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.

CYBER NIYAM

By VP Shintre and Associates *www.vaishalibhagwat.com*

Issue 1 of 2025 – January, 2025

In this Issue

TRENDING CYBER FRAUDS

Digital Arrest – Decoding the Cyber Fraud!

"Digital Arrest" Scam wipes out life savings of a 90 year old"; "A woman made to strip, loses 1.7 lakh after digital arrest threat"; "A student loses Rs. 7.28 lakh in digital arrest scam" "Bengaluru Techie Loses Rs 11.8 Crore In Fake Money Laundering Case" …. The newspapers are full of such headlines related to "Digital Arrest". As per recent news reports, around 1,00,000 Indians have been affected by this scam. With the increasing number of victims and huge sums of money being extorted, in this article we intend to decode this scam to create awareness on the modus operandi of the scammers and how can we prevent ourselves from falling prey to a Digital Arrest scam!

What is Digital Arrest?

"Digital Arrest" refers to a type of cyber fraud where the scammers impersonate law enforcement officers or government representatives such as State Police, CBI, ED, Narcotics Bureau, etc and put the victims under the impression that they are being investigated as a part of a drug racket or money laundering scheme. They pressurize victims into paying large sums of money using psychological tactics and threats over audio/video calls.

Modus operandi –

Step 1 – – Scam begins with a sms, email or whats app message/an automated call where it says you are linked to some serious crime like drug trafficking, financial fraud, pornography etc. This sends the victim in a state of panic

……Continued on page 2

Step 2 – Scammers then ask the victim to call on another number which is a video call either on WhatsApp or Skype. On the other side are Government Officials, Police officers, who are not real, but impersonating them. These officials appear to be genuine as they are wearing uniforms and they are seated in an office like decorum with appropriate setup, which makes it believable for the victim. They may also fabricate evidence to make their accusation seem credible.

Step 3 – Fake officials accuse the victim and create a sense of panic, fear and urgency to address this issue. They threaten the victims to be on-camera 24/7 which is where they monitor each and every action of the affected person. Victims are kept under digital surveillance or 'digital arrest' and are compelled to follow their instructions as they are already in a panic mode.

Step 4 – Victims are put on a video call and under surveillance. They then use intimidation tactics like they will make the information public etc. and the only way to come out of it is to transfer some amount to the bank account as shared by the scammers. By this time the victim is so tormented that they fall for it.

Psychology behind falling for this scam -

One may fall for such scam because of multiple aspects like –

1. **Lack of information/knowledge –** Unfamiliarity with law enforcement procedures makes it difficult for people to differentiate between the legitimate and fake calls
2. **Fear and panic –** Fear or arrest puts the person in a panic situation where the affected person cannot think rationally.
3. **Social Stigma** – Fear of social stigma and impact on family motivates victim to follow the scammers and they think that there is a way to avoid embarrassment
4. **Isolation and Control –** Scammers isolate victim and they are not allowed to speak with their family, friends etc and they are continuously monitored. This gives scammers full control on the victims actions and mind
5. **Use of technology for manipulation** - Use of AI voices, professional logos, and simulated video calls to appear credible because of which victims believe the information to be true

How to Stay Safe?

If you receive a call claiming you are under digital arrest –

1. Report the number immediately to law enforcement
2. Verify suspicious calls and credentials using official websites rather than search engines, as scammers upload the fake profiles and numbers online
3. Remember legitimate investigations cannot end with payments. Any such demand is a red flag

If you have fallen victim for such scam –

1. Remain calm and do not give out any personal information immediately
2. Be aware that legitimate agencies do not conduct these inquiries over the call or demand payments
3. Call helpline 1930 within 15 minutes to freeze the transfer / report to the NCCPR portal/ report to the Bank/ report on National Cyber Crime Reporting Portal at www.cybercrime.gov.in
4. File a complaint to Local Cyber Crime Cell

.....Continued on page 3

GOOD TO KNOW!

What is I4C?

Indian Cyber Crime Coordination Centre (I4C) has been established under **Ministry of Home affairs** (MHA) to act as a nodal point at National level in the fight against cybercrime.

It aims to provide a platform to deal with cybercrimes in a coordinated and comprehensive manner.

One of the important objectives of I4C **is to create ecosystem that brings together academia, industry, public and government in prevention, detection, investigation and prosecution of cybercrimes.**

I4C has envisaged the **Cyber Crime Volunteers Program to bring together citizens with passion to serve the nation on a single platform and contribute in fight against cybercrime in the country**.

Good Samaritans are welcome to register as Cyber Crime Volunteers in the role of Unlawful Content Flaggers for facilitating law enforcement agencies in identifying, reporting and removal of illegal / unlawful online content.

While we are living in the era of information technology and AI, there are countless opportunities out there. At the same time, it also opens doors for multiple frauds and scams using the same. The key to protect ourselves to be aware each day.

LEGAL LANDSCAPE

Salient Features of Digital Personal Data Protection Act, 2023

We live in an era where the Technology has become the defining aspect of Success. At this stage, building strong governance is an inevitable process towards building long term sustainable processes. The Digital Personal Data Protection Act, 2023 applies to the processing of digital personal data within India collected online or offline and later digitalized. It is also applicable to processing digital personal data outside the territory of India, if it involves providing goods or services to the data principals within the territory of India.

Key Concepts –

1. **Data Fiduciary** - means any person or an entity who collects, stores and utilises the personal data for business operations or Example, Educational institutions collecting personal data of students can be termed as Data Fisuciary or social media handles like Facebook collecting our personal data.
2. **Data Principal** - means the individual whose personal data is being collected by the Data Fiduciary In case of a childit includes the parents or lawful guardian of such a child; and in case of a person with disability, includes her lawful guardian, acting on her behalf
3. **Data Processor** - means any person who processes personal data on behalf of a Data Fiduciary. For example, cloud service providers, software solution providers or Apps
4. **Data Protection Officer** - means an individual appointed by the Significant Data Fiduciary who is in charge of ensuring compliance with provisions of DPDP Act, 2023
5. **Personal Data** - means any data about an individual who is identifiable by or in relation to such data. For Example, Email Id, PAN Number, Adhaar number etc
6. **Personal Data Breach** - means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data
7. **Significant Data Fiduciary** - means any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government

The Law protects digital personal data by providing –

- The obligations of Data Fiduciaries for Data Processing
- The rights and duties of Data Principals
- Financial penalties for breach of rights, duties and obligations

Key Provisions –

1. **Consent Based Data Collection for Lawful Purposes** - Organizations must obtain explicit consent before collecting and processing personal data. They are also required to provide a notice while obtaining consent which would include information on type of personal data collected, purpose and manner of collecting and processing data, disclosure of such personal data to other third party and retention and deletion of data, information regarding redressal mechanism and rights of data principal
2. **Processing Personal Data of Children** - The Data Fiduciary shall, before processing any personal data of a child or a person with disability who has a lawful guardian obtain verifiable consent of the parent of such child or the lawful guardian, as the case may be, in such manner as may be prescribed
3. **Processing Personal Data Outside India** - The Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified.

4. Rights of Data Principal – The Rights of Data Principal are a) Right to access the personal data b) Right to correction and erasure of personal data c) Right to be protected from unauthorised use or disclosure of data d) Right of nomination to be exercised in case of death or incapacitation of Data Principal e) Right to withdraw consent

5. Penalties on Data Breach – Upon failing to protect the personal data, the responsible company is obligated to notify the Data Protection Board (DPB) and the affected client. Penalties range up to Rs. 250 crores.

7. Significant Data Fiduciary - The Central Government may assess the Data Fiduciary, on the basis of –

(a) the volume and sensitivity of personal data processed;
(b) risk to the rights of Data Principal;
(c) potential impact on the sovereignty and integrity of India;
(d) risk to electoral democracy;
(e) security of the State; and
(f) public order

Significant Data Fiduciary shall appoint a **Data Protection Officer** as point of contact for grievance redressal mechanism and an independent **Data Auditor** for undertaking measures of periodic Data Protection Impact Assessment and periodic audits.

8. Data Protection Board of India – The Central Government may appoint the Data Protection Board of India for the purposes of this Act namely to direct any remedial or mitigation measures, to inquire into the breach and impose penalty

The enactment of Digital Personal Data Protection Act, 2023 is significant in India's legal framework, where it recognizes privacy as Fundamental Right and provides a framework for data protection.

LATEST HIGHLIGHT

Telecommunications (Telecom Cyber Security) Rules, 2024

The Department of Telecommunications (DoT) has notified the Telecommunications (Telecom Cyber Security) Rules 2024 draft on 21st November, 2024 replacing the earlier draft released for public consultation on 28th August, 2024. The rules aim to safeguard India's communication networks and services, through measures including specified timelines for telcos to report security incidents and make disclosures.

The Telecommunications (Telecom Cyber Security) Rules, 2024, are derived from the Telecommunications Act, 2024, which repeals the Indian Telegraph Act of 1885 and the Indian Wireless Telegraphs Act of 1933. These rules aim to establish standards and assessment measures for telecom services, telecommunication networks, and telecommunication security.

The Rules aim to ensure security of telecommunication industry by requiring telecom entities to implement measures for protecting cybersecurity. The Rules include provisions for telecom service providers to share data with the Central Government for law enforcement purposes and for the installation of infrastructure necessary for data collection, storage, and processing. Additionally, they mandate compliance measures to ensure telecom cyber security and require detailed reporting of security incidents. The appointment of a Chief Telecommunication Security Officer is also stipulated to oversee the implementation of these Rules.

Important definitions –

- **Chief Telecommunication Security Officer** - means the designated employee of a telecommunication entity, appointed under rule 6 of these rules
- **Cyber Security of Telecommunication Networks and Telecommunication Services** or Telecom Cyber Security - refers to tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, assurance and technologies that can be used to safeguard telecommunication networks and telecommunication services, as well as assets of persons, including connected telecommunication equipment, telecommunication services, personnel, infrastructure, applications, and the totality of transmitted and/or stored information, against relevant security risks in the cyber environment

.... continued on page 5

NEWS CORNER

India launches online 'suspect registry'

India has launched online suspect registry containing the data on 1.4 million cybercriminals linked to financial frauds and various cybercrimes. The registry is accessible to states, union territories, central investigation and intelligence agencies and has been developed by Indian Cyber Crime Coordination Centre.

NEWS CORNER

Can WhatsApp messages attract Prosecution under IPC Sections 153A and 295A? – Supreme Court to consider

The Supreme Court has agreed to consider whether the messages sent on WhatsApp could attract criminal proceedings for outraging religious feelings and promoting enmity between groups. The Court's decision came while hearing a petition filed challenging an FIR registered over alleged inflammatory messages shared in WhatsApp group.

.... continued from page 4

- **Security Incident** - means an event having actual or potential adverse effect on telecom cyber security
- **Telecommunication Entity** - means any person providing telecommunication services, or establishing, operating, maintaining, or expanding telecommunication network, including an authorised entity holding an authorisation under sub-section (1) of section 3 of the Act, or a person exempted from the requirement of authorisation under sub-section (3) of section 3 of the Act
- **Traffic Data** - means any data generated, transmitted, received or stored in telecommunication networks, including data relating to the type, routing, duration or time of a telecommunication.
- **Telecommunication Equipment Identification Number** - means a telecommunication identifier bearing one or more of the following characteristics:

(i) international mobile equipment identity (IMEI) number; or
(ii) electronic serial number (ESN); or
(iii) any other number or signal that identifies a unique telecommunication equipment.

Core Provisions –

1. Rule 3 – Collection, Sharing and Analysis of Data

The Central Government and its authorized agencies may collect traffic data and any other relevant information for the purposes of cyber security. Telecom entities may be directed to install infrastructure for seamless data collection, storage and processing. The Central Government or its authorized agencies may for the purpose of analysing the data for enhanced cyber security, for protecting and ensuring telecom cyber security, may share this data with any agency of Central Government engaged in law enforcement and security related activities and shared with Telecommunication entities or users.

The data collected under these rules shall not be used or disclosed for any other purpose, except for ensuring telecom cyber security

2. Rule 4 – Obligations Relating to Telecom Cyber Security –

This rule lays down some important guidelines for Telecommunication Entities in order to ensure Telecom Cyber Security Each Telecommunication Entity shall ensure compliance with following measures to ensure Telecom Cyber Security –

A) **Adopt a Telecom Cyber Security Policy** – The Telecom Cyber Security Policy shall include Security safeguards, risk management approach, best practices and technologies, telecommunication network testing, prevention of cyber security incidents, rapid action to deal with these incidents, forensic analysis of security incidents, and further strengthening of cyber security.

B) **Identify and Reduce the Risk of Cyber Security Incident** and ensure timely response to such incidents

C) **Take appropriate action** for addressing security incident and to mitigate their impact

D) **Ensure implementation of directions and standards by Central Government**

E) Conduct **Periodic Telecom Cyber Security Audits**

F) Promptly **Report the Cyber Security Incident** to the Central Government

G) Establish facilities such as Security Operations Centre (SOC) to address telecom cyber security incidents, attempts, misuse, breaches, to maintain details of threats, to maintain command logs of operation and maintenance, logs of SOC (firewall, Intrusion Detection System (IDS) or Intrusion Prevention System (IPS), or Security Information and Event Management (SIEM) or other such solution); to provide necessary support to the agency or person authorized by the Central Government or the law enforcement agencies for the purpose of investigation related to security incidents

3. Rule 5 – Measures to Protect and Ensure Telecom Cyber Security

- The Central Government shall, identify the telecommunication identifier, the use of which is alleged to have endangered telecom cyber security and the person to whom such telecommunication identifier has been issued by the telecommunication entity, and issue a notice to such person. The Central Government based on the assessment of facts and submissions, may pass an order which may include directions to the telecommunication entity to – a) temporarily suspend the use of relevant telecommunication identifier in the manner and for specified duration b) terminate the use of relevant telecommunication identifier for providing telecommunication services
- If it is necessary or expedient in the public interest, and in such circumstances, the Central Government shall pass an order recording the reasons therefor, with appropriate directions to the telecommunication entity to temporarily suspend use of the relevant telecommunication identifier for the purpose of providing telecommunication services.
- The Central Government may maintain a repository of persons and telecommunication identifiers and may direct telecommunication entities, to prohibit or limit the access to telecommunication services to such persons

4. Rule 6 – Chief Telecommunication Security Officer

Each Telecommunication Entity shall appoint the Chief Telecommunication Security Officer who shall be the citizen and resident of India and responsible to the Board of Directors or similar governing body of the telecommunication entity.

The Chief Telecommunication Security Officer shall be responsible for coordinating with the Central Government for the implementation of these rules, including compliance with any reporting requirements under these rules, including of security incidents

5. Rule 7 – Reporting of Security Incidents

Telecommunication entity within 6 hours of becoming aware of a security incident affecting its telecommunication network/ services should furnish the following information:

- number of users affected by the security incident;
- duration of the security incident;
- geographical area affected by the security incident;
- extent to which the functioning of the telecommunication network/ service is affected
- the extent of impact on economic and societal activities
- remedial measures taken or proposed to be taken

The Central Government can ask the affected telecommunication entity to provide information needed to access the telecommunication network/ services including the telecom cyber security policy and carry out a security audit. As we move ahead in this digital world, these rules become crucial in addressing the growing complexity of cyber threats, and protecting and strengthening trust in Telecommunication Infrastructure.

GLOSSARY OF TERMS

Digital Arrest
"Digital arrest" is a term used in cyber scams to describe a type of fraud where scammers impersonate law enforcement officials to extort money from victims. The term is not recognized in law.

Cyber Terrorism
Cyber terrorism (also known as digital terrorism) is defined as disruptive attacks by recognized terrorist organizations against computer systems with the intent of generating alarm, panic, or the physical disruption of the information system.

Example:

* Hacking of servers to disrupt communication and steal sensitive information.

*Defacing websites and making them inaccessible to the public thereby causing inconvenience and financial losses.

*Hacking communication platforms to intercept or stop communications and make terror threats using the internet.

Cyber Espionage
Cyber espionage is a type of cyber-attack that involves stealing sensitive information from computer networks without authorization. It's a sophisticated form of spying that can be used for a variety of reasons, including: Financial gain, Political motivations, corporate espionage, and State-sponsored actions.

Ransomware
Ransomware is a type of malware that locks and encrypts a victim's data, files, devices or systems, rendering them inaccessible and unusable until the attacker receives a ransom payment. While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called crypto viral extortion

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

Adv Kunal Gokhale
BSC. LLB (Hons.) (Business Law) Degree

Advocate Kunal Gokhale is a legal professional with nearly fourteen years of post-qualification experience. He is a graduate from the National Law University, Jodhpur and holds a BSc LLB (Hons.) (Business Laws) degree. Advocate Kunal Gokhale has significant professional experience in handling civil litigation matters with focus on commercial matters. He also provides advisory services in relation to drafting of various types of agreements and has been associated with firms such as Vaish Associates, Advocates (Delhi), Ernst & Young, India (Mumbai) and Luthra & Luthra Law Offices (Mumbai) in the past.

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

Mrudula Arjunwadkar
BSc., LLB, MPM

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

Anagha Nair
BBA, LLB

Intern, at Adv Vaishali Bhagwat