VOLUME - 13, ISSUE - 08, AUGUST - 2024 • PRINT ISSN No. 2277 - 8160 • DOI : 10.36106/gjra

Original Research Paper | Computer Science

CYBER SECURITY ETHICS FOR MODERN USERS

Dr. Banta Singh Jangra — Asstt. Professor, Deptt. Of Computer Science Govt. College Hansi Hisar Haryana

Uma Sharma — Asstt. Professor, Deptt. Of Computer Science Govt. College Hansi Hisar Haryana

ABSTRACT

In this paper we analyse about today's time issue, challenges and ethics regarding cyber security which plays an important role in the field of information and communication technology. Now the days 90% public using IT equipments like smart phone and using fee free internet services. Securing the personal information has become one of the biggest challenges in the present day for all users. Cyber Security accepts a vigorous role in the area of information and communication technology. The cyber security the main thing that originates in mind is 'cyber crimes' which are aggregate colossally daily. Now the days all governments and private organizations are taking numerous measures to keep these cyber wrong doings for their users. The significant trends of cyber security and the consequence of cyber security discuss in it. The cyber-terrorism could make associations lose billions of dollars in the region of organizations.

KEYWORDS :

INTRODUCTION:

Cyber security is a major issue and headache for each and every users and it is the practice of protecting computers, networks, devices, software's from digital attack by unauthorised access. These cyber attacks are usually aimed at accessing, changing, or destroying sensitive information in the system and data and extorting money from users via ransomware. An effective cyber security method has numerous layers of defense spread across the networks, computers, programs, or information's that one aims to keep non-toxic. In a society, the processes, the people and tools must all accompaniment one alternative to generate a real defense on or after cyber-attacks. Unified threat management systems can mechanism additions across select Cisco Security goods and speed up key security processes functions: discovery, examination, and remediation.

Figure-1: Cyber Security Life Cycle

Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital or a cyber form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking but also during bank transactions a person must take all the required security measures.

Today an individual can receive and send any multimedia information it may be text, image, audio and video, or an email or only through the click of a button but did s/he ever ponder how safe this information transmitted to another individual strongly with no spillage of data? The proper response lies in cyber security, today more than 75% of full industry exchanges are done on the internet, so this area prerequisite high quality of security for direct and best exchanges. Thus, cyber security has become a most recent issue. The extent of cyber security does not merely restrict to verifying the data in IT industry yet also to different fields like cyberspace and so forth. To improving cyber security and ensuring that necessary data systems are vital to each country's security and financial prosperity also.

Today a Lehman like students, farmer, home makers, business men, teachers, employees or even a cart pullers able to send and receive any form of information may be an e-mail or an audio or video just by the click of a button but did he/she ever think how securely his data id being transmitted or sent to the other person safely without any leakage of information?? but the answer is No because of in the background a cyber terrorism is spreading their legs and make their attacks unknowingly. The records are showing more than 75% of total commercial and 50% personal transactions are done online, so this field required a high quality of security for transparent and best transactions. Cyber security has become a latest issue for all IT users worldwide, so that the precautionary measurements are needed to be increase and make secure IT world.

The latest technologies like E-banking, I-banking, cloud computing, mobile computing, E-commerce 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 to protecting Internet users from cyber attacks has become integral to the development of new services as well as governmental policy part thereof.

IT Infrastructure and Cyber Security

Now the day's cyber security assumes a critical role in the area of information and communication technology. The safeguarding is to information has become the greatest difficulty. The cyber security the main thing that raids a chord is cybercrimes which are increasing tremendously step by step. Different administrations and organizations are taking many measures to keep these cybercrimes. Additional the different measures cyber security is as yet an enormous worry to numerous. Some major trends that are changing cyber security give as follows:

Web Control Rooms

The risk of assaults on web applications to separate

information or to circulate malicious code perseveres. Cybercriminals convey their code using good web servers they have traded off. In any case, information taking attacks, a considerable lot of which get the deliberation of media, are also a significant risk

Mobile Networks

The risk of assaults on web applications to separate information or to circulate malicious code perseveres. Cybercriminals convey their code using good web servers they have traded off. In any case, information taking attacks, a considerable lot of which get the deliberation of media, are also a significant risk. Currently, individuals need a more unusual accentuation on securing web servers as well as web applications. Web servers are mainly the pre-eminent stage for these cybercriminals to take the information. Thus, one should reliably utilize an additional secure program, mainly amid vital exchanges all together not to fall as a quarry for these defilements.

Information protecting techniques

It is the method toward encoding messages so programmers cannot scrutinize it. In encryption, the message is encoded by encryption, changing it into stirred-up figure content. It commonly completes with the use of an "encryption key," that demonstrates how the message is to encode. Encryption at the earliest reference point level secures information protection and its respectability. Additional use of encryption obtains more problems in cyber security. Encryption is used to ensure the information in travel, for instance, the information being exchanged using computer systems, mobile phones, wireless radios and so on.

Cyber Crime and Terrorism

Cyber crime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cyber crime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cyber crimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations.

The "Cyber terrorist" may use one of the techniques such as password sniff as procedures to complete their "cyber-attack" on different countries and many big organizations to see their downfall and have control over their systems. The password sniffer is programming which uses to screen organize and in the meantime catch the entire password that passes the system connector.

Social Media and Cyber Security

In 21st century social media become a popular medium to connect peoples worldwide and 95% and above smart phone users are using social media applications i.e. facebook, whatsapp, instagram, twitter and telegram. As we become more social in an increasingly connected world, companies must find new ways to protect personal information. Social media plays a huge role in cyber security and will contribute a lot to personal cyber threats. Social media adoption among personnel is skyrocketing and so is the threat of attack. Since social media or social networking sites are almost used by most of them every day it has become a huge platform for the cyber criminals for hacking private information and stealing valuable data.

In a world where we're quick to give up our personal information, companies have to ensure they're just as quick in identifying threats, responding in real time, and avoiding a breach of any kind. Since people are easily attracted by these social media the hackers use them as a bait to get the information and the data they require. Hence people must take appropriate measures especially in dealing with social media in order to prevent the loss of their information.

Users Precautions Technique

Access control and password security

The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

Authentication of data

The documents that we receive must always be authenticated be before downloading that is it trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the antivirus software present in the devices. Thus a good anti virus software is also essential to protect the devices from viruses.

Malware scanners

This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

Firewalls

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

Anti-virus software

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti virus software is a must and basic necessity for every system.

Prevention of Cyber Attack and Ethics

The capacity to prevent cyber terrorism lies with the capacity to securely verify cyberspace. Cyber security has an intriguing parallel to terrorism. Both are lopsided. Guaranteeing the security of information, data, and correspondence is impressively harder than hacking into a framework of daily life works. Each and every user must have to be smart and secure to safely use of internet and internet of things. The attacker has an inalienable preferred standpoint in both regular terrorism and cyber-attacks. On account of state-supported attacks, the difficulties are of a lot higher greatness. Governments should guarantee that their rules smear to cybercrimes and be wholly actualized and hold fast to; it is essential that the countries of the biosphere take measures to guarantee that its punitive and technical law is satisfactory to address the difficulties presented by cybercrimes.

In the other scenario the cyber ethics are nothing but the code of the internet. We practice these cyber ethics there are good chances of us using the internet in a proper and safer way. Using the cyber infrastructure email and instant messaging make it easy to stay in touch with friends and family members, communicate with work colleagues, and share ideas and information with people across town or halfway around the world within a second.

Best Practices and Precautionary Measurements

- Don't make any types of IDs with wrong information's and details of others, its IT act 2000 offence.
- Don't be a bully on the Internet. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.
- Don't shares own personal ID credentials to friends and others whosoever.
- Internet is considered as world's largest library with information on any topic in any subject area, so using this information in a correct and legal way is always essential.
- Do not operate others accounts using their passwords.
- Never try to send any kind of malware to other's systems and make them corrupt.
- Never surf unauthorized websites which are restricted by Government.
- Never share your personal information to anyone as there is a good chance of others misusing it and finally you would end up in a trouble.
- Don't click on unwanted links which are received on text messages, social media and emails.
- Never share your bank account details with anyone on internet without to confirm.
- When you're online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble.
- Always adhere to copyrighted information and download games or videos only if they are permissible.

REFERENCES

1. Nikita Reddy and GJ ugander Reddy "A Study of Cyber Security Challenges And Its Emerging Trends on Latest Technologies", 2021
2. Rohit, Ranjith Reddy "Cyber Security "Holistika: Associatia Holistika Research Academy (HORA) Vol 10, Issue 2, 2019
3. www.google.com
4. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole
5. Computer Security Practices in Non Profit Organizations – A NetAction Report by Audrie Krause.
6. Bendovschi, A. "Cyber-Attacks – Trends, Patterns and Security Countermeasures" Procedia Economics and Finance, 24-31, 2015.
7. Cabaj, K., Kotulski, Z., Ksi opolski, B., & Mazurczyk, W. Cyber security: trends, issues, and challenges. EURASIP Journal on Information Security, 2018