CYBER SECURITY A CHALLENGE AGAINST CYBER-CRIMES

SREERAJ M K
PG Department of Commerce and Management Studies
SVTB College, Mannampatta
Palakkad, India
sreerajkesavanmk@gmail.com

SOORAJ A M
PG Department of Commerce and Management Studies
SVTB College, Mannampatta
Palakkad, India
iamsoorajam@gmail.com

Abstract*— Privacy and security are two terms which leads the global talks and discussions. Information technologies has opened a breakthrough of technological innovation in collecting, storing, processing, transmission and presentation of information. We all enjoy the benefits of the internet, and in this internet era it has become an indispensable tool for work as well. What is being healthy and what is being unhealthy internet use? This has to be discussed cautiously Drawing out the attention to cyber security happens when the count of cyber-crimes become enormous. The paper focus on the major areas in which cyber-attacks occurs and various types of cyber threats.

Keywords— Cyber Security, Cyber-Crimes, Cyber Ethics, Cyber Law.

INTRODUCTION

Crime is a social and economic phenomenon. It is a legal concept. Crime is an offence which is a legal wrong that can be followed by criminal proceedings which may results in punishments. Cyber-crime is a complicated issue to the species of which genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting the crime. Crimes in internet are also increasing in a continuous manner.

Cyber security has got wider acceptance and it has become a matter of global interest and importance. Making secure is about the protection of assets from various threats posed by certain inherent vulnerabilities. Security enhances or ensures the security control measures. Due to the rapid advancements in technology which paved the way to enhance all the decision making virtually, disruptive technologies has also found their space in this internet era. Security refers to the rules, policies, procedures, and technical and innovative measures to prevent unauthorized access, alteration, theft, physical damage to information systems. The basic objective of information security is the protection of interests of those who depends on information from damages resulting the computer disasters.

Cyber security plays a vital role in the upcoming advancements and developments in IT sector and its services. A comprehensive and broader approach has to be built for the strategies that has to be formulated to defend the cyber-attacks in the national and international framework.

CONTENT

Threats and crimes

1. Cyberbullying

   It is a threat by the use of electronic communication to bully a person, typically by sending constant messages in a threatening nature.

2. Financial crimes

   With the increasing demand and emergence of the on-line banking or e- banking facilities the financial crimes have become very alarming. Financial crimes include credit card frauds, robbery and theft in ATM counters. The criminals get information from their victims asking for their credit information. The common people become prey to this without proper inquiries and acknowledgement and pass their credit card information to these criminals. It is also known as salami attacks.

3. Cyber Pornography

   Pornographic websites are those which allow downloading of pornographic movies, videos, pictures, on-line pornography magazines (photos, writings etc.), all come under this head. Cybersex addiction is a typical sex addiction on internet which are easy to access. Cybersex addiction can erode and even spoil the intimacy in human relationships.

4. Drug Trafficking

   Drug traffickers use latest advanced and innovative technologies to sell narcotics. They pass the relevant information in time and arrange the place, where and how to exchange, using couriers and encrypted mails. Since there is no personal communication between the buyer and dealer, they even don’t know who all are involves in this crime.

5. Cyber Terrorism

   Cyber terrorism is the politically motivated use of computers and information technology to cause severe disruption or creating a widespread fear in society. Section 66F of IT Act 2008 deals with cyber terrorism. Cyber terrorism may include passing the misleading information through internet about bomb attacks which may happen in the future. Terrorism can create a fear in the minds of the people. The victims of the cyber terrorism can be a huge mass. Cyber terrorists threaten or through the act of coercion attacks an individual, an organization or even a government.

6. Cyber Stalking
 Cyber stalking is the repeated use of electronic communications to harass or frightening someone by sending the constant mails with threat messages and useless content. These may include sending messages on the victim's bulletin boards, might be through social networking sites or even through e-mails. Section 354A of IPC deals with the punishments relating to cyber stalking.

7. Hacking
 A hacker is a person who gains unauthorised access to a computer network for profit, criminal mischief or personal pleasure. They are also known to be as crackers. Generally gaining of unauthorised access to data stored in a system software is known as hacking. Section 66 of IT Act deals with hacking.

8. Worms
 Computer worms are those programs that reproduce, execute independently and travel whole across the network connections.it has the ability to destroy crucial files, slowing down , causing critical programs to stop working.

9. Phishing
 Phishing is a method of online identity theft. The use of SPAM, malicious websites, email messages and instant messages to trick people to collect sensitive information such as personal details bank and credit card accounts details.

10. Spyware
 It is the use of technology in collecting information and other private details about a person or organization without their knowledge. Spyware can enter in a computer system as a software virus or as the result of installing a new program.

Other forms of cyber crimes

- Theft in the Services of Telecommunication
- Piracy of Telecommunication
- Dissemination of Offensive Materials
- Laundering E-money and Evasion of Taxes
- Extortion, Terrorism and Electronic Vandalism
- Fraud in Sales and Investments
- Illegal Interception of Telecoms Signals
- Fraud in Transfer of Electronic Funds

Remedies?

Obviously, to eradicate the crimes to certain extend there some remedies against these cyber-attacks. This can be generalized to the cyber securities.

1. Checking system security
2. Use of firewalls
3. Data encryption
4. Installation of antivirus programs
5. Acquisition of software from reliable sources
6. Testing new applications in single computer
7. Use a pop-up advertising blocker
8. Use of strong passwords
9. Avoid clicking on unexpected or unfamiliar links.
10. Secure wireless networks.

CYBER ETHICS

Cyber ethics is quite simple the study of ethics on the internet. It is often called information system ethics and moreover it can be clearly defined as "the study of moral, legal, ethical issues involving the use of information and communication technologies". It simply refers to the code of conduct of safe and responsible behavior for the internet community.

A common knowledge on ethics is that it is old as human civilization. The emerging ethical issues are due to various problems mainly about the popularity of the internet, development in computer systems, introduction of new and efficient storage cost, advanced data mining techniques.

CYBER LAW

Information Technology Act 2000

The major areas or provisions contained in IT Act 2000 are:

1. All the electronic contracts should be legally valid and all the digital signatures should enhance legal recognition.
2. Appointing the certified authorities, controller of certifying authorities
3. Investigating the computer crimes defined under the act and imposing stringent penalties.
4. Establishment of Cyber Appellate Tribunal
5. Take the actions to apply for offences or contraventions committed outside India
6. Power of police officers and other officers to enter into any public place and search and arrest without warrant.
7. Constitution of Cyber Regulations Advisory Committee who will advise the central government and controller.

Information Technology (Amendment) **Act 2008**

The Government of India has brought major amendments to ITA 2000 in form of the Information Technology Amendment Act, 2008. ITA (Amendment) Act 2008 as the new version is often referred has provided additional focus on information security. It has added several new sections on the offences including cyber terrorism and data protection.

CONCLUSION

We live in a wondering time in history. The widespread availability of computers systems and internet connections provides a lot of opportunities to communicate and learn. The government should come forward to enact suitable legislations where and whenever necessary to save the people from the difficulties associated with the usage of computers and internet. This is an era of digitalization. We all are moving to digital economy. In order to enhance a smooth living securities has to be provided for the users.

REFERENCES

[1] Esther Ramdinmawii, Seema Ghisingh, Usha Mary Sharma '*A Study on the Cyber -Crimes and Cyber Criminals: A Global Problem'* International Journal of Web Technology, Volume 3,pp. 172-179, June 2014

[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