JOURNAL OF MULTIDIMENSIONAL RESEARCH & REVIEW

Website: http://www.jmrr.org Vol.2, Iss.3 Pages:25-31

A STUDY OF CHALLENGES AND RECENT TRENDS IN CYBER SECURITY

K Tharmi[1], A Rahana Banu[2], B Subathra[3]

[1]Web Administrator, [2,3]BCA, PG Department of Computer Science,
Holy Cross College, Trichy, Tamilnadu

Article Received: April 2021 Published: October 2021

Abstract

Cyber security is a necessary consideration for information technology as well as Internet services. The people need to recognize the importance of different types of risks that exist in the online world. Enhancing cyber security and protecting critical information are essential to nation's security and economic being. Cyber security issues have become national security issues. Whenever the users think about the cyber security, they think of "cyber-crime" which is increasing day by day. Various government and companies are taking many measures to prevent the cyber-crime. This paper mainly focuses on trends, challenges and cyber ethics in the field of cyber security. Cyber incidents emphasize the importance of staying up-to-date on global cybercrime trends, especially of mobile and personal computing devices.

Keywords: Cyber crime, Cyber security, Cyber crime trends, Cyber ethics.

INTRODUCTION

Today in this technological world people able to send and receive any type facts may be a email, audio or video just by snapping a button but did the users ever think how security their facts is being transmitted to other person without any leakage of information? The answer lies in cyber security. At the present time, Internet is the fastest growing infrastructure in every life. The technology has changed the whole environment of mankind. When looking into it one thing is clear. Technologies will not look like they look. Cybercrimes are increasing day to day. The fight against cybercrime needs a vast and safer approach. Technical measures alone cannot prevent any crime the users need to have law enforcement agencies to investigate and continue with cybercrime effectively. Today many nations and governments are imposing strict laws on cybercrime. However, cyberattacks is faster cheaper and easier than cyber defense. Nearly 90% of business transactions are done on online. So this field need a proper security for clear and best transaction. And cyber security has become a modern issue. It plays a significant role in the ongoing development of information technology.

Cyber Crime: An untechnical definition of cybercrime may be "unlawful acts where in the computer are either a tool or target are both".

Cyber Security performs a vital position in the subject of information technology. In the present day, protecting the information has become one of the most difficult tasks. Cybercrime increases day by day. To prevent these cybercrimes, Governments and various organizations are taking many actions. This paper mainly focuses on difficulties faced by cyber security on the recent technologies and also focuses on types of cybercrime, cyber security, emerging cybercrime trends and cyber ethics.

TYPES OF CYBER CRIME

COMPUTER USED AS TOOL

a. Financial Crime: Financial crime is the crime which is generally committed towards the property, against the laws and conventions of the ownership of the property might be to one's personal use and benefits.

b. Illegal Content: This cyber involve criminal sharing and distributing ill-suited content that can be considered highly distressing and offensive. The content include but is not limited to sexual activity between adults, videos with fierce violent advocating terrorism related acts and child exploitation material etc.

c. Pornography: Cyber pornography is defined as the act of using cyberspace to create, view, distribute import or publish pornography or salacious materials.

d. Online Gambling: Online gambling is the most remunerative business that is developing today in cyber crime. Nowadays, In India many betting in the name of games are through computer and internet. Many cases have come to light related to credit card crimes, offering jobs etc.

e. Email Spoofing: Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. Email spoofing is an approach used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate source. There are different types of email spoofs, but they all have similarities. One main similarity is that you receive an email which claims to be from someone you know but in reality, it has been sent by another source.

f. Cyber Defamation: As per Indian Penal Code (IPC) whoever, by words either spoken or intended to be read, or by signs or visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person is said to defame that person. Cyber defamation is the new form of committing traditional defamation where virtual communication is used to defame an individual or organization.

g. Cyber Stalking: Cyber stalking is a criminal practice in which attacker use internet and other electronic device to persistently harass victims.

Example: State of Maharashtra vs Atul Ganesh Patil

A woman had come for job interview to a company and wrote her mobile number in the entry register. The guard saved her contact details and started sending multiple obscene whatsapp messages and even called her repeatedly to talk obscene things thereby committing crime of stalking her. In this case, victim blocked his number. However, the guard started sending her obscene messages from his friend's mobile phone. A case was registered under IPC354D. The police acted swiftly completing the investigation and prepared a change sheet within 24 hours.

COMPUTER USED AS TARGET

a. Unauthorized Access to Computer or Computer Network: This kind of offence is normally referred as hacking in the generic sense. The Indian law has however given a different undercurrent to the term hacking, so the people will not use the term "Unauthorized Access" interchangeably with the term "Hacking". It is an attempt to exploit the weaknesses for gaining unauthorized access in a computer system or network. As per IT act, hacking is the term used to describe the act of destroying or deleting or altering any information residing in a computer resource or diminishing its value or utility, or affecting it injuriously in spite of knowing that such action is likely to cause wrongful loss or damage to the object, public or a person.

b. Theft of Information Content in the Electronic Form: This includes facts stored in computer hard disks, removable storage media etc. Theft may be either by appropriating the facts physically or by dabbling them through the virtual medium.

c. Email Bombing: Email bombing is a form of an abuse consisting of sending huge email to a single address or recipient in an attempt to overflow the mailbox or overwhelm the server the email address is hosted causing denial of service.

d. Salami Attacks: An attack is made on a system or network that involves making minor alteration so insignificant that in a single case it would go completely unnoticed. These attacks are generally used for the commission of financial crimes.

e. Web Jacking: Web jacking is an advanced phishing technique where attackers make a clone of a website and send that malicious link to the victim. Once, the victims click the link that looks real he will be redirected to fake page where attackers try to extract sensitive data such as card numbers, user names, passwords etc., from the victims.

The following statistics clearly strategies, the percentage of cybercrimes took place in India in the year 2018 – 2019.

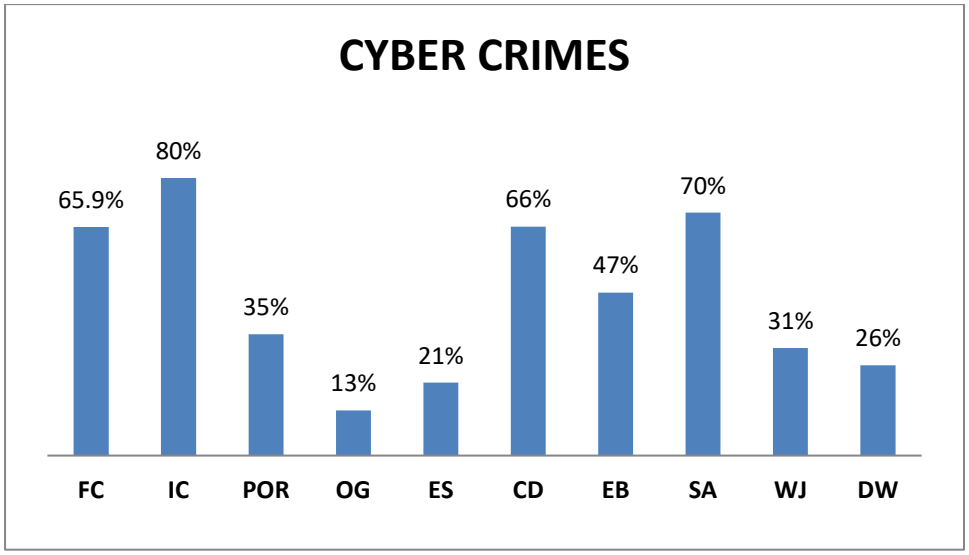

Fig 1 Cybercrimes in India in the year 2018 – 2019

FC - Financial Crime
IC - Illegal Content
POR - Pornography
OG - Online Gambling
ES - Email Spoofing
CD - Cyber Defamation
EB - Email Bombing
SA - Salami Attacks
WJ - Web Jacking
DW - Dark Web

CYBER SECURITY

Normally the privacy and security of the data will always be in the top measures in which any organization takes care. The people are currently living in the world where all their facts are

maintained in digital form or in a cyber form. Usually social networking sites furnish a space where users feel safe to interact with the people. Cyber-criminals would continue to aim social media sites to steal personal data of the home users. And mainly during the bank transactions user must take all the security measures needed.

EMERGING CYBERCRIME TRENDS

1. Ransomware

Among the different malware variants available, ransomware or cryptoware, to be more precise has become the dominant threat. While more 'commercial' data-stealing malware typically still targets desktop windows users, ransomware is more indiscriminate. Its target ranges from individual user's devices to large organisations and even governments.

2. Vulnerabilities

In computer security, vulnerability is a weakness which allows an attacker to reduce a system's information assurance. A criminal can exploit the vulnerabilities and gain unauthorized access to resources. For e.g.: A user opens an email message with attached vulnerable code, which exploits the vulnerable system / application software's present on the user's computer to gain unauthorized access to resource on the victims computer.

3. Dark Web

The deep web is part of the internet where a typical search engine cannot index. The dark web / darknet is a subset of deep web that is intentionally made hidden through overlay networks and require specific software, configurations or authorization to access. Frauds are openly discussed on the underground forums of the dark web where illicit vendors offer fraudulent servicers. These services includes launching a DoS attack on websites, the sale of malware, illegal drugs, weapons, cyber espionage on behalf of clients and the list goes on. Most of the vendors accept the payment through crypto-currencies and specially Bitcoins due to its popularity.

4 Cloud Computing

Cloud computing is nothing but data stored on server computer. Nowadays world is moving towards the cloud. Cloud computing is one of the trend that presence the greatest challenge for cyber security. "N" number of applications available in the cloud. Policy controls for clouds services which are most needed to prevent the threat post by the cyber criminals. Cloud computing provides "N" number of platforms for applications. It must be also concerned that the cloud computing is free of security.

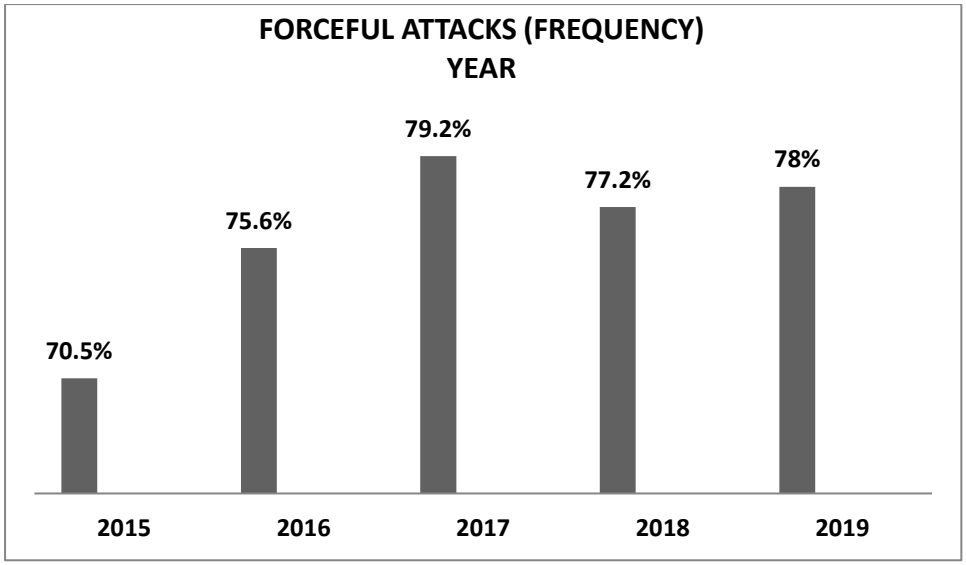

Fig 2 Cyber Attacks in 5 Years

CYBER ETHICS

Cyber is the code of the internet. Cyber ethics are like taking prevention while working on the internet. Some cyber ethics to be followed are: Never sharing personal information, Dont share embarrassing pictures or information's related to any persons, Internet is considered as the world's largest library use legally, Never send any malware to corrupt other system, Never sign into other's accounts and Use the internet to communicate with people around the world.

FINDINGS

Some of the highlights of the cyber security have been discussed in this paper: cybercrime, types of cybercrime, cyber security, emerging cybercrime trends. Till date there is not exact solution for cybercrime but by getting to know all this points which have been discussed in this paper, the people can try their level best to minimize them, in order to have a safe and secure future in cybercrime.

CONCLUSION

Cyber security is the vast topic but it is the most important topic to be discussed in today's world. Nowadays there are lots of critical transaction which are been carried out through internet and through internet networks. Lots of data are been transferred through the internet. Huge collection of data is getting stored in the network. In today's world, cyber security is a crucial part of any business. The people must understand the importance of following the good cyber guidelines to stop intrusions.

REFERENCES

1. Vidhya P.M "Cyber Security -Trends and Challenges" IJCSMC, Vol. 3, Issue. 2, February 2014, pg.586 – 590.
2. 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 ISSN 2229-5518.
3. Eric A. Fischer Senior Specialist in Science and Technology "Cyber security Issues and Challenges: In Brief" August 12, 2016.
4. Dr. Jeetendra Pande, Assistant Professor School of CS & IT, Uttarakhand Open University, Haldwani "Introduction to Cyber Security " ISBN: 978-93-84813-96-3.
5. Veenoo Upadhyay, Dr. Suryakant Yadav "Study of Cyber Security Challenges Its Emerging Trends: Current Technologies" International Journal of Engineering Research and Management (IJERM) ISSN: 2349- 2058, Volume-05, Issue-07, July 2018.
6. Hadi Saeed Alqahtani "Latest Trends and Future Directions of Cyber S ecurity Information Systems" Journal of Information Engineering and Applications www.iiste.org ISSN 2224-5782 (print) ISSN 2225-0506 (online) Vol.6, No.11, 2016.
7. Shashirekha Malgi "Cyber Crimes under Indian IT Laws" The research paper published by IJSER journal is about Cyber Crimes under Indian IT Laws ISSN 2229-5518.
8. Nikhil A. Gupta, "Cyber Crime and Information Technology Act 2000 ~ An Overview ~".
9. G. Nikhita Reddy1, G.J. Ugander Reddy2 "A Study of Cyber Security Challenges and its Emerging Trends on Latest Technologies".
10. Kamini Dashora, PhD "Cyber Crime in the Society: Problems and Preventions" Journal of Alternative Perspectives in the Social Sciences (2011) Vol. 3, No. 1, 240-259.

Cite this article:

K. Tharmi, A. Rahana Banu, B. Subathra, "A Study of Challenges and Recent Trends in Cyber Security", Journal of Multidimensional Research and Review (JMRR), Vol.2, Iss.3, pp.25-31, 2021