IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

OVERVIEW OF CYBERSECURITY

[1]R.Shenbaga kamatchi, [2]B.K.Sweta, [3]M.Narmatha

[1&2] Student, Department of Computer science, Sri Krishna Arts and Science College, Coimbatore.

[3]Assistant Professor, Department of Computer science, Sri Krishna Arts and Science College, Coimbatore.

I.INTRODUCTION:

Computer security was originated in 1970s. The proper cyber security was set about in 1972 with the explore project of on ARPANET (The Advanced Research Projects Agency Network), a precursor to the internet. The actual birth of cyber security was in 1987 (4).1987 was the birth time of saleable antivirus, although there are challenging claims for the go-getter of the first antivirus product (4). Cyber security is the approach of technologies, processes and defends to protect `system, internet programs and devices from cyber-attacks (2). It is also named as information technology security or electronic information security (5).

An effective cyber security tactics has several layers of protection spread transversely the computers, networks, programs, or data that one aims to keep safe. Organizations must have an agenda for how they agree with both endeavored and successful cyber-attacks. Technology is important to giving organizations and individuals the computer security tools to protect ourselves from cyber-attacks (3). This review deals about the types of cyber threats, up-to-date cyber threats and safety tips against cyber-attacks.

II. Types of cyber threats:

By cyber-security the threats are categorized into three:

1. Cybercrime

The crime that includes the customs computer devices and Internet, is known as cybercrime (1). Cybercrime is also called as Computer crime Cybercrime comprises of single member or groups that organize systems to cause interruption and for financial causes (6). This may lead to harm someone's reputation, physical harm, or even mental harm. Mostly cybercrime is purposely used for illegal purposes. Cybercrime have varieties of activities including crime, illegal activities. It depends according to the uses of us. Cybercrime causes loss of billions of USD every year (1).

2. Cyber-attack

Cyber-attack often occurs purposely by political motivated gatherings (1). A cyber-attack is an attack introduced by cybercriminals to against single network or multiple networks by using one or more computers. A cyber- attack can spitefully disable computers, steal data (7). Cyber-attacks can be share of cyber warfare or cyber terrorism (8). Cybercriminals use a variety of methods to launch a cyber-attack, including some common methods like malware, Virus, Phishing, Trojans, Spyware, Ransom ware, Adware, Botnets, SQL injection, Man in the middle attack. (2)

2.1 Malware

Malware sense malicious software. This software is created by the hackers to damage or steal the user's data. This can be done for financial payments and politically motivated (1).

2.2 Virus

A virus is a program that self-replicates the virus with a clean attached file or by creating own malicious code to the computer (9). This corrupts the user's computers and data to steal the information of the user like credit card details, bank transaction details (1)

2.3 Trojans

Trojans is one type of malicious code or software that looks like authorized code or software but it can take the control of our computer (1). This can replicate and execute them. Trojan is planned to steal, interrupt and damage the user's data and their network (8).

2.4 Phishing

Phishing is one of the common cyber-attacks that everyone should study to defend themselves. It is mostly done through E-Mails by sending fraudulent communications that seem to come from a trustworthy source. This aims to steal the victim's sensitive data like credit card details and login information for financial gain (1).

2.5 Spyware

A spyware is a type of program that secretly records the all the data the user does. For example, the bank transaction details so cybercriminals get use of it (1).

2.6 Ransom ware

A ransom ware is a type of malware freeze down a user's files and data with threat until some ransom is paid (1).

2.7 Adware

Adware is a type of malware which advertise to spread the malicious software. This includes like pop up ads on websites (1).

2.8 Botnets

A botnet is a number of computer network devices where cybercriminals perform malicious activities without knowledge and permission of the user (1).

2.9 SQL Injection

An SQL injection is one type of cyber-attacks. It is a type of technique used to snip the data from the database and take switch of the database. This inserts malicious code to the malicious SQL so personal information of the user is gained (1).

3. Cyber terrorism:

The word cyber terrorism is a violent act that discusses about the usage of internet in order to accomplish to undermine the internet connected devices to cause anxiety or panic and even the loss of life (1). Mostly cyber terrorism is stimulated by political or religious causes. According to the U.S. Commission of Critical Infrastructure Protection, likely cyberterrorist aims including the water pipes, electricity, gas, fuel, public transportation control systems, or bank payment systems (9). Cyber terrorism is mainly caused by the methods of inserting computer virus, computer worms, other malicious software and programming codes (10) while connected to the internet which is considered as internet terrorism where terrorist activities include large scale disruption of computer networks and also including personal computer which is attacked by the cyber terrorism (10).

III Up-to-date cyber threats:

Romance scams

In February 2020, the FBI cautioned U.S. citizens to be aware of assurance fraud that cybercriminals commit using dating sites, chat rooms and apps. This takes advantage for the cybercriminal to seek the personal data of the user. The FBI reports that romance cyber threats affected 114 victims in New Mexico in 2019, with financial losses amounting to $1.6 million (1).

Emotet malware

In late 2019, The Australian Cyber Security Centre cautioned national organizations about a widespread global cyber threat from Emotet malware. Emotet is a type of trojan which can steal data and also can load other malware. It is a reminder to keep a secure password to prevent the entry of the malware (1).

IV Safety tips against cyber-attacks

- Always update your software and application systems for a secure protection (1).
- Use antivirus software to prevent the malicious software or code to the system (1).
- Use secure and strong passwords that unknown may not guess.
- Prevent using unknown network connections or Wi-Fi (1).
- Do not open any file attachments from unknown user and avoid using insecure websites (1).
- Use two factor authentications for double protection security (14).
- Always protect your personal data information with a secure form of password or security (11).
- Always review your online bank account and transaction details (11).
- Be aware of the phishing scams, suspicious phone calls or E-mails (11).
- Cyber security is everyone’s responsibility.

CONCLUSION

This article provides the importance of cyber security, threats, and safety measures of cyber security. Knowing the exposures in existing advanced technologies and evolving threats makes it essential to protect our data from in secure and unauthorized networks and users.Future research focus needs to be on the development of a secure and trustworthy internet environment of the next generation. Therefore, an increased awareness of cyber-attacks among individuals and organizations is vital so that solutions can be found quickly. It is imperative that all technology is practiced only after analysing the pros and cons of it as well as security breaches and taking care of their personal information.

Reference:

1. https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security
2. https://www.ijert.org/a-review-paper-on-cyber-security
3. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
4. https://blog.avast.com/history-of-cybersecurity
5. https://www.itgovernance.co.uk/what-is-cybersecurity
6. https://www.kaspersky.co.in/resource-center/threats/what-is-cybercrime
7. https://www.cisco.com/c/en_in/products/security/common-cyberattacks.html
8. https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html
9. https://searchsecurity.techtarget.com/definition/cyberterrorism
10. https://www.logsign.com/blog/what-are-cyberterrorism-and-cyberwarfare/
11. https://cipher.com/blog/10-personal-cyber-security-tips-cyberaware/