

Cyber Security: Threats and Precaution

Vaibhav Bandu Mane

Department of Computer Science and Engineering
Rajarambapu Institute of Technology, India

Abstract— Cyber security is an information technology. It's the main part of Internet services. We must understand the different type of threats that exist in the Internet world. The paper mainly focuses on challenges faced by cyber security and its types in day-to-life.

Keywords: Cyber Security, Threats, Precaution, Information Technology

I. INTRODUCTION

Cyber security is described as the use of technology, processes, and regulations to safeguard systems, networks, programmers, devices, and data from cyber-attack. These practices are used by persons and firms to guard against unapproved access to data centers and other systems. These unapproved accesses are called cyber-attack which is usually targeted at accessing, destroying or changing sensitive information which normally end up by extorting money from users or tending to interrupt normal business processes.

Cyber security is concerned with reducing the danger of cyber-attacks and safeguarding against unauthorized use of systems, networks, and technology.

Cyber-crime is a phrase that refers to "Offenses that are perpetrated against people or groups of persons with a criminal purpose to intentionally destroy the victim's reputation or cause direct harm to the victim directly or indirectly through the Internet."

Unauthorized access to computer systems, data modification, data destruction, and intellectual property theft are the most common types of computer crime. Hacking, conventional espionage, information warfare, and similar actions are all examples of cyber-crime in the context of national security.

II. CYBER SECURITY:

Cyber security is nothing however protective knowledge, networks, and alternative info from unauthorized access, part or absolutely destruction or modification. Cybersecurity will play an awfully vital role in our everyday life as a result of we have tendency to all have an online presence. "It takes twenty years to make a name and a couple of minutes of cyber-incident to ruin it."

This statement presents a real regarding constant as we have a tendency to all square measure exposed to security threats and cyber-attacks. In today's world, several firms square measure developing differing kinds of computer code to shield knowledge.

Cybersecurity is crucial in the contemporary world because it not solely helps to secure info however additionally our system kind virus attacks. It is also important because we have a huge user base I.e., after China, USA, India has the highest number of internet users.

III. CYBER CRIME

Cyber-crime is a term that refers to "offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the victim's reputation or cause physical harm to the victim directly or indirectly, using modern technologies such as the Internet (Email, chat) and through mobile phone (SMS/MMS/Bluetooth)" and involves "offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the victim's reputation or cause physical harm to the victim [5].

A. Hacking:

Getting into private network or system without the owner permission is called as hacking.

B. Cyber Stalking:

It means tracking down other information through internet without their permission.

C. Child Pornography:

Wide use of the Internet is done for sexual child abuse.

D. Denial of service:

It's an attempt to make a computer resource inaccessible to the people who use it. Dos attacks generally overwhelm servers or traffic networks with traffic, making legitimate users' access difficult or impossible.

E. Spyware:

It is a program that is used to monitor a computer system. This software will attempt to obtain all of your secret and sensitive information, such as your bank account numbers, passwords, and other personal information. The sensitive data is then overlooked in order to get access to the accounts of the users. Spywares can also alter the setup of your computer without your knowledge or agreement.

F. Phishing:

Sending electronic messages to try to obtain personal details (such as username and password) by pretending to be from a trusted source, like your bank. This information may then be used to take someone's money.

G. Data Interception:

Data modification done by hacking emails and phishing into other computer networks is considered to be a type of computer crime.

H. Online Gambling:

Online gambling is often outlined as being concerned in counting on casinos or sports over the net. Well, it's conjointly called net Gambling or e- gambling. Usually, credit cards square measure won't to place the bet, and win or losses square measure enjoyed thereby.

IV. CYBER ETHICS:

The code of conduct involves in using information technology in a responsible way to fulfill the needs of individual user without manipulating or destroying information of any other user.

Know the Rules of Cyber Ethics to follow while using the internet are given below

A. Respect other privacy-

Do not try to read or forward another person personal mail without seeking his permission.

B. Obey copyright laws-

Do not copy or post other's content from the Internet.

C. Use appropriate language-

Do not use rude or bad language and even remember to check your spelling and grammar.

D. Data-

Never share your personal information such as ATM pin, Credit Card number, password, OTP, etc., with anyone through e-mail, message, text, or any other means over the internet.

Firewall prevent the switch of huge facts documents over the network in a wish to weed out attachment that could incorporate malware

- Update OS
- You must use most recent security updates for your operating system (Linux, Windows, mac OS) in your device.
- Software programmer's updates programs after certain periods to add new enhanced feature

B. Phishing

Phishing may be a form of social engineering attack usually accustomed to get your data, together with user identification to login and bank card detail. It happens once associate attacker, masquerading as a trustworthy entity, cheat a victim into opening associate email, message, or text message.

Precaution

- Always check to make sure the site is verified
- Never input sensitive information in forms that are present in suspicious emails
- Check for HTTPS (secure connection) at the site of the webpage you are using to browse.

C. DDoS (Distributed Denial of Service)

In networking, a denial of service (DoS) is a method of attacking a particular infrastructure, rendering it useless by repeatedly sending requests to the server on the large scale

- Precaution
- (Unless your organization is large and has a lot of data, it's unlikely that you'll be targeted for a DDoS attack.)
 - Regular software upgrades and online device monitoring will keep your System as safe as possible.

D. Password attacks

A password is simply when a hacker tries to steal or to get your password.

Precaution

- It's always a good idea to stay updating necessary password in certain periods.
- Don't have a same password.
- Password should have a combination of uppercase and lowercase letters, symbols.

E. MITM (Man in the middle)

MITM attack is a common term in which the perpetrator puts himself in a conversation between the user and the application - either by attempting to or imitating one of the parties, making it seem like the normal data exchange is ongoing.

Precaution

- Use encrypted wireless access point (WAP) and virtual private network (VPN)
- Always go through the security of your connection (HSTS/HTTPS)

F. Drive-By Download

This attack occurs when vulnerable computers get damage by just browsing a network.

Precaution

- Avoid going to the website that could be harmful or malicious

V. THREATS AND PRECAUTION IN CYBER SECURITY:



A. Malware

"Malware" is stand for "malicious software"- computer software made to damage and destroy computer without the owner consent.

Precaution

- Suspicious Links
- Don't clicking unknown links
- Always go through the URL and make sure that you visit secure site.
- Update Firewall
- To check and update your firewall is a best option

- Use a secure Search protocol that alert you when you go to unsecure site

G. Malvertising

Malvertising is the term used in the security sector to describe illegally controlled advertisements that infect people and companies on purpose. This may be any ad on any site, and it's likely to be ones you visit on a regular basis. Precaution

- Use an ads blocker extension on the web browser on your device

H. Rogue Software

Rogue software package or applications are types of web fraud exploitation pc malware to confuse users into giveaway money and Social Network information or paying for phony product. As their name imply, these fallacious programs go “rogue” on the web, showing in easy web searches and on internet community

- Precaution

Always install a trusted antivirus or anti spyware and keep your firewall updated.

Challenges in cyber security

- Continued growth of compliance obligations
- Risk management in the cloud
- Continued practice of password re-use
- Balancing security with the open environment of higher education
- Sheer volume of digital assets to protect
- Difficulty in retaining a trained security staff
- Lax security of internet of things devices
- Intrusive data collecting of social media entities
- Threat landscape is growing more complex

REFERENCES

- [1] Cyber Security Challenges and its Emerging Trends on Latest Technologies-To cite this article: K. M Rajasekhara et al 2020 IOP Conf. Ser.: Mater. Sci. Eng. 981 022062
- [2] Rajeyyagari, S., & S. Alotaibi, A. (2018). A study on cyber-crimes, threats, security and its emerging trends on latest technologies: influence on the Kingdom of Saudi Arabia. *International Journal of Engineering & Technology*, 7(2.3), 54. <https://doi.org/10.14419/ijet.v7i2.3.9969>
- [3] Park, H. H. (2020). A Study on Cyber Crime Deterrence Recognition: The Influence of Recognition of Punishment for Cyber Crime on Intention to Report Crime. *Korean Association of Criminal Psychology*, 16(4), 85–98. <https://doi.org/10.25277/kcpr.2020.16.4.85>
- [4] Warikoo, A. (2021). The Triangle Model for Cyber Threat Attribution. *Journal of Cyber Security Technology*, 1–18. <https://doi.org/10.1080/23742917.2021.1895532>
- [5] Nanda, P., He, X., & Yang, L. T. (2020). Security, Trust and Privacy in Cyber (STPCyber): Future trends and challenges. *Future Generation Computer Systems*, 109, 446–449. <https://doi.org/10.1016/j.future.2020.02.010>
- [6] Rajasekhara, K. M., Dule, C. S., & Sudarshan, E. (2020). Cyber Security Challenges and its Emerging Trends on

Latest Technologies. IOP Conference Series: Materials Science and Engineering, 981, 022062. <https://doi.org/10.1088/1757-899x/981/2/022062>