International Journal of Electrical, Electronics and Computer Engineering **13**(1&2): 35-39(2024)

ISSN No. (Online): 2277-2626

A Basic Study of Cyber Security in Cyber Space

Shipali Dhiman*, Vatsal and Shagun

Department of School of Computer Science and Engineering,
Govt. PG College, Dharamshala, Himachal Pradesh Technical University (HPTU), India.

*(Corresponding author: Shipali Dhiman *)*

(Received: 27 January 2024, Accepted: 10 April 2024)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: The term "cyber" has been used to describe almost anything that is connected with networks and computers. In simple words cyber space is the virtual world, the individual are communicate and connected with others virtually. In today's tech-driven world where everything relies on connectivity, understanding cyber security and knowing how to use it effectively is super important. Cyber security which means protecting digital data and systems from unauthorized access, damage or attack. Keeping our digital stuff safe and secure important in the world of technology. Information security is one of the biggest challenges in the present day. Various Governments and companies are taking many measures in order of to prevent the cyber crimes. Here we will discuss the cyber security in cyber space.

Keywords: Cyber Space, Cyber Crime, Cyber Law etc.

INTRODUCTION

Cyberspace is a networked digital realm, interconnected and expansive. Cyberspace is a virtual realm that gained popularity alongside the internet's emergence (Delftani *et al.,* 2019; Warrier, 2002). In simple words cyber space is the virtual world, the individual are communicate and connected with others virtually. The all over world is connected with each other virtually. Some examples of cyber space are social media platforms like Facebook that normally use in daily life by almost everybody in the world, some other examples are linkedin social site, Twitter etc. In some cases are relatives, friends, family members are live in other country, so we can talk to them easily through social media. Both wire and wireless technologies have been used to create connectivity in the cyber space, but 90% all over the world the wired network are running for example submarine(a vessel or ship, that cango under water) cables. The whole world is connected with cables, according to this every country, state get the internet service provider. Cyberspace is an interconnected digital environment. Wire and wireless connection is available under the internet, that connection is further connected to the company, through which a virtual world is created by creating step by step connectivity. And the term used in that world is called cyber space. Network has a lot of contribution in cyber space. Others consider cyberspace to be just a notional environment in which communication over computer network occurs. Connectivity to the network relies on the TCP/IP transmission and internet protocol.

According to Morningstar and Farmer 2003), cyberspace is defined more by the social interactions involved rather than its technical implementation (Morningstar and Farmer 2003). However, many electronic devices must have a unique identity to connect them, such as IP address, which is the logical identity with which each device is associated, this is called cyber space.

CYBER CRIMES

Crimes which take place in the cyber space. Cyber crime is a term for an illegal activity that uses a computer as its primary means of theft. Cyber crime is the context of national security may involve activisim , traditional espionage, or information warfare and related activities (Karamchand, 2012). Usually in common man's language cyber crime may be defined as crime committed using computer and the internet to steal a person's identity or stalk victim's. Cyber crimes can be defined as the unlawful acts where the computer is used either as a tool or a target or both. The term is a general term that covers crimes like phishing, credit card frauds, bank robbery, illegal downloading, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and/or distribution of viruses, Spam and so on. As day by day technology is playing in major role in person's life the cyber crimes also will increase along with technological advance. There are basic two types of cyber crimes:

1. Computer served as both Tools and Target in the digital landscape: The crimes where the computer are the primary targets. These crimes include hacking, virus attacks, DOS attack etc.
2. Computer used as Weapon: Cyber crimes where computer is used as a weapon. These crimes include cyber terrorism, credit card frauds, pornography etc.

DIFFERENT KINDS OF CYBER CRIMES

1. Financial Crimes: Money is the most common reason behind all crime, including cyber crime.

Globally, it's been observed that more cyber crimes are committed for financial motives rather than for revenge or entertainment.

2. Cyber Pornography: Cyber pornography is believed to be one of the largest businesses on the Internet. While pornography is not illegal in many countries, child pornography is strictly prohibited in most nations. Cyber pornography includes pornographic websites, magazines produced using computers and the Internet to download and transmit explicit pictures, photos, and writings.

3. Sale of Illegal Articles: It's increasingly common to find cases where illegal articles like narcotics, weapons, and wildlife are sold online.

4. Online Gambling: Thousands of websites offer online gambling services worldwide. The unique aspect about online gambling is that it is permitted in many jurisdictions, thus, the operators of these websites cannot be prosecuted in their home countries.

5. Intellectual Property Crimes: These encompass software piracy, copyright infringement, trademark infringement, and theft of computer source code among others. A software developer from Bangalore (India) was charged with stealing his employer's source code for a product they were developing. Subsequently, he established his private firm and is alleged to have utilized the stolen source code to release another program.

6. Email Spoofing: Email spoofing is a fraudulent email that looks like it has originated from one place but actually comes from another source altogether.

7. Cyber Stalking: Cyber stalking is when people stalk someone else using the internet, email and other electronic communications. This could be harassing or threatening behaviour that one person carries out frequently, such as following them about, visiting their home or work premises, making annoying telephone calls to them, leaving written notes or items behind .

8. Web defacement: A site hacker will replace an original web page with another usually pornographic or defamatory page (Eddy *et al.,* 2012). Hackers often use religious and government sites for disseminating political or religious views.

9. Email Bombing: It involves sending numerous emails to a target until his/her account fails. The goal of email bombing is to crash the recipient's mailbox. In this type of attack termed as denial-of-service attack, many requests for information are sent to a server rendering it non-operational and thus making the server more difficult to be accessed by users.

10. Data Diddling: One of the most common forms of computer crime is data diddling - illegal or unauthorized data alteration. That is, these changes may occur during input of data, in between the process and output. Data diddling incidences have affected banks, payrolls, inventory records, credit records, school transcripts and every other conceivable type of data processing.

11. Virus/Worm Attacks: Computer viruses are little software programs that infect other computers by copying themselves to spread from one system to another and damage computer functioning. For example a virus could possibly corrupt or erase files on a victim's machine but it may also use the user's e-mail client to send itself to others or even wipe off everything on the victim's hard disk.

12. Web Jacking: In simple terms this means forcibly taking over control of a website just as in traditional hijacking of an airplane physical force is used.

13. Child Pornography: The Internet has emerged as one of the top media through which child sexual abuse can be conducted through meeting children online under the disguise of being teenagers by posing as one themselves or creating a profile similar for their age which they then start befriending them and making them feel comfortable with their friendship then slowly begin sexual chat so as to make them feel at ease with it and later invite them out for personal interaction.

CYBER SECURITY:

Safeguarding computer systems, networks, and data from digital attacks is of great concern for cybersecurity. Cybersecurity involves measures to prevent unauthorized access, data breaches, and other types of cyber threats. Additionally, cybersecurity includes educating users about safe online practices in order to reduce the likelihood of cyber attacks.

Privacy and security are some security measures that organizations will never stop being cautious about regarding their information on any sector. All organizations need to make sure that their IT infrastructure is protected against cyber-attacks regardless of size or nature. Clients and consumers fall prey to business organizations as well as competitors. To succeed as a firm or company an entity has to first establish itself as a provider of safety. Cybersecurity also refers to steps taken in real life to keep away intruders from computer systems, networks and data. It's the responsibility of cybersecurity professionals to ensure that internet, private networks among other computer systems are secure. Cybersecurity confines sensitive information only on those requiring it. There is a necessity for one to have knowledge regarding different types of cyber security for maximum safety. There will be new attacks on Android operating system base devices, but it will not be on massive scale (Reddy and Reddy 2014).

Network security branch of computer security specifically related to the Internet [J. Jeba Praba, (2016)]. Network Security aims to keep harmful programs and unauthorized users out of a network. Network security describes firm's precautions to protect their computer networks from threats like viruses and hackers. In contrast, application security refers to using technological safeguards including anti-virus software, encryption, and firewalls to prevent unauthorized access to and manipulation access to and manipulation of software programs.

We are presently living in a world where all information is maintained in a digital or in a cyber form. Social networking sites provide a space where user feels safe as they interact with family and friends. In the case of home-user 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.

CYBER SECURITY MEASURES

Cyber security measures involve steps to protect computer systems, networks, and data from unauthorized access, attacks, and damage. Cyber security measure involve using strong passwords, implementing two factor or multi-factor authentication, access control to data and systems, use security software, using antivirus programs and firewalls, encrypting sensitive data, backup data regularly, use a Private Virtual Network(VPN) to privatize the Network Connection, updating software time to time, and educating user about potential threats like phishing scams. These measures help prevent cyberattacks and safeguard sensitive information.

Here are some important tips and best practices to keep yourself safe online:

Cyber Security Control measures include some of the basic tips for cyber safety and best practices for cyber security.

1. Strong password should be made use of: All passwords (e.g., computer, laptop, mobile phone, email etc.) must be able to accommodate strong ones. Length, complexity and frequency of changes generally determine a password's strength. Authentication must be done in each device.

a. There must be at least eight alphanumeric characters that it contains.

b. The two non-alphabetic characters must at least appear together with three alphabetic characters.

c. At least one character has to be in small-case while another will have to be capital letter.

d. Avoid using same password to more than one system.

Passwords cannot consist of easily guessed or obtained personal information, names of family members, friend's etc. cyber crimes:

A password keeps from other people going in your personal information.

Some things to keep in mind for cyber security related to passwords are as follows:

a. Authentication - Select multi-factor authentication where possible.

b. Don't share- Don't tell your password because it would led other people to your personal information.

c. Remember Password- Don't use the remember password if you are using a laptop with someone else.

c. Use different password for each account.

d. Mark them hard to guess and easy for yourself to remember.

2. Put Up a Firewall: A Firewall is like a digital barrier that helps protect a network or device from unauthorized access while allowing authorized communication. It can be either hardware or software-based and filters incoming and outgoing network traffic on predetermined security rules.

3. If you are a victim of online fraud: keeps the following things in mind before calling helpline or report in police station:

a. Victim's name

b. Victim's mobile number

c. Nearest Police Station

d. District

e. Name of bank

f. Amount debited

g. Account number UPI ID from which the amount debited

h. Brief of how fraud has happened

4. Use Security Software: Security software protects networks and endpoints from unauthorized access, viruses, cyber threats and malware that put users and systems at risk. Security software include encryption tools, Penetration testing, Network Security Monitoring Tools, Packet Sniffers, Web Vulnerability Scanning tools etc.

a. Whatsapp Security: Some things to keep in mind for cyber security while downloading or using the whatsapp are as follows:

1. Always read the term and conditions before downloading any app

2. To block an unknown number, open that particular chat window go to more option and block

3. Never send private information like bank account details, PINs or passwords through whatsapp

4. Keep automatic downloads disabled

5. Never respond to suspicious message from unknown numbers

6. Deactivate your whatsapp if you lose your number

7. Enable two factor authentications, to ensure that nobody can set up your whatsapp without knowing the secret 6-digit code

8. Manage Whatsapp web effectively, log out from all computers

9. Restrict Access to your profile to only contacts

10. Avoid using whtaspp while connecting to the open Wi-Fi networks

11. Always keep an updated antivirus security solution installed on your mobile device

b. Keep Your Software Up to Date: Keeping Software up to date is crucial for maintain the security and functionality of your digital devices. By regularly updating your software, you can minimize the risk of exploitation by cyber threats and ensure that you have access to the latest features.

c. Beware of identity theft: Fraudsters us victim's identity to commit fraud by obtaining personal or financial information.

Some things to keep in mind for cyber security related to passwords are as follows:

1. Never provide details or copies of identity proofs (PAN Card, Aadhar Card etc.) to unknown person/organization.

2. Do not share sensitive information on public platforms

3. Do not leave your credit, debit or ATM Card receipts behind and never throw them away in public

d. Beware of investment Scams: Never click on any link shared through SMS/Whatsapp to invest money in website/application promising daily returns or double returns in short span of time.

e. Beware of Fake Calls: Victims gat a recorded call from an unknown number and will be told by the caller

stating that his or her mobile number will be soon discarded as his/her number has been detected to have criminal activity links.

1. The caller then ask the victim to click on some numbers during the call and will make the victim to take a fake call centre by the fraudsters.
2. If the victims try to check the authenticity, the fraudsters may come on video calls and will threaten the victim that he/she will be arrested.
3. The victim may also receive a fake notice using the name of Law Enforcement Agencies.
4. After creating a sense of fear, the fraudsters will pretend to help the victim and will request for his/her bank details.
5. Once the details are shared, the fraudsters will take the money from the victim's account.

Some things to keep in mind for cyber security related to fake calls, emails etc. are as follows:

1. Do not click on any links, attachments received from strangers through messages, email and social media.
2. Do not click on any numbers for talking to any customer care during calls from strangers.
3. Do not share banking details like OTP, account number, PIN, password with anyone.
4. Do not share your personal information on social media platforms.
5. Reporting threatening calls/messages to the nearest police station.
6. Report cyber crime at https://www.cybercrime.gov.in or call **1930.**

f. Things to avoid having your phone hacked

1. Don't download apps that aren't official. If you are not sure, look at reviews and do some research before installing.
2. Don't use public WI-FI if you don't have a VPN, VPNs help your connection with encryption and hide your data so that other people can't see it.
3. Don't store password on the device you are using. It can be hard to remember different passwords for every account. Use a secure password manager. You can store all of your secure credentials in a digital vault with these services. This gives you easy access and security you need.
4. Update all your apps. Hackers can take advantages of programming bugs in even trusted apps. Bug fixes are included in app updates to keep you safe from unknown risks. So update your phone when you can.

CYBER LAWS

Cyber or IT Law is referred to as the Law of Internet. Cyber law is the law governing cyber space. Cyber space is a very wide term and include computers, networks, software, data storage such as hard disk USB disk etc., Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.

Cyber law, it is legal infrastructure to deal with cyber crimes. Cyber law or it laws is referred to as law of the internet or digital laws. Cyber law is the term used to describe a law that deals with issues related to the internet, technology and electronic element, communication technology, including hardware, software, computer and information system. Cyber laws, it is legal system designed to deal with the internet, cyber space, computing and related legal issues.

Cyber law deals with cybercrimes can include criminal activities that are traditional in nature such as theft, fraud. Cyber crime is a generic term that refers to all criminal activities one using the medium of communication technology components, cyber space and the world wide web(WWW), the internet.

Cyber law provides legal protection to people using internet business. In today's world most of the people are using computers, mobile phones, social media, email, messages for communication and entertainment. Internet is used very frequently in today's time. According to development of the world it's important for everybody who uses the internet, to be aware of the cyber law of their country and local area so that they easily know about the legal and illegal activities over the internet.

Prime need of cyber law is to maintain law and order during online activities.

1. Cyber law includes laws relating to:

a. Cyber Crimes
b. Electronic and Digital Signatures
c. Intellectual Property
d. Data Protection and Privacy

Cybercrimes are illegal acts where computers are used as a tool or target or both. What happened was there were unexpected occurrences of cyber crime that resulted from the huge expansion in e-commerce (ecommerce) as well as online share trading.

Electronic and Digital Signatures: Electronic signatures authenticate electronic records. One type of electronic signature is digital signatures. The use of technology and efficiency in digital signatures makes them more trustable than handwritten signatures.

Intellectual Property refers to creations of the human mind, such as stories, songs, paintings, and designs. In the realm of cyberspace, various aspects of intellectual property are protected by cyber law, including:

1. Copyright Law: This covers computer software, source code, websites, and cell phone content, along with licenses for software and source code.

2. Trademark Law: It protects domain names, meta tags, mirroring, framing, and linking practices on the internet.

3. Semiconductor Law: This pertains to safeguarding semiconductor and integrated circuits designs and layouts.

4. Patent Law: It addresses the protection of inventions related to computer hardware and software.

Data protection and privacy: An attempt by the laws to strike a balance between the individual privacy rights on one hand and interests of data controllers such as banks, hospitals and email service providers among others who collect store or transmit their data through networks. These laws are designed to tackle threats to privacy that can arise from collecting information using networked databases.

In simple words we can say cyber laws are the frameworks that govern online activities, cybersecurity, digital transaction, addressing issues such as data

protection. Cyber laws are differ from country to country.

There are different purposes of cyber laws. The aim of cyber law is to protect people from becoming the victims of crime through crime happened in the cyber space. Just like other law, cyber law consist of rules that command how people and companies should use the computers and internet, and protect the people from getting trapped into Cyber crime run by malicious people on the in the internet .Freedom of speech, Copyright, Fraud (online transaction), Stalking and Harassment are some features of cyber law. Digital signatures become legal only due to the introduction to cyber law. One of the biggest advantages of cyber law is that it facilitates the e-filling of documents with government department and agencies. Because of the cyber law all the electronic contracts made via secure electronic channels are valid legally.

Cyber Jurisprudence[(Cyber->Cyber law->virtual world), (Jurisprudence-> juris + prudential(the study or knowledge of law)]

Cyber Jurisprudence is study of laws which is directly related to cyber crimes. Cyber Jurisprudence also describes the principles of legal issues, which exclusively regulates the cyberspace internet. Cyber law protects every individual from getting trapped in any cyber violations.

Law includes the rules of conduct:

1. That have been approved by the government, and
2. Which are in force over a certain territory and
3. Which must be obeyed by all persons on that territory.

Violation of these rules could lead to government action such as imprisonment or fine or an order to to pay compensation.

Cyber law is important because it touches almost all aspects of transaction.

Some Categories of Cyber Law:

1.Using a computer to commit crimes example- online transaction fraud, Cyber terrorism etc.

2.Using a computer or other electronic device to target other computer or electronic device example- hacking, attacking, virus etc.

NEED AND SCOPE OF CYBER LAWS

The rise of Information Technology has put pressure on existing regulations. In today's digital world, almost everyone is impacted by cyberspace. Cyber Law is constantly evolving to keep up with these changes. Here are some reasons why it's important:

1. Everyday Transactions: Cyber law covers nearly all aspects of transactions and activities on the Internet, the World Wide Web, and Cyberspace.

2. Dealing with Hackers: It helps in dealing with hackers and those who introduce viruses into computers.

3. Preventing Cybercrime: Cyber Law prevents damage from cyber-criminal activities by safeguarding information access, privacy, communication, intellectual property, and freedom of speech online.

4. Protecting Company Data: Companies rely heavily on their computer networks and store valuable data electronically.

5. E-Governance: Government forms like tax returns and company filings are now done electronically.

6. Online Shopping: Consumers are increasingly using credit cards for online purchases.

7. Digital Evidence: Important evidence in various cases, from divorce to organized crime, is often found in computers and cell phones.

8. Combating Online Fraud: Cybercrime, such as online banking fraud and credit card scams, is becoming more prevalent.

9. Modernizing Business Transactions: Digital signatures and e-contracts are replacing traditional methods of doing business.

CONCLUSION

In this paper, we have discussed about the Cyber Space, Cyber Crimes, Cyber Security etc. which are the major aspects of today's world.Think of cyber space like a big virtual world where we do a lot of stuff, like chatting, shopping, and sharing information. But just like in the real world we lock our doors to keep our stuff safe, we need to do same for the online to protect our personal information. So cyber security is all about using tools and practices to keep our online world safe from cyber crime, like hacking or scams. It's important for everyone to stay safe in cyber space.

REFERENCES

Delftani, Alessandro Arvidsson, Adam (2019). Introduction to Digital Media.

J. Jeba Praba (2016): Cyber Security and Therats.

Morningstar, C., & Farmer, F. R. (2003). The Lessons of Lucasfilm's Habitat. The New Media Reader. Ed. Wardrip-Fruin and Nick Montfort. 664-667.

Reddy, G. N., & Reddy, G. J. (2014). A study of cyber security challenges and its emerging trends on latest technologies. *arXiv preprint arXiv:1402.1842*.

V. Karamchand Gandi, V. (2012). Assistant Professor of Department of Computer Science , Tamil Nadu – South India. : An Overview Study on Cyber Crimes in Internet.

Warrier, V. G. (2002). *" The globe is now officially open for business!": the advertising of cyberspace: globalization and the politics of cyberculture* (Doctoral dissertation, Concordia University).