International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST218674

Introduction to Cyber Security – A Review

Pratik Narendra Gulhane , Yash Vishwas Manwar
CSE, Jawaharlal Darda Institute of Engineering and Technology, Yavatmal, Maharashtra, India

Article Info
Volume 8, Issue 6
Page Number : 484-487

Publication Issue
November-December-2021

Article History
Accepted : 15 Dec 2021
Published : 30 Dec 2021

ABSTRACT

Cyber Security is a process that's designed to protect networks and devices from external threats. It is important because it protects all categories of data from theft and damage. This paper addresses Cyber Security, Need of Cyber security and its Measures. In today's world we found that the amount of threats like data theft, scams, and phishing are increasing day-by-day. So this explains how the cyber security is important while dealing with internet. It can be prevented by following the security measures. To overcome the barriers related to security issues we have to spread awareness about cyber security and its measures. Cyber security is one of the most important aspects of the fast-paced growing digital world. The threats of it are hard to deny, there is no perfect solution for cybercrimes but we should try our best to minimize them.

Keywords: Cyber Security, Security Measures, Cyber warfare, Internet.

I. INTRODUCTION

Today man can send and receive any type of data can be an e-mail or an audio or video just by clicking a button but has he ever thought how securely his data is transmitted or sent to the other person safely without any information leakage?? Answer lies in cyber security. Today the Internet is the fastest growing infrastructure. In technical environment many latest technologies are changing the face of the mankind. But all are unable to secure our private information in a very effective way due to these emerging technologies, cybercrimes are increasing day by day. More than 60 per cent of total commercial transactions are done online today, so this field required a high level of security for transparent and best transactions. [1]

Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. [2]

II. CYBER SECURITY

Cyber security is the practice of protecting against malicious attacks computers, servers, mobile devices, electronic systems, networks, and data. It is also known as security of information technology or

electronic protection of information. [1] As commonly used, the term "cyber security" refers to three things:

1. A set of activities and other measures, technical and non-technical, intended to protect computers, computer networks, related hardware and software, including data and information, as well as other elements of cyberspace, from all threats, including threats to the national security;
2. The degree of protection resulting from the application of these activities and measures;
3. The associated field of professional endeavour, including research and analysis, directed at implementing those activities and improving their quality. [3]

Major areas which are included in the cyber security are:

1. Application security
2. Information security
3. Email security
4. Mobile Devices security
5. Web security
6. Wireless security [1]

Fig. 1: Major Areas in the Cyber Security [1]

III. WHY DO WE NEED CYBER SECURITY?

The range of operations of cyber security involves protecting information and systems from major cyber threats. These threats take many forms. As a result, keeping pace with cyber security strategy and operations can be a challenge, particularly in government and enterprise networks where, in their most innovative form, cyber threats often take aim at secret, political and military assets of a nation, or its people. Some of the common threats are:

1. **Cyber terrorism:** It is the innovative use of information technology by terrorist groups to further their political agenda. It took the form of attacks on networks, computer systems and telecommunication infrastructures.
2. **Cyber warfare:** It involves nation-states using information technology to go through something another nation's networks to cause damage. In the U.S. and many other people live in a society, cyber warfare has been acknowledged as the fifth domain of warfare. Cyber warfare attacks are primarily executed by hackers who are well-trained in use of benefit the quality of details computer networks, and operate under the favourable and support of nation-states. Rather than closing a target's key networks, a cyber-warfare attack may forced to put into a situation into networks to compromise valuable data, degrade communications, impair such infrastructural services as transportation and medical services, or interrupt commerce.
3. **Cyber spionage:** It is the practice of using information technology to obtain secret information without permission from its owners or holders. It is the most often used to gain strategic, economic, military advantage, and is conducted using cracking techniques and malware. [4]

IV. SECURITY MEASURES

The following security measures must be adopted in order to prevent your device to get into any cyber backdoor kind of trouble.

1. **Change default password:** The user has unknowingly built a backdoor by using the default password. To reduce risk, change the default password as soon as possible and use Multi-Factor Authentication (MFA). It can be difficult to remember a distinct password for each program. According to a Malware Bit Labs survey on data privacy, 29 percent of respondents used the same password across several apps and devices.

2. **Monitor network activity:** If the user sees any unusual data spikes, it's possible that someone is using a backdoor on the user's device. Use security measures such as firewalls to track inbound and outgoing traffic from the many apps installed on the user's computer to avoid this.

3. **Carefully selection of applications and plugins:** Backdoors are hidden inside seemingly benign free programs and plugins by cybercriminals. The greatest and most straightforward defense is to ensure that all programs and plugins users install are from a reliable source.

4. **Make use of a reliable cyber security solution:**
Any decent anti-malware solution can prevent cybercriminals from deploying the Trojans and rootkits used to open those troublesome backdoors. [5]

V. CONCLUSION

1. Cyber-security is both about the insecurity made by and through this new space and about the practices or procedures to make it (progressively) secure. Exertion to verify the cyberspace should give a definitive need else the "information technology" will not be viably used by clients. [6]

2. Protecting mobile users: Mobile and flexible working is on the rise. It helps growing business attract and retain great talent and reduce the cost of office space. Many users may consider mobile phone security to be less important than the security of their PCs, but the consequences of attacks on mobile phones can be just as severe. Malicious software can make a mobile phone a member of a network of devices that can be controlled by an attacker (a "botnet"). Configure the device to be more secure. [7]

3. There is no perfect solution for cybercrimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space. [2]

VI. REFERENCES

[1] Arvind Kumar, "Introduction to Cyber Security", in International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.6, Issue 3, page no.522-527, March-2019.

[2] G.NIKHITA REDDY and G.J.UGANDER REDDY, "A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES" in International Journal of Engineering and Technology - UK ISSN: 2049-3444, Volume 4 No.1 January 2014.

[3] B. A. Obotivere and A. O. Nwaezeigwe, "Cyber Security Threats on the Internet and Possible Solutions", in International Journal of Advanced Research in Computer and Communication Engineering Vol. 9, Issue 9, September 2020, DOI 10.17148/IJARCCE.2020.9913.

[4] P.S.Seemma, S.Nandhini and M.Sowmiya, "Overview of Cyber Security", in International Journal of Advanced Research in Computer and Communication Engineering, Vol. 7, Issue 11, November 2018.

[5] Harshitkumar R Panwala, "Advanced Cyber Security", in IOSR Journal of Computer

Engineering (IOSR-JCE), e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 23, Issue 5, Ser. II (Sep. –Oct. 2021).

[6] Rohit Kalakuntla, Anvesh Babu Vanamala and Ranjith Reddy Kolipyaka, “Cyber Security”, in HOLISTICA – Journal of Business and Public Administration, Vol 10, Issue 2, 2019, DOI:10.2478/hjbpa-2019-0020.

[7] Vaishnavi J. Deshpande and Dr. Rajeshkumar Sambhe, “Cyber Security: Strategy to Security Challenges- A Review”, International Journal of Engineering and Innovative Technology (IJEIT), Volume 3, Issue 9, March 2014, ISSN: 2277-3754.

Cite this article as :

Pratik Narendra Gulhane , Yash Vishwas Manwar, "Introduction to Cyber Security - A Review ", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 8 Issue 6, pp. 484-487, November-December 2021. Available at doi : https://doi.org/10.32628/IJSRST218674
Journal URL : https://ijsrst.com/IJSRST218674