A STUDY ON CYBERCRIMES

C. Dhanalaksmi, B.Com. LL.B (Hons), The Tamil Nadu Dr. Ambedkar Law University

ABSTRACT

Any illicit action that uses a computer as its main tool for commission and theft is referred to as cybercrime. Cybercriminals or the hackers who want to generate money commit the majority, but not all, of cybercrime. Individuals or organisations can commit cybercrime. Some cybercriminals are well-organized, employ cutting-edge methods, and possess exceptional technical proficiency. Some hackers are amateurs. Cybercrimes will rise alongside technological advancements as technology plays a larger part in people's lives day by day. Any illicit action that uses a computer as its main tool for commission and theft is referred to as cybercrime. Cybercriminals or hackers who want to generate money commit the majority, but not all, of cybercrime. Individuals or organisations can commit cybercrime. Some cybercriminals are well-organized, employ cutting-edge methods, and possess exceptional technical proficiency. Some hackers are amateurs. Cybercrimes will rise alongside technological advancements as technology plays a larger part in people's lives day by day.

Keywords: cybercrime, cyberhackers, cybercriminals, cyberlaws.

INTRODUCTION:

Cybercrime is a term for any illegal activity that uses a computer as its primary means of commission and theft. Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organisations. Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers. As day-by-day technology is playing in major role in a person's life the cybercrimes also will increase along with the technological advances. Rarely, cybercrime aims to damage computers for reasons other than profit. These could be political or personal. Cybercrime is where a single or whole network is involved to perform illegal to perform illegal activity. In today's scenario cybercrime is an emerging profession in the help of advanced technology and high-speed internet facility it has created a great platform for the individual or groups to earn lots of money illegally. Cybercrime is simply defined as crimes that are directly related to computers and using computers. Cybercrime has been used to describe a wide range of offences, including offences against computer data and system (such as "hacking"), computer related forgery and fraud (such as "phishing")

THE CYBER LAWS:

Law which regulates activities in cyber space is known as cyber law. Cyber law is the law governing cyber space. Cyber space is a wide term and includes computers, networks, software, data storage devices (such as hard disks, USB disks), the internet, websites, emails and even electronic devices such as cell phones, ATM machines, etc. A place that is not real, and where E-message exists while they are being sent from one computer to another computer. Cyberspace is a place without any physical boundaries. There are some sections which punishes the offenders who are indulging themselves in cyber-crimes. The offender gets punishment either in the Information Technology Act, 2000 (IT Act,2000) or in the Indian Penal Code, 1860. The sections involved in IT Act,2000 and IPC,1860 are:

1. Where a person without the permission of owner or any other person in charge damages the computer.[1]

[1] §.43 of IT Act,2000.

2. Whoever, fraudulently or dishonestly makes use of e- signature, password or unique identity feature of another person shall be punished for 3 years or fine up to 1 lakh.[2]

3. Whoever, by means of any communication device or computer resources cheat by personation shall be punished with 3 years or with fine.[3]

4. Punishment for cheating by personation.[4]

5. Making false document.[5]

6. Punishment for forgery.[6]

7. Forgery for purpose of cheating.[7]

8. Forgery for purpose of harming reputation.[8]

SOME OF THE CYBER CRIMES:

IDENTITY THEFT:

From 1964, the term Identity Theft was there. The fraudulent practice of using another person's name and their personal details in order to obtain credit, loans etc. the Identity theft happens when someone commits fraud or another crime using another person's personal information such as their name, identification number, or credit card number and so on without that person's consent. There are four types of identify theft. They are:

Criminal Identity Theft: Criminal Identity theft is a type in which a thief pretends to be someone else when they are caught committing a crime. During an investigation or an arrest, the thief uses the victim's personally identifiable information, such as full name, licence number, social security number, and other details.

[2] §. 66(C) of IT Act, 2000.
[3] §. 66(D) of IT Act,2000.
[4] §. 419 of IPC, 1860.
[5] §. 464 of IPC,1860.
[6] §. 465 of IPC, 1860.
[7] §. 468 of IPC,1860.
[8] §. 469 of IPC, 1860.

Financial identity theft: Although there are many different ways that financial identity theft can occur, it typically entails unauthorized access to your financial cards or account information through theft, by hacking your online account, or through a data breach involving your account information.

Medical Identity theft: Medical Identity theft is when someone steals or uses your personal information such as your name, or social security number or Medicare number to submit fraudulent claims to Medicare and other health insurers without your authorization.

Child Identity Theft: Identity fraud involving children can take many different forms. Even though the majority of youngsters do not have numerous bank accounts or lines of credit, they nonetheless have a wealth of personal data that scammers can access. Fraudsters will steal anything they can, including social security numbers and login information from social media. They may gain access to other internet accounts through compromised logins and passwords, and knowing social security numbers may let them to start new accounts in your child's name.

PHISHING:

Phishing is a type of social engineering in which criminal trick victims into disclosing sensitive information or downloading the malicious software like ransomware. Phishing attempts are getting more and more complex, and they frequently transparently mirroe the site that's being targeted, allowing the attacker to watch everything the victim does there and to breach any further security measures with them. It is an offence where you are electronically impersonating or someone else for financial gain.

Dragnet: They send bulk e-mails to the users and by clicking those mails their information will be taken.

Rod & reel: In this people will be targeted and the fake id will be sent to them for acquiring their identity and the information related to them.

Lobster pot: Targets the genuine website and the domain name will be taken and forged.

VISHING & SMISHING:

The fraudulent phone calls that induce you to reveal personal information is known as vishing.

The vishing is the form of phishing. A cybercriminal conducts a phishing assault by using messages like emails, Texts, chats, phone calls etc, to get sensitive data, login information or money from the victim. One type of phishing is vishing. A criminal often uses phone calls as a voice communication tool.

The fraudulent text messages meant to trick you into revealing data is known as the Smishing. In other words the users will receive a brief text message from the hackers with a terrifying scenario in an SMS-based fraud attack.

DATA THEFT:

If any person without the permission of the owner or any person who is in charge of computer system. Downloads copies or it extracts any data or information from such computer including the data or the information stored in any removable storage medium shall be known as the 'data theft'.

HACKING:

The act of compromising digital devices and networks through unauthorized accesses to an account or a computer system. The destruction or interference in a system network or computer. Destroying or altering the existing information and Introduction to malicious software is known as Hacking.

THE FEATURES OF CYBER CRIME:

1. **Interactive virtual environment:**

It is a networked application that allows a user to interact with both the computing environment and the work of other users. Email, chat and web based document sharing applications are all examples of virtual environments.

2. **Unlimited accessibility:**

Unlimited access is defined as the ability to inquire, update, and or delete information at operating system or data base levels.

3. **Ubiquitous in nature:**

It generally means being present everywhere at once. Ubiquitous computing is a software and computer science concept in which computing appears everywhere and anytime.

ANATOMY OF CYBER WORLD:

1. SURFACE WEB:

The surface web is also called the 'VISIBLE WEB', 'INDEXED WEB'. 'INDEXABLE WEB'OR 'LIGHTNET'. It is the portion of the world wide web that is readily available to the general public and searchable with standard web search engines. Which constitutes only 4% of cyberspace. The Facebook, WhatsApp, and other social media and online websites are part of the surface web.

2. DEEP WEB:

It generally not directly accessible but accesses through ID's and passwords. Which constitutes only 90% of cyberspace. The medical records, legal documents, government files, organisation-specific repositories, financial records and other virtual information are the examples of Deep web.

3. DARK WEB:

All the illegal acts are performed in this space like pornography, illicit trade, illegal drug trade through like silk route. Which constitutes only 6% of cyberspace. The part of the world wide web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable.

CASE LAW:

SONY SAMBANDH.COM CASE

Sony India Private Ltd, which runs a website called www.sony sambandh.com, targeting non resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online.

The company undertakes to deliver the products the products to the concerned recipients. In May 2002, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless head phone.

At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase.

The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court therefore released the accused on probation for one year.

The judgement is of immense significance for the entire nation. Besides being the first conviction in a cybercrime matter, it has shown that the IPC can be effectively applied to certain categories of cyber crimes which are not covered under the Information Technology Act, 2000. Secondly, a judgement of this sort sends out a clear message to all that the law cannot be taken for a ride.

SUGGESTIONS:

1. Use Anti-virus software and keep the software updated.
2. Use strong passwords
3. Never ever open attachments in spam emails.
4. Do not unnecessary open spam emails or untrusted websites.
5. Unnecessary don’t give personal information.
6. Don’t share the OTP or any other Passwords to anyone

CONCLUSION:

Cyber-attacks targeting critical information infrastructures in India such as energy, financial services, defence and telecommunication, have the potential of adversely impacting upon the nation’s economy and public safety. From the perspective of national security, the securing of the critical information, infrastructure has become a top. Cyber security has a major component of national security, strategies in states across the globe.

REFERENCE:

- Cyber laws – Justice Yatindra Singh.
- https://blog.ipleaders.in/
- What Is Financial Identity Theft and How Does It Happen? (idtheftcenter.org)
- https://oig.hhs.gov/fraud/consumer-alerts/medical-identity-theft/
- What is Child Identity Theft? - Experian