A Quarterly insight to Cyber Law!

Cyber Niyam means rules of the Cyberspace. This quarterly newsletter aims to create awareness about the rules and regulations of cyberspace, cyber security and data protection. This is also an effort to create awareness about digital safety, trending cybercrimes and effective reporting mechanisms.

Disclaimer

This newsletter does not intend to advertise or solicit work and is for private circulation only. This newsletter is for the purpose of education and creating awareness on Cyber law and its latest developments. It does not intend to be comprehensive nor intends to provide any legal advice. Though every effort is made to share accurate, reliable and current information, Cyber Niyam is not responsible for any errors or omissions in information made available through this Newsletter. Sharing of this Newsletter does not intend to create attorney – client relationship between authors and reader.

CYBER NIYAM

By Adv. Vaishali Bhagwat *www.vaishalibhagwat.com*

Issue 1 – July, 2024

In this Issue

- CASE SPOTLIGHT – TRENDING CYBER FRAUDS
  Falling for the Trap: Inside FedEx Scam and Digital Arrest
- LEGAL LANDSCAPE
  Key Developments in Technology and Cyber Law
- LATEST HIGHLIGHT
  MEITY Advisory on Regulating AI
- Good to know
  What is Chakshu Portal?
- News Corner
  Maharashtra Cyber Saves Rs 222 Crores
- GLOSSARY OF TERMS –
  - Phishing
  - Smishing
  - Vishing
  - Social Engineering
  - Instant Messaging (IM) Attack

CASE SPOTLIGHT – TRENDING CYBER FRAUDS

Falling for the Trap: Inside the FedEx Scam and Digital Arrest

One normal afternoon you get a call regarding a FedEx parcel you had sent. Hey! but I haven't booked any parcel with any courier company but still out of curiosity you 'dial 1' for more information. A customer care representative informs you that there are drugs found in a parcel which you have booked along with some passports and Ids! Whoa…! before you realize there is a police officer on the line carrying out an interrogation! This is a very common scene of fraudsters impersonating reputed courier companies and police officers and then carrying out extortion.

The digital age has no doubt streamlined many aspects of our lives but it has also opened doors for criminals to exploit technology and manipulate emotions with devastating effectiveness. By creating a false sense of urgency and impersonating trusted entities, these scammers have successfully deceived many.

A typical scam scenario is that the victim is put under investigation by the "Narcotics Department, Mumbai". The call is then further transferred to a senior officer where the victim would be interrogated on a skype call / video call. The officer shows the ID's as evidence, to win the victim's trust and ask her to co-operate and follow all his instructions. After detailed discussion, he needs to track the victim's bank account for any illegal activities and ask the victim to screenshare the login details. The callers will keep threatening the victim. If the victim doesn't co-operate, they would act on the already filed FIR, for serious charges of drug activities and money laundering. This is how these fraudsters use fear to manipulate the victim and not let them think logically in the moment. Now, to lure the victim further, they assure that a certain amount will be credited to the victim's account to trap the people who are framing the victim, as a part of their investigation.

……Continued on page 2

The victim is further instructed to add beneficiaries and transfer money with a reassurance that the money that is transferred, would be reversed and that, victim would be getting a police clearance certificate.

By now you know, the investigation is staged, the police are fake and the money has vanished.

We have seen cases of victims who are men and women who have been kept under a threat by the fraudsters on a video call for 8 to 10 hours at a stretch. The victims had to beg for washroom breaks or to have food. This is the level of fear that is instilled in the victim. They are people like you and me! One is a scientist working at a very reputed central government organization, one is a counsellor and a healing practitioner, the other is a retired CFO! This scam is a great leveller, it doesn't differentiate between the educated and the illiterate, men from women, or the old from young… all fall prey!

The money has exchanged many hands sometimes have crossed borders making the recovery and the investigation very difficult. But if one acts swiftly there is chance that the money gets blocked in some account and there is a chance for recovery.

Filing a complaint of the national cybercrime portal www.cybercrime.gov.in, swiftly is very important as it automatically triggers tracing of the money and putting a debit freeze on the accounts. For the victims, the investigation was real. The fear was real. The anxiety and apprehension were real. The fear of being dragged in an investigation involving drugs, money laundering, child pornography, terrorism is intense and inexplicable.

Sometimes it is easy for us to judge these victims …the most very common response we hear when we narrate these cases are "How did they believe it? Why would someone transfer money?" We don't have answers. The victims too done have answers. They were just trying to prove their innocence.

YOU COULD BE THE NEXT ONE!

So, how to protect yourself against such scams? Here are some quick tips -

1. Avoid interacting with links sent via SMS, email, or WhatsApp
2. Directly check the status of any package on the official FedEx / courier website.
3. In case of any alleged police investigation, go to the nearest police station and offer to co-operate. Don't be afraid of threats of arrests. Don't fear police investigation and do not have the fear of being exploited by the Police
4. If a call raises suspicions, hang up immediately. Scammers use sophisticated psychological tactics to manipulate their targets. Confide immediately with a family member or a trusted friend / acquaintance**.**

Suspected fraud communication can be reported at https://sancharsaathi.gov.in/sfc/

If you have already lost money due to financial fraud or are a victim of cybercrime, please report at cybercrime helpline 1930 or website https://www.cybercrime.gov.in

……Continued on page 3

GOOD TO KNOW!

What is Chakshu Portal?

The Chakshu Portal is a platform to report suspicious communication like fraudulent calls, SMS or messages on social media. This platform is developed by Department of Telecommunication (DoT) to facilitate citizens to report suspected frauds. The portal aims to detect and prevent suspected fraud calls and messages.

Things you can Report on the Chakshu Portal

1. KYC related to banks, electricity, gas connections, insurance policies etc.
2. Impersonation as Government official/relative
3. Fake customer care helpline
4. People offering suspected online jobs, lottery, gifts, and loan offers
5. Sextortion
6. Multiple automated/ robotic communication
7. Messages containing malicious links/websites
8. Any other suspected fraud

LEGAL LANDSCAPE

Key Developments in Technology and Cyber Law

This article is in 4 parts and aims to create awareness on the laws applicable to cyberspace in India

What is cyberspace?

A dictionary meaning of cyberspace is - *a place that is not real, where electronic messages exist while they are being sent from one computer to another.*

"cyberspace" means the sphere of actions and conduct carried out using the interdependent network of information technology infrastructures that includes the internet, internet-related telecommunications networks, computer systems and internet connected devices. The prefix "cyber" is used to characterize actions which are carried out using such information technology infrastructures.

As our lives become increasingly digital, the need for a legal framework to govern cyberspace become imperative and hence the set of rules and regulation that govern the use of the internet, digital technology and electronic communication and aims to protect individuals, business and government from the risks and challenges posed by the digital world is known as cyber law.

Cyber Law is -

- Law that governs cyberspace
- Law that regulates use of computers and Internet
- Collection of Laws
- Civil and Criminal Law
- Procedural and Substantive Law

Legislative history of the development of Information Technology Act 2000:

- 1998 – Draft E-Commerce Act made available based on the UNCITRAL MODEL LAW on ecommerce
- 2000 – Information Technology Act enacted with amendments to Indian Penal Code IPC, Indian Evidence Act, Bankers Book Evidence Act. The object to promote ecommerce and e-governance, give legal recognition to electronic records and digital signatures and create civil and criminal liabilities for contraventions with the provisions of the Act
- 2005 – Amendments to IT Act Bill presented - in light of the Gurgaon Karah Bahree Case and E-bay case some amendments were proposed
- 2006 - Bill returned by standing committee for modifications. The standing committee rejected the proposed amendments under the chairmanship of Mr Nikhil Kumar
- 2008 -09 IT Act Amendment Bill re-tabled and received presidential assent on 5th February 2009. These amendments included
- Intermediary liability and due diligence
- Procedure and Safeguards for Interception, Monitoring and Decryption notified
- Procedure and Safeguards for Blocking for Access of Information by Public notified
- 2011 - Reasonable Security Practices and Procedures & Sensitive Personal Data Rules Notified; Guidelines for Cyber Cafes Rules Notified
- 2013 - National cyber security policy – This policy aims to create workforce of IT professionals to better protect India from cyber attacks
- 2015 - S 66A repealed; Supreme Court Judgment on the intermediary liability regime under Section 79 – requirement of a judicial order for removal of content to be directed specifically at the intermediary
- 2018 - Supreme Court Judgments on Section 65 B Certificate
- 2018 – Supreme Court Judgment on the Right to Privacy and Data privacy
- 2018 - Supreme Court Judgment on Content regulation by intermediaries on (violent content / child pornography)
- 2021 - Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (Due diligence)
- 2022 Amendment to the First Schedule of the Information Technology Act making digitization of DPNs, Powers-of-Attorney and Immovable Property Contracts legally valid
- 2023 - IT Amendment Rules, 2023, the due diligence requirements of intermediaries have been amended even further. (Challenged before the Supreme Court in the case of Kunal Kamra v Union of India)
- 2023 - The Digital Personal Data Protection Act

......Continued on page 4

NEWS CORNER

Maharashtra Cyber Saves Rs. 222 Crores

As per the report published by The Week magazine, The Maharashtra Cyber has managed to put on hold Rs. 222 crores between May 2021 to May 2024.

The 1930 helpline is to report cyber frauds/crimes, which has 23 functional lines and 110 persons working round the clock. There are additional 10 officials focusing specifically on follow up procedures as well as communicating with banks and law enforcement agencies to expedite complaint resolution. This was under the MH Dial 1930 Project for reporting Financial frauds.

Key Developments in Technology and Cyber Law, continued from Page number 3

A) Key components of the Information Technology Act 2000

- Electronics record to be treated at par with a document
- Amendment in the Evidence Act, Bankers Book Evidence Act, Indian Penal Code
- Legal recognition to Electronic signatures:

Properties of an electronic signature are –

- is unique to a document
- Fulfils all the three requirements of a physical signature of identity authentication, content authentication and non-repudiation,
- Technically impossible to forge

B) Offences under the IT Act

1. Unauthorised access
2. Unauthorised downloading, extracting any data, computer database or information
3. Introduces virus or a computer contaminant into any computer
4. Causing damage
5. Causing disruption
6. Causing denial of access
7. Provides assistance to facilitate access in contravention of the provisions of the Act.
8. Charges the services availed of by a person to the account of another person
9. Destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously
10. Steals, conceals, destroys, alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage

C) Crimes under the IT Act

1. Cyber Offences with mensrea
2. Source Code Theft
3. Receiving and retaining stolen computer resource
4. Identity theft – Phishing
5. Cheating by impersonation – Spoofing
6. Violation of privacy – captures, publishes or transmits image of a private area of a person
7. Publication and transmission of obscene material
8. Publication and transmission of material containing sexually explicit act
9. Child Pornography
10. Cyber Terrorism

……Continued on page 5

Supreme Court Judgment in the case of Shreya Singhal Vs Union of India repealing Section 66A

- The Supreme Court struck down Section 66A of the IT Act 2000, relating to restrictions on online speech, as unconstitutional on grounds of violating the freedom of speech guaranteed under Article 19(1)(a) of the Constitution.
- The Court further held that the Section was not saved by virtue of being a 'reasonable restriction' on the freedom of speech under Article 19(2).
- The Supreme Court also read down Section 79 and Rules under the Section. It held that online intermediaries would only be obligated to take down content on receiving an order from a court or government authority.
- The case is considered a watershed moment for online free speech in India

To be continued in next issue of Cyber Niyam….

LATEST HIGHLIGHT
MEITY Advisory on Regulating AI

MEITY Advisory on Regulating AI dated March 15, 2024 (revised)

Artificial Intelligence (AI) has emerged as a transformative technology with the potential to revolutionize various sectors, including healthcare, agriculture, education, and governance. Recognizing the immense potential and challenges associated with AI, the Ministry of Electronics and Information Technology (MeitY) in India has laid down comprehensive advisory guidelines to steer the development, deployment, and governance of AI in the country. These guidelines aim to promote ethical use, innovation, and inclusive growth through AI.

These guidelines applicable to intermediaries and platforms provide a comprehensive roadmap for harnessing the potential of AI to drive economic growth, improve public services, and enhance the quality of life for all citizens, casting certain compliance obligations on intermediaries and platforms that will develop, use and deploy AI in its products and services

Key areas covered under this advisory:

1. **Use of AI models / LLMs / Generative AIs / software(s) or algorithm(s) to be compliant with IT Rules and IT Act** – Intermediaries / platforms must ensure that use of AI models / LLMs / generative AI / software / algorithm does not permit its users to host, display, upload, modify, publish, transmit, store, update or share any unlawful content as outlined under Rule 3(1)(b) of the IT Rules or violate any other provision of the IT Act and other laws in force.

2. **Restrict any bias or discrimination** – The intermediaries or platforms are advised to ensure that their computer resource, including through use of AI models / LLMs / Generative AI / software / algorithm, do not permit any bias or discrimination, or threaten the integrity of the electoral process.

3. **Label AI models** – Intermediaries and platforms are advised to label the possible inherent fallibility or unreliability of the output generated from the AI models and implement a consent mechanism that explicitly informs users of the fact that the content is derived from an AI technology.

4. **Create user awareness by amending terms of service** – Intermediaries or platforms must inform users about the consequence of dealing with unlawful information on their platform, including disabling of access, or removal of content, or suspension or termination of user accounts, and punishment under law.

5. **Ensure labelling or embedding unique metadata / identifier for potential misinformation or deepfakes** – intermediaries operating in India will need to implement watermarking and/or labelling technology to identify the type of content that has been altered or synthetically created, either by tools available on their platform, or are otherwise uploaded by the users publishing or hosting content on their platforms.

GLOSSARY OF TERMS

Phishing

Phishing is an email fraud method where the perpetrator sends you a legitimate-looking email in an attempt to gather your personal and financial information. Typically, the messages appear to come from well-known and trustworthy web sites.

Smishing

Smishing is similar to email and IM attacks. Links are delivered to your mobile device via text messaging. In this case, malware is launched when you click on a hyperlink that then links you to a malicious website.

Vishing

The telephone version of phishing is vishing. In phone phishing, you may receive a message asking you to call a number. The purpose is to get your personal information, which could be used to access your account or open new credit cards in your name.

Social Engineering

This term describes a non-technical kind of intrusion that relies heavily on human interaction, and often may involve tricking you into breaking normal security procedures or divulging confidential information. The perpetrator may try to appeal to your vanity, authority level and/or greed.

Instant Messaging (IM) Attack

Similar to email attacks, links are delivered via instant messaging versus email. They work much like email attacks, where malware is launched when you click on a hyperlink that then links through to a malicious website. The malware can be spread through your IM chat sessions.

ABOUT THE AUTHORS

Adv Vaishali Bhagwat

Vaishali Bhagwat is a practicing lawyer with 25 years of experience in civil and cyber litigation and advisory practice in Pune and Mumbai.
Vaishali has a prior degree and work experience in the field of Computer Science, a Post graduation certification in Cyber Security and Information Assurance and is a certified Privacy Lead Assessor.

She is an advisor to several companies on Cyber law and privacy compliance and advisor to various educational institutions on Protection of children from sexual offences.

She has successfully conducted several prominent cases for corporate espionage and Data theft, Data Privacy, Digital Financial Frauds, Cyber-crimes against women and children, take down orders and IP infringement in cyberspace.

Vaishali is a *TCS Chevening Scholar on "Cyber Policy and Cyber Defense" and has earned the Post Graduate certification from Cranfield University UK. She is also a Disha Alumni which is a prestigious program of the British high Commission on Innovative Leadership chaired by UK PM David Cameron and PM Manmohan Singh.*

www.vaishalibhagwat.com

Mrudula Arjunwadkar

BSc., LLB, MPM

POSH Consultant
Helping organizations in end to end POSH Compliance, External member to IC, POSH trainings

Adv. Tanvi Pandey

LLB

Recent law graduate with keen interest in cyber law and criminal law Assisted in various cybercrime related matters

Adv. Shyamal Marathe

MSc. (Electronics Sc), LLB, Certified Marriage Counsellor

Engaged in training students of 11th, 12th 1st year engineering in Math and Physics subjects.
Head of Institute Centre for Excellence since last 10 years in Pune training students for IITJEE, IISER, CET entrance exams in Math and Physics and Electronics science

VAISHALI VB BHAGWAT
ADVOCATES