INDIA'S CYBERCRIMES: A SYSTEMATIC EVALUATION

Yogiraj Sadaphal, B.A. LL.B., Bharati Vidyapeeth New Law College, Pune

INTRODUCTION

As a result of technological advancements, today man is completely dependent on the internet for all of his requirements. The internet has a power to allowed man to have everything while seated in one location, such as social networking, online purchasing, online education, and online employment, among other things.

Cybercrime, which includes everything from electronic theft to denial-of-service attacks, is a broad term used to describe criminal activities in which computers or computer networks are a tool, a target, or a location. Cybercrime is distinct from other types of crime that take place in society. The reason is because it has no geographical limits and that no one knows who the cybercriminals are.

HOW CYBERCRIMES OPERATES:

Anywhere there is digital data, opportunity, or motive, cybercrime may begin. Cybercriminals exist in a wide variety of forms, from a single user who engages in cyberbullying to state-sponsored assault. Cybercrime is, in many ways, a scattered phenomenon; it does not occur on its own. Cybercriminals use a number of attack pathways to execute their cyberattacks, and they are constantly searching for new strategies to accomplish their goals without being discovered or caught. Cybercriminals usually employ malware and other sorts of software, but ethical hacking is generally a crucial step in the performance of the majority of cybercrimes.

DIFFERENT TYPES OF CYBERCRIMES:

1. IDENTITY FRAUD

When a fraudulent person gains access to a user's personal information, hackers have the ability to commit fraud with regard to taxes or health insurance, extract money, or acquire classified information. Additionally, they can set up a phone or internet account, plan illegal acts, and submit applications for government assistance in your name using the person's name. They

might accomplish this by intercepting user passwords, obtaining user data from various sources, or disseminating phishing emails.

2. PHISHING

In these types of attacks where the hackers send victims emails with malicious attachments or Links in an attempt to penetrate their accounts or computers. As krte h

hackers are becoming more organized, many of these communications are not classified as malware. Users are tricked into opening links in emails that claim they must update their payment information or change their password, giving fraudsters access to their accounts.

3. SOCIETAL ENGINEERING

Criminals utilise societal engineering to get in touch with you directly, typically through phone or email. Typically, they take on the role of a customer care representative to win your confidence and get the data they need. This data may contain your bank account number, employer name, and passwords. Before attempting to add you as a friend on social media networks, cybercriminals will research you as much as they can online. Once they get access to your account, they can start new accounts in your name or invade your privacy.

4. CYBERSTALKING

Cyberstalking is the practise of being followed by criminals on personal social media profiles in order to get your confidential details and exploit it to their advantage. They have a variety of methods for gathering your information. They might be able to do this by intercepting user passwords, obtaining personal information through social media, or disseminating phishing emails or by any other way. This form of behaviour includes, but is not limited to, threats, defamation, slander, sexual harassment, and other attempts to intimidate, control, or otherwise harm the victim.

5. BOTNETS

Networks of compromised computers that are controlled remotely by hackers are known as botnets. Then, remote hackers utilise these botnets to send spam or attack other computers. Additionally, botnets may be employed for malicious purposes and as spyware.

6. OBJECTIONAL MATERIAL

Cybercriminals transmit inappropriate and extremely distressing information in this kind of cybercrime. Here, objectionable and upsetting material isn't only restricted to sexually explicit content; it also includes violent videos, illegal videos, and clips about terrorism. Both the regular networking and the dark web, an anonymous network, contain this kind of information.

7. DEFAMATION

By hacking into someone's email account and sending offensive emails to other people's accounts, one is attempting to diminish the dignity of the victim is known as defamation of the victim.

8. ONLINE TIME STEALING

In essence, hacking includes time stealing on the Internet. It involves the unlawful use of Internet time that has been paid by another individual. Anyone who obtains another person's ISP user ID and password, whether through hacking or other illicit means, uses them to access the Internet without that person's knowledge. If, despite little usage, your Internet time needs to be recharged frequently, that is a sign of time stealing.

INDIAN LEGISLATION GOVERNING ONLINE CRIMINALITY

Cybercrime is punishable by a number of statutes and rules that have been passed by various authorities. Numerous cybercrimes are punishable under the Indian Penal Code of 1860 (IPC) and the Information Technology Act of 2000 (IT Act), therefore it is not unexpected that many of their provisions overlap. A number of modern offences that have developed as a result of computer exploitation are addressed under the Information Technology Act of 2000. The IT Act immediately revised the Indian Penal Code of 1860, the Bankers' Books Evidence Act of 1891, the Indian Evidence Act of 1872, and the Reserve Bank of India Act of 1934. The Sections under the Acts were amended in order to bring them into compliance with modern technology. These changes aimed to tame down all electronic transactions/communications by ensuring strict official status, bringing them under the scrutiny.

Cybercrime under IT Act

• Sec. 65 - Tampering with Coumpter Documents.

• Sec. 66 - Hacking Computer System, Data alterations.

• Sec. 67 - Publishing Objectionable Information.

• Sec. 70 - Unauthorized access to other's system.

• Sec. 72 - Breaching of Privacy and Confidentiality.

• Sec. 73 - Publishing false digital signature certificates.

Cybercrimes under IPC

• Sec. 503 - use email to communicate threatening messages.

• Sec. 499 - Defamation through email.

• Sec. 463 - Falsification of digital records.

• Sec. 420 - False websites and online scams.

• Sec. 463 - Spamming emails.

• Sec. 383 - Web-Jacking.

• Sec. 500 - Email Violence.

Cyber Crimes under the Special Acts

• Drugs sold online in violation of Narcotic Drugs and Psychotropic Substances Act.

• Online sale of Arms in violation of Arms Prohibition Act.

LANDMARK JUDGMENTS

a) Yahoo v. Akash Arora

This incident was among the first instances of cybercrime in India. A permanent injunction was requested by plaintiff in this case because the defendant, Akash Arora, was charged of using the domain name "yahooindia.com."

b) Vinod Kaushik and others v. Madhvika Joshi and others

In this case, the court determined that it is unlawful to obtain the email accounts of the husband and the father-in-law outside their permission in accordance with Section 43 of the IT Act, 2000.

c) Shreya Singhal v. UOI

The two women were detained in accordance with Section 66A of the IT Act on suspicion of posting offensive remarks on Facebook regarding Mumbai's total closure following the death of a political figure.

Three concepts—discussion, advocacy, and incitement, were covered by the court as it announced its ruling. The court held that section 66A is unclear and it also violates the right to free speech and expression and also includes innocent speech in its purview. It amended the IT Act, 2000 to eliminate an arbitrary clause and supported Indian citizens' fundamental right to free speech. It was of the concluded that even after section 66A is repealed, provisions of Indian Penal Code, 1860 will still be applicable, forbidding communication that is racist, insults a woman's modesty, promotes hostility, uses abusive language, intimidates criminals, is racist, etc.

d) Shamsher Singh Verma v. State of Haryana 2015 SCC OnLine SC 1242

After having his request to display the Compact Disc submitted to the court for defence and to have it proven by the Forensic Science Laboratory rejected by the HC, the accused filed an appeal before the SC.

The Supreme Court reached the decision that, in accordance with Section 294 (1) of the CrPC, a document does not have to be personally admitted or denied by the accused, complainant, or witness in order for it to be accepted.

STEPS TO PREVENT CYBERCRIMES

- Use Strong and Unique Passwords:

Create complex passwords with a combination of letters, numbers, and symbols. Avoid using easily guessable information like names or birthdates. Use a different password for each online account.

- Enable Two-Factor Authentication (2FA):

Enable 2FA whenever available. This adds an extra layer of security by requiring a second form of verification, such as a code sent to your mobile device, in addition to your password.

- Keep Software Updated:

Regularly update your operating system, antivirus software, web browsers, and other applications. Updates often include security patches that fix vulnerabilities that could be exploited by cybercriminals.

- Install Reliable Security Software:

Use reputable antivirus and anti-malware software on all your devices. Keep them up to date and perform regular scans to detect and remove any malicious software.

- Secure Your Wi-Fi Network:

Change the default password on your home Wi-Fi router. Use WPA2 or WPA3 encryption and a strong password to protect your network from unauthorized access.

- Be Mindful of Social Media Usage:

Be cautious about the personal information you share on social media platforms. Adjust privacy settings to limit who can see your posts, and be cautious of friend requests or messages from unknown individuals.

- Educate Yourself:

Stay informed about the latest cyber threats, scams, and security best practices. Learn to identify warning signs of phishing attempts and other malicious activities.

- Be Skeptical:

Be cautious of unsolicited communications, requests for personal information, or offers that seem too good to be true. Verify the authenticity of such requests independently before taking any action.

CONCLUSION

As a result of the advent of digital technology, cyberspace now encompasses the entire globe. As a result, cybercrime is on the rise everywhere, even in India. The biggest problem with cybercrime is that it is constantly changing due to the continuing development of digital technologies. As a result, new cybercrime strategies and tactics are used. Because of this,

cybercrime should be treated with the same seriousness as other crimes that take place in our society, such as theft, rape, and murder.