Beautiful and correct said about the abundance of the cyber attacks and threats is in [1], where a parallel to the history battles is drawn. No two are alike, which is so true in todays reality. This means that similar strategies and tactics are used, because the persons / hackers have seen they are effective and efficient and time saving. Nobody will re-invent the wheel unless is absolutly a necessity. As mentioned in [1] they will use common techniques which have been used with a high success rate, like malware, phising and others.

Another source [2] aknowledges that the sophisticated criminals can easily exploit the human errors and computer vulnerabillities. From these attacks the results can differ from criminals accessing your personal and financial informations, to preventing your ability to use the device and many other possibilities which only leave you vulnerable to the possibility of loosing your identity. There is already a Criminal Code Act from 1995, but there is so much the law can do now, because it is so hard to find the responsible person hidding behind the similar tactis and strategies used.

Attacks can be stopped and dodged by simply using one of the many security measures found online, from a computer scan to installing anti-malware software to complexer solutions.

Regarding the informations we just gathered from different sources, the attacks are divided in at least two categories, as active and passive. As seen by [3] the major difference between these two types is that in the active attacks the connection is intercepted, and information is altered, as in passive attacks the informations are read and analyzed but not modified.

**Definition of active attacks** - are the attacks in which the attacker tries to altere the information or creates a false message, which the user identifies as real. To prevent these attacks the user has quite a lot to do. It is difficult because of a broad range of potential network and software vulnerabilities. Instead of prevention, the detection of the attack and recovery from disruption or delays are wanted. These attacks are most of the time in form of interruption, modification and fabrication.

**Definition of passive attacks** - the attacks where unauthorized eavesdropping, monitoring the transmission or gathering of information occurs. No allteration takes place when reading the information and data, therefore it is harder to detect, unlike the active attack. Which means that the user remains oblivious to the attack happening in his system. This can be dodged by encripting the files with a complex key-system or with certificates which do not allow other parties to get the content of the files / data. For this type the prevention is emphasized rather than detection.

A passive attck can be divided in two types: the release of message content and traffic analysis.

**Key differences** mentioned by [3] are as follow:

1. The active attack means messages are modified. On the other hand, in passive attacks, the attacker doesn’t commit any changes.
2. The active attack causes harm to the system while the passive attack doesn’t cause any harm.
3. A passive attack is a threat to data confidentiality. Where, an active attack is a threat to the integrity of the data.
4. In active attacks the victim is aware of the attack and in case of passive attacks the victim is uninformed.

As another source [4] states the threats can be categorized in four: direct, indirect, veiled and conditional.

**Direct Threat** – it describes a choosen target which is attacked with a specific act. The attack is delivered clear and straightforward for the victim. This category is used not only online but can be adressed directly to the victim.

**Indirect Threat** – it describes a vague, unclear and ambiguous threat. Every detail from the plan, motivation victim and more are masked and not divulged. It is possible to occur, but not garantied.

**Veiled Threat** – it implies but does not explicit threatens violence. It is left to the victim to be interpreted and to give a meaning.

**Conditional Threat** – it is usual for extrosion cases. A violent act will happen if certain demands or terms are not fullfiled.

All the attacks and threats can be classified in different categories. It is important to keep in mind that the division is based on the actors, either the victim or the attacker. When talking about these attacks keep in mind that you are never protected enough, they find even the smallest security gap and use it for their advanteges. So, stay safe while browsing.!