International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Unmasking Cybercriminals: A Comprehensive Analysis of Modern Cyber Crimes

Chandana A R

Student, Dayananda Sagar College of Engineering

Abstract:
In today's digital world, the Internet is wonderful and liberating, but it also hides a growing threat : cybercrime. This paper explores cybercrime, the people who commit it, and why they do it. Also I want to discuss in detail the different types of cybercrimes and the challenges in preventing and investigating them. To protect ourselves, we need to be aware of cyber threats, use strong passwords, keep our software updated. In this dynamic online world, understanding cybercrime and practicing good cybersecurity is the key to keep ourselves and our information secure.

Keywords: Hackers, Cybercrime, Criminals, security, illegal activities, vulnerabilities, Cybersecurity, Internet, devices, networks.

1. Introduction:

Cybercrime is not a new phenomenon, with its roots tracing back to as early as 1834. In 1992, India began experiencing its own share of cybercrimes. Cybercrime, in essence, involves using a computer or other technological means to commit illegal activities. On the other side, cyber security is the protection of internet-connected systems, including hardware, software and data, from cyber attacks.

It is also referred to as information technology security, the rapid expansion of the Internet, coupled with the proliferation of freely accessible websites, has contributed to the growing importance of cyber security in our increasingly interconnected world.

Cybercrime refers to illegal activities that involve the use of a computer. To understand, investigate, or stop these crimes, you need to know a lot about computers. It includes things like stealing someone's identity online, selling illegal stuff, harassing people, or causing problems with harmful computer programs. Cybercrime can happen on the internet or with computers, and it can be done from inside or outside an organization. The term "cybercrime" has changed over the years as more and more people started using the internet globally.

The term "cybercrime" encompasses a range of other terms that are occasionally employed to characterize illegal activities carried out through computer systems. These include but are not limited to computer-related crime, computer crime, internet crime, e-crime, and high-tech crime.

1.1 Cyber security-related definitions:

Cyber terrorism

Cyber terrorism is defined as the act of using computer systems or electronic devices with the intention of carrying out terrorist activities. It involves accessing, or assisting in accessing, computer networks to

consciously engage in or attempt terrorist acts. Cyber terrorists generally employ computers as tools or targets to gather sensitive information for illegal purposes.

Cybernetics

The term" cybernetics" is embedded in the study of information and its application. Cybernetics is a scientific field that intersects neurophysiology, information theory, computing machinery, and automation.

Phishing

Phishing refers to a deceptive tactic that utilizes email programs to trick or betray internet users into revealing confidential information. This information is also exploited for illegal purposes.

Cyberspace

Cyberspace is a virtual area where individuals engage in activities such as chatting, exploring, researching, and playing on the internet.

Cyber squatting

Cyber squatting involves registering, selling, or using a domain name with the intent of benefiting from the reputation of someone else's trademark. It can be considered a form of cybercrime and is related to the act of occupying abandoned physical spaces, known as squatting.

Cyber punk

In the area of science fiction literature, the terms" cyber" and" punk" emphasize the two fundamental rudiments of cyberpunk" technology" and" individuality."

Cyber warfare

Cyber warfare refers to the use of information- based attacks against an unsuspecting opponent's computer networks, with the aim of disrupting and disabling their operations. This concept is nearly linked to historical contexts involving attacks on critical structure, alongside the notion of cyber terrorism.

2. Who are Cybercriminals?

People who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company data or particular data, and generating profit.

Hackers are like computer experts who use their computer skills to break into digital systems, networks, and devices.

- **White- hat hackers** use their skills for good such as to protect companies, governments, and consumers by testing and improving digital security.
- **Black- hat hackers** are bad actors who engage in criminal activity, such as breaking into protected digital systems without authorization and also engage in unethical behavior
- **Gray-hat hackers** usually don't reveal information or crash computer systems.They might illegally search a private system for vulnerabilities, also contact the owner and offer to fix a previously unknown issue.

3. Different types of cybercriminals:

Type 1: Cybercriminals - Seeking Recognition

- **Hobby Hacker**s: These are people who enjoy testing the limits of what technology can do, like tinkerers. They might even change how hardware or software works just for fun.
- **IT Professionals (Social Engineering)**: Some people who work in IT use their skills for good, like ethical hackers who try to find and fix security problems.
- **Politically Motivated Hackers**: These hackers work to support various causes, like anti-globalization movements, using the internet to promote their objectives.
- **Terrorist Organizations**: These groups use the internet for cyber terrorism, which means they carry out attacks online as part of their terrorist activities.

Type 2: Cybercriminals - Not Seeking Recognition

- **Psychological Perverts**: These are individuals whose online behavior deviates from what's considered normal.
- **Financially Motivated Hackers**: They're in it for the money, making cash through cyberattacks.
- **Bots-for-Hire**: Some people hire hackers to do things like fraud, steal information, or send spam.
- **State-Sponsored Hacking**: Governments may employ highly skilled hackers for various purposes, including espionage.
- **Hacktivist**: These are individuals or groups motivated by political and social causes, often using hacking to promote change.
- **Extremely Professional Groups**: Some groups work for governments and are very skilled at breaking into the networks of media companies, big corporations, and defense departments.

Type 3: Cybercriminals - Insiders

- **Disgruntled or Former Employees**: Sometimes, unhappy or former employees may seek revenge by damaging or stealing from their company's computer systems.
- **Competing Companies**: In some cases, rival companies might use their own employees to gain an advantage by causing harm or stealing valuable information from their competitors.

4. Classification of Cybercrimes:

1. Cybercrime against an individual

• Electronic mail spoofing and other online frauds
• Phishing, spear phishing, vishing, smishing
• spamming
• Cyber defamation
• Cyber stalking and harassment
• Computer sabotage
• Pornographic offenses
• password sniffing

2. Cybercrime against property

• Credit card frauds
• Intellectual property(IP) crimes
• Internet time theft

3. Cybercrime against organization

• Unauthorized accessing of computer
• Password sniffing
• Denial-of-service attacks
• Virus attack
• E-Mail bombing
• Salami attack/ Salami technique
• Logic bomb
• Trojan Horse
• Data diddling
• Computer network intrusions

4. Cybercrime against Society

• Forgery
• Cyber terrorism
• Web jacking

5. Crimes emanating from Usenet newsgroup

• Distribution/sale of pornographic material
• Distribution/sale of pirated software packages
• Distribution of hacking software
• Sale of stolen credit card numbers
• Sale of stolen data/stolen property

5. Motives behind Cybercrime:

- Financial Gain: Some individuals engage in cybercrime because they are motivated by greed, aiming to make money illegally.
-Quest for Influence: Others seek to gain power or control through cybercrime, wanting to manipulate or impact digital systems.
- Yearning for Attention: There are those who commit cybercrimes in pursuit of publicity, seeking attention or recognition.
- Seeking Revenge: Some individuals engage in cybercrime as a form of revenge, wanting to harm others who they believe have wronged them.
- Desire for Thrills: A sense of adventure and excitement drives certain individuals to access restricted or forbidden information, seeking a thrill.
- Destructive Intentions: Some cybercriminals have a destructive mindset, intending to cause harm or chaos in digital environments.
- Profit from Security Services: On the other hand, some may engage in cybercrime with the intention of selling their services to enhance network security, albeit through unethical means.

6. Survival Mantra for the Netizens:

The 5P Netizen mantra for Cybersecurity is:
(a) Precaution

(b) Prevention
(c) Protection
(d) Preservation
(e) Perseverance

7.How Criminals Plan the Attacks:

Criminals employ various techniques and instruments to identify weaknesses in their intended target, which can either be an individual or an organization.

Active attacks are usually used to alter the system (i.e., computer network) whereas passive attacks attempt to gain information about the target.

Phases are involved in planning cybercrime:

- **Reconnaissance (Information Gathering)**: This initial phase involves gathering information, and it's considered a passive step, meaning no direct attack is launched at this stage.
- **Scanning and Scrutinizing**: After collecting data, the next step involves checking the accuracy of the information gathered and identifying any weaknesses or vulnerabilities.
- **Executing an Attack (Accessing and Maintaining the System):** In this phase, the actual attack is initiated, with the goal of gaining access to the system and maintaining that access over time.

8. A few ways how Cyber Crimes occur:

8.1 Social Engineering

It is a technique that involves influencing and deceiving people to get them to provide information or take specific actions. It relies on the natural human tendency to trust others rather than exploiting weaknesses in computer security. People are the vulnerability that makes social engineering possible.Social engineers typically use communication tools like phones or the internet. They build inappropriate trust relationships with insiders to gain access to sensitive information or unauthorized privileges. It's essentially an art of exploiting people's trust, often going unnoticed in normal conversations.The ultimate goal of a social engineer is to trick someone into sharing valuable information or granting access to it. To achieve this, social engineers study human behavior, leveraging people's willingness to help, their trust in others, and their fear of getting into trouble. Successful social engineers can obtain information without arousing any suspicions Classification of Social Engineering

- Human-Based Social Engineering
- Computer-Based Social Engineering

8.2 Stalking

Repeated and unwanted communications through phone calls, mail, or social media sites. Following the victim to work, school, home, or other places where they frequently visit. Repeatedly sending the victim unwanted gifts

The behavior includes : monitoring, transmission of threats, ID theft, damage to data or equipment, solicitation of minors for sexual purposes. Cyber stalking has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to harass another. Cyber stalking refers to the use of Internet and/or other electronic communications devices to stalk another person.It involves harassing or threatening behavior that an individual will conduct repeatedly

Types of Stalkers
There are primarily two types of stalkers.

- Online stalkers
- Offline stalkers

Online stalkers:

- Start the interaction with the victim directly with the help of the Internet.
- EMail and chat rooms are the most popular communication medium to get connected with the victim, rather than using traditional instrumentation like telephone/cell phone.
- The stalker makes sure that the victim recognizes the attack attempted on him/her.

Offline stalkers:

- Attack using traditional methods such as following the victim, watching the daily routine of the victim, etc.
- Searching on message boards/newsgroups, personal websites, and people finding services or websites are most common ways to gather information about the victim using the Internet.
- The victim is not aware that the Internet has been used to perpetuate an attack against them.

8.3 Botnets

Bot is an automated program for doing some particular task, over a network. It is a collection of software robots, or bots. Botnets can run automatically or under the control of a remote attacker. Malicious software but can also refer to the network of computers using distributed computing software. A bot is simply an automated computer program one can gain the control of computer by infecting them with a virus or other malicious code that gives the access. Computer system may be a part of a botnet even though it appears to be operating normally. Botnets are often used to conduct a range of activities, from distributing spam and viruses to conducting denial-of-service (dos) attacks.

A Botnet (also called a zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge.

- Ensure following to secure the system
- Use antivirus software and keep it up-to-date
- Set the OS to download and install security softwares automatically
- Use a firewall to protect the system from attacks when it is connected to the Internet
- Disconnect from the Internet when you are away from your computer
- Download the freeware only from websites that are known and trustworthy
- Take immediate action if the system is infected

9. Conclusion:

In conclusion, cybercrime is a pervasive and a developing threat to our progressive digital world. Cybercriminals, ranging from hackers seeking financial gain to politically motivated actors and also insiders, exploit vulnerabilities in technology and human behavior to commit illegal activities online. Their motives may differ, but the consequences can be significant, including financial loss, privacy breaches, and damage to personal and organizational reputations.

To protect ourselves from cybercrime, it's crucial to prioritize cybersecurity. This involves

1. Awareness - Staying informed about possible cyber threats and understanding the tactics employed by cybercriminals is the first step in defense.
2. Alert - Being cautious when sharing particular information, especially online, and verifying the legality of requests for sensitive data.
3. Strong Passwords - Using strong, unique passwords for online accounts and regularly updating them.
4. Security Software - Employing reliable antivirus andanti-malware software and keeping it up to date.
5. Regular Updates - Ensuring that operating systems, software, and devices are regularly updated with the latest security updates.
6. Education - Promoting digital knowledge and cybersecurity awareness in schools, associations, and communities to empower individuals to make safer online choices.
7. Incident Response - Developing a plan for responding to cyber incidents, including data breaches, to minimize damage and recover quickly.
8. Collaboration - Encouraging collaboration between individuals, associations, and governments to share threat intelligence and combat cybercrime collectively.
9. While we can not eliminate cybercrime entirely, a foresight approach to cybersecurity can significantly reduce the risks and consequences associated with these crimes, helping us navigate the digital landscape with greater safety and security.

References:

1. Cyber stalking India, www.indianchild.com.
2. Kabay, M. E. (2000). Studies and Surveys of Computer Crime, Focus. http://securityportal.com/cover/coverstory2001211.html
3. Neelesh Jain and Vibhash Shrivastava (2014) "Cyber Crime Changing Everything – An Empirical Study" https://www.researchgate.net/publication/275709598_CYBER_CRIME_CHANGING_EVERYTHING_-_AN_EMPIRICAL_STUDY
4. Maras, Marie-Helen. (2014). Computer Forensics: Cybercriminals, Laws and Evidence, second edition. Jones and Bartlett.
5. Maras, Marie-Helen. (2016). Cybercriminology. Oxford University Press