This is a deeper introduction to security related to browsers, I pretend to make a deeper conversation about this topic.

A lot of you probably don't know how easy is to steal information from someone using a PC or a Laptop. I don't know if Linux and MacOS works in the same way, but MacOS is the most secure operating system

, and the one that is most likely to not have this issues.

I have some Windows knowledge and I will try to do my best explaining how things work, how easy is to steal your information, and a possible solution

to escape from this.

First of all, we need to understand how a computer works, from inside and outside. Lets get started!

BIOS/UEFI

BIOS

, which stands for "Basic Input/Output System," is a fundamental software component, the most important one, found in every PC or Laptop. It is responsible for initializing and controlling essential hardware components during the system's startup process, as well as to boot to the operating system itself. Although modern systems are transitioning to newer firmware standards like UEFI

(Unified Extensible Firmware Interface), the term "BIOS" is still commonly used to refer to the system firmware in general. Both do the same in different ways, so lets just call it BIOS

Bitlocker

Bitlocker

is a disk encryption method from Microsoft, the owner of Windows. Its purpose is very simple, it encrypts the drive

you want, and anytime you want to have access to it, you need to introduce a password to decrypt

it. It's possible to encrypt it later with a command in CMD

and Powershell

, or just restarting your computer. You can encrypt your drive where Windows is hosted too!

Website Cookies

Cookies

are text files for each website, and they contain information about your activities, preferences, tracking, etc… You've probably seen in some websites this message:

[

image

763×447 54.5 KB

](https://global.discourse-cdn.com/apecoin/original/2X/1/1d48c382862c8df792e7f060409eb9b166674ec3.jpeg)

If you agree with it, you are giving that website the permission to use cookies. In some websites they don't have that option because you are already agreeing

to use cookies, and it's stated on the terms of use

page.

First of all, you are using a browser right now to access this page, and therefore, every action you do in your browser is stored in your system. Lets say in simple words. Imagine you are logging into your social media account, and you don't want to waste your time typing your password every time you go there, right? So you just check that box "remember me"

and next time you enter in that social media, you automatically authenticate

without typing any information. This is where the cookies

joins the conversation.

Until now, we know that the social media we logged in, stored the necessary information in my system to login automatically

the next time I go there. Pretty simple to understand.

And if someone emailed you with a malicious link

to download a PDF file, and you thought it was an important email? If your antivirus don’t detect it, you are infected

now. Imagine two people working in the same machine, the same Windows user, at the same time… That’s gonna happen if you get infected. The virus will compress your browser’s files into one, and send it to the virus’s owner, and therefore, if he installs the browser you were using, and decompress that file into the browser’s files location, BOOM! He now have access to that social media that you checked the box “remember me”. And the worst part? He doesn’t need your password, because he’s already inside your account

! And if you have some passwords saved in your browser, he have access to it too

!

This whole situation can occur in the same way if someone steals your computer, or just the drive itself. Just plugging the drive inside another PC and BOOM! That “someone” can pull the files to his computer without any issue, just like the virus did!

Okay, I know this sounds kinda scary, and it is, but I got some solutions for you:

Protect your PC BIOS with a password

This will prevent

someone that stole your computer to run any other system through a flash drive

to have access to the files without a Windows User.

Encrypt all drives with Bitlocker

This will prevent

someone that stole your drive to pull your files. It will ask for a 48 digit recovery key

. This key will be given to you at the time you encrypt the drive, and it’s used when you lost the password, or when someone’s trying to access the drive with another computer.

Be careful browsing in the web

And for virus, you should be very careful

with what you click in the internet. Don’t rely on the antivirus, it’s never 100% virus proof

.

There’s a lot of things to talk about in the security topic, and I haven’t spoke about the account protection

, that’s a new and complex story.

Should I make a new topic about the account protection?

- Sure!
- Nah, Its fine.

0

voters

Tell me if you find this topic helpful, and spread some love! Took me some time to build this!!