JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CYBER CRIME & CYBER LAW'S IN INDIA

ADVOCATE MUNMUN DUTTA (BARRACKPORE COURT)

Munmun Dutta
Advocate
Barrackpore Court

ABSTRACT

The world has made significant progress due to the advancement of communication, particularly with the emergence of the Internet. However, this progress has also led to the rise of e-crimes, commonly known as the cybercrime. This widespread issue presents a major challenge to society today, affecting nations, companies, and individuals worldwide.

Cybercrime has reached every corner of the globe, victimizing millions of people. Given the seriousness of e-crime, its global impact, and the far-reaching consequences it brings, it is crucial to establish a shared understanding of this criminal behaviour in order to effectively combat it. This research focuses on exploring the definitions, types, and instances of e-crime, with a specific emphasis on India's legislation against such activities.

KEYWORDS: cybercrime, e-crime, global, India,people

1.INTRODUCTION

A computer is a device that stores and processes information based on user instructions. The Internet, also known as cyberspace, has facilitated the exchange of data and information between different networks, making it more convenient and efficient. Internet technology serves various purposes, including online transactions and interactions. Throughout the years, the majority of computer users have utilized computers for personal or other advantageous reasons. Consequently, administrators have placed significant emphasis on security concerns, leading to the emergence of "Cyber Crimes." Cyber Crimes pertain to offenses committed using computers or computer networks, primarily over the Internet. In simpler terms, cybercrimes are unlawful activities that occur through electronic communications or information systems. Cybercriminals may employ devices to gain unauthorized access to personal information, confidential business data, government information, or to disable devices. The unauthorized sale of private data or information is also considered a cybercrime. Individuals involved in such activities are commonly referred to as hackers. Hence,

cybercrimes are also known as electronic crimes, e-crimes, computer-related crimes, high- tech crimes, digital crimes, and new age crimes. Presently, cybercrime has inflicted significant harm on individuals, organizations, and even governments. To combat crimes related to the internet, various laws and methods have been implemented. In India, the "Cyber Law" was enacted to address legal systems concerning cyberspace, online security, online privacy, and other pertinent issues. Cyber Law encompasses regulations governing cybercrimes, digital and electronic signatures, data protection, privacy, and more. The General Assembly of the United Nations has also acknowledged the necessity for international cooperation in combating cybercrime.

DEFINITION OF CYBER CRIME:

Sussman and Heuston were the first to introduce the term "Cyber Crime" in 1995. Cybercrime does not have a single definition; it is considered as a collection of actions or behaviours that are based on the material offense object and modus operandi, which impact computer data or systems. According to the definition, Cybercrimes are criminal acts carried out through the use of a computer or other electronic communication devices. In simpler terms, acts that are punishable under the Information Technology (IT) Act of 2000 are referred to as "Cyber Crimes". In India, the IT Act of 2000 addresses cybercrime issues. Amendments were made to this Act in 2008, resulting in the passing of the Information Technology (IT) Act of 2008, which covers a wide range of areas such as online commercial transactions, digital signatures, e-commerce, and more. Therefore, "Cyber Crime" can be defined as any wrongdoing or offenses where electronic communications or information systems, including devices, the Internet, or a combination of both, are involved.

Categorization of cyber offenses

1. **Cyber Theft** is a form of cybercrime utilized by criminals to unlawfully obtain information or money from a remote location using a computer or the internet. It encompasses various types of crimes, including Identity Theft, Phishing, Forgery, Web jacking, Cyber Embezzlement, Corporate Espionage, and Plagiarism.

Identity Theft involves individuals creating fake identities on the internet to fraudulently steal money from bank accounts, credit or debit cards, etc. This act is considered a punishable offense under Section 66C of the IT Act, 2008.

Phishing is another common cybercrime method employed by hackers to acquire personal information such as passwords, usernames, bank account numbers, credit card details, etc. It is often carried out through email spoofing.

Forgery entails the creation of false documents, signatures, currencies, revenue stamps, etc.

Web jacking refers to the hijacking of a victim's account using a fake website to either cause damage or alter the information on the victim's webpage. The attacker sends a link to the victim's email, and upon opening the link, a new page appears prompting the victim to click on another link. By doing so, the victim is redirected to a fake page.

Cyber Embezzlement is a crime committed by employees who already have legitimate access to a company's computerized system. They misuse their access to carry out fraudulent activities.

Corporate Espionage involves individuals committing crimes to gain a competitive advantage in the market. The cybercriminal, whether from within or outside the company, utilizes the company's network to steal client lists, marketing strategies, financial data, trade secrets, etc.

Plagiarism is the act of stealing someone else's original writings and presenting them as one's own. With the abundance of online data and increased internet and computer accessibility, the issue of plagiarism is on the rise. Certain software programs are used to detect and prevent plagiarism.

2. The action of impeding service availability

A denial-of-service attack is an extremely rudimentary technique that exploits the computing power of the target computer, resulting in the denial of access to other machines on the server. Hackers employ various methods to compromise a server.

3. Email Harassment:

Techopedia defines email spoofing as a deceptive email practice employed to conceal the true origin of the email message, while giving the appearance that it originated from a trustworthy source11. This technique has become increasingly prevalent in recent times. These fraudulent tactics are typically employed by spammers with malicious intentions, such as obtaining unauthorized access to an individual's banking details or disseminating viruses. Offenders engaging in such activities can be prosecuted for forgery under Section 463 of the IPC.

4. Hacking

Hacking necessitates gaining unauthorized access to a device and altering it in order to maintain access, along with modifying the target machine's configuration, objective, or service without the knowledge or consent of the system owners.

5. Stalking

Cyber stalking is a criminal act in which an individual utilizes the Internet to systematically harass or threaten someone. It involves intentional behaviour by the cyber stalkers through various online platforms such as email, social media, and chatrooms, which causes the victim to experience fear, intimidation, or harassment. Typically, the stalker is acquainted with their victim, and a majority of the victims are women. Previously, cyber stalkers were prosecuted under Section 509 of the Indian Penal Code (IPC) due to the absence of specific punishment under the Information Technology (IT) Act of 2000. However, with the amendment of the IT Act in 2008, cases involving cyber stalking can now be charged under Section 66A of the Act. Offenders can face imprisonment for up to three years and may be fined.

6. Child sexually abusive material (CSAM):

Cyber pornography, also known as cybersex, refers to the use of the internet to create, display, distribute, or publish explicit or obscene materials. This includes engaging in sexual or erotic activities online. There are numerous websites that showcase pornographic content, such as photos and videos, which can be easily and inexpensively produced using techniques like morphing or the exploitation of women and children. Morphing involves altering an original image using a false identity or unauthorized user, which is considered a punishable offense under the Indian Penal Code and Section 66 of the Information Technology Act, 2000. Unfortunately, the internet is also a platform for child pornography, where underage individuals are coerced into participating in pornographic productions or are sold or forced into cybersex or lives of prostitution. These crimes often originate in impoverished nations where victims face dire economic circumstances.

7. Cyberbullying:

A cyberbully is a person who partakes in the act of tormenting or intimidating others using electronic devices like computers, mobile phones, laptops, and similar gadgets.

Cyberbullying refers to the act of bullying that occurs through the use of digital technology. The use of social media, messaging platforms, gaming platforms, and mobile devices is commonly seen in such cases. Often, this involves repetitive behaviour with the intention of instilling fear, anger, or humiliation in the targeted individuals.

8. Unauthorized Use of Credit Card and Debit Card:

Unauthorized transactions made using someone else's credit or debit card are considered fraudulent and are done with the intention of accessing the cardholder's funds. This fraudulent activity can occur when a criminal gains access to the cardholder's credit or debit card number, as well as their personal identification number (PIN). It is important to note that this information can be obtained by dishonest employees or hackers.

9. Fraudulent Job Scam:

The Reserve Bank of India (RBI) has recently issued a warning to individuals seeking employment about the prevalence of online job fraud schemes. These fraudulent activities aim to deceive job seekers by offering them lucrative positions with higher salaries, only to dash their hopes and leave them empty-handed. In their statement released on March 21, 2022, the RBI not only shed light on the modus operandi of these scams but also provided valuable advice to the general public on how to protect themselves when pursuing job opportunities, both within India and overseas.

10. Sextortion on the Internet:

Online sextortion happens when a cybercriminal threatens to publish private and sensitive material on the internet in order to obtain sexual images, sexual favours, or money from their victims.

11. Sexual Exploitation:

Cyber grooming is when someone builds a relationship with a teenager and tries to pressure them into engaging in a sexual act. They use strategies like luring and teasing to manipulate the teenager.

12. Spreading the Virus:

This type of illegal activity involves unauthorized access to the operating system through the installation of new applications known as ss bug worms or logic bombs. Deleting machine data or disabling internet function without authorization is clearly illegal and is commonly referred to as computer sabotage.

13. Machine Forgery:

Data changes and processes in computerized records. Machines can also be used for forgery. Computerized colour laser copies have made dishonest modification or replication more prevalent.

14. Salami Attack:

salami attack occurs when a criminal makes small, unnoticed modifications to deduct tiny sums, such as 2.50 per month, from all of the bank's customer's accounts and deposits it into their account. In this scenario, the changes are subtle and prevent account managers from noticing any wrongdoing.

15. Network Attack:

Viruses are software that can bind to a computer or file, and then spread to other files and computers within a network. They often impact a computer's data by altering or deleting it. In contrast, worms do not need a host to connect to. They create functioning duplicates of themselves and continue this process until all available memory on a computer is utilized.

16. Logic Bombs:

The occurrence of a specific condition determines the commission of the crime. The most evident illustration is the Chernobyl virus, which remained inactive for the majority of the year and only became operational on a designated date.

17. Trojan Malware:

A trojan is a malicious program that deceives by posing as a legitimate software, thus concealing its true purpose and operating from within.

The act of stopping cybercrimes:

In line with the guidelines set by the International Maritime Organization (IMO), the approach to cyber-attack risk should be structured as follows:

The initial step involves outlining the roles and duties of the staff in charge of managing cyber risks. The subsequent step is the identification of the systems, assets, data, or functions that could jeopardize operations if disrupted. To safeguard against potential cyber incidents and ensure uninterrupted operations, it is crucial to establish risk management protocols and emergency plans. Equally important is the swift detection of a cyber-attack, coupled with the development and execution of plans to restore critical systems for ongoing operations. Lastly, determining and implementing measures to back up and recover any affected systems is essential.

Preventive actions against Cyber Crimes

Cybercrimes, being borderless in nature, require innovative measures to address the issue of advanced crime. Therefore, in addition to Cyber Laws, the following points should be considered for safety in Cyberspace while using the Internet:

i. Awareness should be raised among students at the grassroots level, providing knowledge about cybercrimes and cyber laws. This should be incorporated into Computer Centres, Schools, Colleges, and Universities. A cyber law awareness program can be implemented in any educational institution to offer basic knowledge of Internet and Internet security.

ii. Regularly reviewing bank and credit card statements can help reduce the impact of identity theft and online crimes.

iii. Keep your operating system up to date to keep intruders away from your computer, as this prevents attackers from exploiting software defects that could otherwise allow them access your system and exploit it for unauthorized activities, it is important to use unique and strong eight-character passwords that consist of a combination of symbols, words, and numbers, especially for online activities such as banking.

iv. In order to protect your system against unauthorized access and hacking, it is important to create unique and strong passwords. These passwords should consist of at least eight characters and should include a combination of symbols, words, and numbers. It is also crucial to avoid using easily traceable personal information, such as email IDs, login names, last names, dates or months of birth, as passwords for online activities like banking. Additionally, it is recommended to use different passwords for different online services, rather than using the same password for everything. To ensure the security of your webmail or social media account, it is important to enable Two-step Authentication. By adding your mobile number to your mail account, you will receive notifications if someone else attempts to access your account. With Two-step Authentication, your username and password are necessary to open your account, but a verification code is sent to your registered mobile number if you forget your password for personal security purposes. Even if a hacker manages to crack your password, they will not have access to your account without the temporary verification code.

v. Additionally, it is essential to protect your computer with security software to safeguard against online threats. Programs such as antivirus and firewall software are necessary to remain safe online. The firewall controls who and what can
communicate with your computer over the internet, while the antivirus protects the system against viruses and worms. Nowadays, integrated security programs like Norton Internet Security are popular because they provide all the necessary security software for online protection in one package. These programs protect against Trojan horses, harmful applications, and maintain all online activity, including email messages and web browsing. They combine Firewall, Antivirus, Antispyware, and other features like Antispam and parental controls.

vi. Nowadays, comprehensive security programs like Norton Internet Security, which incorporate Firewall, Antivirus, Antispyware along with additional features like Antispam and parental controls, have gained popularity as they provide all the necessary online protection software in a single package.

vii. Additionally, it is important to refrain from responding to emails that request personal information and avoid clicking on any links in these messages as they could lead to deceitful and harmful websites. It is advisable to carefully review the privacy policies on the company's website and software before providing any personal data, as reputable companies never solicit personal information through email.

India requires laws and regulations to combat cyber crime

In countries like India, where the internet is widely used, cyberlaw holds significant importance. The legislation was implemented to safeguard individuals and businesses from cybercrime. It grants the authority for legal recourse to individuals and organizations in the event that someone violates the regulations outlined in the law.

There may be a need for cyberlaw in the instances that follow:

- With all stock transactions now being conducted in demat format, individuals involved are safeguarded by cyber law in the event of fraudulent activities. The majority of Indian companies maintain electronic records and may require this law to protect against misuse of the data. As technology continues to advance, government forms like income tax and service tax returns are now submitted electronically, creating a potential for misuse if government portal sites are hacked.

- Cyber law is necessary to enable legal action in such cases. With the prevalence of online shopping, credit and debit cards are commonly used, but unfortunately, the internet has also become a platform for cloning these cards, allowing criminals to steal personal information. Cyberlaw, specifically under Section 66C of the IT Act, can help prevent such crimes.

- If someone attempts to fraudulently or dishonestly use an electronic password, they could face a three-year prison sentence and a fine of up to one lakh rupees. Digital signatures and electronic contracts are commonly used for business transactions, and those involved can easily misuse them. Cyberlaw offers protection against these fraudulent activities.

CONCLUSION

that cybercriminals exploit the vulnerabilities in the system for personal gain. Therefore, the enforcement of cyber laws is crucial to protect every individual from any potential threat in the digital world. With the complexity of cyberspace, there are activities that fall into a grey area and are difficult to govern by law. Collaboration among legislators, ISPs, financial institutions, e-commerce platforms, and other intermediaries is crucial. Nevertheless, the responsibility to actively combat cybercrime ultimately falls on the users. The advancement of online security and resilience relies on the collective efforts of these stakeholders, ensuring their compliance with cyber laws.

References

- http://blog.ipleaders.in/cyber crime
- http://cybercrime.org.za/definition
- http://indiakanoon.org/doc/1439440
- https://probono-india.in/blog-detail.php?id=218
- http://www.researchgate.net
- Section 66 of IT Act