymous. Which is what you WANT for your own good, and at the end, better world!

Unfortunately, you have seen through the rabbit hole.

From here you have couple of choices:

- Just ignore and be a cheap product. Let them direct you and imagine being yourself.

- Get P*ro Level pdf* to make everything super secure and private to mess with them.

Kezer.

**** What does Pro Level pdf have?***

- Creating anonymous online identities.

- Hardening your hardware.

- Setting up personal nextcloud server.

- Hardening your OS – Windows, MacOS.

- Starting with Qubes.

- Backing up anonymously.

- Covering your tracks.

- Removing traces of your identities on search engines.

- Escaping when you got burned.

- Limited mail support

Note: Pro version ETA is 01.01.2022. If you donate more than $50 you will get Pro version as a thank you gift for supporting my work.

After it is released, it will cost a lot more.

After the donation, please send me e-mail with the transaction information.

BTC:
bc1qe7t4ckuq8wt00h6d3qdpuwesjjn4zxfy4nzjmw

ETH:
0x3F838Fb407b750655632088bDf1D0430F53AC8F3

wrkezer@pm.me