India’s Suspect Registry and Cybersecurity Initiatives

Source: IE

Why in News?

India’s **online suspect registry** has saved around Rs 5,100 crore by blocking 13 lakh fraudulent transactions, and it has quickly become a key tool in **India’s fight against cybercrime**.

What is a Suspect Registry?

- **About:** Launched in 2024, the suspect registry was created based on the **National Cybercrime Reporting Portal (NCRP)** and developed by the **Indian Cyber Crime Coordination Centre (I4C).**
    - It contains data on **1.4 million cybercriminals** linked to financial fraud and other cybercrimes, which has been shared with all banks.
    - The data has been shared with all banks and is accessible to States, UTs, and central investigation and intelligence agencies
- **Objective: The registry helps banks and financial institutions verify customer credentials and monitor transactions to suspected accounts in real time.**
    - Using data from the NCRP, it strengthens fraud risk management and flags potential cybercriminals.
- **Need for Suspect Registry:** India loses over Rs 1,000 crore every month to cyber fraud. More than 80% of cybercrime cases involve financial fraud.
    - The rising scale of digital transactions demands stronger fraud risk management and real-time monitoring.
- **Impact:** As of December 2024, over 6.1 lakh fraudulent transactions worth around Rs 1,800 crore were blocked.
    - Banks froze 8.67 lakh mule accounts, 7 lakh SIMs, and 1.4 lakh devices. Since 2021, around Rs 3,850 crore in frauds have been intercepted, and suspicious online contents were blocked under the Information Technology Act, 2000.

Cybercrime Trends in India

- **Rising Cybercrime Losses:** According to the **NCRP** India witnessed a massive surge in cyber fraud, with total losses of around Rs 33,165 crore (2021-24).
- **Emergence of Tier 2 & 3 Cybercrime Hotspots:** Cities like Deoghar, Jaipur, Nuh, Mathura, Kolkata, Surat, Bengaluru Urban, and Kozhikode have been identified as hotspots, reflecting that cybercriminals are increasingly targeting smaller cities.

TYPES OF CYBERCRIMES

Personal Threats to Individuals

- **Phishing** 🎣 : Scams via email/texts to steal personal or financial info.
- **Smishing** 📱 : SMS-based scams targeting mobile users.
- **Vishing** ☎️ : Fraudulent calls asking for OTPs or account info.
- **Identity Theft** 🆔 : Misusing personal data for fraud.
- **Digital Arrest Scams** 👮 : Fake threats of arrest via video calls.
- **Cyber Stalking** 👁️ : Persistent online harassment.
- **Deepfakes & AI Content** 🤖 : Fake videos/audio for social engineering.

Targeted Attacks on High-Value Individuals

- **Whale Phishing** 🐋 : Fraudulent emails or messages designed to trick senior executives into sharing sensitive data.
- **Spear Phishing** 🎯 : Personalized scams targeting a specific person, group, or department to steal information.
- **Trojan Horse** 🐴 : Malicious software hidden inside seemingly safe files or apps to gain access to systems.

Financial & System-Level Threats

- **Ransomware** 💻 : Locks files until a ransom is paid.
- **Ponzi & Investment Schemes** 💰 : Websites promising unrealistic returns.
- **Botnet:** It is a network of malware-infected devices, remotely controlled by a cybercriminal (bot herder), used for large-scale attacks like data theft, and spam.

Click here to Read: Cyber Frauds

What are India's Cybersecurity Initiatives?

- **Constitutional Context: Police and public order are state subjects. States/UTs handle crimes, including cybercrime, while the Centre provides guidance, coordination, and funding.**
- **Policy Mechanisms:**
  - Information Technology Act, 2000: Covers cybercrime offences like phishing, smishing, and vishing with fines and imprisonment.
  - New Criminal Laws: Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, the Bharatiya Nyaya Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023, address modern cyber threats.
  - National Cyber Security Policy, 2013: Aimed at protecting cyberspace, building cyber defense capabilities, reducing vulnerabilities, and strengthening national digital security.
- **Institutional Mechanisms**
  - **Indian Cyber Crime Coordination Centre (I4C):** Attached office under MHA for coordinated response to cybercrime.
    - The **National Cyber Crime Reporting Portal (NCRP)** under I4C enables the public to report all types of cybercrimes, with a major focus on crimes against women and children.
    - **Cyber Fraud Mitigation Centre (CFMC)** under I4C brings banks, financial intermediaries, telecom service providers, IT intermediaries and law enforcement agencies (LEAs) under one roof for real-time action.
    - **Samanvay Platform** a web-based portal for cybercrime data, analytics, mapping, and coordination among Law Enforcement Agencies nationwide.
    - **Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS)** platform for immediate action on financial cyber fraud complaints via helpline 1930.
  - **CERT-In (Indian Computer Emergency Response Team):** National agency under IT Act, 2000 for handling cybersecurity incidents, vulnerabilities, and coordinated response.
    - CERT-In runs the **National Cyber Coordination Centre (NCCC)** for situational awareness of cyber threats and the **Cyber Swachhta Kendra** to detect and remove malware, offering free tools and cybersecurity guidance for citizens and organizations.
- **International Cooperation:** Central Bureau of Investigation (CBI) **participates in Interpol-led cybercrime cooperation initiatives.**
  - The CBI is the nodal agency for G-7 24/7 network, which is a secure channel for making data preservation requests in cases related to cyber crime.
- **Digital Mechanisms**
  - **'.bank.in' Domain for Banks:** Exclusive internet domain for Indian banks to reduce cyber fraud and strengthen digital trust.
  - **e-Zero FIR:** Converts cyber financial crime complaints above Rs 10 lakh into **First Information Report (FIR)** automatically.
  - **MuleHunter.AI:** AI tool developed by RBI to detect **"mule accounts"** used for transferring stolen funds.
  - **ASTR:** Developed by Department of Telecommunications (DoT) **Artificial Intelligence and Facial Recognition powered Solution for Telecom SIM Subscriber Verification (ASTR)** is used to identify suspected mobile connections taken by the same person in different names.

Drishti Mains Question:

Q. Discuss the institutional and digital mechanisms established by India to prevent and respond to cybercrime.

UPSC Civil Services Examination, Previous Year Questions (PYQs)

Prelims

Q.1 In India, under cyber insurance for individuals, which of the following benefits are generally covered, in addition to payment for the loss of funds and other benefits? (2020)

1. Cost of restoration of the computer system in case of malware disrupting access to one's computer
2. Cost of a new computer if some miscreant wilfully damages it, if proved so
3. Cost of hiring a specialised consultant to minimise the loss in case of cyber extortion
4. Cost of defence in the Court of Law if any third party files a suit

Select the correct answer using the code given below:

(a) 1, 2 and 4 only
(b) 1, 3 and 4 only
(c) 2 and 3 only
(d) 1, 2, 3 and 4

Ans: (b)

Q.2 In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centres
3. Body corporate

Select the correct answer using the code given below:

(a) 1 only
(b) 1 and 2 only
(c) 3 only
(d) 1, 2 and 3

Ans: (d)

Mains

Q. What are the different elements of cyber security ? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. **(2022)**