RESEARCH ARTICLE OPEN ACCESS

# UNDERSTANDING CYBER CRIME AND SECURITY

Sheetal Kandhare
(Computer Engineering, Savitribai Phule Pune University, India
Email: sheetalkan1999@gmail.com)

************************-

## Abstract:

In the current era with the internet booming in every aspect and Personal and Government or every kind of data is processed online, maximum information of every person is available online and this leads to cyber-attacks and misuse of data. The attacks are motivational and can be done in groups or individuals. This paper gives an understanding of types of cybercrimes and who all are the criminals or who perform the cybercrimes. It aims to explore cybercrimes and types of criminals. The human dependence on online services and platforms increases so as the threats of attacks the awareness for cybercrime and cyberbullying is elaborated in this paper. Emerging trends and threats such as networking and social media platforms etc.

Cybercrime and Cybersecurity go hand in hand. As on base, both are important. It plays an important role to secure and protect confidential data from attacks.

*Keywords* — **Cyber Attacks, Cyber Crime, Cyber Security, Cyberthreat**

************************-

## I. INTRODUCTION

Cybercrime, or computer-related crime, is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrimes can be defined as "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as the Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)".Cybercrime may threaten a person or a nation's security and financial health. Cybersecurity is the body of technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access.

In recent years, Cybercrime has risen and many users' data are been leaked causing damage to individuals and companies. In the period of the covid pandemic, UN report states 350 percent rise in phishing websites.[1][5] As organizations around the world continue to trudge through the disruption caused by the COVID-19 pandemic[5], cybercriminals keep coming up with even more menacing ways of dragging them down. According to research conducted by Cybersecurity Ventures, cybersecurity experts have predicted that cybercrime will cost the global economy $6.1 trillion annually by 2021. With the pandemic serving as a catalyst, cybercrime is expected to soon become the world’s third-largest economy.[1]

The Best way to protect your data on online platforms is to educate people about the prevalent cybersecurity and also the cyber-attacks.

Now a day’s social media is one of the major cause of cybercrime and cyberbullying, the growth in data of social media is on stake and thus the majority of threats lies there. Many models have been developed to reduce the risk but data mining techniques and big data have all the major data for the benefit of companies' rise and profits.

The main goals of cyber-attacks include:

- Loss of Integrity
- Loss of Availability
- Loss of Confidentiality

The Loss of integrity refers to modification and changes made in the system or been destroyed by an unauthorized entity.[4]

The Loss of Availability indicated that when a user needs particular data or information that is not available for that system or at that time. The most common is 404 error occurrence in many websites.

The Loss of Confidentiality is the disclosure of confidential information or data to unauthorized users or individuals. The most common example is an employee leaking their company's confidential data to unauthorized individuals for his/her own profit.

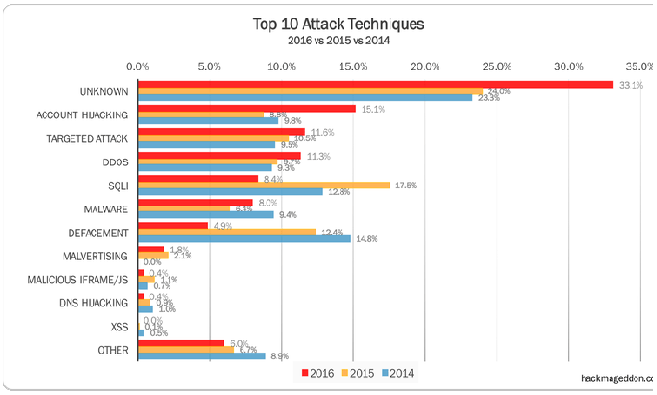


FIG.[2]

## II. TYPES OF CYBERCRIMINALS

Cyberspace is growing very fast thus the rate of cybercrimes. Cybercriminals can be for their personal revenge or group of institutional management.

- Identity Thieves

Identity thieves are cybercriminals who try to access every personal data of the indivdual. They use this data to impersonating or to perform financial transactions.

- Cyber Terrorists

Cyber Terrorists are developed groups or individuals who hack or attack other governments and attempt to steal, Modify or use against the countries or businesses.

- Hackers

Hackers has intension to cause losses to satiate owns or group's motive. Hackers can be white hackers or black hackers. White hackers are those who hack a system to know its disadvantages and protect confidentiality.

Black hackers are who unauthorized and have bad motives.

- Cyber Bulls

Cyberbullying is harassment and bullying someone on the internet via social media platforms or different means. Posting abusive comments and creating fake profiles or chat rooms, spreading rumours.

- Salami attackers

These are the attackers who want financial commissions. Bank employees, illegal transactions are some examples.[2]

- Pranksters

These are individuals performing perpetrate activities.[2]

- Phishing Scammers

Phishers are cybercriminals who try to get all the information that is confidential and sensitive through victims computer or mobile.[7]This often done by capturing small businesses and sites and imitating same aspects. Those computers which are not even suspected can fall to such activities by unknowingly providing personal information including home addresses, social security numbers, and even bank passwords. When such information that is confidential is obtained, phishers either use the data themselves for identity fraud scams or cross sell it on the dark web. It's important for businesses to constantly be aware of phishing scams, particularly scams that may be trying to copycat their own business site. Such sites can tarnish the company's reputation and brand, which could potentially lead to a decrease in earnings.[10]

## III. CLASSIFICATION OF CYBER CRIMES

### *A. Computer as a tool*

- When the individual is that the main target of the crime the pc or computer are often thought-about as a tool of a target.
- These crimes don't seem to be done by technical consultants.
- Examples: Spam, Cyber stalking, Cyber Larceny, etc.

### *B. Computer as a target*

- These crimes are committed by a specific cluster of individuals with technical information.
- Destruction of data within the computer or pc by spreading virus and worms.
- Examples: Disfiguration, Cyber Terrorist act, etc.

### *C. Computer as an instrumentality*

- The crime is committed by manipulating the contents of computer systems.
- With the advent of computers, the criminal has started using the technology as an aid for its perpetuation.
- Eg: Drug trafficking, money laundering, etc.

### *D. Crime associated with the prevalence of computers*

- Copyright violation
- Material traced from various sources that aren't property authorized while not permission of the copyright holder.
- Copyright violation causes legal problems.

## IV. TYPES OF CYBER CRIMES

There are many types of cybercrime, which can cause permanent damage or can terminate the user's access to a particular site and files which are confidential. [9]

### *A. Computer fraud*

International duplicity for personal gain via. The use of computer systems.

### *B. Privacy violation*

Unmasking or exposing personal data such as email address, phone numbers, and account details, etc. on social media or website.

### *C. Sharing copyright files/information*

This involves distributing copyrights protected files such as eBooks and computer programs etc.

### *D. Electronic fund transfer*

This involves gaining unauthorized access to the bank's computer networks and making illegal fund transfer.

### *E. Electronic money lauding*

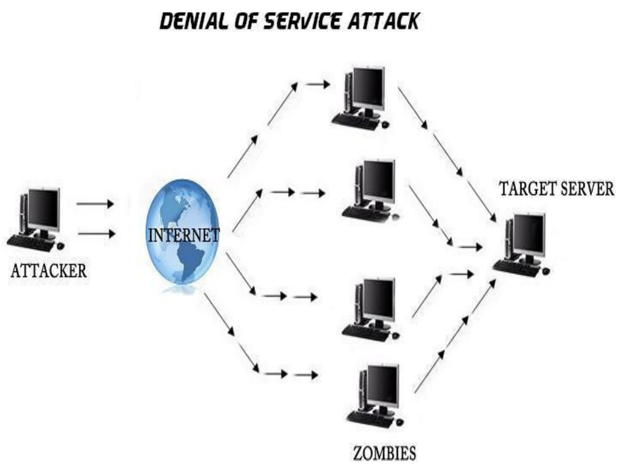
This involves the use of the computer to launder money.

### *F.ATM frauds*

This involves intercepting ATM details such as account number and pin number .these details are used for withdrawal of funds from the intercepted accounts.

### *G. Denial of services*

This involves the employment of computers in multiple locations to attack servers with a read of motility them down. Denial of Service involves flooding laptop resources with additional requests than it handles. This causes the resources to crash thereby denying licensed users the service offered by the resources.



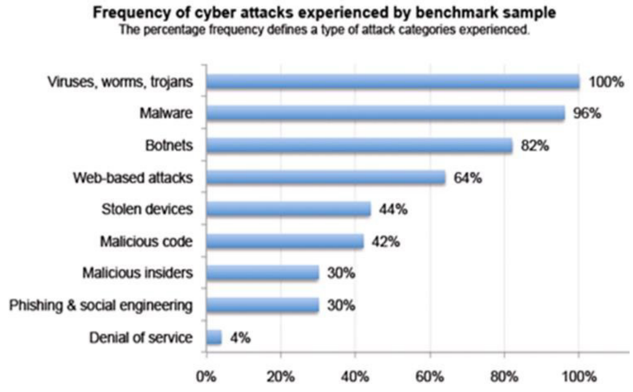
### H. Spam

Sending unauthorized emails .these emails usually contain advertisements. Example: spoofing.

### I. Virus /Worms

Virus/Worms square measure program that attach themselves to a laptop or a file and so the flow into themselves to alternative files and to alternative computer on a network. They sometimes have an effect on the information on the laptop, either by sterilization or deleting it. Worms are not like virus don't want the host to connect themselves to

THE FREQUENCY OF ATTACKS BASED ON ITS TYPES


Frequency of cyber attacks experienced by benchmark sample

The percentage frequency defines a type of attack categories experienced.

## V. TRENDS CHANGING IN CYBERSECURITY

### A. Web Servers

The threats of attacks on web applications to extract data or to gain control over data via web servers. Web servers are the most efficient and best platform for criminals to steal data. Hence individuals must use a safe and protected browser.[8]

### B. Social Media Networking

The Growth of social media since 2012 has increased and the intends to cyber-attacks and cyberbullying too. Companies should increase their policies and laws against more advanced technologies such as data leaking, cyberbullying, and log file analysis.

### C. Cloud Computing

The significant advantages firms get from the cloud, attract firms and individuals to move towards clouds. All firms from small to large are emerging into clouds thus creating a traffic and big challenge.

Thus due to vast advancement and forensic analysis, incident response the matter of cloud will be taken into attention.[8]

### D. New platforms and new devices

New platforms and new devices will create new maps and new routes for cybercriminals to gain data access and threats for individuals. In the early years, only Microsoft and android were running. But with increasing technologies and advancements I-phones, IPad and many more devices are developed which creates new threats and new cybercrimes to happen.

### E. Mobile networks

We are able to connect every people all around the world which is possible with mobile networks. As an advantage, it also has a big security concern. These days firewalls and security concerns have become porous. So, require various securities and a lot of care and awareness about it.[8]

### F. Protecting Systems Rather than Information

Protecting the system will create more impact on protecting the data or information within. It will not just protect the system but also avoid criminals to crack the system. To avoid leaking data or frauds.

## VI. PREVENTION FROM CYBERCRIME

- It is not possible to eliminate cybercrime from cyberspace. It is quite possible to check them.
- Awareness is the first step in protecting yourself.
- Invest in Anti-virus, Firewall, and SPAM blocking software for your PC.
- Change passwords regularly
- Use complex passwords (include numbers and special characters)
- Avoiding the use of unauthorized software.
- Avoid opening unknown emails.
- Use internet filtering software.
- Data Level Security Using encrypting software
- Disable remote connectivity (such as Bluetooth)

## VII. CONCLUSION

This manuscript puts all the aspects on happening cybercrimes and understanding each cybercriminal and also cybercrime. It states the understanding of various cybercriminals and the causes or reason behind the attacks. Prevention needs to be undertaken and with the rise in global cybercrime rates, each individual must have knowledge about attacks and prevention and protection of their data.

The paper gives an eye to the rise in attacks and ways to prevent them. Cybercrime and security should be given a boost to make awareness of a rise in usage of the internet and big data.

## REFERENCES

[1] https://securityboulevard.com/2020/12/cybercrime-expected-to-rise-at-an-unprecedented-rate-in-2021/

[2] Hemraj Saini et.al Cyber-crime and their impacts: A review

[3] Cyber Crime, Cyberthreat, Cyber Security Strategies and Cyber Law in Nepal. SHAILENDRA GIR

[4] https://commissum.com/blog-articles/the-cia-triad-the-key-to-improving-your-information-security

[5] https://www.newindianexpress.com/business/2020/aug/08/increasing-cybercrime-un-reports-350-per-cent-rise-in-phishing-websites-during-pandemic-2180777.html

[6] http://en.wikipedia,org/wiki/Computercrime

[7] http://en.wikipedia,org/wiki/Computersecurity

[8] A STUDY OF CYBERSECURITY CHALLENGES AND ITS EMERGING TRENDS ON LATEST TECHNOLOGIES G.NIKHITA REDDY

[9] https://searchsecurity.techtarget.com/definition/cybercrime

[10] https://online.norwich.edu/academic-programs/resources/who-are-cyber-criminals