# HOW SECURE ARE WE?

## CYBER ATTACKS AND SECURITY

By - Mr. Upender Thakur, Advocate

# CYBER ATTACKS

**Criminal activity that is carried out using computer, computer system, computer network or network device**

**CAUSES**

**Economic Motivation -** One of the primary causes of such crime is money. When you hide behind a network, the risk of being caught is lower and the monetary gain is much higher, making money one of the major motivators for most of the criminals. Owing to this, a huge group of cyber criminals target online banking accounts.

**Personal Grudges -** Since cybercrimes involve lower risk, a lot of individuals, who are well-versed with hacking, vent out their personal grudges by hacking someone's social media accounts or even websites. For example, an unhappy employee may install viruses in the computer networks of an organization just to take out his grudge against his/her employer.

# CYBER SECURITY (Section 2(nb) of the Information Technology Act, 2000)

**Protecting information, equipment, devices, computer, computer resources, communication devices and information stored therein from unauthorized access, use, disclosure, disruption , modification or destruction.**

India has progressed from aligning with the UNCITRAL Model Law on Electronic Commerce to provide legal sanctity to electronic documents under the Information Technology Act, 2000, to implementing robust measures for their security through subsequent amendments, rules, and frameworks addressing data protection, cybersecurity, and intermediary accountability.

# PLAYERS INVOLVED IN CYBER CRIME

- **Insiders -** Disgruntled employees and ex-employees, spouses, lovers
- **Hackers** - Crack into networks with malicious intent
- **Virus Writers -** Pose serious threats to networks and systems worldwide
- **Terrorists** - Use to formulate plans, to raise funds, propaganda
- **Foreign Intelligence** - Use cyber tools as part of their Services for espionage activities

# Cyber criminals are not anonymous to us as we may think. It can be one amongst us. As per Professor Federico Varese

"Understanding cybercrime isn't just about the victims. You have to look at the supply of the activity. For too long the emphasis has been put on cybercrime as a global activity, but it is a very localised issue. Cybercrime thrives in those places where they can operate with less fear of arrest or punishment. The people involved are not necessarily sophisticated or even high tech, criminal masterminds. They are everyday people with a motivation and an opportunity. Almost anyone can do it. If we really focus on where this activity is taking place, we should see a reduction in crimes committed."

Section 75 of the Information Technology Act, 2000, serves as a reflection of this principle. Sub-section (1) extends the Act's applicability beyond the bounds of nationality, emphasizing its extraterritorial jurisdiction. Simultaneously, sub-section (2) localizes this applicability by stipulating that the act or conduct constituting the offence or contravention must involve a computer, computer system, or computer network located within India.

**Who are the cyber criminals?**

- ❖ Not anonymous people
- ❖No high-tech criminal minded persons
- ❖But every day people with motivation and opportunity

# ROLE OF INTERMEDIARIES

- **Who are Intermediaries?**

- Section 2(1)(w) of the Information Technology Act, 2000 exhaustively defines intermediary with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record.

- **It includes:**
  - Telecom service providers
  - Network service providers
  - Internet Service Providers (ISPs)
  - Web-hosting service providers
  - Search engines (e.g., Google).
  - Online payment sites (e.g., Razorpay)
  - Online-auction sites
  - Online-market places (e.g., Amazon, Flipkart).
  - Cyber cafes

**Liability of Intermediaries**

Intermediaries are exempted from liability for any third-party information, data, or communication link made available or hosted by them, subject to the provisions/obligations casted under sub-section (2) and (3) of section 79 of the IT Act, 2000, which inter-alia, includes observing due diligence.

# CLASSIFICATIONS OF CYBER CRIME

# BANKING AND FINANCE-RELATED CYBERCRIMES

- Fraudulent Electronic Fund Transfers: Unauthorized electronic fund transfers, often achieved via phishing, malware, or fraudulent OTPs.
- Culpability and Liability:
  - Section 43 and section 43A of IT Act, 2000: Civil liability to pay damages by way of compensation.
  - Section 66 of IT Act, 2000: Imprisonment up to 3 years and/or fine up to ₹5,00,000.
- Mule Accounts: Bank accounts that facilitate illegal transactions by receiving and transferring funds from unlawful activities, with or without the complicity of the account holders.
- Culpability and Liability:
  - Section 66D: Imprisonment up to 3 years and fine up to ₹1,00,000.
  - IT Act, 2000: Section 43(a) (unauthorized access) and Section 66D (cheating by impersonation).
- ATM Skimming or Card Cloning: Stealing card information using skimmers or creating cloned cards to withdraw money.
- Culpability and Liability: Section 66C of IT Act, 2000: Imprisonment up to 3 years and fine up to ₹1,00,000.

- 9 out of 10 mule accounts in an Indian bank goes undetected as significant portion uses VPNs, indicating international involvement.
- Cities like Bhubaneswar, Lucknow and Navi Mumbai, along with regions in West Bengal, have reported higher incidences of mule account activity.
- Mule accounts related frauds account for 55% of all frauds in India. These are mainly used for money laundering and tax evasion, making the same also prosecutable under the Prevention of Money Laundering Act.
- RBI tightened customer due diligence norms in October 2023 by updating its guidelines with the objective to minimize mule account operations. In terms thereof, banks are ordained to identify mule accounts and report suspicious transactions to the Financial Intelligence Unit.

- Cyber Extortion: Threatening to harm or reveal sensitive digital information unless a ransom is paid. A new form of extortion by the name, Sextortion, is also on the rise nowadays, which means blackmailing someone by threatening to release explicit content unless demands are met.

- Culpability and Liability: Section 66E of IT Act, 2000: Imprisonment up to 3 years and/or fine up to ₹2,00,000 and/or Section 67 of IT Act, 2000: Imprisonment up to 5 years and fine up to ₹10,00,000 and/or Section 67A of IT Act, 2000: Imprisonment up to 7 years and and fine up to ₹10,00,000.

- Cyber arrest: It occurs when individuals are wrongfully detained by imposters posing as law enforcement or cybercrime authorities. These fake officials deceive victims, coercing them into divulging sensitive information or visiting specific websites.

- Culpability and Liability:

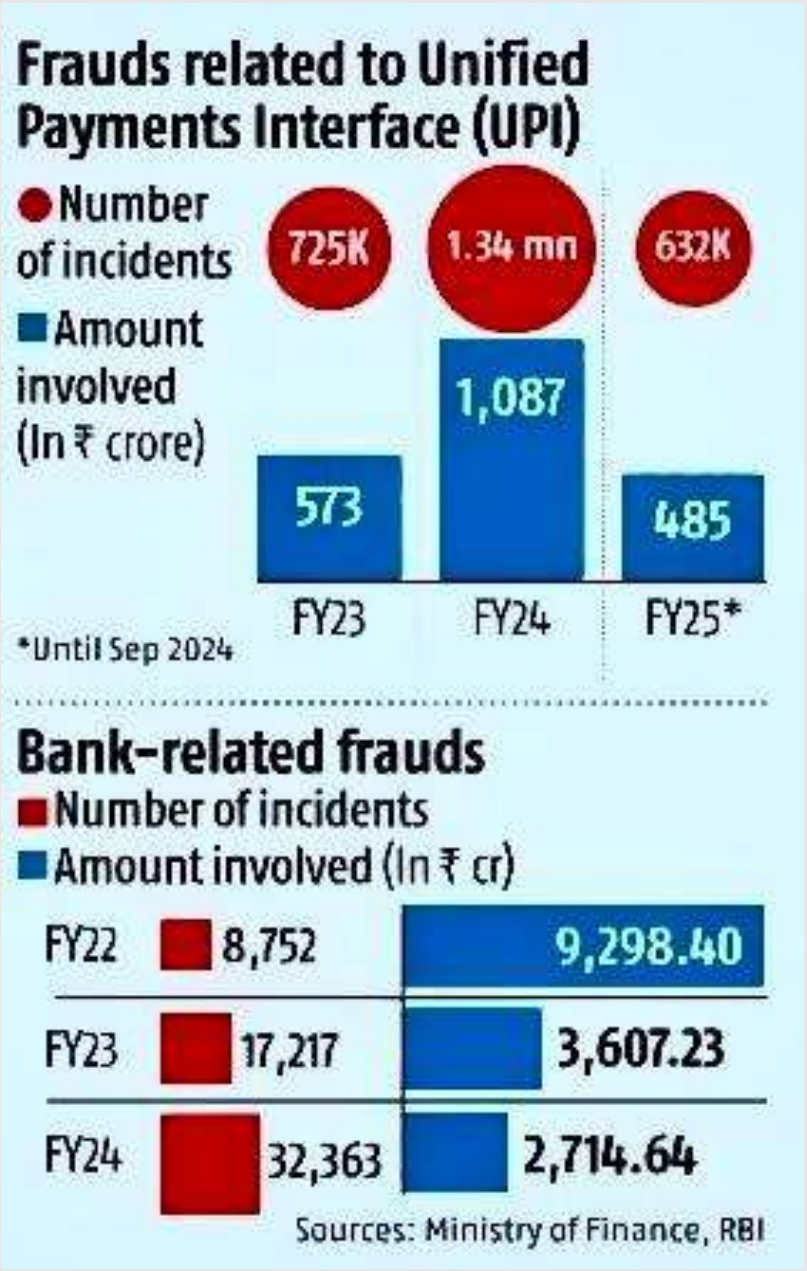
- Section 66E of IT Act, 2000: Imprisonment up to 3 years and/or a fine up to ₹2,00,000 and/or Section 66D of IT Act, 2000: Imprisonment up to 3 years and a fine up to ₹1,00,000 and/or : Section 66C of IT Act, 2000: Imprisonment up to 3 years and fine up to ₹1,00,000.

- UPI Payment Frauds: Unauthorized transactions carried out using a victim's UPI account, often by tricking them into sharing sensitive information such as UPI PINs or OTPs, or through malicious apps.

- Culpability and Liability: Section 43 and section 43A of IT Act, 2000: Civil liability to pay damages by way of compensation and/or Section 66 of IT Act, 2000: Imprisonment up to 3 years and/or fine up to ₹5,00,000.

- . OTP-Based Frauds: Frauds where either victims are deceived into sharing One-Time Passwords (OTPs) sent to their registered mobile numbers or *otherwise*, enabling unauthorized access to their bank or payment accounts.

- Culpability and Liability: Section 43 and section 43A of IT Act, 2000: Civil liability to compensate the victim and/or Section 66 of IT Act, 2000: Imprisonment up to 3 years and/or fine up to ₹5,00,000.



# CHILDREN-RELATED CYBERCRIMES

- Online Child Sexual Abuse Material (CSAM): Creation, transmission, or viewing of sexually explicit content involving children.
  - Culpability and Liability: Section 67B of IT Act, 2000: Imprisonment up to 7 years and fine up to ₹10,00,000.
- Cyber Grooming: Building a relationship with a child online for the purpose of exploitation or abuse.
  - Culpability and Liability: Section 66E of IT Act, 2000: Imprisonment up to 3 years and/or fine up to ₹2,00,000.
  - Section 95 of Bharatiya Nyaya Sanhita (BNS), 2023, it penalizes hiring, employing or engaging a child to commit an offence with an imprisonment which shall not be less than 3 years but may extend to 10 years, and with fine.
- Cyber Bullying: Harassment, threats, or intimidation of children through online platforms.
  - Culpability and Liability: POCSO Act, 2012 prescribes penal provisions based on severity.

- Every 6th child in 44 countries in the world is a target of cyber bullying. (WHO)
- 1 out of 3 children in 30 countries is a victim of cyber bullying. (UNICEF)
- 1 out of 5 children leave school because of cyber bullying. (UNICEF)
- Every 4th child in India is a victim of cyber bullying and 70-80% reports are never even registered. (UNICEF report on India)
- There was a 95% increase in searches related to child sexual abuse after COVID. (NCRB)

# DATING AND MATRIMONIAL-RELATED CYBERCRIMES

- Dating or Romance Scams: Deceiving individuals into fake relationships for financial gain or exploitation.
  - Culpability and Liability: Section 66D of IT Act, 2000: Imprisonment up to 3 years and fine up to ₹1,00,000.
- Cat Phishing: Using fake profiles or identities to lure victims into scams.
  - Culpability and Liability: Section 66C of IT Act, 2000: Imprisonment up to 3 years and fine up to ₹1,00,000.
- Honey Traps: Seducing individuals for blackmail or extortion using intimate exchanges.
  - Culpability and Liability: Section 67 of IT Act, 2000: Imprisonment up to 5 years and fine up to ₹10,00,000.

- There was an increase of 24% in dating scams in the year 2022. (NCRB)
- There is a loss of approximately INR 200 Crores through dating scams. (I4C)
- 66% of the online users gets cheated upon in dating and matrimonial scams. (I4C)
- An amount of INR 13.23 Crores was lost in dating and matrimonial scams in the month of January-February 2024. (I4C)

# OTHER CYBERCRIMES ON THE RISE

- Cyberstalking: Persistent online harassment or monitoring of an individual.
- Culpability and Liability: Section 66E of IT Act, 2000: Imprisonment up to 3 years and/or fine up to ₹2,00,000.
- Revenge Porn: Sharing intimate images or videos without consent to defame or blackmail.
- Culpability and Liability:
  - Section 67 of IT Act, 2000: Imprisonment up to 5 years and fine up to ₹10,00,000.
  - Section 67A of IT Act, 2000: Imprisonment up to 7 years and fine up to ₹10,00,000.
- Cyber Defamation: Publishing defamatory content about someone online.
- Culpability and Liability: Section 66 of IT Act, 2000: Imprisonment up to 3 years and/or fine up to ₹5,00,000.
- Ransomware Attacks: Encrypting or locking data and demanding ransom for its release.
- Culpability and Liability: Section 66 of IT Act, 2000: Imprisonment up to 3 years and/or fine up to ₹5,00,000. and/or Section 66F of IT Act, 2000: Life imprisonment for large-scale attacks affecting national security viz cyber terrorism.

## General Statistics

- 7000-8000 cyber complaints are registered everyday. (I4C)
- 2-2.5 lakhs cyber complaints are registered every month. (I4C)
- 25-30 lakhs cyber complaints are registered every year. (I4C)
- There has been an increase of 150-200% in the number of cyber complaints in 2023 from previous year.
- 1 lakh crores are lost every year in cyber crimes. (I4C)

# ADDRESSING CYBERCRIME CHALLENGES through LEGISLATURE

- **The Information Technology Act, 2000**: Establishes the legal framework for electronic governance, defining offences like hacking (Section 66), publishing obscene material (Section 67), and ensuring extraterritorial jurisdiction (Section 75) for cybercrimes involving systems in India.
- **The Information Technology (Amendment) Act, 2008**: Strengthens cybersecurity with provisions addressing identity theft (Section 66C), cheating via impersonation (Section 66D), lawful interception of communication (Section 69), and protection of critical infrastructure (Section 70).
- **The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2011**: Requires intermediaries to inter-alia, moderate content, ensure traceability, and remove unlawful material within 36 hours of notification while protecting user data.
- **The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011:** Establishes mandatory guidelines for organizations to implement reasonable security practices, inter-alia, protecting sensitive personal data from unauthorized access, defining security obligations, and providing recourse in case of data breaches.
- **The Finance Act, 2017**: Inter-alia, expanded the jurisdiction of the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) to include matters previously under the Cyber Appellate Tribunal, consolidating appellate functions related to cyber disputes.
- **The Jan Vishwas (Amendment of Provisions) Act, 2023**: Inter-alia, decriminalizes minor cyber offences to simplify compliance, promoting ease of doing business and streamlining penalties in cyber-related laws.
- **The Digital Personal Data Protection Act, 2023**: Regulates inter-alia data processing activities, ensures privacy, and enforces obligations on organizations to secure personal data while addressing cybersecurity risks.

# ADDRESSING CYBERCRIME CHALLENGES through JUDICIARY

- In **Shreya Singhal v. Union of India, (2015) 5 SCC 1**, the Hon'ble Supreme Court struck down **Section 66A** of the IT Act, 2000, for violating **Article 19(1)(a)** of the Constitution, citing its vague and overbroad nature that stifled free speech. The judgment emphasized the need for precise, constitutionally compliant laws to balance free expression and online regulation.

- In **Google India v. Vishakha Industries, (2020) 4 SCC 162**, the Hon'ble Supreme Court clarified intermediary liability under **Section 79** of the IT Act, ruling that platforms like Google are not liable for third-party content if they exercise due diligence and act promptly upon receiving notice of illegality. The judgment reinforced the safe harbor provision and emphasized adherence to the Intermediary Guidelines to avoid liability.

- In **Bank of India v. Sri Sandeep**, the Hon'ble TDSAT vide judgment dated 20.12.2019 in re: Cyber Appeal 3 of 2018 held the bank liable under Section **43A** of the IT Act, 2000, in the facts of the case, for failing to implement reasonable security practices, leading to unauthorized transactions and also held the Telecom Service Provider liable under sections **43A** and **43(g)** of IT Act, 2000. The Hon'ble Tribunal held that there is a contributory negligence on part of the bank and the Telecom Service Provider paving the way for siphoning off money from the victim's account.

- In **Vodafone Idea Ltd. v. Union of India and Others**, the Hon'ble TDSAT vide judgment dated 25.09.2024 in re: Cyber Appeal 16 of 2015 held the Telecom Service Provider liable under Sections **43(g)** and **43A** of IT Act, 2000 as a reiteration and reaffirmation of the ratio laid down in **Bank of India v. Sri Sandeep.**

# ADDRESSING CYBERCRIME CHALLENGES through ADMINISTRATION

**1930**
Helpline Number

- **CERT-In (Indian Computer Emergency Response Team):** Functions as the national nodal agency for cybersecurity incident response, providing advisories, vulnerability assessments, and coordination for cyber threat mitigation.
- **Cyber Jaagrookta Campaign:** Focuses on raising awareness about cyber threats and safety measures through targeted public campaigns.
- **Cybercrime Reporting Portal (www.cybercrime.gov.in):** A dedicated platform for citizens to report cybercrimes such as fraud, harassment, and online abuse. It also provides resources to educate users about cyber safety.
- **National Investigation Agency (NIA):** Empowers India's fight against terrorism and cyber terrorism through robust investigations, cross-border collaborations, and cutting-edge digital forensics.
- **'Chakshu' feature on the Sanchar Saathi portal:** Enabling users to report fraudulent communication, including calls, SMS, and WhatsApp messages designed to deceive users.
- **Cyber Swachhta Kendra:** Offers tools for detecting and removing malware, promoting digital hygiene, and protecting devices from cyber threats.
- **#CyberDost Campaign:** A public awareness initiative using social media platforms to educate citizens on cyber safety, fraud prevention, and digital literacy.
- **Partnerships with International Organizations** like **INTERPOL**, **UNODC (United Nations Office on Drugs and Crime)**, that aligns with the **Budapest Convention** to strengthen cross-border cybercrime cooperation.
- **National Cybersecurity Coordinator (NCTC):** Acts as the central body for coordinating all cybersecurity-related efforts and implementing policy frameworks to counter cyber threats.
- **National Cyber Forensic Laboratory (NCFL):** A facility for forensic analysis and investigation of cybercrime by use of the latest digital technology to support investigations undertaken by Law Enforcement Agencies.

# EMERGING LEGAL CONCERNS

## Cryptocurrency and Blockchain

- Cryptocurrency is a digital or virtual currency secured by cryptography, often using blockchain technology. Popular examples include Bitcoin and Ethereum.
- The *Cryptocurrency and Regulation of Official Digital Currency Bill, 2021* was proposed to prohibit private cryptocurrencies while creating a framework for the RBI's Central Bank Digital Currency (CBDC). However, the bill has not been passed and is currently pending.
- The Indian government is working on a consultation paper for cryptocurrency regulations, led by the Department of Economic Affairs (DEA). Expected to be released in 2024, the paper aims to gather public input on cryptocurrency policies. However, as of now, it has not been released yet.
- The Reserve Bank of India (RBI) is actively working on the Digital Rupee, which is in the pilot phase.
  - Cybersecurity Threats:
- Cryptocurrencies can be used for illicit activities such as money laundering and terrorism financing due to their pseudonymous nature.
- Crypto wallets and exchanges are vulnerable to hacking, phishing, and fraud.

India's cryptocurrency exchange WazirX experienced one of the largest cyberattacks in July, affecting approximately 15 million users and leading to the theft of $235 million in investor holdings. The Netherlands-based blockchain intelligence firm, *Crystal Intelligence*, reported that the stolen funds were laundered via *TornadoCash*, an open-source platform that anonymizes crypto transactions, leaving only $6 million of Ether (ETH) traceable.

# EMERGING LEGAL CONCERNS

## Artificial Intelligence (AI)

- AI refers to the simulation of human intelligence in machines, enabling them to perform tasks like decision-making, pattern recognition, and problem-solving.
- India has no dedicated AI legislation. However, the *National Strategy for Artificial Intelligence (NSAI), 2018* by NITI Aayog provides policy guidance on AI development and regulation.

◦ **Cybersecurity Threats:**

- **Deepfakes and Misinformation:** AI can be used to create convincing fake images, videos, and news, leading to social and political harm.
- **AI-powered Attacks:** Hackers use AI to automate and enhance phishing, brute force attacks, and malware creation.
- **Bias and Discrimination:** Unregulated AI systems may perpetuate biases, leading to ethical and legal disputes.
- **Autonomous Systems:** AI-driven devices or systems (e.g., drones, self-driving cars) may malfunction or be hijacked, raising concerns about liability and accountability.

**The Artificial Intelligence Act, 2024**: The world's first and only comprehensive legislation on AI, introduced by the European Union, extending extraterritorial jurisdiction over entities impacting the EU.

# EMERGING LEGAL CONCERNS

## Internet of Things (IoT)

- IoT refers to the network of physical devices (smart devices) connected to the internet, enabling data exchange and remote control. Examples include smart thermostats, wearable health monitors, and industrial sensors.
- India lacks dedicated IoT-specific laws. However, the Bureau of Indian Standards (BIS) has issued **IoT security guidelines**, though these are not enforceable as binding laws.
  - **Cybersecurity Threats:**
- **Data Breaches:** IoT devices collect vast amounts of personal data, making them attractive targets for hackers.
- **Weak Security Protocols:** Many IoT devices lack robust encryption and authentication mechanisms, exposing them to vulnerabilities.
- **Botnets:** Compromised IoT devices can be exploited to form botnets, launching Distributed Denial-of-Service (DDoS) attacks.
- **Critical Infrastructure Risks:** IoT is increasingly used in healthcare, transportation, and utilities, making its compromise a national security threat.

# SAFETY FROM CYBER ATTACKS

- **Use Strong Passwords:** Combine uppercase, lowercase, numbers, and symbols.
- **Enable Two-Factor Authentication (2FA):** Add an extra layer of security.
- **Keep Software Updated:** Install updates and patches regularly.
- **Avoid Clicking Unknown Links:** Be cautious of phishing emails and suspicious links.
- **Use Antivirus and Firewalls:** Protect devices with reliable security tools.
- **Secure Wi-Fi Networks:** Use strong passwords and avoid public Wi-Fi.
- **Backup Data Regularly:** Store backups offline or on secure cloud platforms.
- **Be Mindful of Sharing Information:** Limit sharing sensitive data online.
- **Monitor Financial Transactions:** Check bank statements for unauthorized activity.
- **Educate Yourself:** Stay informed about common cyber threats.

# DIGITAL MINIMALISM

'***A philosophy of technology use in which you focus your online time on a small number of carefully selected and optimized activities that strongly support things you value, and then happily miss out on everything else'*** **- Cal Newport** (Digital Minimalism: Choosing a Focused Life in a Noisy World)

- **Declutter Devices:** Uninstall unnecessary apps and files.
- **Limit Screen Time:** Set daily limits for social media and digital use.
- **Prioritize Meaningful Content:** Focus on apps and websites that add value.
- **Turn Off Non-Essential Notifications:** Minimize distractions.
- **Schedule Tech-Free Time:** Create daily or weekly breaks from digital devices.
- **Use Technology Intentionally:** Only use devices when necessary.

# THANK YOU!