Hacking has been growing exponentially along with the growth of internet. Initially hacking have been hobby and fun thing for teenagers and later it turn into a crucial crime which we are calling as "Cyber Crime". The roots of Hacking and viruses in computers are found in the year of 1986 by two Pakistani hackers Basid and Amjad. Later there are many versions of viruses are written. Internet security labs reports say that at least thousands of viruses are being generated and attacking web and computer every day. The sources for these attacks are from a group of organized hackers who are making millions of dollars with hacking. These groups hire intellectual programmer to program the viruses and testers to test the malicious codes. Banking Trojans are the one of the most active attack used by hackers groups where they capture internet user bank details in an organized way and they loot their accounts. Key loggers are also the best weapons for hackers to attack common people; hackers install key loggers on internet users and capture almost everything. Hackers analyze captured data, extract the password, other confidential information and make use of them to get some revenue. There are several well known cyber criminals according to FBI and other government organization throughout the world. Whenever Interpol official's tries to catch cyber criminals, these guys switch their location (IP addresses) between the countries and finally make their identity unknown to the world. This shows hackers level of expert in web technology and networking sciences. But it does not means that hackers are not traceable, even there are a lot of ethical hackers who are more intellectual to cyber criminals and they can find the criminals by techniques like decrypting and reverse engineering. If we do not take care of internet security we are into deeper problems soon. Governments across the world have to make strict rules to punish the people behind the organized cyber crime groups.

One of these cyber crime groups and a famous group is 'Anonymous'. It is a strongly ideological group that hacked all the popular websites in the past few years. The best part of his group is that they never tried to gain money through their attacks and they claimed that their main motto is to prevent government intervention in the usage of internet. Due to the active growth of attacks, both public and private organizations are allocating billions of dollars for their information security. There are few researches going on which are focusing on the hackers thinking and their social life. With these results, they are able to arrest few hackers in the world. The interesting thing is that few hackers are depressed due to they are not well planned about how to spend the money they are getting in back of attacks. Studies shows that the socio-economical conditions made most of the hackers to commit crime and loot the money from other in a tricky way. Robbery gangs found cyber crime as a simple way of stealing others wealth.

Stuxnet a computer virus which was written in the year of 2010 posed a strong challenge to the cyber-forensic experts. The Stuxnet virus is one of complex viruses and programmed by highly skilled geeks and its main targets are programmable logical controllers (PLC). Stuxnet has three modules: a worm that executes all routines related to the main payload of the attack; a link file that automatically executes the propagated copies of the worm; and a root kit component responsible for hiding all malicious files and processes, preventing detection of the presence of Stuxnet. It attacked all the industry systems which uses PLC'S. Stuxnet reportedly ruined almost one-fifth of Iran's nuclear centrifuges. Cyber – forensic experts first decrypted the virus file and then analyzed the program logic of code. They clearly explored the system function calls, timers and data structures used the virus code. Finally after lot of research they cracked and found solution to crack down the Stuxnet virus.

Hacking is not only specific to computer devices, it can be attacked any of the devices that we use. Devices like mobiles, cars and medical devices can be hacked by a hacker which is an alarming warning to all of us. The successful attacks in medical related equipment by hackers are trigger ICD identification, disclose patient such as name, diagnoses, and other data, discloses cardiac data, change patient name, change ICD's clock, change therapies, inducing fibrillation and power denial of services.

The active attacks reported in cars are of two types. First type is long range wireless attack where hacker takes control of car computer aided components using internet, radio signals or nearest wireless signals. Second type is short range wireless attack where hacker take control of car computer aided components by directly installing new component to computer parts or by connecting new components to the existing spare parts. By using the two types of attacks hackers are able to apply brakes wirelessly, disable the brakes wirelessly and are able to install malware on car's telematics computer over the physical connection. In most of cases hackers completely in to the car's security system and compromises the car security features during the theft. They disable the car locate feature and they bypass anti theft system features.

Researches proves that hackers using reflections to capture smart phones passwords. Hackers have prepared tools to find out what people are typing even from different directions and angles. After recording few sessions they are able to tell what a person is typing including passwords with at least 90% of accuracy.

Global positioning systems (GPS) have revolutionized the usage of maps in real time. Apart from its benefits it has got its own side effects to human privacy. To come over this problem techies have invented GPS spoofer tools. But the unfortunate thing is that hackers are using same tools in a negative way to fool the users. The complexity of this problem arises when it deals with airplane and ships tracking. It would pose a bigger problem for internal security of a country.

More and more, nations are waging attacks with cyber weapons — silent strikes on another country's computer systems that leave behind no trace. One of the live examples for it is Stuxnet virus attack on nuclear weapons of Iran. Cyber weapons are heating up the nations for real wars and extreme nuclear wars. It became active war between India, Pakistan, and many other countries around the globe.