Gurukul International Multidisciplinary Research Journal (GIMRJ)*with*
International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0027

e-ISSN No. 2394-8426
Special Issue on
Cyber Crime and Social Media
Issue–III(II), Volume–XIII

Cybercrime grows rapidly in new form and its Important Cluses

Dr.Nandkishor S. Bhagat
Assistant Professor and HOD, Criminology and Correctional Administration,
Athawale College of Social Work, Bhandara.
Email: drnandkishorbhagat1973@gmail.com,
Mob. No.: 9922585982

Abstract:

Cybercrime is on the rise due to advanced technology which has raised many eyebrows. Cyber Guna can be defined as follows. When someone interferes with electronic devices, internet, technology and personal information and takes financial advantage of himself and damages the person's physical and mental income and reputation, then it is a cyber crime. E.g. Phishing, Vishing, Smishing, Hacking, Cyber Bullying, Stalking etc.

In 1995, Nokia company launched its first phone 'Nokia-2110'. The first internet call in India was made on July 31, 1995 by the then Chief Minister of West Bengal Shri JyotiBasu from Kolkata to the then Union Telecom Minister Shri Sukhram. The call was connected from Reuters Building in Calcutta to Sanchar Bhawan in Delhi. Later, with the availability of Blackberry and later Apple and Android smartphones in the early 2000s, people shifted from basic handsets to smartphones. Since the year 2010, a mini computer has appeared in the pocket of consumers. In the year 2012, Airtel was the first company to offer 4G network services in India. In the year 1998, there were only 8 lakh mobile phone customers in India, the number has increased to over 120 crores, the reason being that in the year 2016, Jio company's mobile and SIM card became easily available in the market. Jio company launched low cost mobile calls and fast data services and now in the year 2022 Airtel company has launched 5G service. In all these developments, the need for smart phones increased a lot. Basic human needs like food, clothing, shelter, health, education have all come down to the smartphone in the form of technology.

Key Words: Cyber Crime, Technology, Phishing, Vishing, Smishing, Hacking, Cyber Bullying, Stalking

Introduction :

The use of internet and social media has increased due to the easy availability of smartphones to the people, while the positive use of the internet along with the misuse of the common man's life system of the nation has started to shake. Android phones require an email to start. E-mail is a social media tool. We see that every day spam mails are sent to our emails, unnecessary call messages are sent to mobile phones, password ID hacking, viruses, malware, trojans, email frauds, threats, ransom demands are going on. Cybercrime is said to have started from this district of Jharkhand in the triangle of Jamtada, Dhanbad, Kolkata, Patna, Rachi about eight to ten years ago. Sitaram Mandal and his brothers invented online fraud techniques and further expanded their cyber crime network. Jamtada is a land surrounded by jungle, rivers, swamps and small hills. 80 percent of the total cyber crime in the country is operated from this area. Cybercriminals, whatever their crime modus operandi, divert money from a person's account in the following Five ways:

1. By receiving the OTP
2. By forcing a link to be clicked
3. By receiving card details
4. By forcing money into a bank account
5. Digital House Arrest

Some types of cyber crime include:

Phishing

A type of fraud that involves sending emails that appear to be from a legitimate source to steal personal information. The emails may include links that direct the user to a fake website where they are asked to update their personal information.

Identity theft

Hackers steal personal data from a victim to impersonate them and profit financially.

Malware attacks

Harmful software is installed on computers to take control of systems, steal data, or use ransomware to encrypt data.

Denial of service

An internet server is flooded with bogus requests to deny legitimate users from using the server or to crash it.

Cyberbullying

The use of electronic means or modes such as social media to intimidate, harass, defame, or otherwise mentally degrade someone.

Cyberstalking

A type of online harassment where the victim is bombarded with online messages and emails.

Trade secrets

The theft of data and trade secrets from internet organizations.

Other types of cyber crime include:

1. Software piracy
2. Social media frauds
3. Online drug trafficking
4. Electronic money laundering
5. Cyber extortion
6. Intellectual- property infringements

Digital House Arrest

"Digital House Arrest" is a type of cyber crime in India. In this scam, cybercriminals pose as law enforcement officials to force victims to stay at home and transfer money to them.

Here's how the scam works:

Contact

Scammers contact victims by phone and then switch to video calls on platforms like WhatsApp or Skype. They may impersonate police officers, CBI agents, customs officials, or other law enforcement officials.

Threaten

Scammers threaten victims with a digital arrest warrant and claim that they are under investigation for a serious criminal offense.

Intimidate

Scammers may create a fake police station setup to convince victims that the call is legitimate. They may also use AI-generated voice or video calls to create a sense of urgency.

Exploit

Scammers coerce victims into transferring money to their accounts to avoid legal action or arrest. They may claim that the money is for "clearing their name", "assisting with the investigation", or "refundable security deposit/escrow account".

To avoid becoming a victim of this scam, you can:

Be suspicious of calls from fake officials claiming that you are in trouble.

Remember that genuine law enforcement agencies do not ask for money to avoid legal action.

Official communication from police or CBI is unlikely to occur via unplanned video calls.

According to the National Crime Records Bureau, in India in 2017, over 21,000 cyber crimes were reported under the state. In 2018, over 25,000 were recorded. In 2019, over 44,000 were registered. In the year 2020, this number reached over 50,000. In the year 2022, there is an increase in cyber crime by eleven percent over the previous year. Looking at this record, cyber security has become a matter of concern. 60 percent of people in India say the internet is becoming more insecure day by day. So it is necessary to take measures on it. It has become a global problem in modern times. Most importantly, people from all walks of life seem to be victims of such crimes. A large number of young women, senior citizens, business entrepreneurs, employed class, labor class and farmers are also affected. In cybercrime, especially educated people become the victims, perhaps this is the misunderstanding of educated people that their cyber fraud can never happen. But overconfidence is what leads to cybercrime. Emotions also play an important role in cybercrime. Because any cyber crime whether it is financial fraud or social media related chatting, cybercriminals make the victim feel greedy, sad, anxious, worried and then the victim is under the influence of that feeling and is not alert and then he becomes a victim. To fall victim means to suffer loss Loss is defined in Section 44 of the Indian Penal Code. There are five types of damage, physical, mental, economic, income and reputation. A large number of women are victims of social media cybercrime. Cyber crimes like blackmailing and sexual exploitation are seen taking an extreme role like female suicide. It was decided to make strict laws to deal with all these types of cybercrime incidents. And this is why the ITI Act 2000 came into being. Cyber laws are something everyone who uses the internet should know. Internet is like life, interesting but also annoying. With the boom in technology and easy internet access across the country, cybercrime has become commonplace.The Government of India has enacted the Information Technology Act 2000 to regulate such activities that violate the rights of internet users. In this the following important clauses are seen being used in the police department.

Section 65 :- Tampering with computer source documents.

Section 66 :- Computer offences

Section 66A :- Punishment for sending offensive message through communication service

Section 66B :- Punishment for receiving stolen computer source or suppression device and dishonestly
Section 66C :- Stealing and using identity of another person
Section 66d :-:Cheating using computer resources
Section 66 etc :- Punishment for breach of privacy
66 F :- Punishment for cyber terrorism
Section 67 :- Transmission of obscene material in electronic form
Section 67A :- Publication of sexually explicit material in electronic form
Section 67B :- Punishment for publishing sexually explicit material of children in electronic form

It is necessary to pay attention to many aspects like users, beneficiaries of new technology and most importantly safeguarding the security of the country. After the implementation of the Information Technology Act-2000, many of its errors came to light. It was amended in 2008 to introduce the controversial Article 66(a). Therefore, the issue of privacy protection arose. The court struck down the clause as violative of Article 19(1)(a) of the Constitution. However, while upholding Section 69(A) of the same Act, the court had mentioned that the sovereignty and security of the country are also important along with individual freedom. However, the law's limitations in terms of curbing cyber security challengers, as well as preventing breaches of privacy, are also becoming apparent. Some highlights about "Information and Technology Act 2008" – Drafting of this bill started in 1998. It was first introduced in the Parliament on 16th December 1999. It was approved by the President in August 2000. The Act came into force on 17th October 2000. In 2005, the original draft law underwent important amendments over time. For this, a committee was constituted under the chairmanship of Information and Technology Secretary Brijesh Kumar. In August, 2008, this committee submitted the study report to the Ministry of Information and Technology.

2008 after approval by the Parliament, the amended Act was assented to by the President on 05/02/2009.

Thereafter the amended "Information and Technology Act 2008" came into effect in real terms from 27/10/2009.

The Act "Information and Technology Act 2008" has a total of 13 chapters and includes a total of 90 sections. Due to the inclusion of earlier 4 Acts, the total number has become 94. According to this Act, the analysis of cyber crime and punishment is mentioned in Sections 65 to 78.

Reference Bibliography:

1)https://www.esakal.com/sampadakiya/editorial-articles/editorial-article-writes-it-law-20-pjp78
2)https://maharashtratimes.com/editorial/cyber-law/articleshow/48397140.cms
3)https://mumbaipolice.gov.in/Specialunitsinfo?specialunits_category=2
4) Indian Social Acts, Edited Book, Sai Jyoti Publication, Nagpur, July, 2022, Page No. 253-256