IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111243

CYBER SECURITY: A REVIEW

Ms. Kanika Kundu

Dept. of Computer Science, Maharaja Surajmal Institute, C-4, Janakpuri, Delhi, India

Abstract: Cyber security has become a vital part of information technology. The need to secure the information has increased manifolds during the present scenarios. While making one's data authentic one has to face various challenges. Cyber security has come into limelight due to the high rate of cybercrime in our society. Although government and companies are taking various steps to curb it but all seems to be in vain for a majority of people. This paper mainly focuses on the various threats imposed by cybercrime and the measures taken to prevent it. It basically deals with the different types of hackers in our society.

Keywords: Security,Internet,privacy, Hackers, cybercrimes, Integrity,Phishing,identity theft, Authentication.

I. INTRODUCTION

Now a days we are able to exchange data of any form whether it's an image, audio, video or a document by just pressing a single button but have we ever wondered that how is this data reaching its destination? Is the sent data reaching without any loss or breach? The solution to these questions is just a single word "Cyber security". Presently the usage of internet is touching high rates day by day as a result of which the need to secure the data has increased. Face of mankind is changing due to the various emerging technologies which gives rise to cybercrime as an individual is not able to safeguard his/her data in an effective and efficient manner. Almost all the commercial transactions are done online therefore we require a mechanism to provide good security for the smooth functioning of one's work. Therefore cyber security has now become an integral part of our lives which needs to be dealt with seriously. In cyber security we secure the information of information technology sector as well as from other sectors as well.

Every organization implements certain security techniques such as security and privacy to keep its data safe and sound. Latest technologies like mobile computing, e-commerce etc used by various firms and offices also require a high level of security. It is important to secure these applications as it holds the confidential data about an individual. For a country's economic well being and social security we need to have a dynamic infrastructure which caters to prevention of loss of data. As per the development of services and government policies it is mandatory to protect the users of the internet and make its usage safer. We need to follow a comprehensive and critical approach in order to curb cybercrime. The law enforcement agencies must investigate the issues and must reach to a solution in order to tackle cybercrime apart from the technical measures which are being used.

Many countries and it's government are now imposing strict cyber laws in order to protect and save their information and data from intruders or a third party. There must be general awareness among the citizens of a country about the cyber security and cyber crime so that each one of us can make our information and data safe. [1][2]

II. ETHICAL AND LEGAL ASPECTS OF CYBERCRIME

Every technological invention has got both positive and negative impacts on the society. For example, ICT provides easier and efficient means of storage and retrieval of information but at the same time suffers from piracy of copyrighted materials, software, data, music, video etc. at large scales. Internet provides instant access to all sorts of useful information at finger tip but at the same time suffers from plagiarism, illegal uploading, downloading, copying, stealing and misuse of intellectual property. ICT has created high-end job opportunities for the techies in one hand and on the other hand has created sever unemployment among non-tech groups. Communication Technology has made trade, investment, business simpler and unruffled through e-commerce and on-line transactions but suffers from cybercrimes, forgery, sabotage, hacking and loss.Internet has made the whole world a small intellectual village but at the same time is polluted with horrid contents like pornography, spam, worms and viruses. Therefore, it is high time now for careful inspection of the legal and ethical aspects of cybercrime as there are not enough guidelines available in, this field as compared to those available in conventional branches of science and technology. More importantly, now ICT is not limited to the scientists and software engineers alone rather it has become a widespread phenomenon, affecting people at various stages in their role, as customers, service provider, participants, middlemen etc. So it has become the moral responsibility of the sociologist, business people and scientists to decide in which way ICT can be best utilized [3].

DOI: 10.17148/IJARCCE.2022.111243

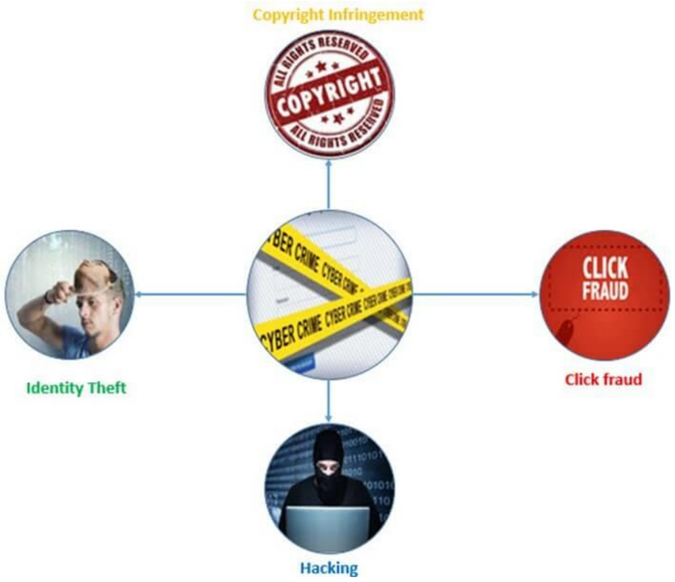

Figure 1: Security Issues in ICT

New advances particularly in the field of information technology have brought new scientific gains to humans but it should be noted that the entry of new scientific and technological fields will always have ethical issues and limitations. One of the interesting and, of course, new topics in the field of information technology science is computer ethics or IT ethics. The study of computer ethics has long been considered by the researchers. Today, in the digital age, the society is dependent on computers in almost all its affairs, and the study of ethics in the field of computer and information technology must always be considered.

The growth and development of the Internet has made it possible to store a large number of individuals' personal data by relying on advanced information systems and the abuse of personal data and privacy violations in the field of information technology is increasing [6].

The lack of scientific integrity in educational environments that make the most use of technology is an issue that should be considered. Illegal downloading of software is common among all social classes specially the students. The use of social networks is an inseparable part of the lives of many people and the nature of students. These cases have different effects on their lifestyle, especially on their academic performance and the length of their studies [7], [8].

On the other hand, the number of unethical sites is rising every day and the conditions for access to these sites are easier than before and the mean age of people who visit these sites is reduced. Being exposed to the unethical sites also has the dangers of high-risk sexual behavior, social dilemmas and mental and psychological problems. Communicating with anonymous people and visiting them is increasing [9].

A large percentage of users are exposed to moral damages and IT abnormalities, and having a virtual identity has become a commonplace cause of many social abnormalities. The phenomenon of Internet addiction has long been considered in the developed countries as one of the consequences of the ever increasing development of the electronic communications network and has caused various harms to the individual, family and society.

The excessive use of social networks can lead to addiction and is not tolerated by many physical communities. The theft of software, films, music, etc. with copyrights has become common in some societies. Unauthorized access to the systems (hacking) is done using different and new methods and is increasing every day. Today hackers have posed the greatest challenge against IT ethics and with a widespread violation, they make numerous attempts to influence the commercial and banking accounts of individuals and try to violate individuals' privacy [4].

Many computer games are violent and stimulate aggressive antisocial behavior in addition to violent thoughts and feelings. Today, forging digital documents such as counterfeiting digital signatures, digital images, etc. is an important topic in the field of information security and computer ethics. Online gambling (using online websites where members

DOI: 10.17148/IJARCCE.2022.111243

can participate in a variety of games without having to be present at the site, in which everything is done online from opening an account to transferring funds, withdrawals, playing games, etc.) is increasing.

Cases such as cyber bullying and communicating with anonymous individuals, visiting them, sharing the stimulating content on the Internet, and sharing personal information on the Internet have been recognized as the dangers of Internet communications in the new era [10].

All of these cases are examples of issues that affect ethics in information technology and it is necessary to rank such issues in terms of society in order to provide a better insight to provide strategies and programs in which negative measuresare converted to the positive affairs or ethical issues in the field of information technology are observed.

III. TYPES OF CYBER SECURITY

The high use of the Internet has led to the negligence of other important parts of life, including sleep, work, and academic achievement. Users in the Internet environment can be anonymous and engage in behaviors that are inappropriate in most physical communities. On the other hand, providing fast, cheap and convenient access to the unethical sites can be considered as a disadvantage of the use of the Internet. [11]

There are various types of cyber securities which are as follows:

1. Network Security

- It involves implementing the hardware and software to secure a computer network from unauthorized access, intruders, attacks, disruption, and misuse.
- This security helps an organization to protect its assets against external and internal threats.

2. Application Security

- It involves protecting the software and devices from unwanted threats. This protection can be done by constantly updating the apps to ensure they are secure from attacks.
- Successful security begins in the design stage, writing source code, validation, threat modeling, etc., before a program or device is deployed.

3. Information or Data Security

- It involves implementing a strong data storage mechanism to maintain the integrity and privacy of data, both in storage and in transit.

4. Identity Management

- It deals with the procedure for determining the level of access that each individual has within an organization.

5. Mobile Security

- It involves securing the organizational and personal data stored on mobile devices such as cell phones, computers, tablets, and other similar devices against various malicious threats.
- These threats are unauthorized access, device loss or theft, malware, etc.

6. Cloud Security

- It involves in protecting the information stored in the digital environment or cloud architectures for the organization.
- It uses various cloud service providers such as AWS, Azure, Google, etc., to ensure security against multiple threats.

IV. CYBER ATTACKERS

Studies have shown that a high percentage of employees in the workplace use the Internet for non-work purposes. Meanwhile the most common non-work activities are: visiting the chat rooms, sports websites and stock investment websites [9]. Apart from all of this, computers and the Internet have the potential to violate the privacy of users by hackers [10], [11]. Research shows that 75 percent of American children are willing to share their personal data and information with other Internet users in exchange for access to services and products provided on the Internet, which can be very dangerous [13].

There are various types of attackers in our society out of which some of them are discussed here:

1. Cyber Criminals

- Cybercriminals are individual or group of people who use technology to commit cybercrime with the intention of stealing sensitive company information or personal data and generating profits.

2. Hactivists

- Hacktivists are individuals or groups of hackers who carry out malicious activity to promote a political agenda, religious belief, or social ideology.

3. State Sponsored Attackers

- State-sponsored attackers have particular objectives aligned with either the political, commercial or military interests of their country of origin.

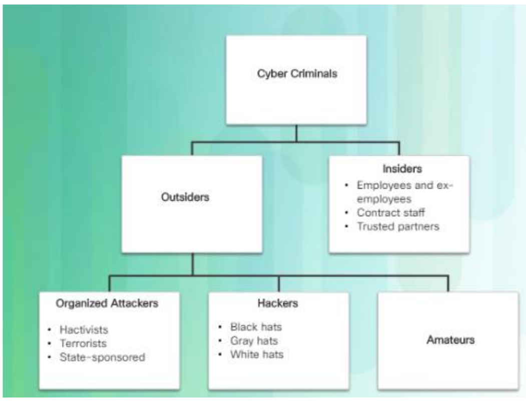

Figure 2: Types of Attackers

V. TARGET OF ATTACKERS

There are no significant differences regarding privacy issues at different points as well as gender which indicate that privacy is a concern for all individuals. In this section a set of soft targets are discussed which are attacked by an attacker: [12]

1. Communication

- Cyber attackers can use phone calls, emails, text messages, and messaging apps for cyber attacks.

2. Finance

- This system deals with the risk of financial information like bank and credit card detail. This information is naturally a primary target for cyber attackers.

3. Government

- The cybercriminal generally targets the government institutions to get confidential public data or private citizen information.

4. Transportation

- In this system, cybercriminals generally target connected cars, traffic control systems, and smart road infrastructure.

5. Healthcare

- A cybercriminal targets the healthcare system to get the information stored at a local clinic to critical care systems at a national hospital.

6. Education

- A cybercriminals target educational institutions to get their confidential research data and information of students and employees.

VI. CYBER THREATS

A threat in cyber security is a malicious activity by an individual or organization to corrupt or steal data, gain access to a network, or disrupts digital life in general. [14]

DOI: 10.17148/IJARCCE.2022.111243

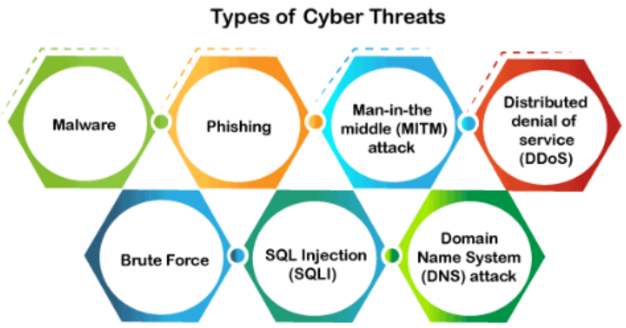
Types of Cyber Threats
Malware
Phishing
Man-in-the middle (MITM) attack
Distributed denial of service (DDoS)
Brute Force
SQL Injection (SQLI)
Domain Name System (DNS) attack

Figure 2: Types of Cyber Threats

1. Malware
- Malware means malicious software, which is the most common cyber attacking tool.
- It is used by the cybercriminal or hacker to disrupt or damage a legitimate user's system.

2. Virus
- It is a malicious piece of code that spreads from one device to another.
- It can clean files and spreads throughout a computer system, infecting files, stoles information, or damage device.

3. Spyware
- It is software that secretly records information about user activities on their system.

4. Trojans
- It is a type of malware or code that appears as legitimate software or file to fool us into downloading and running.
- Its primary purpose is to corrupt or steal data from our device or do other harmful activities on our network.

5. Ransomware
- It's a piece of software that encrypts a user's files and data on a device, rendering them unusable or erasing.

6. Worms
- It is a piece of software that spreads copies of itself from device to device without human interaction.
- It does not require them to attach themselves to any program to steal or damage the data.

7. Adware
- It is advertising software used to spread malware and displays advertisements on our device.
- It is an unwanted program that is installed without the user's permission.

8. Botnets
- It is a collection of internet-connected malware-infected devices that allow cybercriminals to control them. It enables cybercriminals to get credentials leaks, unauthorized access, and data theft without the user's permission.

9. Phising
- Phishing is a type of cybercrime in which a sender seems to come from a genuine organization like PayPal, eBay, financial institutions, or friends and co-workers.
- They contact a target or targets via email, phone, or text message with a link to persuade them to click on that links.
- This link will redirect them to fraudulent websites to provide sensitive data such as personal information, banking and credit card information, social security numbers, usernames, and passwords.
- Clicking on the link will also install malware on the target devices that allow hackers to control devices remotely.[15]

10. Man-In –The- Middle Attack
- A man-in-the-middle attack is a type of cyber threat (a form of eavesdropping attack) in which a cybercriminal intercepts a conversation or data transfer between two individuals.

11. Distributed Denial Of Service
- It is a type of cyber threat or malicious attempt where cybercriminals disrupt targeted servers, services, or network's regular traffic by fulfilling legitimate requests to the target or its surrounding infrastructure with Internet traffic.

12. Brute Force

DOI: 10.17148/IJARCCE.2022.111243

- A brute force attack is a cryptographic hack that uses a trial-and-error method to guess all possible combinations until the correct information is discovered.
- Cybercriminals usually use this attack to obtain personal information about targeted passwords, login info, encryption keys, and Personal Identification Numbers (PINS).

13. SQL Injection

- SQL injection is a common attack that occurs when cybercriminals use malicious SQL scripts for backend database manipulation to access sensitive information.
- Once the attack is successful, the malicious actor can view, change, or delete sensitive company data, user lists, or private customer details stored in the SQL database.

14. DNS Attack

- A DNS attack is a type of cyber attack in which cyber criminals take advantage of flaws in the Domain Name System to redirect site users to malicious websites (DNS hijacking) and steal data from affected computers

VII. CONTROLLING STRATEGIES

Following measures must be taken to prevent cyber crime and promote cyber security:

- Keep your software updated. Only 20 percent of Android devices are running the newest version and only 2.3 percent are on the latest release.
- Everything from your operating system to your social network apps are potential gateways for hackers. Keeping software up to date ensures the best protection
- Make sure to select security software from a trusted provider and keep it up to date.
- Install a firewall. Installing a firewall provides you with much stronger protection against digital threats and allows you to safeguard your online privacy.
- Always use a pass code. Remember that loss or physical theft can also compromise your information.
- Download apps from official app stores. Both the Google Play and Apple App stores vet the apps they sell; always read the end-user agreement.
- Install Antivirus software
- Ignore spams.
- Secure your network and have a back up of your data.

VIII. CONCLUSION AND FUTURE WORK

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cyber crime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cyber crimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

REFERENCES

[1] www.wikipedia.org

[2] Bertrand Meyer, “Ethics of free Software”, Software Development, March 2000

[3]S. Patnaik, Information Technology, DhanpatRai& Co Pvt. Ltd, 2001

[4] Reynolds G, (2011) Ethics in information technology. Cengage learning.

[5] Thompson LA, Dawson K, Ferdig R, Black EW, Boyer J, Coutts J, Black NP (2008) The intersection of online social networking with medical professionalism. Journal of general internal medicine 23(7): 954-957.

[6] Kirschner PA, Karpinski AC (2010) Facebook® and academic performance. Computers in human behavior 26(6): 1237-1245.

[7] Kopecký K, Szotkowski R, Krejčí V (2012) The risks of Internet communication 3. Procedia-Social and Behavioral Sciences 69: 1348- 1357.

[8] Korkeila J, Kaarlas S, Jääskeläinen M, Vahlberg T, Taiminen T (2010) Attached to the web—harmful use of the Internet and its correlates. European Psychiatry 25(4): 236-241

[9] Pontell HN, Rosoff SM (2009) White-collar delinquency. Crime, Law and Social Change 51(1): 147-162

[10] Akbulut Y, Şendağ S, Birinci G, Kılıçer K, Şahin MC, Odabaşı HF (2008) Exploring the types and reasons of Internet-triggered academic dishonesty among Turkish undergraduate students: Development of Internet-Triggered Academic Dishonesty Scale (ITADS). Computers & Education 51(1): 463-473.

DOI: 10.17148/IJARCCE.2022.111243

[11] Akbulut Y, Uysal Ö, Odabasi HF, Kuzu A (2008) Influence of gender, program of study and PC experience on unethical computer using behaviors of Turkish undergraduate students. Computers & Education 51(2): 485-492

[9] Bijari B, Javadinia SA, Erfanian M, Abedini M, Abassi A (2013) The impact of virtual social networks on students' academic achievement in Birjand University of Medical Sciences in East Iran. Procedia-Social and Behavioral Sciences 83: 103-106.

[10] Fallahi V (2011) Effects of ICT on the youth: A study about the relationship between internet usage and social isolation among Iranian students. Procedia-Social and Behavioral Sciences 15: 394-398.

[11] Baase S (2003). A gift of fire. Social, Legal, and Ethical Issues in Computing. Prenctice-Hall.

[12] Wright PJ, Randall AK (2012) Internet pornography exposure and risky sexual behavior among adult males in the United States. Computers in Human Behavior 28(4): 1410-1416.

[13] Wolak J, Finkelhor D, Mitchell KJ (2012) How often are teens arrested for sexting? Data from a national sample of police cases. Pediatrics 129(1): 4-12.

[14] Nespor K, Csemy L (2007) Health Risks of Computer Games and Videogames. CESKA A SLOVENSKA PSYCHIATRIE 103(5): 246.

[15] Coeckelbergh M (2007) Violent computer games, empathy, and cosmopolitanism. Ethics and Information Technology 9(3): 219-231