Malware is a software designed specially to do harm to a computer, server or network. It causes damage after the succesful implantation in its target system. It can have many form from executable code, scrip to active content and other software. Malware exploits security defects, vulnerabilities and other problems in the design of the operating system.

Malicious computer programs are constantly growing as the “vendors” apply patches to their systems and the malware evolves once the targeted system becomes more complex. Malware attacks consist as stated in [1] in 2011 from 17 different categories, which only continued to grow until the present days, which means these will only continue to evolve until they won’t look anything like the malware types we currently battle.

Only in 2015 where reportet, as stated in [2], that 884,774 new mobile malwares were introduced, triple the number they fought in 2014. From these new malwares only 6% where new mobile malware categories, where more than 40% are variants of old existing malwares, this is also explained in [2]. The same documentation [2] presents, briefly, the first malware dataset created in android malicious software, which contained in 2011 1,260 Andoid malware from 49 different categories collected in over a year, from August 2010 to October 2011. This only emphasisez the problem the world is facing, that malware is one today’s greatest threats.

Malware isn’t only found in the problems of big companies or important personalities. Malware is a breaking point in computer forensics. As stated in [3], criminal uses malware defence to ty and get away with their criminal activities while claiming they did nothing wrong. Computer security focuses on keeping the cyberspace protected, computer forensics is fighting to bring the digital footprint to the court.

As seen for now malwares are found everywhere and people fighting against it, have a non-stop job and many barriers. For the computer forensics as [3] describes, the struggle is to bring a clear, simple and direct way to present the behaviour of malwares without all the technical jargon. They even categoriezed the malware types as simple as possible, so that everyone can understand the implications of each category. Presented below we see the categories from perspective of [3].

1. Residency Attacks – malware shows its existence but does not have any impact on th sistem or files
2. Integrity Attacks – malware can either change the system time or modify time stamps of files so that the integrity is violated
3. Content Attacks – malware will change the content of files so what the user sees doesn’t have to be the result of his actions
4. Offensive Attacks – malware will attack others, which will result in law suit
5. Destruction Attacks – malware will remove files from users computer or crash or destroy the users entire file system

In most cases, the presence of malware is obvious, even though you may not know how it infected your device. In fact, most people have no idea that malware was installed until their computers would start glitching. You may notice some changes on your computer, including strange pop-ups, even if you do not browse the web. You may also have unwanted changes and a slower PC experience.

In particular, watch out for ads that appear a few seconds after uploading a web page. These ads often contain inappropriate content, are difficult to close, and show intermittent colors while blocking what you want to see. Take all these signs seriously. Another sign for malware is the link shown on the bottom of the webpage when hoovering the mouse over a clickable button / link on the page. The malware has longer strange looking adress than the safe and correct web adresses. We expect to find the name of the object / adress in that link, so if there is no match don’t click it.

Another scenario where people are prone to have their computer infected is because they neglect to update their anti-virus/malware software or other progrmas. Updating the feature of zour computer is jusr as important as checking the car. You won’t drive an unsafe car, so why wouldn’t you protect your data?

Malware means that when you got it, it will only leave you open to more intrusions and attacks.

When wanting to get rid of malware is important to stop the connection to the internet. This is to ensure that the malware can not transmit data to a third party like a cybercriminal and an active connection can be the reason why the malware was activated in the first place. After you have done this, run a scan of the computer, this should find all the infected files and clean it. As another precaution delete the temporary files and cache.

From what we learned from the different sources, it is important to be sure about the apps and files we install and download. The most malware infects our computers simply because we fall for the traps on the internet, from great deals to discounts or just because of the pop-ups which never disappear from the web pages. As seen in [1] the malware just keeps evolving, but so is the anti-malware software. This is what [2] discusses. They influence eachother and they force changes. As one fights the other fights back. It is an important aspect of our life now, because when using the correct software, we help others to stop the criminals which want to steal our information.