सत्यमेव जयते
Goverment Of India

DOT Initiatives and Sanchar Saathi

Presented by
Mohamed ilias A,
Assistant Director(Technology),
Tamil Nadu LSA,
Department of Telecommunications ,
Government of India.

सत्यमेव जयते
Goverment Of India

Introduction to DoT

Department of Telecommunications

- Nodal agency under Ministry of Communications
- Responsible for telecom policy, licensing, and spectrum management
- Backbone of India’s digital ecosystem

👉 Plays a key role in enabling **Digital India, connectivity, and innovation**

सत्यमेव जयते
Goverment Of India

Vision & Mission of DoT

Vision:
Secure, reliable, and affordable telecom for all

Mission:
Expand digital infrastructure
Promote innovation & investment
Ensure inclusive growth

सत्यमेव जयते
Goverment Of India

Production Linked Incentive (PLI) Scheme – Telecom Sector

- Launched by Department of Telecommunications (DoT) on **24 Feb 2021**
- Focus: **Telecom & Networking Products Manufacturing**
- Total Outlay: **₹12,195 crore**
- Duration: **5 years (FY 2021–22 to FY 2025–26)**

Objective:

- Boost **domestic manufacturing**
- Reduce **import dependency**
- Promote **“Make in India”**
- Increase **exports & global competitiveness**

सत्यमेव जयते
Goverment Of India

Key Features of the Scheme

Incentives:

- 4%–7% on incremental sales
- Based on production beyond base year (2019–20)

Eligible Segments:

- 4G/5G equipment
- Wireless & IoT devices
- Routers, switches
- Customer premises equipment (CPE)

Design-led Incentive:

- Extra **1% incentive** for products designed in India

Implementation Agency:

- Small Industries Development Bank of India (SIDBI)

सत्यमेव जयते
Goverment Of India

Impact & Outcomes

- Investments: **₹4,081 crore+**
- Total Sales: **₹78,000+ crore**
- Exports: **₹14,000+ crore**
- Jobs Created: **26,000+**

Impact:

- Strengthened **telecom manufacturing ecosystem**
- Encouraged **global & domestic companies**
- Supported **5G ecosystem development in India**

https://www.myscheme.gov.in/schemes/dot-pli-scheme
https://www.pli-telecom.udyamimitra.in/

Telecom PLI beneficiaries 2025-2026

There are Seven Telecom PLI beneficiary are in Tamil Nadu.

1. M/s Nokia, Oragadam,
2. M/s Flextronics Technologies (India) Private Limited, Sriperumbudur,
3. M/s Sanmina- SCI India Pvt Ltd, Oragadam,
4. M/s Syrma SGS Technologies, Chennai,
5. M/s Rising Star High Tech Pvt Ltd, Sriperumbudur,
6. M/s Alphion India Private Limited , Chennai,
7. M/s VVDN Technologies Private Limited, Pollachi.

Financial Year	2021-22	2022-23	2023-24	2024-25	2025-26	Total
Incentive Disbursed for the above companies (in Rs Crore)	0	18.43	109.85	219.5	264.21	611.99

सत्यमेव जयते
Goverment Of India

Rural & Remote Connectivity

What are these Initiatives?

- A group of programmes to provide **telecom & internet connectivity in rural and hard-to-reach areas**
- Focus on **last-mile connectivity & digital inclusion**

Key Initiatives Covered

- BharatNet – Fiber connectivity to Gram Panchayats
- PM-WANI – Public Wi-Fi access
- National Broadband Mission – Broadband infrastructure expansion
- LWE & Border connectivity schemes

Objectives

- Universal **mobile & broadband access**
- Bridge **urban–rural digital divide**
- IN Support **Digital India vision**

सत्यमेव जयते
Goverment Of India

BharatNet

What is BharatNet?

- World’s **largest rural broadband connectivity project**
- Aims to connect **all Gram Panchayats (GPs)** with high-speed internet
- Implemented by **Bharat Broadband Network Limited**
- Uses **optical fiber (OFC)** for reliable connectivity

सत्यमेव जयते
Goverment Of India

Objectives

- Provide **affordable broadband** in rural areas
- Enable **Digital India services** (e-Governance, e-Health, e-Education)
- Bridge the **urban–rural digital divide**
- Support **5G backhaul & future telecom infrastructure**

सत्यमेव जयते
Goverment Of India

Major Achievements

- ✔ **2 lakh+ Gram Panchayats connected** via optical fiber
- ✔ Over **6 lakh km OFC laid** across India
- ✔ **Rural Wi-Fi hotspots enabled** in thousands of villages
- ✔ Boost to schemes like **Digital India**
- ✔ Enabled **online education & telemedicine** in remote areas
- ✔ Strengthened **digital payments ecosystem (UPI penetration in villages)**
- ✔ Supported **startup & CSC ecosystem growth**

सत्यमेव जयते
Goverment Of India

Impact on Society

- Internet access in **remote villages**
- Growth of **online learning platforms**
- Improved **telemedicine services**
- Rural employment via **Common Service Centres (CSCs)**
- Boost to **digital economy & inclusion**

सत्यमेव जयते
Goverment Of India

National Broadband Mission (NBM)

What is NBM?
Launched in **2019** to accelerate broadband access across India

Vision: **“Broadband for All”**
Aims to strengthen **digital infrastructure & connectivity**

Key Goals

- Broadband access to **all villages**
- **50 Mbps** connectivity to every citizen
- Fiberisation of **70% telecom towers**
- Enable strong backbone for **5G rollout**

सत्यमेव जयते
Goverment Of India

Key Features & Strategy

- Expansion of **optical fiber network (OFC)** across the country
- Promotion of **Right of Way (RoW) reforms** for faster infrastructure deployment
- Development of **National Digital Grid**
- Encourages **infrastructure sharing** among telecom operators
- Focus on **satellite broadband & remote connectivity**
- Supports initiatives like **Digital India**

सत्यमेव जयते
Goverment Of India

Achievements & Impact

Major Achievements

- ✔ Rapid increase in **tower fiberisation (~40%+ and growing)**
- ✔ Significant boost in **rural broadband penetration**
- ✔ Faster rollout support for **4G & 5G networks**
- ✔ Improved **Ease of Doing Business** in telecom sector
- ✔ Enabled growth of **OTT, EdTech, and digital services**

Impact

- Reduced **digital divide (urban vs rural)**
- Growth in **online education & skill development**
- Boost to **digital economy & startups**
- Enhanced **telemedicine & e-Governance services**

सत्यमेव जयते
Goverment Of India

PM-WANI

What is PM-WANI?

- Launched in **2020** to expand **public Wi-Fi access** across India
- Full form: **Prime Minister Wi-Fi Access Network Interface**
- Aims to create a **nationwide Wi-Fi ecosystem**

Key Objectives

- Affordable & accessible **internet for all**
- Enable **small shopkeepers** to become Wi-Fi providers (PDOs)
- Increase **internet penetration in rural & urban areas**
- Boost **Digital India ecosystem**

Key Components

- **PDO (Public Data Office)** – local Wi-Fi providers
- **PDOA (Aggregator)** – manages multiple PDOs
- **App Providers** – user authentication & discovery

सत्यमेव जयते
Goverment Of India

Achievements & Impact

Major Achievements

- ✔ Rapid growth of **public Wi-Fi hotspots** across India
- ✔ Enabled **low-cost internet access** without SIM/KYC barriers
- ✔ Created **income opportunities for small businesses**
- ✔ Strengthened support for **Digital India**

Impact

- Improved connectivity in **railway stations, markets, villages**
- Supports **online education & digital literacy**
- Boost to **local entrepreneurship & startups**
- Helps bridge the **digital divide**

सत्यमेव जयते
Goverment Of India

LWE & Border Connectivity

What are these Schemes?

- Targeted initiatives to provide **mobile connectivity in Left Wing Extremism (LWE) and border areas**
- Focus on **strategic, remote, and security-sensitive regions**

Key Objectives

- Ensure **network access in uncovered villages**
- Strengthen **communication for security forces**
- Expand **4G connectivity in difficult terrains**
- IN Promote **inclusive development & national integration**

Key Features

- Installation of **mobile towers in remote/forest/border regions**
- Deployment of **4G services (phased upgrades)**
- Use of **satellite backhaul & solar-powered infrastructure**
- Covered under broader plans like **Comprehensive Telecom Development Plan**

सत्यमेव जयते
Goverment Of India

Comprehensive Telecom Development Plan (CTDP)

What is CTDP?

- A flagship initiative to expand telecom connectivity in **remote, border & Left Wing Extremism (LWE) areas**
- Focus on providing **mobile and broadband services in uncovered villages**

Key Objectives

- Ensure **connectivity in difficult terrains** (hills, forests, border regions)
- Expand **4G mobile coverage in rural/remote areas**
- Strengthen **strategic & security communication infrastructure**
- IN Promote **inclusive digital development**

Key Areas Covered

- North-East region
- Himalayan & border areas
- LWE-affected districts

सत्यमेव जयते
Goverment Of India

Achievements & Impact

Major Achievements

- ✔ Thousands of **mobile towers installed in remote regions**
- ✔ **4G services extended** to previously uncovered villages
- ✔ Improved **connectivity in border & security-sensitive areas**
- ✔ Enhanced coordination for **defence & emergency services**

सत्यमेव जयते
Goverment Of India

5G Rollout

What is 5G?

- Next-generation mobile network with **ultra-fast speed & low latency**
- Supports technologies like **IoT, AI, Smart Cities**

Launch in India

- Officially launched in **October 2022**
- Led by telecom operators:
  - Reliance Jio
  - Bharti Airtel

Key Features

- Speeds up to **10x faster than 4G**
- Ultra-low latency (<10 ms)
- Massive device connectivity

सत्यमेव जयते
Goverment Of India

Achievements & Impact

Major Achievements

- ✔ One of the **fastest 5G rollouts globally**
- ✔ Coverage expanded to **hundreds of cities within months**
- ✔ Rapid deployment of **5G base stations (lakhs installed)**
- ✔ Strong ecosystem support via **Make in India telecom gear**

Impact

- ✓ Enables **Smart Cities & IoT applications**
- ✓ Supports **remote healthcare & telemedicine**
- ✓ Enhances **AR/VR-based education & training**
- ✓ Boosts **Industry 4.0, automation & innovation**
- ✓ Drives **digital economy growth**

सत्यमेव जयते
Goverment Of India

Satellite Communication Reforms

What are SatCom Reforms?

- Policy reforms to **liberalize and simplify satellite communication** in India
- Aim to enable **high-speed connectivity in remote & underserved areas**

Key Policy Changes

- **Administrative allocation of spectrum** (instead of auctions for SatCom)
- Easier approvals for satellite services & ground infrastructure
- Opening sector to **private players & global companies**
- Support for **LEO/MEO/GEO satellite constellations**

सत्यमेव जयते
Goverment Of India

Achievements & Impact

Major Achievements

- ✔ Boost in **private participation in SatCom sector**
- ✔ Faster rollout of **satellite broadband services**
- ✔ Improved connectivity in **remote, hilly & island regions**
- ✔ Strengthened **disaster communication systems**

Impact

- Internet access in **hard-to-reach areas (no fiber/mobile towers)**
- Connectivity for **maritime & aviation sectors**
- Enables **telemedicine & emergency response**
- Supports **digital education in remote regions**
- Complements **5G & BharatNet infrastructure**

सत्यमेव जयते
Goverment Of India

Sanchar Mitra – Overview

What is Sanchar Mitra?

- A student volunteer initiative to promote **telecom awareness & digital literacy**
- Engages **college students** as “Digital Ambassadors”

Key Objectives

- Spread awareness on **safe & responsible telecom usage**
- Educate public on **cyber fraud & telecom scams**
- Promote **Digital India initiatives**
- Encourage **youth participation in governance**

Key Activities

- Conducting **awareness campaigns, workshops & outreach programs**
- Promoting platforms like **Sanchar Saathi (fraud prevention tools)**
- Engaging with **schools, villages & communities**

सत्यमेव जयते
Goverment Of India

Achievements & Impact

Major Achievements

- ✔ Thousands of **students onboarded as Sanchar Mitras**
- ✔ Conducted **nationwide awareness campaigns**
- ✔ Increased awareness on **cyber safety & digital fraud**

prevention

- ✔ Strengthened outreach of **Digital India**

Impact

- Improved **cybersecurity awareness among citizens**
- Promotes **digital literacy at grassroots level**
- Provides **leadership & communication skills to students**
- Builds a **digitally aware and responsible society**

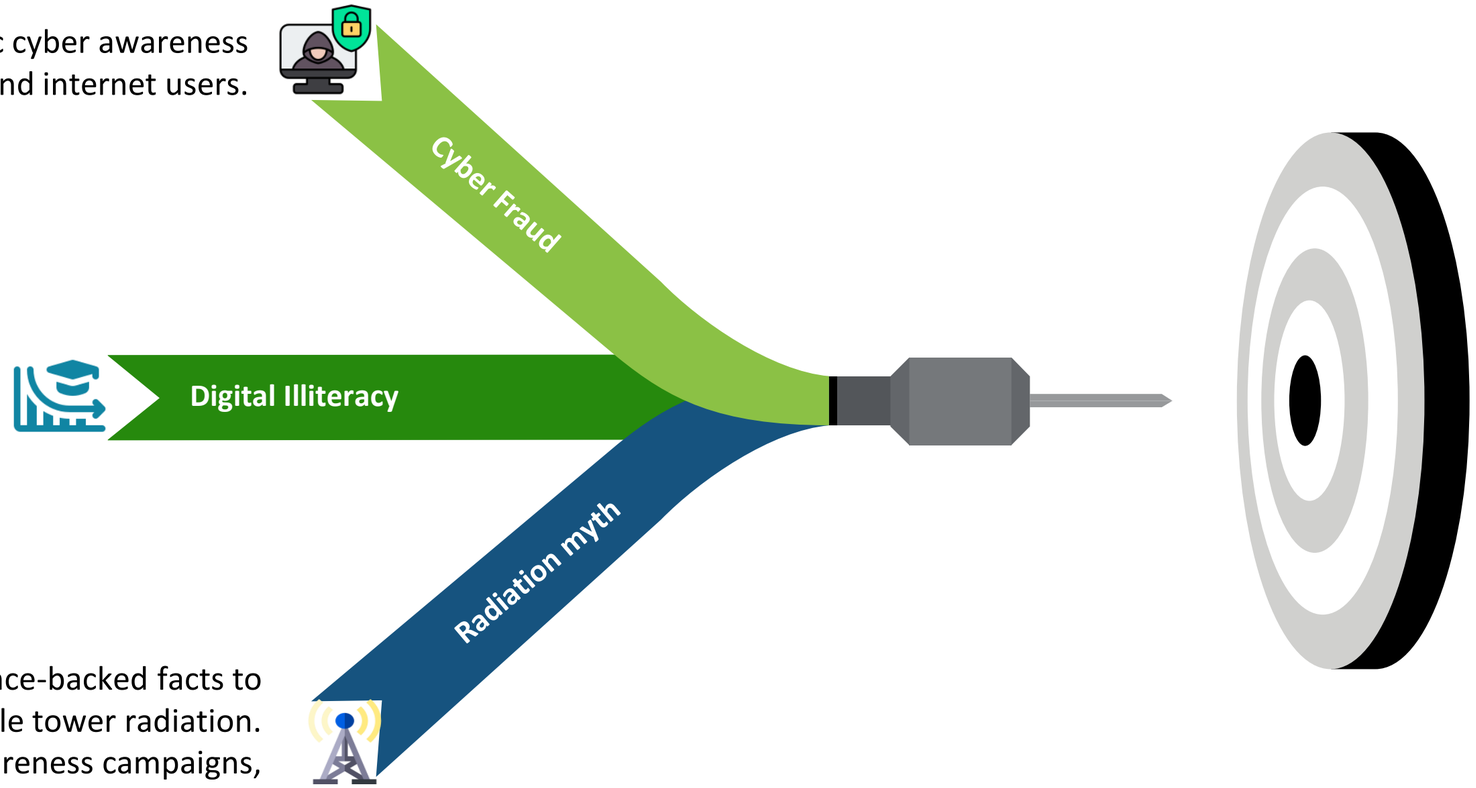
Aim of Sanchar Mitras

To address key challenges:

Reduce cyber fraud by building basic cyber awareness among everyday mobile and internet users.

Tackle digital illiteracy by turning student volunteers into “digital ambassadors” who educate citizens on using telecom and internet services safely and effectively. Through community outreach and awareness sessions, they promote basic digital skills, cyber hygiene, and responsible mobile and online behavior so that more people can participate confidently in the digital economy.

Educates citizens with science-backed facts to dispel myths about mobile tower radiation. Volunteers lead awareness campaigns, promoting safe and responsible mobile use



Public awareness is key to secure, responsible, and inclusive telecom usage

Expectation from Volunteers – Sanchar Mitra

Learn and Teach

- *Get trainings from DoT*
- *Conduct awareness drives (schools, Colleges, RWAs, public spaces, Industry, Police,Old age homes, etc.)*
- *Promote Sanchar Saathi, Tarang Sanchar etc.*
- *Educate citizens on EMF, fraud prevention, cyber safety*
- *Collaborate with LSA, NGOs, VLEs, and local bodies*
- *Participate in various activities of DoT like hackathon etc.*

Sanchar Mitra volunteers are expected to undergo training, conduct community awareness sessions on telecom safety and cyber hygiene, and serve as digital ambassadors promoting responsible mobile/internet use

Expectation of Volunteers – Sanchar Mitra

Recognition ,Opportunities and Self pride

- *Participation in R&D and Innovation Projects*
- *Industry Engagement and Internships*
- *ITU Standards and Policy Work*
- *Participation in DoT Projects and Initiatives*
- *Sanchar Mitra Kits*
- *Recognition and Certifications*

Sanchar Mitra volunteers will earn certification and contribute to national digital empowerment

सत्यमेव जयते
Goverment Of India

Tarang Sanchar Portal

What is Tarang Sanchar?

- An online portal for **information on mobile towers & EMF radiation compliance**
- Enhances **transparency and public awareness**

Key Objectives

- Provide details of **mobile towers across India**
- Enable citizens to **check EMF radiation compliance status**
- Allow **online EMF testing requests**
- Promote **trust in telecom infrastructure**

Key Features

- Public access to **tower location & compliance data**
- Online **EMF radiation measurement request system**
- Ensures adherence to **safety norms (well below global limits)**

सत्यमेव जयते
Goverment Of India

Achievements & Impact

Major Achievements

- ✔ Improved **transparency in telecom tower deployment**
- ✔ Easy access to **EMF compliance information for citizens**
- ✔ Strengthened **public confidence in mobile networks**
- ✔ Simplified **grievance redressal & testing process**

Impact

- Increased **awareness about EMF safety standards**
- Reduced public concerns regarding **radiation from towers**
- Promotes **digital governance & citizen participation**
- Supports expansion of **mobile & 5G infrastructure**

सत्यमेव जयते
Goverment Of India

Telecom Reforms (2021 onwards)

What are these Reforms?

- A comprehensive set of policy changes introduced from **2021** to revive and strengthen the telecom sector
- Aim to make India a **globally competitive telecom market**

Key Reform Measures

- **Rationalization of AGR (Adjusted Gross Revenue) definition**
- **Moratorium on spectrum & AGR dues** for telecom operators
- Simplified **licensing & compliance procedures**
- Allowed **100% FDI under automatic route** in telecom sector
- Promoted ease of doing business & investment

सत्यमेव जयते
Goverment Of India

5G Use Case

What are 5G usecase labs?

- Labs set up in **engineering institutions across India**
- Aim to **develop, test, and demonstrate 5G applications**

Key Objectives

- Promote **innovation in 5G technologies**
- Involve **students & startups in R&D**
- Develop solutions for **industry-specific use cases**
- IN Build a strong **indigenous 5G ecosystem**

Focus Areas

- Healthcare (remote surgery, telemedicine)
- Smart mobility & autonomous systems
- Industry 4.0 (automation, robotics)
- Smart agriculture & IoT

सत्यमेव जयते
Goverment Of India

Achievements & Impact

Major Achievements

- ✔ **100+ 5G labs established** across institutions in India
- ✔ Collaboration between **academia, industry & government**
- ✔ Development of **India-specific 5G solutions**
- ✔ Support to **startup innovation ecosystem**

Impact

- 🎓 Hands-on learning for **engineering students**
- 💡 Encourages **research, innovation & entrepreneurship**
- 🏢 Accelerates **industry adoption of 5G technologies**
- 🌍 Positions India as a **global 5G innovation hub**

FY 2025-2026: 5G Use case Labs

- 5G Use Case Test Labs have been established in 9 institutes across Tamil Nadu, providing a platform for start-ups and telecom providers for the innovations in 5G and IoT technologies.
- As part of the 5G Hackathon initiatives, 269 use case proposals have been submitted by Tamil Nadu from the Institutes and Start-ups.

COLLEGE OF ENGINEERING GUINDY	**70**
NIT Puducherry	11
NIT Tiruchirappalli	59
Pondicherry University	10
SASTRA Deemed University	19
SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL SCIENCES	33
Sri Sivasubramaniya Nadar College of Engineering	20
SRM Institute of Science and Technology	23
Vellore Institute of Technology	24

FY 2025-2026: 5G Use case Labs Utilization

Outcome	Numbers
No. of projects utilizing the lab	100
Contributions related to 5G and beyond in International journals or Standardization organizations such as ITU/3GPP/ISO/IEEE/ORAN alliance etc	63
No. of product/ solutions/ use cases developed	16
No. of IPs generated	2

सत्यमेव जयते
Goverment Of India

Performance of 5G Use Case Labs in Tamil Nadu

Of these 269 use case proposals submitted, 19 proposals were shortlisted by the Zonal Committee and forwarded to the National-level Technical Evaluation Committee for further review.

- **1st place Secured by VIT Chennai**
- **3rd place secured by NIT Trichy.**

सत्यमेव जयते
Goverment Of India

5G Testbeds

What are 5G Testbeds?

- Indigenous platforms to **develop, test, and validate 5G**

technologies in India

- Developed with support from DoT and leading institutions like
  - Indian Institutes of Technology

Key Objectives

- Enable **R&D and innovation in 5G ecosystem**
- IN Promote **Atmanirbhar Bharat (self-reliance in telecom)**
- Support **startups, MSMEs, and academia**
- Test **5G applications before commercial deployment**

Key Features

- End-to-end **5G network testing environment**
- Supports **multiple use cases (IoT, AI, Industry 4.0)**
- Open access for **researchers, industries, and startups**

सत्यमेव जयते
Goverment Of India

Achievements & Impact

Major Achievements

- ✔ Successful development of **India’s own 5G testbed platform**
- ✔ Enabled testing of **indigenous 5G technologies**
- ✔ Reduced dependence on **foreign telecom equipment**
- ✔ Strengthened collaboration between **academia & industry**

Impact

- Boosts **innovation and product development**
- Provides hands-on experience to **students & researchers**
- Accelerates **5G rollout and adoption**
- Positions India as a **global telecom R&D hub**

सत्यमेव जयते
Goverment Of India

AOC Testbed

What is AOC Testbed?

- A national-level platform to **research and test next-generation optical communication technologies**
- Focus on **high-speed fiber networks for future telecom needs**

Key Objectives

- Develop **ultra-high-speed optical communication systems**
- Support backbone for **5G, 6G & broadband networks**
- IN Promote **indigenous R&D in optical technologies**
- Enable collaboration between **academia, industry & startups**

Key Features

- High-capacity **optical fiber transmission systems**
- Testing for **long-distance, high-bandwidth communication**
- Supports **advanced technologies (DWDM, photonics, etc.)**

सत्यमेव जयते
Goverment Of India

Centre of Excellence for 6G

What is this Centre?

- A dedicated initiative to drive **research in 6G technologies**, including **classical & quantum communications**
- Supports India's vision of becoming a **global leader in next-gen telecom**

Key Objectives

- Develop **6G technologies & standards**
- Advance **quantum communication for ultra-secure networks**
- IN Promote **indigenous innovation & self-reliance**
- Foster collaboration between **academia, industry & startups**

Focus Areas

- Terahertz communication (ultra-high speed)
- Quantum key distribution (QKD)
- AI-driven intelligent networks
- Integrated terrestrial & satellite communication

Located at IITM Research Park

सत्यमेव जयते
Goverment Of India

Achievements & Impact

Major Achievements

- ✔ Established dedicated **6G research ecosystem in India**
- ✔ Early-stage development of **quantum-secure communication technologies**
- ✔ Collaboration with leading institutions & global partners
- ✔ Supports India’s **Bharat 6G Vision**

Impact

- Positions India as a **future 6G technology leader**
- Enables **ultra-secure communication networks**
- Drives **cutting-edge innovation & research**
- Creates opportunities for **students, researchers & startups**

सत्यमेव जयते
Goverment Of India

Telecom Technology Development Fund

What is TTDF?

- A funding scheme to promote **indigenous telecom technology development**
- Supports **startups, MSMEs, academia, and R&D institutions**

Key Objectives

- IN Reduce dependence on **imported telecom equipment**
- Boost **innovation in telecom sector**
- Support development of **4G/5G/6G technologies**
- Enable solutions for **rural & remote connectivity**

Key Features

- Financial support for **research & product development**
- Focus on **IPR creation & commercialization**
- Encourages **collaboration between industry & academia**

सत्यमेव जयते
Goverment Of India

Achievements & Impact

Major Achievements

- ✔ Funding support to **multiple startups & research projects**
- ✔ Development of **indigenous telecom solutions**
- ✔ Promotion of **Make in India telecom ecosystem**
- ✔ Support to cutting-edge areas like **5G, IoT, AI in telecom**

Impact

- Accelerates **innovation & product development**
- Strengthens **startup & MSME ecosystem**
- Enhances **self-reliance in telecom infrastructure**
- Positions India as a **global telecom technology hub**

TTDF Symposium Initiative

- ➢ Knowledge-sharing platform
- ➢ Hosted by DoT &Ind ian Institute of Technology Madras

सत्यमेव जयते
Goverment Of India

Capacity Building & Skill Development

What is this Initiative?

- Focus on **training, upskilling, and capacity building** in telecom & digital technologies
- Targets **students, government officials, and industry professionals**

Key Objectives

- Develop **skilled workforce for telecom sector**
- Build expertise in **5G, IoT, AI, cybersecurity**
- Support **Digital India & emerging technologies**
- IN Promote **innovation & research culture**

Key Platforms & Programs

- National Communications Academy Technology (NCA-T) – Apex training institute
- Sanchar Mitra Scheme – Student engagement
- Training through **workshops, webinars & certification programs**

सत्यमेव जयते
Goverment Of India

Student Internships & Academic Collaboration

What is this Initiative?

- Programs to engage **students, researchers, and academic institutions** in telecom sector development
- Promotes **industry–academia collaboration**

Key Objectives

- Provide **hands-on experience through internships**
- Encourage **research in telecom & emerging technologies**
- Build strong **industry–academia partnerships**
- IN Support **innovation & skill development**

Key Areas of Collaboration

- 5G/6G technologies & testbeds
- AI, IoT, cybersecurity in telecom
- Digital infrastructure & policy research
- Linked with initiatives like **Telecom Technology Development Fund**

सत्यमेव जयते
Goverment Of India

Ericsson Educate Program (DoT Collaboration)

Content:

- Joint initiative by Ericsson and Department of Telecommunications (DoT)
- Launched: **March 2024**
- Covers **10,000 students** across **100 institutes**
- Focus: **5G & Emerging Technologies Training**

Objective:

- Build **5G-ready talent pool**
- Promote **innovation & local 5G use cases**

सत्यमेव जयते
Goverment Of India

Targeted Learning Areas:

- Artificial Intelligence (AI)
- Internet of Things (IoT)
- 5G Technology
- Automation
- Machine Learning

Target Audience:

- 2nd year & above UG students
- Postgraduate students
- Research scholars
- **Platform Access:**
- Free access to **Ericsson Educate platform**

सत्यमेव जयते

SANCHAR SAATHI

भारत दूरसंचार
INDIA TELECOM

Citizen centric
Sanchar Saathi Initiative
for prevention of misuse of telecom resources and cyber frauds

Department of Telecommunications (DoT)

Government of India

14.04.2026

Agenda

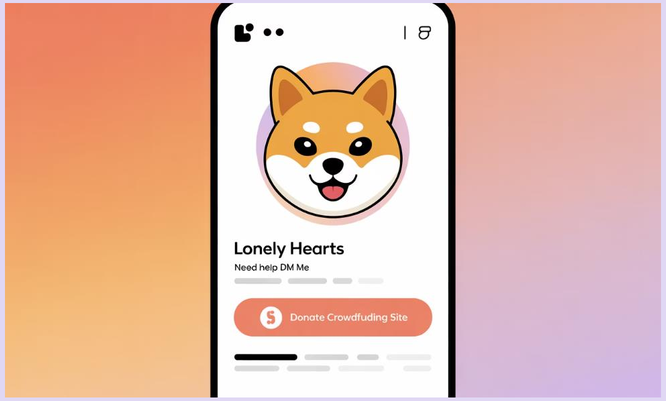
- Cyber Threat Landscape
- Understanding Cyber Crimes
- Common Digital Frauds
- Cyber Hygiene – Do’s and Don’ts
- What to do if you are a victim
- DoT’s Initiatives for Consumer Safety

Have You Encountered These?

Mystery Callers

WhatsApp audio/video calls from unknown national or international numbers attempting to establish contact

Fake Friend Requests

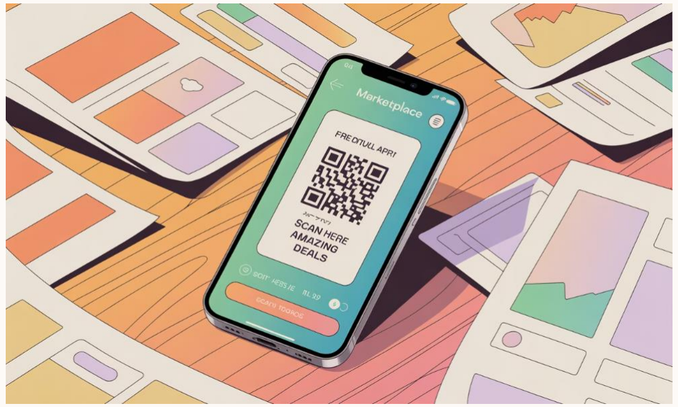


Messages from WhatsApp or Instagram accounts resembling your friends' profiles, urgently asking for money transfers

Authority Impersonation

Calls from supposed any government officials/police claiming your mobile number has been reported and will be disconnected

QR Code Tricks



QR codes sent by buyers on OLX or Quikr claiming "scan to receive money" but actually requesting payment

Too-Good-To-Be-True Offers

Free Netflix or Disney+ subscription links in group chats, plus Instagram ads offering expensive items at impossibly low prices

Fake Opportunities

Fraudulent scholarship, internship, or job forms requesting Aadhaar details or processing fees upfront

Welcome to the world of Cyber Crime!!!

Cyber Threat Landscape

Nation

'Social media misuse' constitutes bulk of cybercrime cases in MP, youngsters most affected

Out of the 511 cybercrime cases reported this year, more than 47% cases (242 cases) are related to social media misuse.

Indians lost staggering ₹7,000 crore to online scams in 5 months of 2025: Report

In just five months of 2025, India has lost a staggering ₹7,000 crore to online scams, primarily orchestrated by operators from Southeast Asia. This alarming trend reveals the scale of cyber fraud and the urgent need for enhanced cybersecurity measures to protect citizens.

Nation

Cybercrimes hit rural, semi-urban India hard with over 400 per cent rise

Data prepared by the Union Ministry of Home Affairs (MHA) reveals a staggering increase of over 400 percent in cybercrime incidents over the last four years.

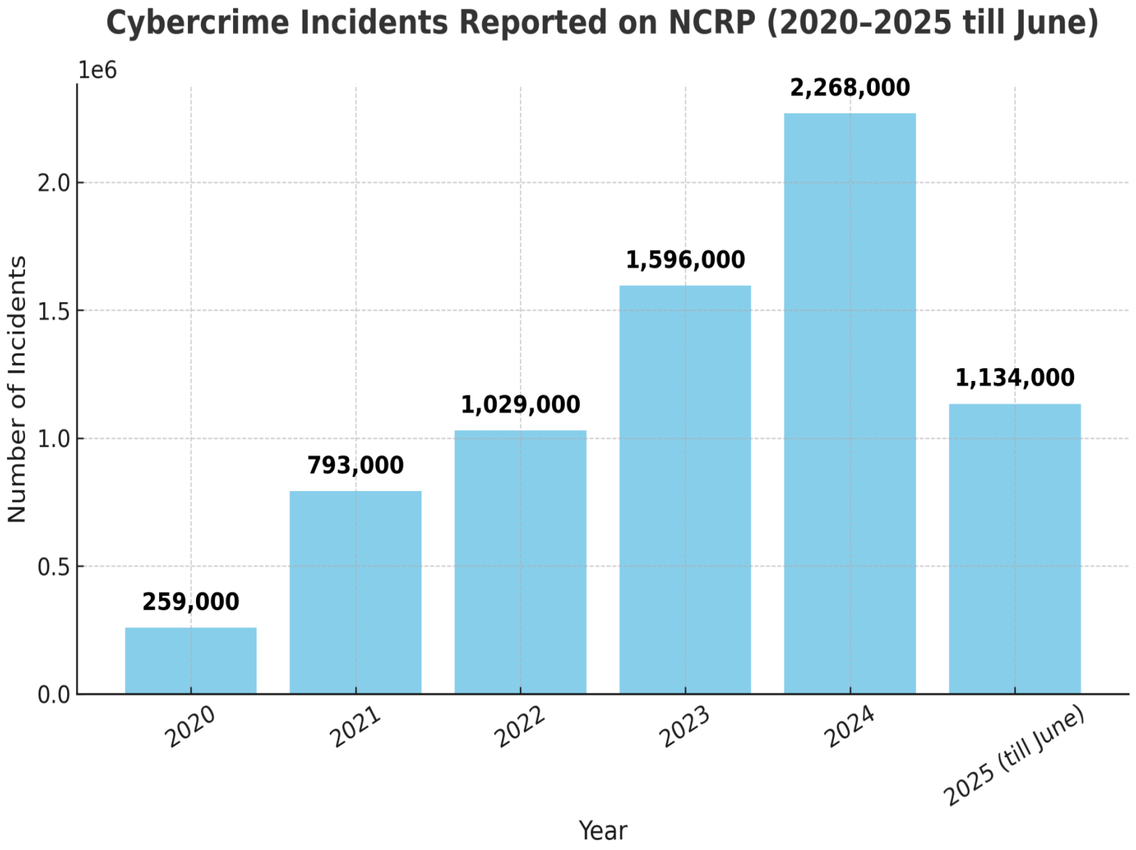
Govt blocks 6.69 lakh SIM cards, 1.32 lakh IMEIs to check cyber crimes

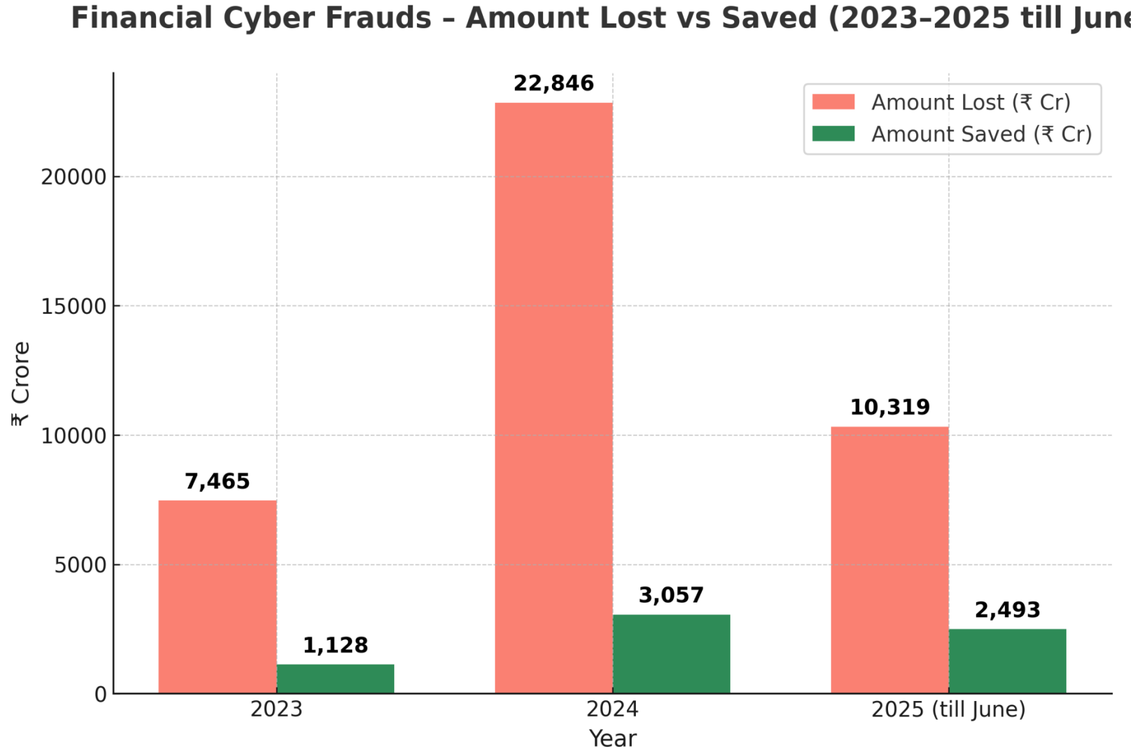
"Such international spoofed calls have been made by cyber criminals in recent cases of fake digital arrests, fedex scams and impersonation as government and police officials," the minister said.

PTI

Updated On Nov 28, 2024 at 08:06 AM IST

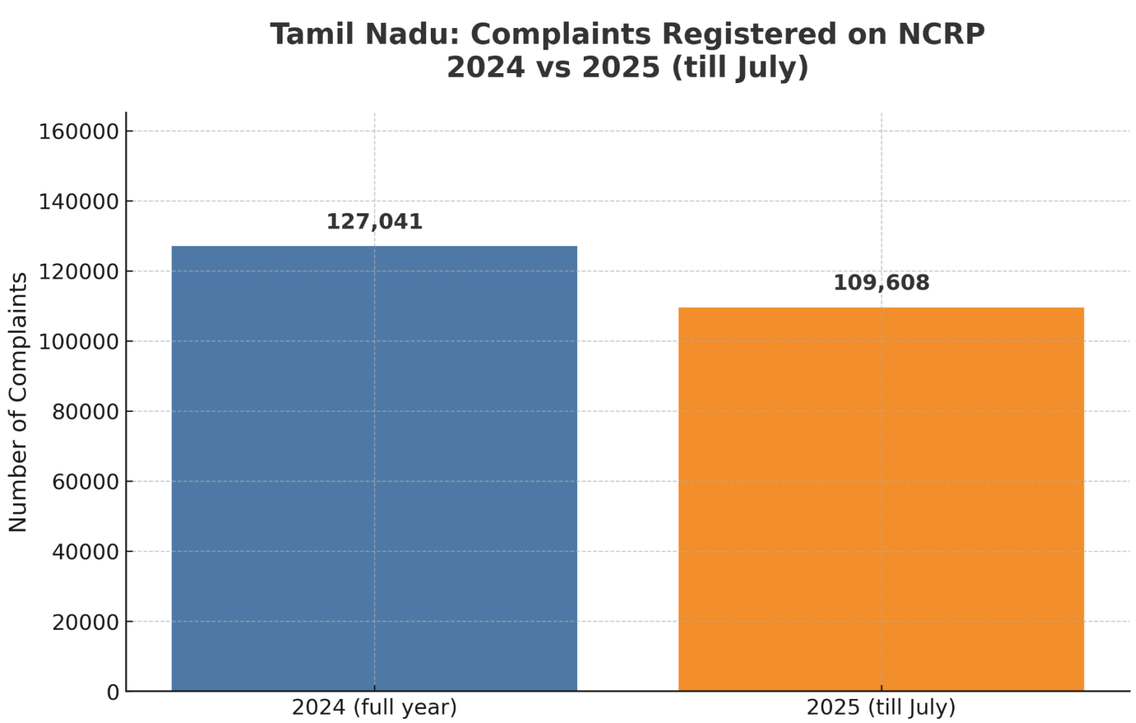
Cyber Threat Landscape-National Statistics

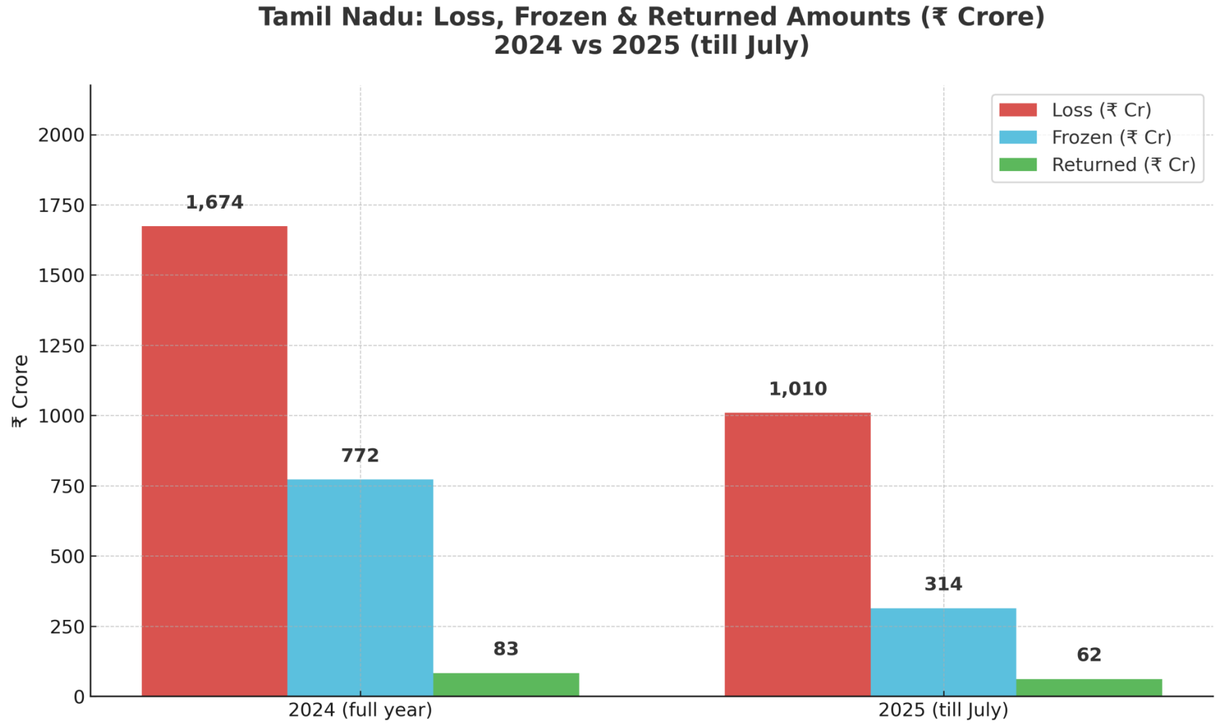




(Source: Lok Sabha Unstarred Question No. 344, answered on 22.07.2025 by MHA)

Cyber Threat Landscape-Tamil Nadu statistics





Source: Tamil Nadu Police (figures as quoted in *The New Indian Express*, Feb & Sept 2025; *Telecom Live*, Jan 2025; *DT Next*, Aug 2025)

Understanding Cyber Crimes

Means

Computers, digital devices, networks, and internet as primary tools

Target

Systems, data, individuals, Businesses and critical infrastructure

Goals

Financial gain, data theft, disruption, espionage, or malicious damage

Any criminal activity involving computers, digital devices, or networks as the primary instrument, target, or environment of the offence.

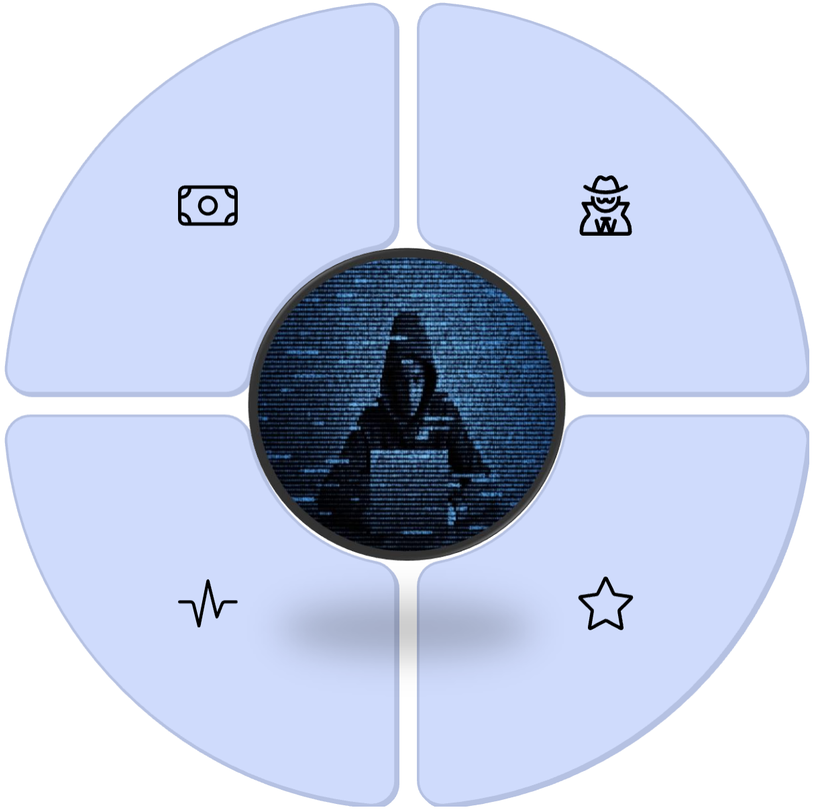
Motives of Cyber Frauds/ Attacks:

Financial Gain

Primary motive: stealing money, banking credentials, or valuable personal information for profit.

Hacktivism

Cyber attacks motivated by political, social, or ideological causes to raise awareness or protest.



Corporate Espionage

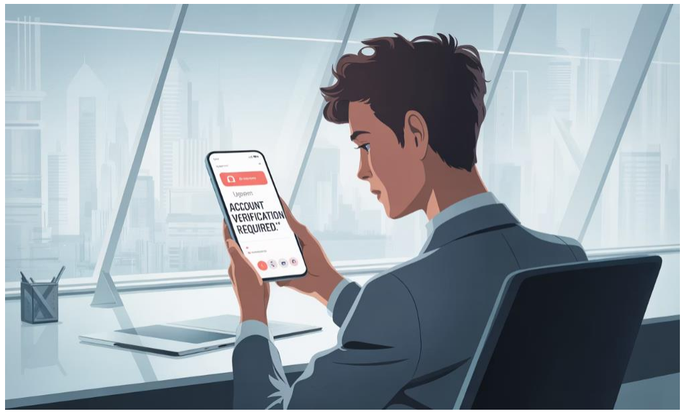
Stealing sensitive business data, trade secrets, or intellectual property from competitors.

Disruption & Sabotage

Creating chaos through DDoS attacks, ransomware, or system shutdowns to damage operations.

Cybersecurity Scenarios: Can You Spot the Threats?

The Urgent Bank Email

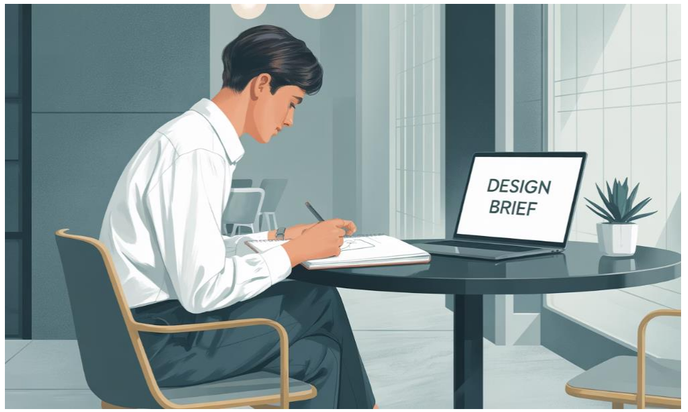


You receive an email from your "bank" asking you to urgently update KYC details by clicking a link. The email looks official but something feels off.

What type of cybercrime is this?

Phishing Attack

Free Café Wi-Fi Trouble



Whilst connected to free café Wi-Fi, you log into your Gmail account. Later, you notice unknown logins from abroad in your security settings.

What happened to your account?

Man-in-the-Middle Attack

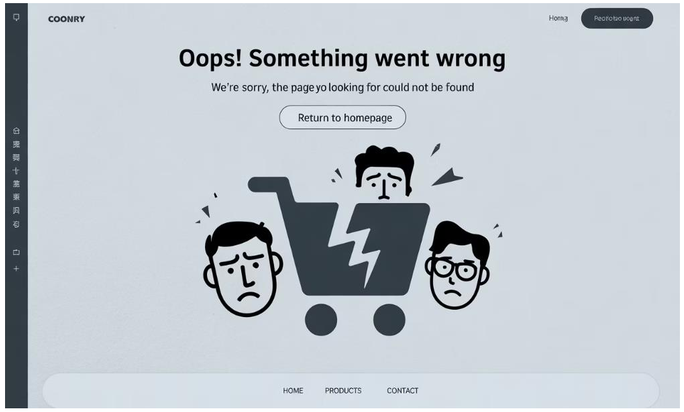
Locked College Files

You try to open your college notes, but all files are locked. A pop-up demands ₹10,000 in Bitcoin to unlock your precious coursework.

What attack has infected system?

Ransomware Attack

Website Goes Down

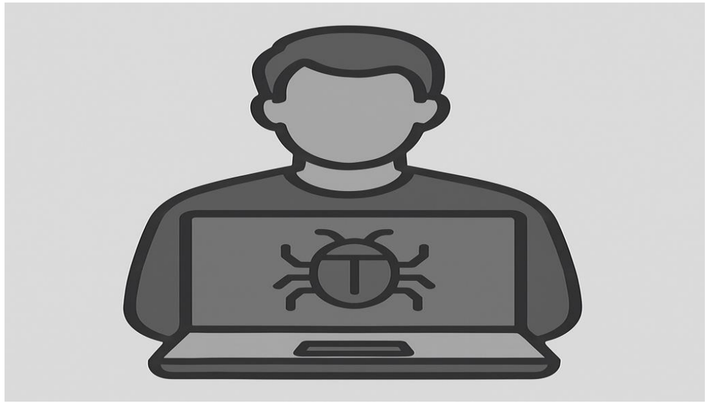


Suddenly, your favourite shopping website goes offline because too many requests flood the server simultaneously. Legitimate users cannot access the site.

What type of attack caused this?

DDoS Attac

Free downloads…expensive loss



You download a “FREE cracked version” of a popular game from an unknown website. After installing, the laptop starts behaving strangely — files disappear, weird ads, and passwords get stolen. Later your bank account is compromised

What type of cyber attack is this?

Malware/virus Attack

Library System Breach

On the library site search box, a student types ' OR '1'='1 instead of a book name. Suddenly, the system shows all records including admin information.

What coding vulnerability was exploited?

SQL Injection Attack

Printed from
THE TIMES OF INDIA

Servers of two city hospitals hacked; police register FIR

TNN | Jun 13, 2025, 11.40 PM IST

New Delhi: Delhi Police has registered an FIR after the servers of two hospitals in north Delhi, Sant Parmanand Hospital in Civil Lines and NKS Super Speciality Hospital in Gulabi Bagh, were allegedly hacked. Patient data, financial records and administrative files were accessed during the breach, which took place late Tuesday night.

The cyberattack allegedly led to major disruptions in the functioning of both hospitals, prompting police action under relevant sections of the IT Act. "A case has been registered under section 66 (Computer related offences) of the Information and Technology Act and the help of technical experts is being taken to trace the source of the hack," DCP (north) Raja Banthia said.

Pakistani hackers attacked 1.5 million-plus Indian websites after Operation Sindoor: Failure rate, names of 7 Pakistani hacker groups; techniques used and more

TOI Tech Desk / TIMESOFINDIA.COM / Updated: May 14, 2025, 10:47 IST

Share | AA | Follow Us

Following the Pahalgam terror strike, Maharashtra Cyber identified seven APT groups, primarily Pakistan-allied, responsible for over 1.5 million cyber attacks targeting critical Indian infrastructure. While only 150 attacks succeeded, these groups employed malware, DDoS attacks, and misinformation campaigns. The attacks originated from Pakistan, Bangladesh, the Middle East, and Indonesia, with some successful defacements and alleged data theft.

Read Less

ETPrime

Cyber hackers launched 650 attacks on Indian infrastructure between May 7–10: Report

ETtech • Last Updated: May 23, 2025, 09:06:24 PM IST

FOLLOW US | SHARE | FONT SIZE

Synopsis

The cyber assault by Pakistan-aligned actors began on April 17, weeks before India's counterterrorism strikes under Operation Sindoor. Quick Heal Technologies' Seqrite Labs, a malware analysis facility, identified 650 spear-phishing attacks, malware infections, website defacements, and data leaks carried out by 35 hacktivist groups.

Types of Cyber Attacks

Type	What It Is	Example
Malware / Virus Attack	Malicious code to damage systems, steal data, or spy.	*Servers of two Delhi hospitals hacked — June 2025*
Ransomware Attack	Data encrypted, ransom demanded to unlock.	*AIIMS Delhi ransomware attack (2022)* disrupted hospital servers.
Denial of Service (DoS/DDoS)	Flooding traffic to crash websites/servers.	*Indian govt portals attacked post-geopolitical conflict (2022).*
Phishing / Spear-Phishing	Fake emails/websites to steal login or banking info.	*Fake RBI emails offering Covid-relief in 2021.*
SQL Injection / Exploit Attacks	Injecting malicious queries into databases.	*Indian e-commerce sites targeted (2023).*
Man-in-the-Middle Attack	Criminal intercepts communication between two parties.	*Banking details stolen on unsecured Wi-Fi networks.*

Common Cyber Fraud/Digital Fraud Scams

Digital Arrest Scam

Investment and Trading Scam

WhatsApp-delivered Malicious APK Scam

Sextortion Scam via Video Call

Online Job and Lottery Scams

Digital Arrest Scam

Contact

Impersonated official calls.

Accusations

Claims of money laundering, tax evasion.

Pressure

Threats of arrest, fake warrants.

Fake Authority

Accomplices pose as officers.

Demand Payment

Demand 'fine' to avoid arrest.

Printed from
THE TIMES OF INDIA

‘Digital arrest’ scam: Retd BHEL supervisor loses Rs 68 lakh

TNN | Sep 13, 2025, 12.48 AM IST

Bhopal: A 71-year-old retired BHEL supervisor has fallen victim to a two-month-long "digital arrest" scam, losing Rs 68.3 lakh to cyber fraudsters who posed as officials from the CBI, Delhi Police and the Telecom Dept. The criminals falsely accused him of involvement in terrorism, money laundering, and human trafficking.

According to police, the complainant, 71, received a WhatsApp call from fraudsters who introduced themselves as senior officers. They falsely claimed that a SIM card was issued using his Aadhaar card in Chandni Chowk, Delhi, and was being misused for illegal activities.

Printed from
THE TIMES OF INDIA

Elderly man duped of Rs 3.72 cr in 'virtual arrest' scam in Kollam

Sep 14, 2025, 12.03 AM IST

Kollam: A 79-year-old man lost Rs 3.72 crore in a ‘virtual arrest’ cyber fraud case in Kollam.

According to police, the victim received a WhatsApp call on July 7 from a person who introduced himself as a BSNL official.

He claimed that the victim's mobile number was under the scrutiny of Mumbai cyber police for its alleged use in illegal activities. Subsequently, another person, appearing on a WhatsApp video call in police uniform, introduced himself as a Mumbai cyber police officer. alleged that a bank account was fraudulently opened using the victim's Aadhaar details and was being misused for criminal activities..

Investment and Trading Scam

Initial Contact

Victim contacted on social media with 'exclusive' offer.

Fake Platform

Manipulated platform shows false high returns.

Build Trust

Small investments show inflated returns.

Large Investment

Encouraged to invest large sums, then stolen.

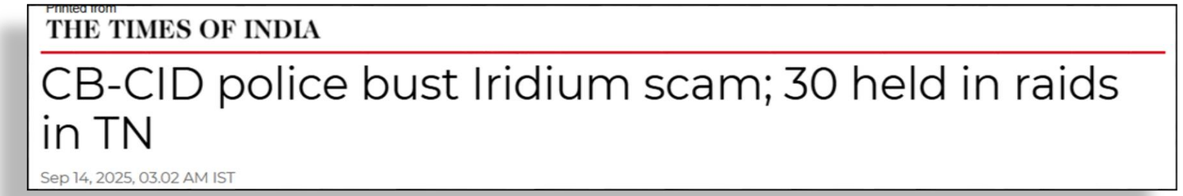
Blocked Withdrawal

Withdrawal requests met with 'taxes' or fees.


Printed from
THE TIMES OF INDIA

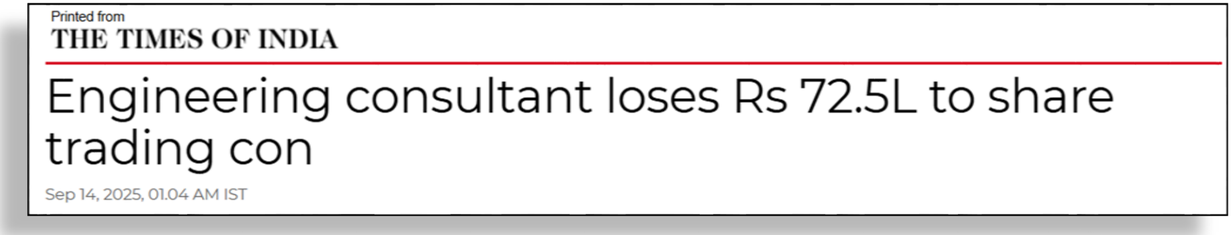
Cybercrooks create fake website of pharma major to dupe investors

Sep 11, 2025, 10.30 PM IST


Printed from
THE TIMES OF INDIA

CB-CID police bust Iridium scam; 30 held in raids in TN

Sep 14, 2025, 03.02 AM IST


Printed from
THE TIMES OF INDIA

Engineering consultant loses Rs 72.5L to share trading con

Sep 14, 2025, 01.04 AM IST

WhatsApp-delivered Malicious APK Scam

Trusted Contact
Receives link from trusted contact

Malware Installs
APK installs, granting data access

Silent Theft
Malware steals data, conducts transactions

Printed from
THE TIMES OF INDIA

Cyber police arrest two men for financial fraud using fake Parivahan app

TNN | Jul 21, 2025, 02.33 AM IST

Kochi: Kochi city cyber police arrested two men from Varanasi who were involved in a nationwide online fraud through a fake Parivahan application. The accused defrauded several people by sending fake APK files via WhatsApp and convincing them that the application was for paying vehicle fines.

Printed from
THE TIMES OF INDIA

Bengaluru man loses Rs 5 lakh after clicking fake RTO challan file

Sep 9, 2025, 05.34 AM IST

Bengaluru: A farmer lost over Rs 5 lakh after he clicked on a message with a link to an apk file named RTO Challan in a WhatsApp group on Aug 15.

Crores lost to WhatsApp scam: Don't fall prey to online scams, know latest scam tricks

Curated by *Ira Alok Puranik*, ET Online | Dec 10, 2024, 05:27:49 PM IST

Sextortion Scam via Video Call

Fake Profile
Attractive profile, friend request, conversation

Recorded Call
Pre-recorded content, secretly records victim

Blackmail
Threatens to share recording for payment

Hindustan Times

Delhi Police busts sextortion, cyberfraud rackets, 6 held

PTI |

Published on: Jun 03, 2025 07:36 pm IST

Delhi Police busts sextortion, cyberfraud rackets, 6 held

According to the police, a money trail of over ₹5 crore has been identified by different teams of Crime Branch.

Printed from
THE TIMES OF INDIA

Police bust sextortion racket using fake SIM cards and synthetic accounts in Delhi

TNN | Jun 18, 2025, 09.40 PM IST

New Delhi: Police have busted a sextortion module and arrested two accused linked to over 60 cybercrime complaints for defrauding over 100 people across the country.

Online Job and Lottery Scams

Modus Operandi

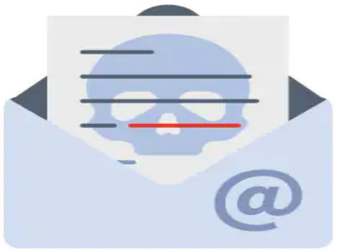
1. Victim receives message about job opportunity or lottery win
2. Asked to pay "processing fee," "registration charges," or "verification amount"
3. May be asked to complete small tasks initially to build trust
4. Promised compensation never materializes
5. Communication cuts off after payment

Red Flags

- Jobs offering high pay for minimal work
- Winning lotteries you never entered
- Upfront payment requirements

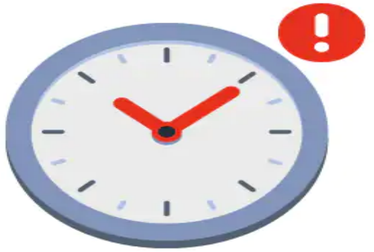
Social Engineering Tactics to Watch For

Knowing the red flags can help you avoid becoming a victim.



Your ‘friend’ sends you a strange message.

Your emotions are heightened.



The request is urgent.

The offer feels too good to be true.

You’re receiving help you didn’t ask for.

The sender can’t prove their identity.

Cyber Hygiene – Do’s & Don’ts

For Individuals

Password Hygiene
Strong, unique passwords with Multi-Factor Authentication enabled

Scam Awareness
Verify suspicious calls, emails, and avoid clicking unknown links

Safe Transactions
Official banking apps only. Never share OTP, CVV, or PIN details

Device Protection
Updated antivirus, OS, and applications for robust security

Social Media Care
Limit personal information sharing and verify friend requests

Emergency Response
Report incidents immediately to 1930 or cybercrime.gov.in

For Organisations

Security Framework
Zero Trust Architecture with regular system updates and patches

Access Control
Multi-factor authentication and role-based access monitoring

Employee Training
Regular cyber hygiene sessions and phishing simulations

Data Protection
Encrypted data storage with regular offline backup systems

Incident Response
Security Operations Centre with tested response protocols

Compliance
CERT-In, RBI guidelines with mandatory incident reporting

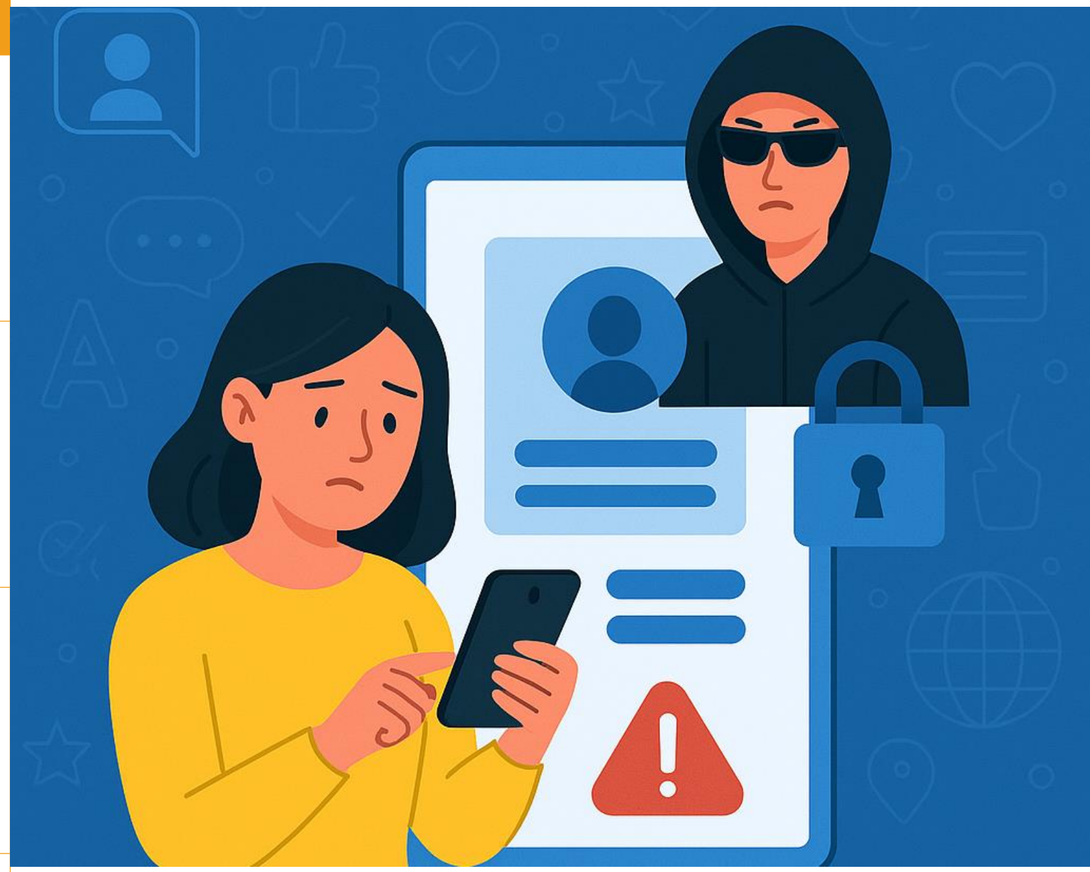
Keep Your Smartphone Safe: Mobile Hygiene Tips

☑ Do This	✕ Avoid This
Lock your phone with PIN or biometrics	Leaving phone unlocked in public
Use only official app stores	Installing APKs from unknown sources
Enable remote tracking & wipe options	Ignoring theft/loss preparedness
Update apps and OS regularly	Skipping security patches
Set app permissions carefully	Allowing full access unnecessarily
Turn off Bluetooth/Wi-Fi when not in use	Staying connected to open networks

भादूविप्रा
TRAI

Be Smart on Social Media

☑ Do This	✖ Don’t Do This
Set your account to ‘Private’ — control who sees your posts and stories.	**Don’t overshare** — birthday, Aadhaar, or bank details don’t belong on the internet.
Review app permissions — limit access to your location, contacts, photos.	**Don’t accept friend requests from strangers** — scammers often pose as known people.
Think before you post — personal info like phone number, school, or vacation plans can be misused.	**Don’t click on “giveaway” or free gift links** — most are phishing traps.
Follow only verified accounts — beware of lookalike or fake profiles.	**Don’t reuse the same password across apps** — one breach = all accounts exposed.



भादूविप्रा
TRAI

What to do incase you fall a victim to Cyber Crime?

Call ***1930*** and report.

Inform your bank that you've been a victim.

File a complaint *https://cybercrime.gov.in* with additional details

Remember:

It is good to report as early as possible.

DoT’s Citizen Centric Initiatives

(sancharsaathi.gov.in)

Empowering citizens -Sanchar Saathi portal/ App: www.sancharsaathi.gov.in

Citizen Centric Services

1. CHAKSHU - REPORT SUSPECTED FRAUD & UNSOLICITED COMMERCIAL COMMUNICATION / SPAM
2. BLOCK YOUR LOST / STOLEN MOBILE HANDSET
3. KNOW MOBILE CONNECTIONS IN YOUR NAME
4. KNOW GENUINENESS OF YOUR MOBILE HANDSET
5. REPORT INCOMING INTERNATIONAL CALL WITH INDIAN NUMBER
6. KNOW YOUR WIRELINE INTERNET SERVICE PROVIDER
7. New — TRUSTED CONTACT DETAILS

Regional languages – Inclusive Approach

25 Cr+ visitors

Real time Dashboard

Jan Bhagidari to fight cyber frauds – Our Citizens our Strength

CHAKSHU

SUSPECTED FRAUD COMMUNICATIONS

Report Suspected Fraud Communication facility

चक्षु - Report Suspected Fraud Communication

(Report any suspected fraud communication received within last 30 days)

Chakshu

Chakshu facilitates citizens to report the suspected fraud communications with the intention of defrauding telecom service users for cyber-crime, financial frauds, non-bonafide purpose like impersonation or any other misuse through Call, SMS or WhatsApp.

Few examples of suspected fraud communications are communication related to Bank Account / Payment Wallet / SIM / Gas connection / Electricity connection / KYC update / expiry / deactivation, impersonation as Government official / relative, sextortion related etc.

Note: If you have already lost money due to financial fraud or are a victim of cyber-crime, please report at cyber crime helpline number 1930 or website https://www.cybercrime.gov.in. Chakshu facility does not handle financial fraud or cyber-crime cases.

Continue for reporting →

Medium of Suspected Fraud Communication

Please select how you received the communication*

Medium
Select Medium

- Select Medium
- Call
- SMS
- WhatsApp

Suspected Fraud Communication Details

All * marked fields are mandatory.

Select Suspected Fraud Communication Category

Category
Select Category

- Select Category
- KYC related to Bank / Electricity / Gas / Insurance policy etc
- Impersonation as Government official / relative
- Fake Customer Care Helpline
- Online job / lottery /gifts/loan offers
- Sextortion
- Multiple automated / robo communication
- Malicious link / website
- Any Other Suspected Fraud

Complaint details

500 characters remaining

Proactive citizen reporting, **OTP** based verification, **Computer vision** on screenshot uploaded, Real time **dashboard**

Personal details

All * marked fields are mandatory.

Enter your name*

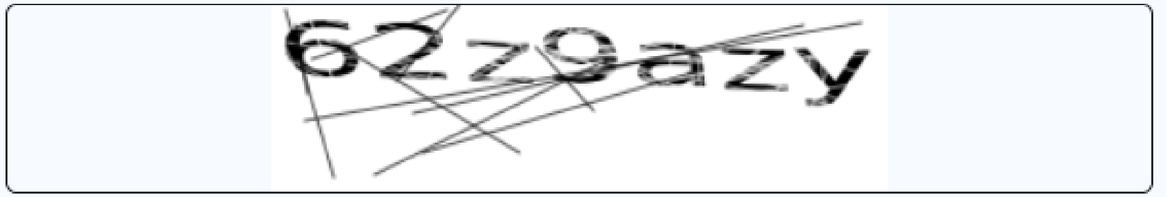
First Name

Last Name

Enter the phone number on which suspected fraud communication was received*

+91 9999999999

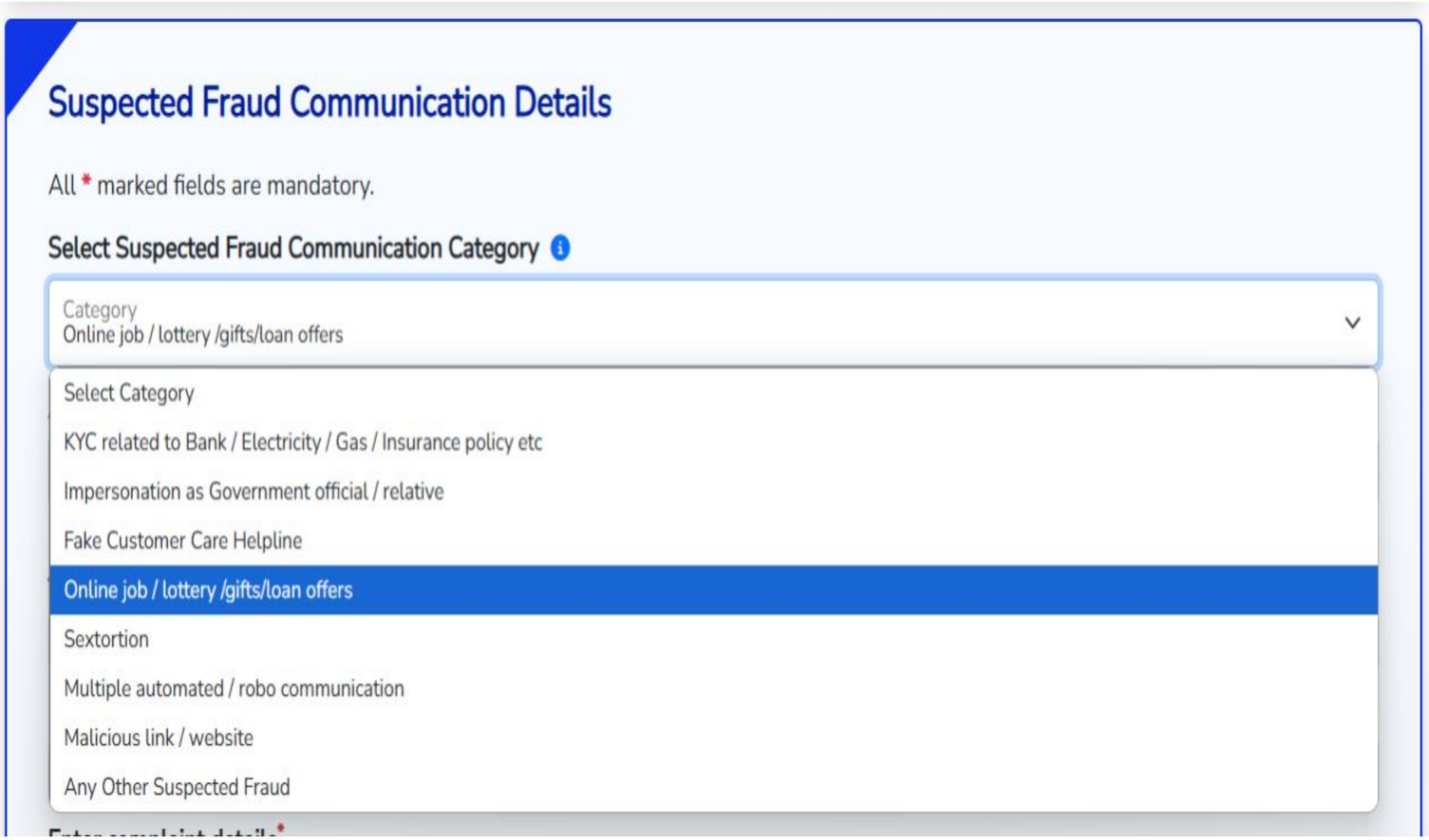
OTP Verification and Submission



Enter the text in image

Verify Mobile via OTP

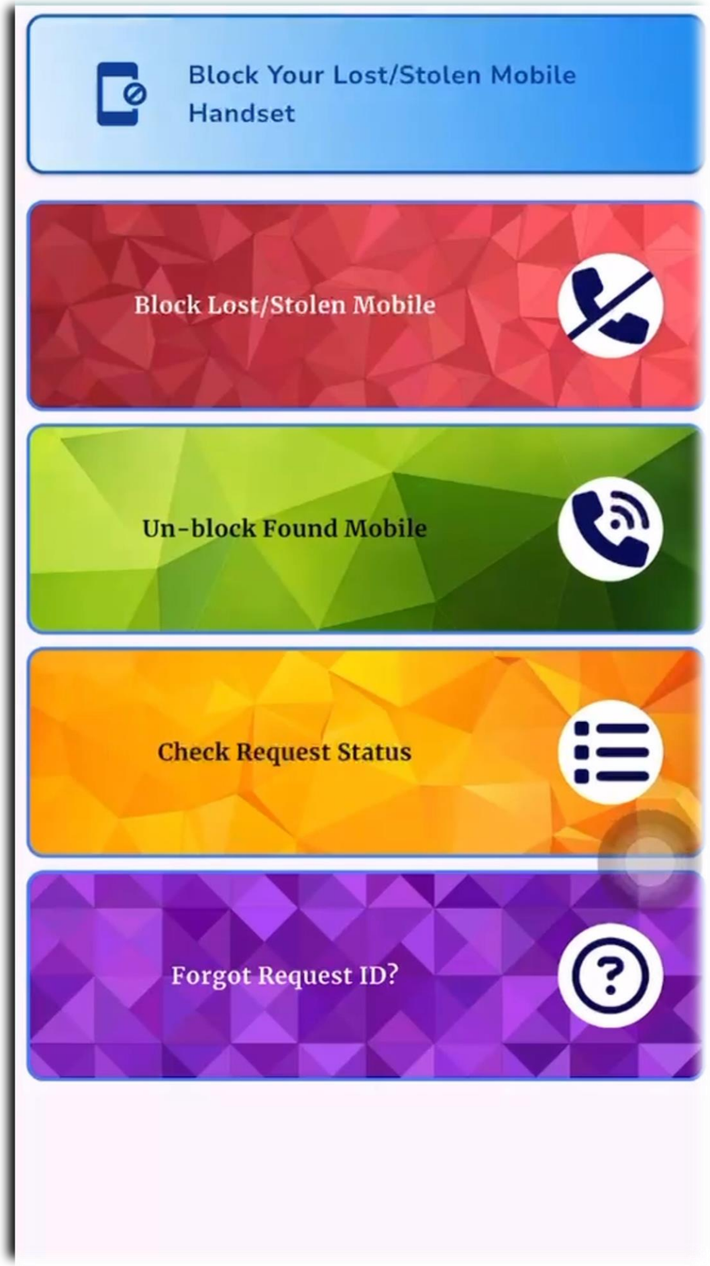
Sanchar Saathi- Facilities
चक्षु - Report Suspected Fraud Communication



CEIR

REPORT LOST/STOLEN MOBILES

BLOCK YOUR LOST/STOLEN MOBILE HANDSET



- Online reporting by Citizens & Police
- Pan India blocking and tracing across TSPs
- Unblocking once found and returned to owner

- Integrated with Crime and Criminal Tracking Network & Systems (**CCTNS**), Zonal Integrated Police Network (**ZIPNET**) of Police
- Real time tracing reports to **15000+ police stations** across country

- Traceability reports to citizens
- Real time status update
- Tracking of request
- Paper less, hassle free

BLOCK YOUR LOST / STOLEN MOBILE HANDSET

42.30 lakh+ mobiles blocked

26.21 lakh+ mobiles traced

Block your lost / stolen mobile handset

Block lost / stolen mobile handset
CLICK HERE

Unblock found mobile handset
CLICK HERE

Check lost / stolen mobile handset request status
CLICK HERE

Forgot request ID
CLICK HERE

CEIR Services | Applications | Contact Us | Help | Public Notices | How to block? | Login

- Block Stolen/Lost Mobile
- Un-Block Found Mobile
- Check Request Status
- Forgot Request ID

equest for blocking lost/stolen mobile

CEIR service is now available for all India subscribers.

 # All (*) marked fields are mandatory.

Request for blocking lost/stolen mobile

CEIR service is now available for all India subscribers.

 # All (*) marked fields are mandatory.

Device Information

Mobile Number 1* +91 Mobile Number 1

Mobile Number 2 +91 Enter if dual sim mobil

IMEI 1 Enter 15 digit IMEI Number

IMEI 2 Enter if dual sim mobile

Device Brand* Select

Device Model Device Model

Upload invoice Choose File No file chosen

Lost Information

Lost Place* Lost Place

Lost Date* 2024-04-24 17:14:40

Select State/UT* Select

Select District* Select

Select Police Station* Select

Police Complaint Number* Police Complaint Number

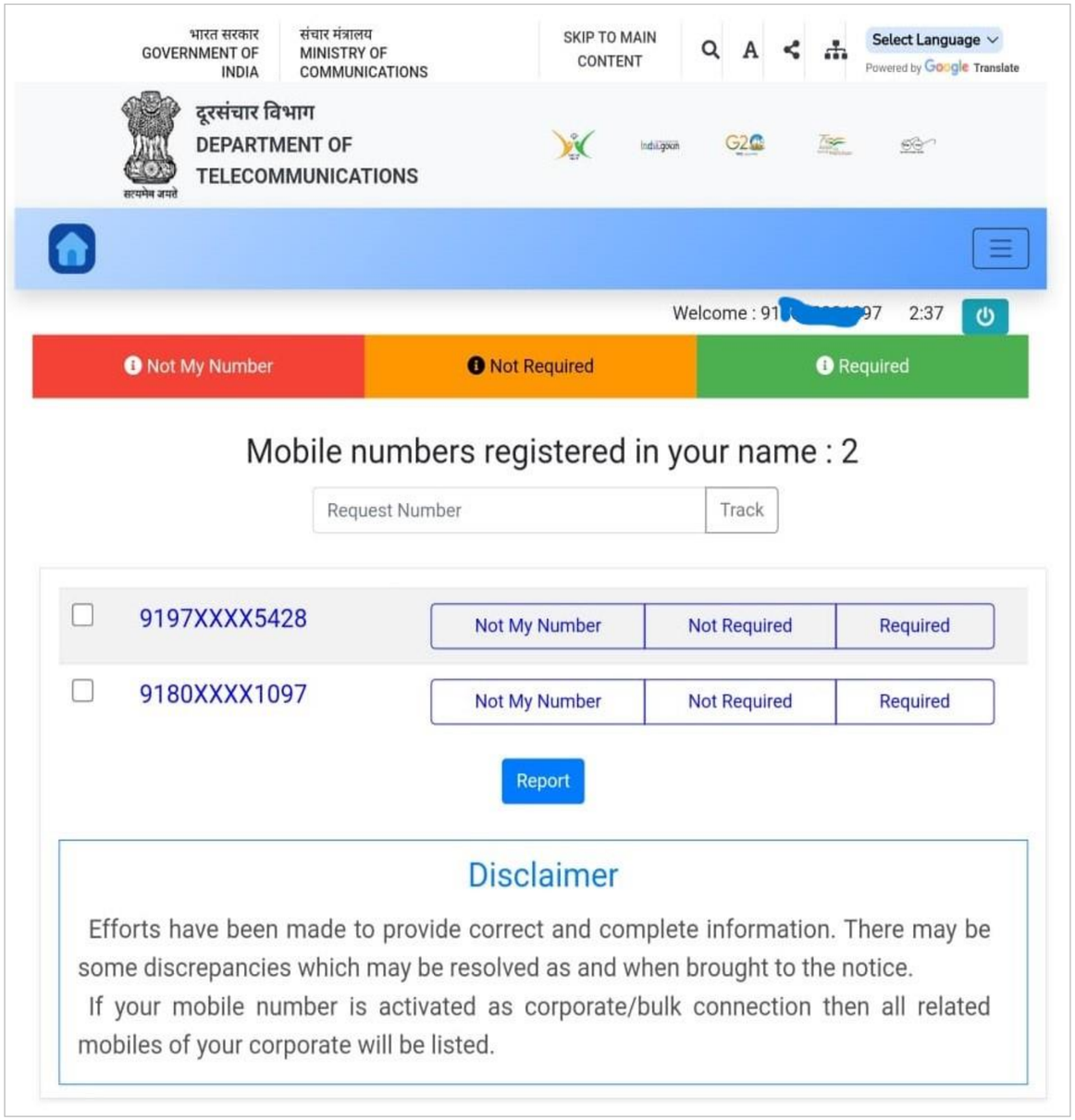
Upload Police Complaint* Choose File No file chosen

+Add more

TAFCOP

KNOW YOUR MOBILE CONNECTIONS

Know Your Mobile Connections facility



- Check all mobile connections in your Name
- Unique grouping created
- AI powered backend

Citizens can report mobile connection

- **Not My Number**
- **Not Required**
- **Required**

- Integrated with TSPs
- Automated process of re-verification,
- Real time status update
- Tracking of request
- Paper less, hassle free

Citizen Centric Service

- Chakshu – Report Suspected Fraud Communication
- Block Your Lost/Stolen Mobile Handset
- Know Mobile Connections in Your Name
- Know Genuineness of Your Mobile Handset
- Report Incoming International Call with Indian Number

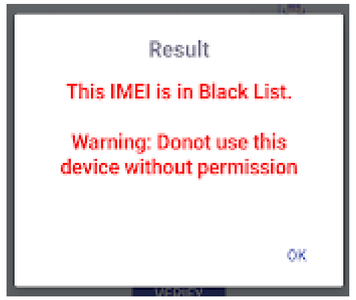
KYM

Know Your Mobile facility for IMEI verification

Citizen Centric Service

- Chakshu – Report Suspected Fraud Communication
- Block Your Lost/Stolen Mobile Handset
- Know Mobile Connections in Your Name
- Know Genuineness of Your Mobile Handset
- Report Incoming International Call with Indian Number

Help in checking Genuineness of Mobile handset



RICWIN

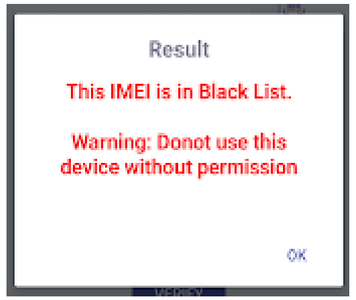
FOR

REPORTING INTERNATIONAL CALLS THROUGH INDIAN NUMBERS

Citizen Centric Service

- Chakshu – Report Suspected Fraud Communication
- Block Your Lost/Stolen Mobile Handset
- Know Mobile Connections in Your Name
- Know Genuineness of Your Mobile Handset
- Report Incoming International Call with Indian Number

Help in checking Genuineness of Mobile handset



Report Incoming International Call With Indian Number (RICWIN)

Alternatively you can report on 1963/1800110420

International call details

All * marked fields are mandatory.

Receiving Mobile Number *

+91 Enter your 10 digit Mobile Number on which call was received

Indian Number displayed during the call *

+91 max 10 digit Indian Number displayed during the call

Date of the call *

Time of the call

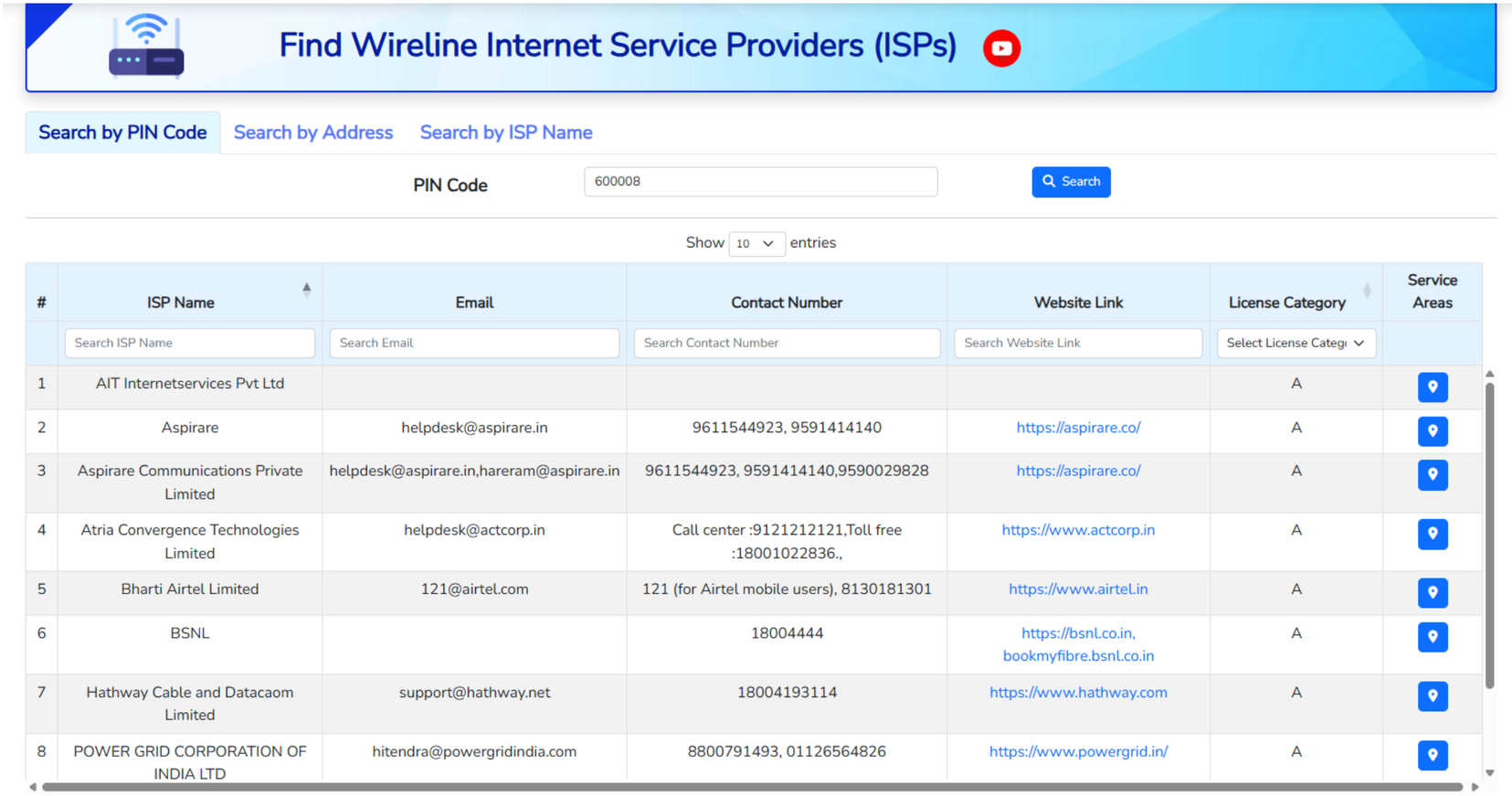
Country from where the International call is received

Select Country

Any other information you want to share

Remark

Know Your
Wireline Internet Service Provider

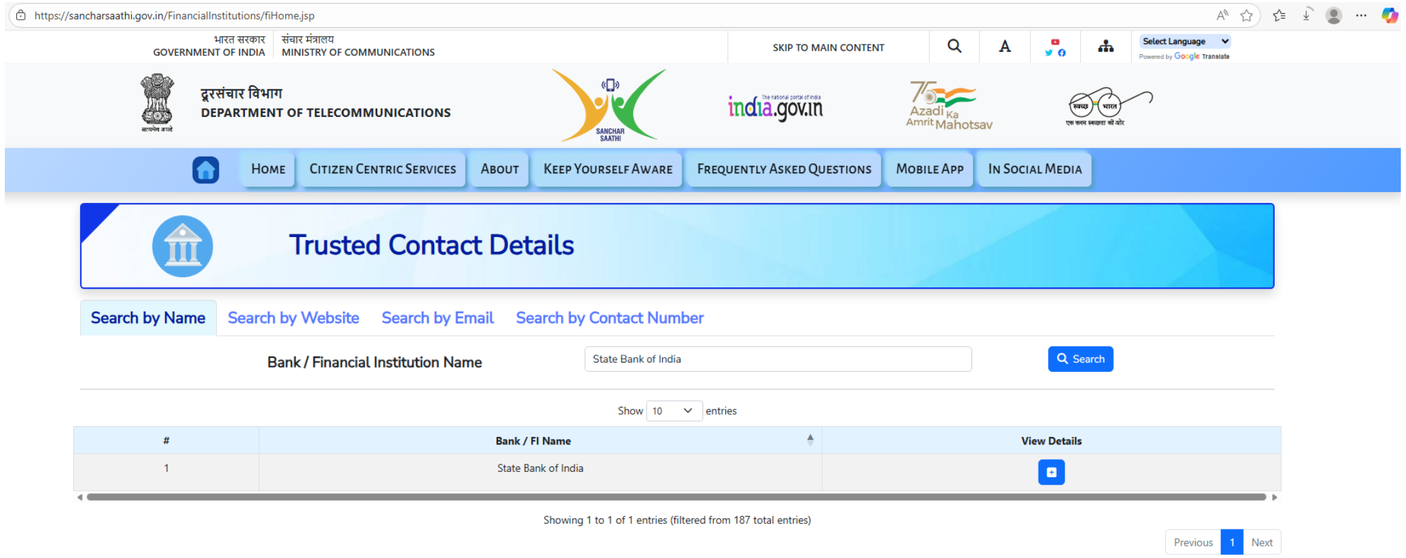


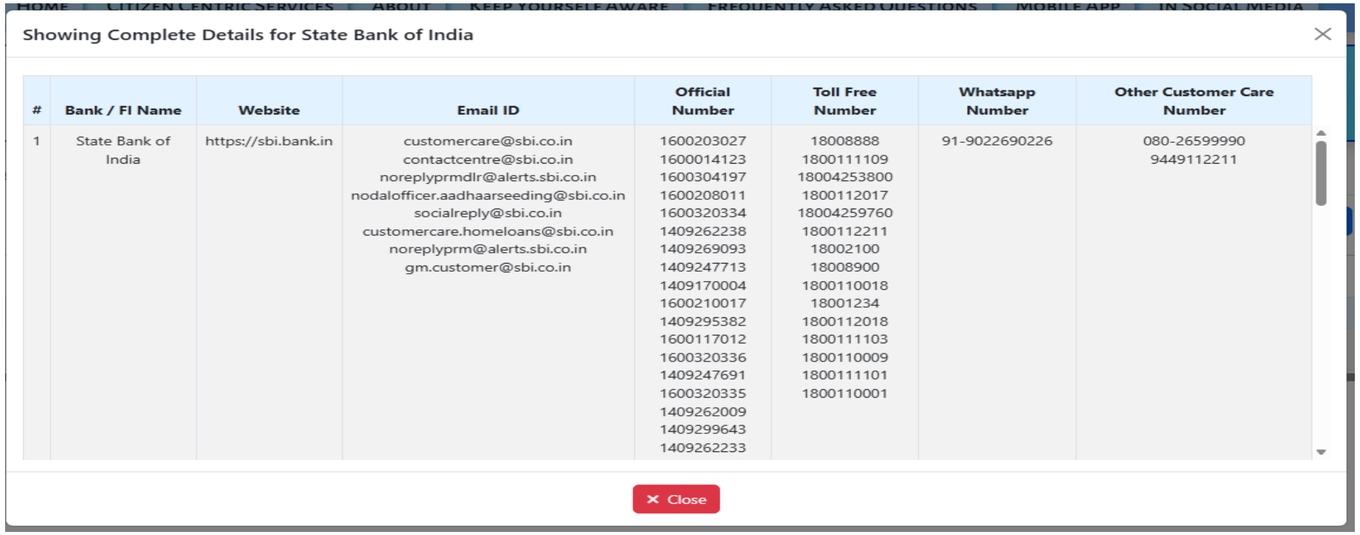
#	ISP Name	Email	Contact Number	Website Link	License Category	Service Areas
	Search ISP Name	Search Email	Search Contact Number	Search Website Link	Select License Categ	
1	AIT Internetservices Pvt Ltd				A	
2	Aspirare	helpdesk@aspirare.in	9611544923, 9591414140	https://aspirare.co/	A	
3	Aspirare Communications Private Limited	helpdesk@aspirare.in,hareram@aspirare.in	9611544923, 9591414140,9590029828	https://aspirare.co/	A	
4	Atria Convergence Technologies Limited	helpdesk@actcorp.in	Call center :9121212121,Toll free :18001022836.,	https://www.actcorp.in	A	
5	Bharti Airtel Limited	121@airtel.com	121 (for Airtel mobile users), 8130181301	https://www.airtel.in	A	
6	BSNL		18004444	https://bsnl.co.in, bookmyfibre.bsnl.co.in	A	
7	Hathway Cable and Datacaom Limited	support@hathway.net	18004193114	https://www.hathway.com	A	
8	POWER GRID CORPORATION OF INDIA LTD	hitendra@powergridindia.com	8800791493, 01126564826	https://www.powergrid.in/	A	

- Enables citizens to verify Wireline Internet Service Providers (ISPs) and check their presence across the country using PIN code, address, or ISP name.

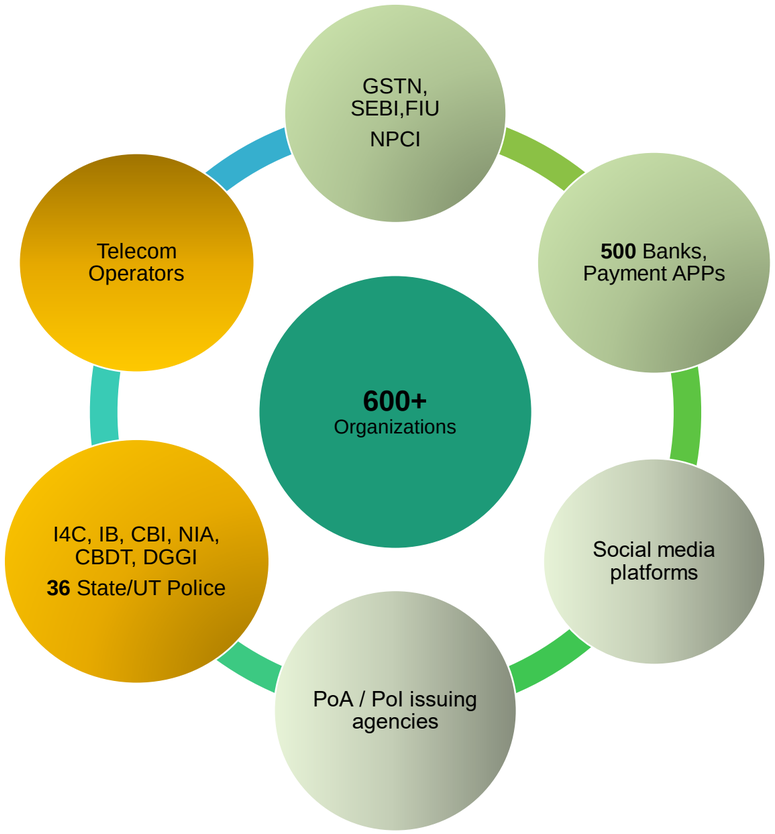
Sanchar Saathi- **Trusted Contact Details**

- All emails IDs, contact numbers (toll free/ 140/ 160 series), website details, WhatsApp number
- Facility for uploading tollfree, customer care available for Banks, FIs on DIP
- Whitelisted by TSPs
- 250 banks have shared data



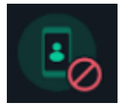


Sanchar Saathi: Outcomes & Impact



Near Real Time Intelligence Sharing

2+ Crore
Mobile connections disconnected



2.2 Lakh
WhatsApp Accounts, groups and Communities disengaged

42.30 Lakh
Total handsets blocked

26.21 Lakh
Handsets traced

7.28 Lakh
Handsets recovered

Collaborative Citizen Awareness with District Administration, State Government

Sanchar Saathi awareness on Pune Smart City Displays

Arunachal Pradesh State Government's awareness through websites

Sanchar Saathi Posters, Banner, Video Links for Public Awareness on pan India basis	
Sanchar Saathi awareness materials (website banner, standee, backdrop, and short video):	https://drive.google.com/drive/folders/1vZapT123lqQdLpJKoaoAnPGYiU1bUJFN
All 6 citizen centric features of Sanchar Saathi	https://youtu.be/xtHFviq_-ac?si=VlfgleUNIlI8LGrR
Report Your Lost/Stolen Handset	https://youtu.be/nSxeK_seERE?si=LnqUL16Ka0CNthhO
CHAKSHU	https://youtu.be/5lWWhlqaJmI?si=7pnyjpCa7mPSxdcL
Know Your Mobile Connections	https://youtu.be/JIZzww0S51Y?si=tqLEDlN-rKJ5NYcJ
Chakshu- UCC / Spam	https://www.youtube.com/watch?v=0K6q92Y7Rm8
Know Your Mobile (KYM)	https://youtu.be/X7ufwI4Z2Wo?si=iNWzDBqGTddFyLjZ
Know Your Wirelines Internet Service Provider (KYI)	https://youtu.be/MGJn4iXRBr4?si=XrPVbZVelVYP98Lg
Report Incoming International Call With Indian Number (RICWIN)	https://youtu.be/4D6HdrnInjc?si=M54Klad-v3w1KKjx
International Spoofed Calls	https://youtu.be/0mApNOtkZL8?si=cbjr0EEqp9rV636w

ASTR

Artificial Intelligence and Facial Recognition powered Solution for Telecom SIM Subscriber Verification

ASTR (अस्त्र)

Breaking the Nexus of cyber-crime and fake SIMs

ASTR Analysis

100 SIMs, 76 names posing male and female

ASTR (अस्त्र) Pan India Analysis	
No. of mobile connections analyzed	134 Cr
Suspected connections detected	66.98 lakh
Disconnected after re-verification	65.25 lakh
PoS (SIM Agents) blacklisted	70,895
Total FIRs registered	365
No. of PoS against whom FIR lodged	1,890

FRAUD

FRI

Financial Fraud Risk Indicator

Financial Fraud Risk Indicator (FRI)

Launched May 2025 by DoT's Digital Intelligence Unit

Medium Risk
Flagged for potential suspicious activity patterns

High Risk
Elevated fraud probability requiring additional verification

Very High Risk
Immediate intervention recommended to prevent fraud

Data Intelligence Sources

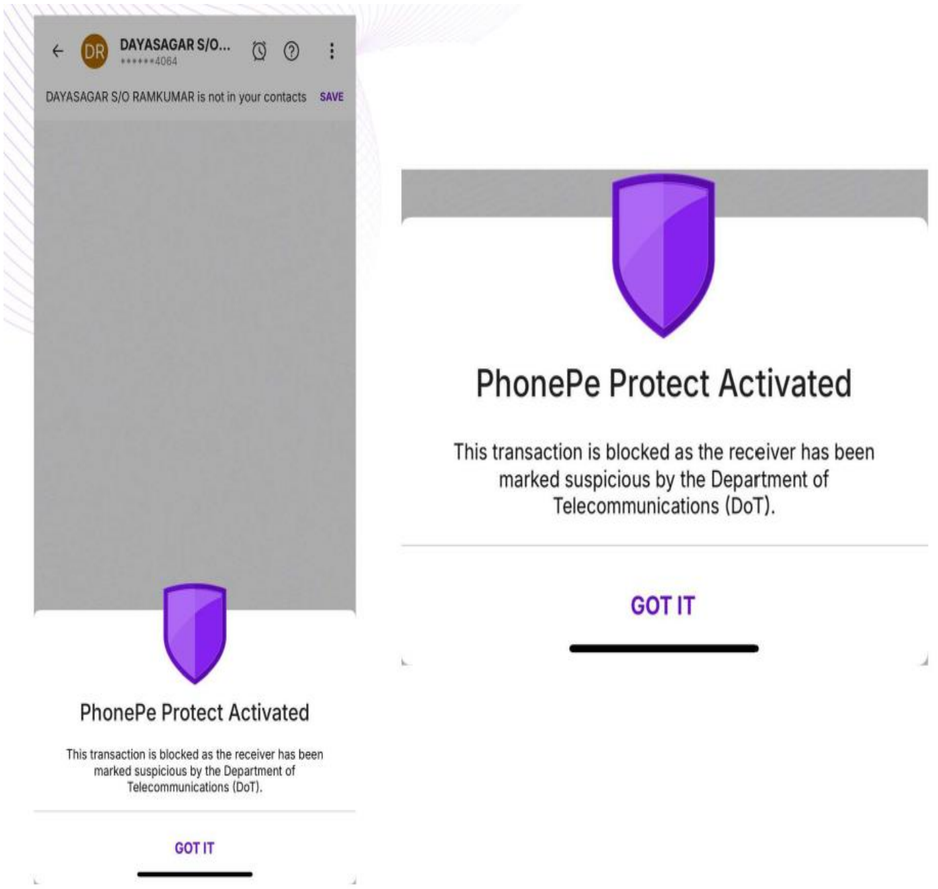
- **NCRP Portal**
- **Chakshu Platform**
- **Financial Institutions**

Real-time Protection

Banks and UPI applications leverage FRI data to decline, delay, or warn users about suspicious transactions, safeguarding millions of digital payment users.

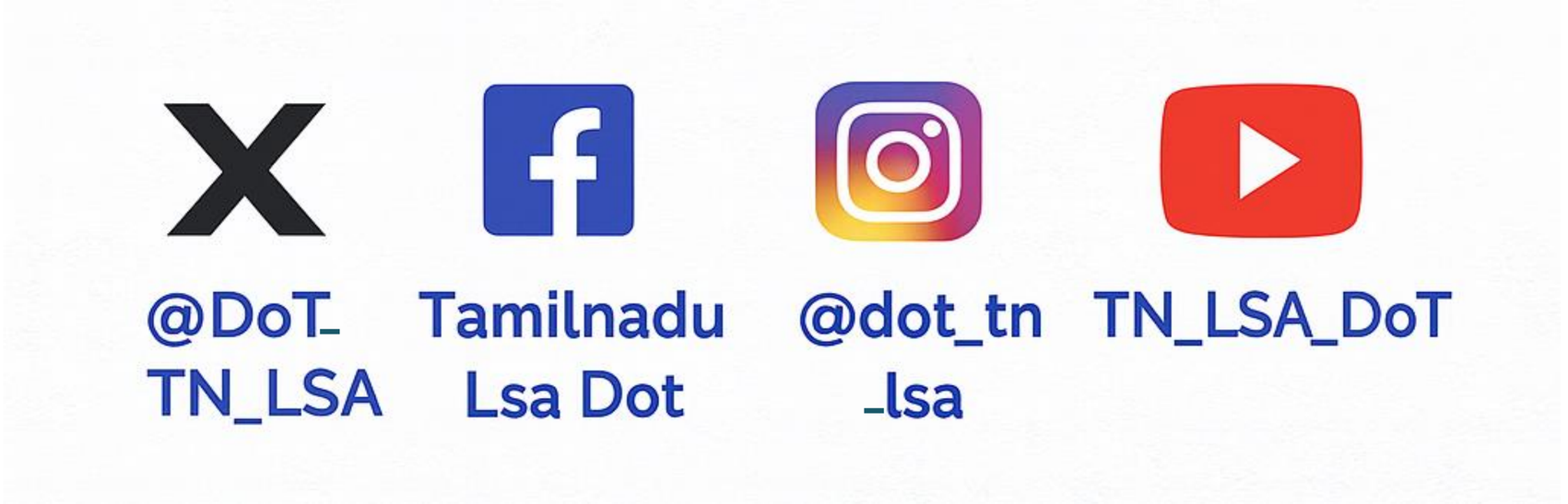
Volume of UPI Transactions

19.47B	**25.08 Lakh crores**
Total Transactions	Transaction Value
628M	**₹80,919 crores**
Daily Average	Daily Value



PhonePe integrated with DIP's FRI displays alert for suspected numbers

Follow us on !!



Thank you !!