iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** IX **Month of publication:** September 2021

DOI: https://doi.org/10.22214/ijraset.2021.38023

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IX Sep 2021- Available at www.ijraset.com

Security in Cyber Crime

Prof. Simranpreet Kaur
CSE, Dronacharya Group of Institutions

Abstract: ***The crime that involves and uses computer devices and Internet, is known as cybercrime. Cybercrime can be committed against an individual or a group; it can also be committed against government and private organizations. It may be intended to harm someone's reputation, physical harm, or even mental harm. Due to gradually increase of the internet users and netizens, abusage of technology is broadening gradually which tends to cyber-crimes. Cybercrime causes loss of billions of USD every year. Cyber Security, a mechanism by which computer information and the equipments are protected from unauthorized and illegal access. This paper illustrates and focuses on cybercrime, how society suffered, types of threats, and cyber security.***
Keywords: Cybercrime, Types, Protection, Cyber security, Hackers, Impact.

I. INTRODUCTION

Cybercrime, also called **computer crime**, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.

Because of the early and widespread adoption of computers and the Internet in the United States, most of the earliest victims and villains of cybercrime were Americans. By the 21st century, though, hardly a hamlet remained anywhere in the world that had not been touched by cybercrime of one sort or another.

Cybercrime is not an old sort of crime to the world. It is defined as any **criminal activity** which takes place on or over the medium of computers or internet or other technology recognised by the Information Technology Act. Cybercrime is the most prevalent crime playing a devastating role in Modern India.

II. CYBER CRIME

New technologies create new criminal opportunities but few new types of crime. What distinguishes cybercrime from traditional criminal activity? Obviously, one difference is the use of the digital computer, but technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Criminals do not need a computer to commit fraud, traffic in child pornography and intellectual property, steal an identity, or violate someone's privacy. All those activities existed before the "cyber" prefix became ubiquitous.

Cybercrime, especially involving the Internet, represents an extension of existing criminal behaviour alongside some novel illegal activities.

Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. In other words, in the digital age our virtual identities are essential elements of everyday life: we are a bundle of numbers and identifiers in multiple computer databases owned by governments and corporations. Cybercrime highlights the centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity.

A. Generally, it is Classified into two forms of Categories

1) Crimes targeting computer devices or network directly. Examples of crimes targeting computer devices or network directly would include,

a) Malicious and Malware code

b) Denial-of-service

c) Computing viruses

2) Prime target is independent of device or computer network. Examples of crimes whose prime target is independent of device or computer network would include,

a) Cyber stalking
b) Fraud and identity theft
c) Phishing scams
d) Information warfare

III. TYPES OF CYBERCRIME

Let us now discuss the major types of cybercrime –

A. Hacking

It is an illegal practice by which a hacker breaches the computer's security system of someone for personal interest.

B. Unwarranted Mass-surveillance

Mass surveillance means surveillance of a substantial fraction of a group of people by the authority especially for the security purpose, but if someone does it for personal interest, it is considered as cybercrime.

C. Child Pornography

It is one of the most heinous crimes that is brazenly practiced across the world. Children are sexually abused and videos are being made and uploaded on the Internet.

D. Child Grooming

It is the practice of establishing an emotional connection with a child especially for the purpose of child-trafficking and child prostitution.

E. Copyright Infringement

If someone infringes someone's protected copyright without permission and publishes that with his own name, is known as copyright infringement.

F. Money Laundering

Illegal possession of money by an individual or an organization is known as money laundering. It typically involves transfers of money through foreign banks and/or legitimate business. In other words, it is the practice of transforming illegitimately earned money into the legitimate financial system.

G. Cyber-Extortion

When a hacker hacks someone's email server, or computer system and demands money to reinstate the system, it is known as cyber-extortion.

H. Cyber-Terrorism

Normally, when someone hacks government's security system or intimidates government or such a big organization to advance his political or social objectives by invading the security system through computer networks, it is known as cyber-terrorism.

IV. PROTECTION FROM CYBERCRIME

A. The best ways to protect computer from cybercrime:
B. Keep software and operating system updated
C. Use anti-virus software and keep it updated
D. Use strong passwords
E. Never open attachments in spam emails
F. Do not click on links in spam emails or untrusted websites
G. Do not give out personal information unless secure
H. Contact companies directly about suspicious requests

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IX Sep 2021- Available at www.ijraset.com

V. CYBER SECURITY

Cyber security is a potential activity by which information and other communication systems are protected from and/or defended against the unauthorized use or modification or exploitation or even theft.

Likewise, cyber security is a well-designed technique to protect computers, networks, different programs, personal data, etc., from unauthorized access. All sorts of data whether it is government, corporate, or personal need high security; however, some of the data, which belongs to the government defense system, banks, defense research and development organization, etc. are highly confidential and even small amount of negligence to these data may cause great damage to the whole nation. Therefore, such data need security at a very high level.

A. How to Secure Data?

Let us now discuss how to secure data. In order to make your security system strong, you need to pay attention to the following −

1) Security Architecture
2) Network Diagram
3) Security Assessment Procedure
4) Security Policies
5) Risk Management Policy
6) Backup and Restore Procedures
7) Disaster Recovery Plan
8) Risk Assessment Procedures

Once you have a complete blueprint of the points mentioned above, you can put better security system to your data and can also retrieve your data if something goes wrong.

VI. TYPES OF HACKERS

These criminals or hackers are usually engineers, doctors, MBA students etc all educated people who tries to gain the access of other's system. These are:

1) *Script Kiddies:* Script kiddies are non-technical expertise and hack the weakly secured systems. They cannot seriously harm the victim.
2) *Scammers:* Scammers sends the fake mails to the targeted victim like fraud prizes (lottery), discount pharmaceuticals, etc by which they access the victim's system and corrupts it.
3) *Hacker Groups:* They anonymously work and hacks the system for no criminal reasons. They are basically hired by government agencies, organizations, etc. to examine the security and handle the fraud cases.
4) *Phishers:* They request the confidential information over the network under false pretences to fraudulently get credit card details, passwords and other personal information. Phishing is carried out by mail spoofing and directs the users to get details at a fraud website that is almost identical to the legitimate one.
5) *Political/religious/commercial Groups:* These types of hackers develop malicious threats or malwares for political concern ends and have no interest in any kind of financial gain. They tries to access the confidential information of the opponent groups.
6) *Insiders:* These attackers are very dangerous as they reside in the organization only. By residing in the organization they acquire complete knowledge and details of the organization and easily corrupt the system attack and harm the security of the company.
7) *Advanced Persistent Threat (APT) Agents:* This is responsible for highly targeted attacks which are carried out by well organized and state-sponsored groups. They have higher technical skills and have access to the vast computing resources.
8) *White Hat Hackers:* They are ethical hackers who basically focus on securing and protecting IT systems. White hat hackers are those who attempts to break into network or system in order to help the holder of the system by making an effort to aware them of the security flaws. Many such kind of people are employed by the companies concerning about the computer security; these are professional sneakers and the collective group of them are often categorised as tiger teams.
9) *Black Hat Hackers:* An individual who compromises with the security of computer system without any acknowledgement from the authorized party. They uses their knowledge to exploit the systems.
10) *Grey Hat Hackers:* A Grey Hat Hacker is considered as a skilled hacker in the security community who at times acts legally, and sometimes not. They are considered as hybrid between black and white hat hackers. They basically do not hack with the malicious intentions.

VII. IMPACT OF CYBERCRIME

Worms are the most strong form of cyber attack which causes severe disruption. In the month of September, in 2010, Stuxnet infected and affect the unknown number of industrial controls around the whole world, and stealthily give invalid instruction's to the machinery and some false readings to the operators. Potentially, it destroys gas pipelines, causes nuclear plant to malfunction or causes boilers of factory to explode. This worm was known to be active mostly in Iran, on the same Indonesia, Pakistan, India also reported as infections.

1) *Crime Against People:* In this, the criminal provides numerous false promotions and gives the people an illusion of security by forcing them to administer their personal information. It includes child pornography, a dominant offence. Social networking sites and the chat groups can also be concluded as a serious cyber crime at times.
2) *Crime Against Property:* Criminals can easily with their techniques steal the personal information of the other people computer system and the theft gains the unauthorized access to an internet connection, can be a cyber crime.
3) *Crime Against Business:* In this crime, criminal basically hacks the system or machine of any business organization; they store and steal the confidential and the sensitive data of the system on the server. They acquire unauthorized access to the secured and confidential data of the company and via this, they transfer fund's of the company to their accounts that makes the organization bankrupt.
4) *Crime Against Government:* Cyber terrorism is a term used against government crime in which hackers hacks the secured and confidential database of the government with the urge to use sensitive and personal information of the government that reduces the faith of the citizens.

VIII. CONCLUSION

In this modern era of technology, the role and usage of internet is increasing worldwide rapidly, therefore it becomes easy for cyber criminals to access any data and information with the help of their knowledge and their expertise. Cyber crime is an unlawful act or a menace that needs to be tackled firmly and effectively. There is a need to create more awareness among the people and basically users of internet about cyber space, diverse forms of cyber-crime and some preventive measures as “Prevention is always better than cure”, so it is seriously advised to take some previous precautions while operating the internet. Security nowadays is becoming a prominent and major concern. In the following paper, some security issues are introduced, threats, Trojans, and attacks over internet. Computer security becomes critical in many of the technology-driven industries which operate on the computer systems. Computer security is nothing more than computer safety. Countless vulnerabilities and computer or network-based issues are acts as an integral part of maintaining an operational industry.

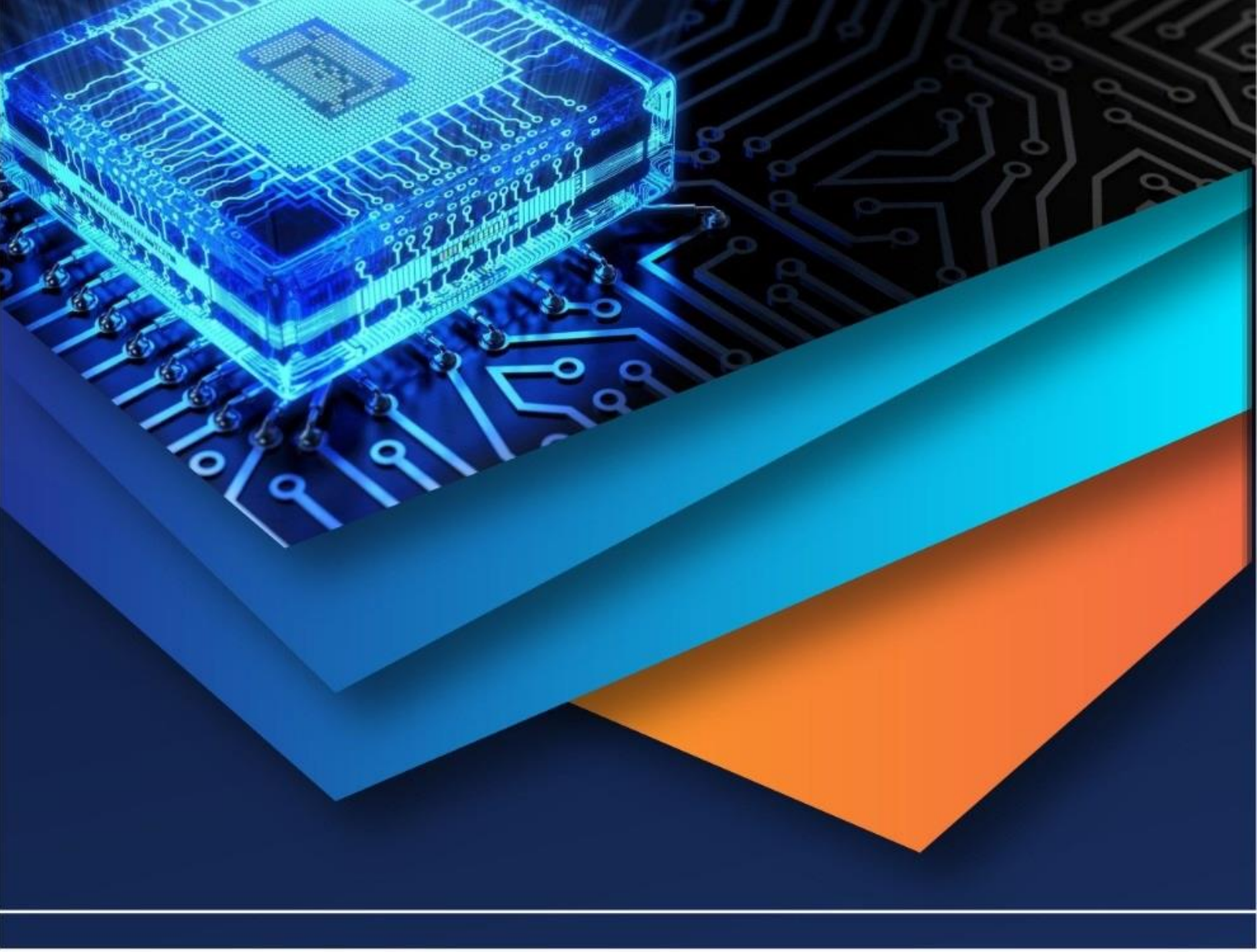
IX. ACKNOWLEDGMENT

We would like to thank everyone, especially faculty members and our respected mentors, friends, and family members who provided support and followed up with us for such a long period, and trusted us regarding the content of the paper.

REFERENCES

[1] Pooja Aggarwal , Neha, Piyush Arora , Poonam , “REVIEW ON CYBER CRIME AND SECURITY”, IJREAS, Vol. 02, Issue 01, Jan 2014.
[2] Ammar Yassir and Smitha Nayak, “Cybercrime: A threat to Network Security”, IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.2, February 2012.
[3] Atul M. Tonge, Suraj S. Kasture, Surbhi R. Chaudhari, “Cyber security: challenges for society- literature review”, IOSR Journal of Computer Engineering (IOSR-JCE) , Volume 12, Issue 2 (May. - Jun. 2013), PP 67-75.
[4] C. Catlett (ed.), “A Scientific Research and Development Approach to Cyber Security”, Report submitted to the U.S. Department of Energy, December 2008.
[5] Seema Vijay Rane & Pankaj Anil Choudhary, April 2012-September 2012, “Cyber Crime and Cyber Law in India”, Cyber Times International Journal of Technology and Management, Vol. 5 Issue 2.
[6] Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. London: Academic Press, 2011: Pp. 5-19.
[7] Richards, James. Transnational Criminal Organizations, Cybercrime, and Money Laundering: A Handbook for Law Enforcement Officers, Auditors, and Financial Investigators. Boca Raton, FL: CRC Press, 1999: Pp. 21-54.
[8] Ravi Sharma, Study of Latest Emerging Trends on Cyber Security and its challenges to Society, International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1 ISSN 2229-5518 IJSER © 2012.
[9] BinaKotiyal, R H Goudar, and Senior Member, A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India PritiSaxena, IACSIT International Journal of Information and Education Technology, Vol. 2, No. 2, April 2012.
[10] B.T. Wang and H. Schulzrinne, “An IP traceback mechanism for reflective DoS attacks”, Canadian Conference on Electrical and Computer Engineering, Vol. 2, 2-5 May 2004, pp. 901 – 904.

[11] Y. C. Hu, A. Perrig, and D.B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks", in Proceedings of the 22 nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM ˝03), vol. 3, San Francisco, CA, Mar. 2003, pp. 1976-1986.
[12] Shio Kumar Singh, M P Singh, and D K Singh, "A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks", International Journal of Computer Trends and Technology- May to June Issue 2011.
[13] M. Cagalj, S. Capkun, and J.P. Hubaux, "Wormhole-based Anti-Jamming Techniques in Sensor Networks" from http://lcawww.epfl.ch/Publications/Cagalj/CagaljCH05-worm.pdf.
[14] A. T. Zia, "A Security Framework for Wireless Sensor Networks". 2008, http://ses.library.usyd.edu.au/bitstream/2123/ 2258/4/02whole.pdf.
[15] en.wikipedia.org/wiki/Cyber_security_standards.
[16] en.wikipedia.org/wiki/Cyber_crime.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY