International Journal of Criminal, Common and Statutory Law

E-ISSN: 2789-9500
P-ISSN: 2789-9497
IJCCSL 2025; 5(1): 01-03

www.criminallawjournal.org
Received: 02-10-2024
Accepted: 06-11-2024

Dr. Rekha
Assistant Professor in Commerce
GCW, Sonipat, Haryana, India

Corresponding Author:
Dr. Rekha
Assistant Professor in Commerce
GCW, Sonipat, Haryana, India

A study on cyber crime and it's categories

Rekha

Abstract
Cyber crime has become a significant threat to humanity, affecting social, cultural, and security aspects. To combat this, "The Indian government" passed "Information Technology Act in 2000" and amended various laws. However, cybercrimes can transcend national borders, making it difficult to investigate and prosecute them legally. Worldwide harmonization and coordination are necessary. Cybercrimes are unacceptable, and victims should file cases at the nearest police station. The articles defines the term cyber crime, different types of cyber crime and cyber space safety. It is descriptive in nature.

Keywords: Cyber crime, cyber space safety, IT act, harmonization

1. Introduction
The invention of the computer has facilitated human life, serving diverse purposes from individual use to major companies worldwide. A computer can be simply defined as a device that has the ability to store, modify, and execute data or user-inputted instructions. For decades, the majority of computer enthusiasts have been misusing computers, either for their own gain or the gain of others. As a result, "Cyber Crime" was born. As a result, people began engaging in socially forbidden acts. Cybercrimes are crimes that are typically done over the Internet or other cyberspace and involve computers or computer networks. Cybersecurity is the application of technology, protocols, and policies to "protect systems, networks, programs, devices, and data" from cyberattacks. It aims to "prevent illegal use of networks, systems, and technology" and reduce the likelihood of cyberattacks. It is crucial to the continuous advancement of Internet services and information technology. Improving cybersecurity and protecting critical information infrastructures are essential to the security and economic well-being of any nation. Government policies and the development of new services now heavily concentrate on keeping the Internet secure (and protecting Internet users). Deterring cybercrime is an essential part of a national cyberspace, along with "critical information infrastructure protection policy." Specifically, this comprises passing suitable laws to stay away from the improper use of ICTs for illegal or other activities that compromise the integrity of the country's vital infrastructures. Consequently, an all-encompassing strategy is necessary towards the development as well as execution of a nationwide cybersecurity framework along with strategy. "Cybersecurity" tactics, such as the creation of technological defenses or user education to keep people from falling prey to cybercrime, can assist in reducing cybercrime risk. One of the most important aspects of combating cybercrime is the creation and maintenance of cybersecurity plans. Humanity is changing as a result of several of the newest technologies available today. However, we are unable to adequately safeguard our personal data due to these new technologies, and that's why cybercrimes are increasing constantly. Since online transactions currently account for more than 60% of all commercial transactions, this sector requires an elevated degree of protection to guarantee the most successful and transparent transactions. As a result, cybersecurity is a new issue. The scope of cybersecurity encompasses many additional areas, including cyberspace, in addition to safeguarding data in the IT industry. Even the newest technologies, including "cloud computing, mobile computing, e-commerce, net banking," etc., need high levels of security. Since these technologies hold certain personal data, their security has become essential. Fighting cybercrime calls for a more comprehensive and safe approach. Since technological safeguards alone cannot prevent all crime, law enforcement organizations must be able to efficiently investigate and prosecute cybercrime.

Cyber crime
Cybercrime is any crime that involves computers and a network. The computer may have been used in the commission of an offense or it may have been the object of one.

Cybercrime can jeopardize a person's security and financial stability. Any act in which computers or networks are utilized as a weapon, target, or a place for unlawful activity is commonly referred to as cybercrime. There are several issues with this broad concept. For example, if the offender occurred to hit and kill someone with a keyboard, it would include more traditional offenses like murder.

Cybercrime Classifications

There are four main categories into which cybercrime falls. Here are a few:

a) Against Individuals: Cybercrimes committed by cybercriminals targeting a person or individuals are referred to as cybercrimes against individuals. The following are some examples of cybercrimes against individuals:

One strategy is email spoofing, which entails creating a fake email header. This suggests that the message appears to have originated from a source that is not genuine or authentic. These tactics are usually used in phishing or spam campaigns since people are more inclined to read a text or electronic message if they think it comes from a trustworthy source. -

Sending unsolicited emails, sometimes referred to as garbage emails, is a practice known as spamming. Most people who use email today have to cope with spam, which became more common in the mid-1990s. The receivers' email addresses are retrieved by spam bots, which are automated programs that look up email addresses online. The spammers create email distribution lists using spam bots. In the hopes of receiving a few responses, a spammer typically transmits an email to thousands of email accounts.

The harm done to an individual's image in the view of other people through the internet is known as cyber defamation. Most people who use email today have to cope with spam, which became more common in the mid-1990s. The receivers' email addresses are retrieved by spam bots; these are automated programs used to look up email addresses online. The spammers create email distribution lists using spam bots. In the hopes of receiving a few responses, a spammer typically transmits an email to thousands of email accounts. To harm the person's reputation is the aim of a defamatory statement.

Internet Relay Chat, or IRC, is a phenomenon where individuals from around the globe congregate on one platform, commonly called a room, and engage in communication with each other. Essentially, it is used for gatherings by cybercriminals. It is used by hackers to discuss their techniques. To lure small children, predators utilize it. Blackmailing someone for ransom, vowing to publish the victim's nude pictures or videos publicly if they don't pay, and utilizing chat to win their trust before participating in sexual harassment are some of the variables that lead to IRC crime. Some individuals, referred to as pedophiles, torture youngsters for their own benefit. Selling lottery tickets and fake jobs is one way that some people utilize IRC to generate income.

Phishing is a kind of fraud or crime when the attacker uses email or other communication methods to seem to be a reliable individual or organization in an effort to get information, including account details or login passwords. Additional examples include credit card fraud, malicious code, trafficking, distribution, uploading, hacking, indecent exposure, net extortion, and other types of cybercrimes against individuals. An individual is hardly at a higher danger of harm through such a malefaction.

a) Cybercrimes against property: Cybercrimes against property include computer vandalism, intellectual property violations (which include items such as "copyright, patents, and trademarks"), property crimes, and online threats. Intellectual property-related crimes include: Unauthorized software copying is known as software piracy.

Copy Infringement: The breach of an individual's or an entity's copyright can be referred to as copyright infringement. The unapproved use of copyrighted content, such as software, music, books, and so on, is another definition of piracy. Trademark infringement is the use of a trademark or service mark without permission.

b) Cybercrimes committed against organizations: It includes the following types of crimes: unauthorized deletion or modification of data. the unauthorized reading or duplication of private content without any alterations or removals.

DoS attack: This kind of attack involves the attacker overloading the victim's resources, which prevents or makes it difficult for users to access the networks, servers, or systems.

Email bombing: This type of online abuse involves sending a lot of emails to a certain mailbox in an effort to flood the server that hosts the email address or overwhelm the mailbox.

Salami attack: Another name given to the salami attack is salami slicing. An online database is used by the hackers in this attack to gather client data, including bank account details and credit card numbers. The attacker gradually takes small amounts out of each account. In this attack, no complaint is made because the customers are unaware of the slicing, and the hackers evade detection. Trojan horses, logic bombs, and data diddling are additional cybercrimes directed at corporations.

c) Attacks by cybercriminals on society

This category of criminal activity includes

Forgery: Forgery is the process of creating a fake document, signature, currency, revenue stamp, etc.

Web jacking: Web jacking gets its name from hijacking. When a victim clicks on a link on the con artist's fake website, a fresh page with an announcement telling readers to proceed by clicking on another link appears. If the victim taps on the link that looks authentic, he will be directed to a fake page. The goal of these types of attacks is to take over or obtain access to another person's website. The attacker may also change the content of the victim's webpage.

Cyberspace safety

While making use of the internet, keep the following points in mind

- Whenever feasible, use a strong password and confirm that two-step authentication is enabled in webmail.
- It is essential to make sure your webmail and social media accounts are secure.
- Strong password rules: The password should contain at least eight characters. One or more capital, lowercase, numeric, and symbolic characters must be used. Modify

the character that is similar. For example, we can substitute I for lowercase l, 0 for O, and so on. An example of a strong password HelL0 (%there %); A common mistake to avoid when making a password is employing a simple one that is straightforward to figure out.

- The password Personal data ought not to be employed as a password, and repeated characters should be avoided. As an example, aaaacc.
- Employing the same password on multiple websites is not recommended.
- Make use of two-step verification. A verification code is sent to the registered contact number along with your username and password as part of this additional security feature. Without the temporary and unique verification code, a hacker should not be allowed to access your account, even if they are able to get past your password. Always keep your password confidential.
- Never send or exchange sensitive information, such as a password, bank account number, or ATM pin, via an unencrypted channel, including email. Websites without the https mark and the https protocol are considered unencrypted. Websites that do not have the https sign as well as a lock icon in the web address bar of the browser are considered unencrypted. The website's security is indicated by the character "s," which stands for secure.
- Avoid creating an account on any social networking website even though you are old enough. Don't forget to update the operating system.
- Installing and updating firewall, antivirus, and anti-spyware software on a computer is a good idea.
- Steer clear of unreliable websites and don't click on links from unfamiliar or unreliable websites.
- Don't respond to spam.
- Before storing critical data on the cloud, make sure it is encrypted.
- Stay away from pop-ups: Sometimes pop-ups include malicious software. Accepting or clicking on the popups causes a background download of malware or other dangerous applications. We call this a "drive-by download." Pop-ups offering online polls on e-commerce websites or equivalent products should be disregarded since they may be infected with harmful viruses.

Conclusion

The emergence of new technology has led to an increase in cybercrimes in recent years. Cybercrime has become a major threat to humankind. Cybercrime prevention is crucial for a country's social, cultural, and security elements. The Indian government enacted the “IT Act in 2000” to address cybercrimes. “The Indian Penal Code of 1860, the Banker's Books Evidence Act of 1891, the Indian Evidence Act of 1872, and the Reserve Bank of India Act of 1934” are also amended by the Act. Cybercrimes can originate online and cross national boundaries anywhere in the world, making it challenging to conduct legal and technical investigations and prosecutions. Global harmonization initiatives, coordination, and collaboration amongst many jurisdictions are required to tackle cybercrimes. The public's education on cybercrime is the main objective of this paper. To sum up this essay, "A Brief Study on Cyber Crime and Cyber Laws of India," we would like to say that cybercrimes will never be tolerated. If you have been one of the victims of a cyberattack, please come forward and report it to the nearest police station. Offenders will never stop if they are not held responsible for their acts.

References

1. Pal P. Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India. ResearchGate. Jan 8, 2022. Available from: https://www.researchgate.net/publication/337818340_Cyber_Crime_An_Analytical_Study_of_Cyber_Crime_Cases_at_the_Most_Vulnerable_States_and_Cities_in_India
2. Shrivastava S. A study of Emerging Issues of Cyber Law. CALR. Jan 8, 2022. Available from: https://calr.in/a-study-of-emerging-issues-of-cyber-law/
3. Das S, Nayak T. Impact of Cyber Crime: Issues and challenges. Int J Eng Sci Environ Technol. 2013;6(2):142-153. Available from: https://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf
4. Dewanjee R, Vyas R. Cyber Crime: Critical View. Int J Sci Res. 2016;5(1):85-87. Available from: https://www.ijsr.net/get_abstract.php?paper_id=NOV152579
5. Singh P, Kaur K. Role of Social Networking Sites as a Component in Modern Social Structure: A Study on College Students. Int J Educ Manag Stud. 2020;10(4):447.
6. Vumetric Cyber Portal. Missing encryption of sensitive data vulnerability in WokkaLokka Wokka Watch Q50 firmware. Available from: https://cyber.vumetric.com/vulns/CVE-2021-44480/missing-encryption-of-sensitivedata-vulnerability-in-wokkalokka-wokka-watch-q50-firmware/
7. Amo T. How to Sell a Car to a Private Party Through an Installment Plan. The Nest. Jan 7, 2022. Available from: https://budgeting.thenest.com/sell-car-private-party-through-installment-plan-24980.html
8. My First Property. Sticking to Budget at Auction. Available from: https://www.myfirstproperty.co.uk/firsthome/sticking-budget-at-auction
9. Paul R. Cybercrime more profitable than illicit drug sales? Ars Technica. Jan 8, 2022. Available from: https://arstechnica.com/uncategorized/2005/11/5648-2/
10. Kori A. Critical Analysis of Cyber Laws in India. iPleaders. Jan 8, 2022. Available from: https://blog.ipleaders.in/cyber-laws-in-india/