Cyber Criminals and its types

Cyber crime is taken very seriously by law enforcement. In the early long periods of the cyber security world, the standard cyber criminals were teenagers or hobbyists in operation from a home laptop, with attacks principally restricted to pranks and malicious mischief. Today, the planet of the cyber criminals has become a lot of dangerous. Attackers are individuals or teams who attempt to exploit vulnerabilities for personal or financial gain.

Types of Cyber Criminals:

1. Hackers: The term hacker may refer to anyone with technical skills, however, it typically refers to an individual who uses his or her skills to achieve unauthorized access to systems or networks so as to commit crimes. The intent of the burglary determines the classification of those attackers as white, grey, or black hats. White hat attackers burgled networks or PC systems to get weaknesses so as to boost the protection of those systems. The owners of the system offer permission to perform the burglary, and they receive the results of the take a look at. On the opposite hand, black hat attackers make the most of any vulnerability for embezzled personal, monetary or political gain. Grey hat attackers are somewhere between white and black hat attackers. Grey hat attackers could notice a vulnerability and report it to the owners of the system if that action coincides with their agenda.

- **(a). White Hat Hackers –** These hackers utilize their programming aptitudes for a good and lawful reason. These hackers may perform network penetration tests in an attempt to compromise networks to discover network vulnerabilities. Security vulnerabilities are then reported to developers to fix them and these hackers can also work together as a blue team. They always use the limited amount of resources which are ethical and provided by the company, they basically perform pen testing only to check the security of the company from external sources.

- **(b). Gray Hat Hackers –** These hackers carry out violations and do seemingly deceptive things however not for individual addition or to cause harm. These hackers may disclose a vulnerability to the affected organization after having compromised their network and they may exploit it .

- **(c). Black Hat Hackers –** These hackers are unethical criminals who violate network security for personal gain. They misuse vulnerabilities to bargain PC

frameworks. theses hackers always exploit the information or any data they got from the unethical pentesting of the network.

2. Organized Hackers: These criminals embody organizations of cyber criminals, hacktivists, terrorists, and state-sponsored hackers. Cyber criminals are typically teams of skilled criminals targeted on control, power, and wealth. These criminals are extremely subtle and organized, and should even give crime as a service. These attackers are usually profoundly prepared and well-funded.

3. Internet stalkers: Internet stalkers are people who maliciously monitor the web activity of their victims to acquire personal data. This type of cyber crime is conducted through the use of social networking platforms and malware, that are able to track an individual's PC activity with little or no detection.

4. Disgruntled Employees: Disgruntled employees become hackers with a particular motive and also commit cyber crimes. It is hard to believe that dissatisfied employees can become such malicious hackers. In the previous time, they had the only option of going on strike against employers. But with the advancement of technology there is increased in work on computers and the automation of processes, it is simple for disgruntled employees to do more damage to their employers and organization by committing cyber crimes. The attacks by such employees brings the entire system down.