Cyber Fraud and Abuse: An Analysis

Dr. Amit Dipakbhai Mehta
Assistant Professor
Law College Godhra

Abstract:
India's ambition is to convert its society into an information society by implementing 'Digital India'. Government, private sector, and even the entire individual depends on the internet for any transactions, services, and to store informational data. And here in this research only, we as victims can't do anything except be trapped and make our loss only.

Cyber fraud and abuse were first time dealt as an issue by the SC in the landmark case of Vishaka v/s the state of Rajasthan. In this case dealt with the issue to protect women from sexual harassment.

Cybercrime is a serious offence just because it is virtual doesn't make it any less real. Cyber fraud is the most common and dangerous form of fraud that takes places everywhere. The cyber-world has been growing and growing throughout the twenty-first century.

Fraudsters can use the information which they gather to then financially fund a crime that is committed mostly in the cyber world and is expanding its roots in almost every aspect of life. The information technology act 2000 covers all these types of crime.

Keywords: *'Digital India', Cyber fraud, Cyber crime*

1. Under Cybercrime and fraud, six acts are prohibited namely
Obtaining, or looking to get, national security data with the aim to utilize it to harm the United States or to unjustifiably advantage any remote nation. Intentioned, getting to, coming about within the obtaining of data contained within the records of a budgetary institution, credit card guarantor, or consumer-reporting agency.

Intentionally getting to a government intrigued computer and anticipating authorized utilization of any data or computer administrations when the misfortune sums to more than $1,000 in a one-year period or includes therapeutic treatment. Be that as it may, the concept of "loss" was not restricted to real money related misfortunes. For case, financial specialists may lose on a stock if the stock projections have been modified to create them show up more alluring. This area moreover incorporates other get to, such as programmers of restorative information.

- Trafficking in passwords.
- Intentionally changing, harming, or wrecking certain computerized data having a place to another.
- Knowingly accessing, without authorization, a federal interest computer resulting in the obtaining of anything of value beyond the mere use of the computer with intent to defraud.

2. How Serious is Cyber Fraud and why is Cyber Fraud?
The cyber-world is expanding. Within the advanced age, we store more individual information like monetary data and versatile phone numbers online than ever recently as a result of which cyber extortion and manhandling is on the rise. Cyber Extortion can be characterized as any false movement conducted over the Web, as each fraudster can get to people's individual data over the web, e.g. their

bank account numbers, online exchanges, and after that they utilize that cash for their own use or for subsidizing fear monger exercises.

When there are a parcel of managing account offices and numerous dependents, at that point a few people will unquestionably take advantage of the portable app, which will open up more possibilities than ever for cybercriminals. There's no question that usually an awfully genuine wrongdoing ought to be managed with force.

3. Classification of Cyber Fraud

3.1 Cybercrimes against individuals

- Email spoofing is a form of cyber attack in which a hacker sends an email that has been manipulated to seem as if it originated from a trusted source. For example- a spoofed email may pretend to be a well-known shopping website, asking the recipient to provide sensitive data, such as a password or credit card number.
- Spamming is the use of electronic messaging systems like emails and other digital delivery systems and broadcast media to send unwanted bulk messages indiscriminately. Cyber defamation is that which provides harm to the reputation of an individual in the eye of another individual through cyberspace.

3.2 Cybercrimes against property

- Unauthorized Computer Trespassing is a sort of computer crime that involves gaining unauthorized access to computers in the United States. It's classified as computer fraud and abuse.
- Copyright infringement occurs when a work protected by copyright law is used for a purpose for which authorization is not necessary.
- Taking confidential data and information from someone's online sources without their knowledge.
- Some online crimes occur against property such as the internet or server.

3.3 Cybercrimes against the government

- Cyber extortion is the act of cyber-criminals extorting money from a victim by threatening them with destructive activities.
- Cyber terrorism is the use of the internet to carry out violent activities that result in the death or serious physical injury of people in order to gain political advantage through threats.

4. How Do We Get Trapped into Cyber Fraud?

The only thing that can stop a bad guy on the internet is a good guy on the internet.' It has now grown so widespread that even the government's highly secure website has been hacked. The most typical way of hacking is for the hacker to send a link to the victim's email or social media account, and when the victim clicks or opens the link, the hackers get access to the victim's computer systems. We've also seen occasions when we've received scam emails claiming that we've won a reward and, in exchange, they've asked for our bank account information.

This is where many individuals, including the educated, fall into the trap. The preceding examples were all commonplace and something that anyone could perform. However, cybercrime has also produced some extremely famous cybercriminals, also known as cybercrime celebrities.

He was a programmer who dropped out of school just like Mark Zuckerburg and Bill Gates but chose to use his skills to contribute to the opioid epidemic Paul le Roux, a well-known criminal, is linked to cybercrime because he exploited his advanced programming talents in drug and arms dealing.cs in the U.S.A by supplying the drug to the common citizens of the U.S.A.

5. Cyber Abuse

The term "cyber bullying" refers to a wide spectrum of online abuse, including harassment, reputation attacks, and revenge pornography. Cyber bullying or harassment is a type of bullying or harassment that takes place through the internet. As the digital environment has expanded and technology has evolved, it has grown more widespread, particularly among teenagers.

- It is a pattern of behaviour intended to frighten, anger, or shame individuals who are being targeted.
- Rumours about someone publishing embarrassing images of themselves on social media, for example.
- Threatening others for selfish gain, as well as sending hurtful comments on their behalf.

Face-to-face bullying and cyber bullying can often happen alongside each other. But cyber bullying leaves a digital footprint. The informational technology amendment Act also provides remedies for cyber bullying. Section 66 A of the IT Act defines punishment to a person who sends offensive things by using internet tools for communication.

6. Present Scenario

66E defines punishment for invading privacy. Section 67 defines punishment for publishing any obscene picture.

Presently, there is a huge increase in cyber abuse and cyber bullying cases. But no. Of cases are reported less because many of the people didn't tell anyone about getting bullied. According to child rights and You 1 in 3 adults get bullied every day and most of their age is between 13-18 years.

7. The shocking statistics on cybercrime's impact on our society to date

- The global cost of cybercrime will reach $6 trillion by 2021.
- 48% of data security breaches are caused by acts of malicious intent.
- Cybercrime will more than triple the number of unfilled cyber security jobs by 2021.

Some of the famous case Studies

Ritika Sharma Case

Ritika Sharma who was a student in a reputed Delhi school was stalked by a Facebook friend whom She unfriended months ago and whom she gave all her information including residential address, school address, and even cell phone no. She told her brother regarding this and her brother filed a complaint against this. After this incident, Delhi police organized awareness programs where all the students were told not to send any personal data to strangers.

8. Ritu Kohli's Case

This is the case that should be mentioned while discussing cyber bullying and cyber abuse. This was India's first reported case of cyber stalking. In 2001, a girl called Ritu Kohli filed a complaint alleging that someone else was using her identity on social internet and that she was receiving calls from several numbers, including calls from abroad. A case was also filed under Indian penal code Section 509. As a result, we can conclude that cyber legislation is an essential tool in the fight against cyber-attack.

9. How to Tackle the Situation of Cyber Fraud and Abuse?

Resist the urge to respond as people who say hurtful things often do so just to get a reaction.

Save evidence as our immediate reaction might be to make the abusive content disappear but it is important to keep evidence of that.

- Report and block options should be used.
- Check out tailored advice
- Seek help for legal advice or we have to go for legal help.

- Save your data
- Protect your e-identity

10. Laws Governing Cyber Crimes

The United Nations Commission on International Trade Law adopted the Model Law on Electronic Commerce.. As a signatory, India was required to alter existing legislation in accordance with the Model Law. The IT Act established some punishments and offences, and revisions were made to existing statutes such as the Indian penal code and the Indian Evidence Act, among others, to address offences classified as cybercrimes. The Computer Fraud and Abuse Act of 1988, Section 18,prohibits activity that harms computer systems. It's a piece of cyber-securitylegislation.

It protects them from trespassing, threats, property destruction, and corruption because cyber-crimes frequently target issues that are specified and discussed by the Information Technology Act, the act makes these crimes even more punishable. The Indian Penal Code is the country's primary legal framework for dealing with traditional offences. Because the scope of these crimes has broadened in recent years as a result of the technological revolution, a subset of them can readily be categorized as cyber-crimes.

11. As a result, cybercrime in India is largely dealt with under the following two legislation:

- Information Technology Act, 2000.
- Indian Penal Code, 1860.

Following the amendment of the Indian penal code, 1860 in 2013, there are some laws to rely on, including Section 499 of the IPC, which defines defamation, Section 292A, which defines printing matter intended to blackmail, Section 354A, Section 354D, and Section 509, which defines any word or act intended to insult a woman. As a result, cyber legislation has become necessary.

After politicians realised the importance and gravity of these crimes, they enacted the Information Technology Act of 2000, which has been amended several times. However, loopholes still exist, as seen by the growing number of cybercrime cases. **Shreya Singhal v. Union of India** is a well-known case.

The court held that every expression used is nebulous in meaning. 'What may be offensive to one may not be offensive to another. Hence the court held 66A as violative of rights to freedom of speech and expression and is not covered under the ground of reasonable restrictions given under Article 19(2). The court also determined that information blocking for public access under Section 69A of the IT Act is constitutionally permissible.

Mr. Tushar Mehta, an Additional Solicitor general from the defendant's side contended that any matter which is posted on the internet or made available to the citizens is certainly more. It's there. It is more broadly accessible than any other medium and, unlike other media, is not constrained by any particular boundary.ore becomes obvious that this requires more regulations. The growing crime rate is becoming difficult to tackle with the current law system.

12. Impact of Covid-19 on Cyber Fraud and Abuse

As a result of the covid-19 pandemic and the imposed lockdown, more people are confined at home and increasingly rely on the internet. 'The Covid- 19 pandemic has taken a very heavy toll on India's economy. Due to the pandemic reduces the risk of physical criminal activities, but now the cyber crimes are increasing rapidly. Cyber criminals are adapting their tactics and now are targeting people by their homes or by their working places.

They attempt to access corporate data, customer information and intellectual property are not only a threat to business. Authorities have also reported many increased cases during the pandemic of cyber crimes. Police officials of Maharashtra State have registered 400 cyber crimes cases against people who were using hate speech on the internet and give a different angle to the pandemic.COVID-19. On the other hand, it gives criminals greater opportunity to strike and mix in with regular web traffic.

Promises of false financial opportunities are another popular. This phenomenon has spread around the world, and both INTERPOL and the United Nations have issued warnings about specific online frauds like this one involving the COVID-19.One of the first corona virus phishing scams was identified by consultants. "Go through the accompanying document on safety measures surrounding the propagation of corona virus," the email, purportedly from a virologist, urged potential targets. This small step could save your life" (Newman 2020). "Scammers are taking advantage of worries around the corona virus," an FTC official said in early February.

They're creating false websites to offer phone products, and they're employing ruses like fake emails, messages, and social media postings to steal your money and personal information" (Tressler 2020). Comparing the first three months of 2019 to the first three months of 2020, while including a month when the coron avirus was not present.

13. Conclusion

Young people are drawn into a perilous zone by using the internet. Concerns have been raised about the need for a concerted effort to mitigate the negative consequences of young people accessing and using the Internet.

The print media has a responsibility to inform unsuspecting parents and children about the risks involved. when it comes to walking perilous territory in the cyber-world. Cyberspace Security Management has already been implemented. Military-related scientific research has become an important component of national security management. Security and intelligence management are managed all around the world. Intrusions in the future threats to our national security may not necessarily originate on the other side of the physical border.

References

1. https://bestpractice.bmj.com/topics/en-us/696
2. https://lawcirca.com/cybercrime-a-critical-analysis-of-judicial-decisions-in-india/
3. https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119205654.app3
4. https://www.legalserviceindia.com/legal/article-797-an-analysis-on-cyber-crime-in-india.html
5. https://www.researchgate.net/publication/228165485_Rape_by_Fraud_and_Rape_by_Coercion
6. https://www.unodc.org/e4j/zh/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html