

CENTRAL RESERVE POLICE FORCE

DECEMBER-2025

# CYBER BYTE



Govt confirms Indian airports were hit by cyber attack involving GPS spoofing

New Cyber Fraud: Aadhaar + SIM = UPI Hijack

# 1. CYBER GEEKS NEWS

## (A) Govt confirms Indian airports were hit by cyber attack involving GPS spoofing

The central government has confirmed reports that seven major airports across India were targeted by cyber attacks, leading to disruptions at key aviation hubs. The confirmation follows reports of technical anomalies, including the spoofing of navigational systems, at several big airports nationwide.



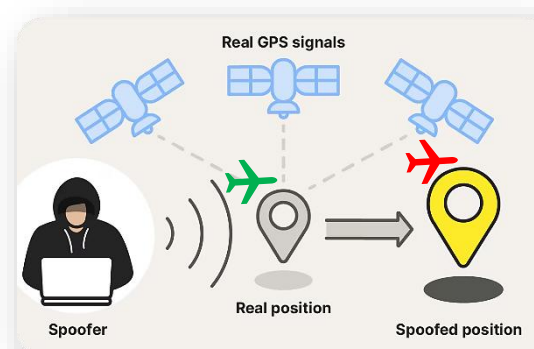
According to a report, Union Civil Aviation Minister informed the Parliament that flights approaching these airports reported GPS spoofing while using GPS-based landing procedures at Runway 10 of the IGI Airport in Delhi. The government acknowledged that the airports of Delhi, Mumbai, Kolkata, Hyderabad, and Bengaluru were among those affected by the cybersecurity incidents.

The primary mode of the cyber attack involved the reported spoofing of Global Positioning System (GPS) signals, particularly affecting flights approaching the Indira Gandhi International Airport in Delhi. GPS spoofing occurs when false GPS signals are broadcast to receivers, misleading aircraft navigation systems about their actual position and altitude.

### What exactly is GPS spoofing?

GPS spoofing is when someone sends fake GPS signals to a device so it thinks it's in the wrong place. Normally, GPS devices figure out their location by listening to signals from satellites, but spoofing replaces those real signals with stronger, fake ones. As a result, the device calculates a false position or time. In simple terms, it's a trick that makes GPS receivers believe they're somewhere they're not.

Spoofing, if successful, can mislead aircraft and create errors in route or altitude.



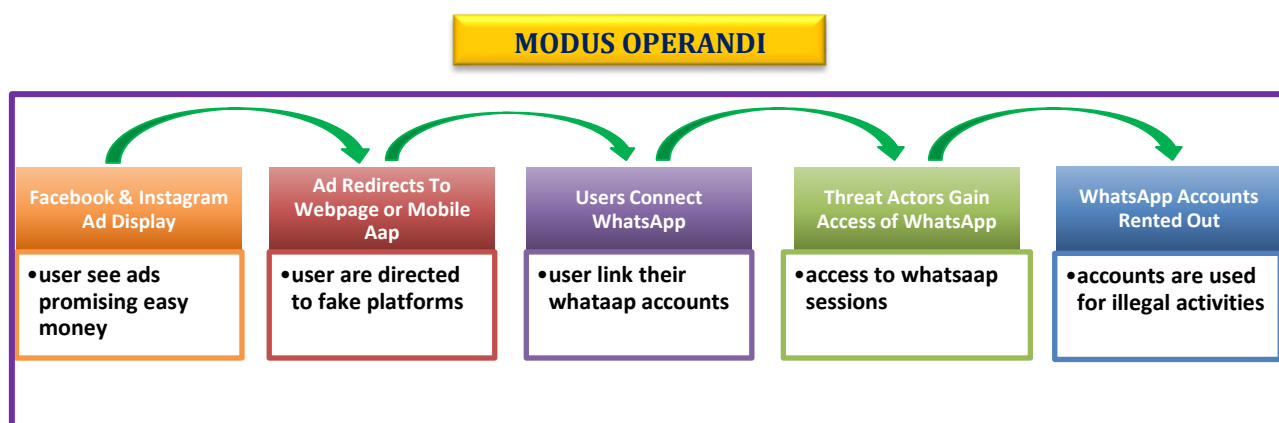
- To enhance cyber security against global threats, AAI is implementing advanced cyber security solutions for IT networks and infrastructure. These actions have been taken in accordance with the National Critical Information Infrastructure Protection Centre (NCIIPC) and Indian Computer Emergency Response Team (CERT-In) guidelines.

- ✚ "Cyber security is ensured by continuous upgradation. As the nature and type of the threat changes, new protective measures are being taken.

## **(B) WhatsApp Web Account Renting Scam – using Facebook & Instagram**

The National Cybercrime Threat Analytics Unit has found a new type of scam spreading through Facebook and Instagram ads. These ads claim that people can “earn money automatically” just by linking their WhatsApp accounts. When users click on these ads, they are taken to fake websites or made to download unsafe **.apk** apps that pretend to be real earning platforms. These sites then ask users to scan a QR code to “activate” their earnings, but the QR code actually gives scammers access to the user’s WhatsApp through the linked-device feature just like WhatsApp Web. Once scammers get in, they start using the person’s WhatsApp as a “mule account” to commit fraud, send scam messages, or perform other illegal activities.

The victim thinks they are joining an earning program, but their WhatsApp is silently taken over and misused. This can put the person in legal trouble, cause data loss, and help criminals spread more scams, so it’s important to avoid such ads and never scan QR codes from unknown sources.



- ✚ Never scan WhatsApp QR codes from unknown apps/websites.
- ✚ Avoid advertisements claiming “automatic income” or “earn ₹5,000 per day”.
- ✚ Do NOT install .apk files from untrusted sources.
- ✚ Check Linked Devices in WhatsApp regularly. (WhatsApp > Settings > Linked Devices)
- ✚ Enable two-step verification in WhatsApp.



### ❖ **! If You Already Scanned Such a QR Code**

- ❖ Immediately open WhatsApp → Linked Devices → Log out from all devices
- ❖ Turn on Two-step verification
- ❖ Run mobile antivirus scan
- ❖ Report the incident at [www.cybercrime.gov.in](http://www.cybercrime.gov.in)
- ❖ Warn your contacts if any unusual messages were sent

## 2. CYBER FRAUDS

### (A) Cyber Fraud Using SIR Process: Fake Enumeration Form Links Target Voter Data and Money: -

Cybercriminals have started a new fraud method by misusing the SIR (Self-Information Report) / voter verification process. They send fake links or messages claiming that citizens must “update voter details,” “fill enumeration forms,” or “complete voter verification to avoid deletion of their name from the voter list.” These links look official but actually redirect users to phishing websites designed to steal personal information such as voter ID details, Aadhaar numbers, phone numbers, and addresses. In many cases, after people enter their details, the website displays a message saying a “verification fee” or “processing charge” must be paid, tricking users into sending money.



The fraudsters use these collected details for identity theft, SIM card fraud, loan scams, or creating fake digital profiles. This scam spreads quickly during election-related activities, as people believe the message is from the Election Commission.



- ✚ Never click voter-related links received via SMS, WhatsApp, or social media.
- ✚ Use only official Election Commission platforms (<https://eci.gov.in>).
- ✚ Do NOT enter voter ID, Aadhaar, or personal details on any site except ECI's official pages.
- ✚ Beware of messages claiming your name will be deleted from the voter list.
- ✚ Never pay any “verification fee” or “processing charge” (Updating voter details is completely free).
- ✚ Check website spelling, fake sites often look similar.
- ✚ Warn family members especially elderly relatives about such scams.
- ✚ Report suspicious links on ([www.cybercrime.gov.in](http://www.cybercrime.gov.in)).

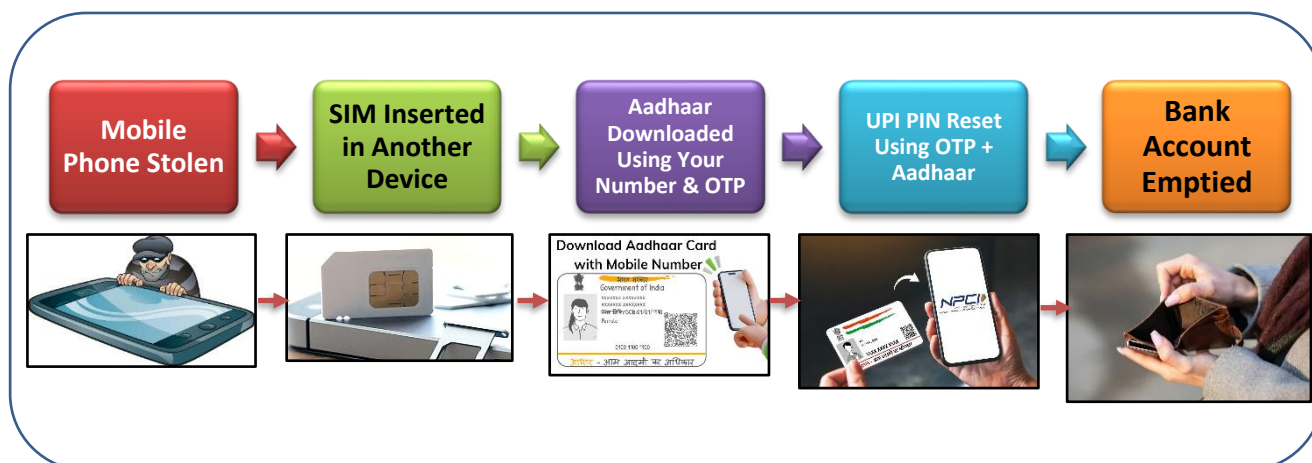
## (B) New Cyber Fraud: Aadhaar + SIM = UPI Hijack

Cybercriminals have started a dangerous new fraud technique where, after stealing a victim's mobile phone, they misuse the SIM card + mobile number to hack UPI accounts. Once they have the phone and SIM, the thieves insert the SIM into another device and use the victim's mobile number to receive OTPs. With these OTPs, they can download the victim's Aadhaar card from official portals, because Aadhaar download requires the registered mobile number and the OTP sent to the registered mobile. After getting the Aadhaar PDF, criminals now have full identity details-name, DOB, address, last four digits of Aadhaar, etc.



Using above information plus the active SIM, they can easily reset the UPI PIN on apps like PhonePe, Google Pay, Paytm, or even the bank's UPI app. Once the UPI PIN is reset, the fraudsters can instantly transfer money, empty bank accounts, and even link the victim's bank account to multiple new UPI apps. This makes mobile theft extremely dangerous today because **stolen phone + active SIM + Aadhaar download = complete UPI takeover within minutes.**

### MODUS OPERANDI



- ✚ Set up a SIM Lock (SIM becomes useless even if removed from the phone).
- ✚ Immediately block your SIM (Call your telecom operator & block the SIM).
- ✚ Disable UPI from your bank.
- ✚ Lock your phone via Find My Device.
- ✚ Report fraud at 1930 & [www.cybercrime.gov.in](http://www.cybercrime.gov.in)



### 3. TIPS OF THE MONTH

#### (a) Lock Down Your SIM (Strongest Defence in 2025): -

Enable SIM Lock / eSIM PIN on your phone. It blocks criminals from using your number for OTP or UPI fraud.

**SIM Lock ON = OTP Fraud GONE**

#### (b) Use Passkeys Instead of Passwords: -

Most major services (Google, Microsoft, Amazon, Paytm, banks) now support passkeys (fingerprint/FaceID-based login), which cannot be phished or hacked easily.



#### (c) Protect Your Aadhaar (Most Targeted in 2025)

- ✚ Lock Your Aadhaar Biometrics using m-Aadhaar app.
- ✚ Regularly check Aadhaar authentication history (Check Where Your Aadhaar Is Used)
- ✚ Use Masked Aadhaar
- ✚ Keep Aadhaar Email & Mobile Updated
- ✚ Avoid Carrying Physical Aadhaar Everywhere



## 4. Cyber Fraud Occurred With CRPF Personnel In Last Month

On 18/11/2025 at approximately 1100 hrs, a Head Constable of 182 Bn was targeted in an **impersonation-based cyber fraud**. The victim received a message from Facebook Messenger, an individual falsely claiming to be a DIG, CRPF. Under this false identity, the caller informed the Head Constable that a Commandant was being posted to his location.

Shortly thereafter, a second individual, impersonating the said Commandant called the Head Constable and stated that he had obtained the Head Constable phone number from the DIG. The impersonator claimed that certain “official luggage” was being dispatched to the Head Constable residence and demanded money under the pretext of parcel delivery and transportation charges. The Head Constable declined the request, citing lack of funds.



The fake DIG again pressured the Head Constable via message, directing him to transfer at least ₹20,000/- immediately, assuring that the balance could be paid after 20 days. Following this, the impersonating “Commandant” contacted the Head Constable on WhatsApp and insisted that the amount be sent through Google Pay/PhonePe. Believing the request to be authentic, the Head Constable transferred ₹20,000/- at 1129 hrs and shared the transaction screenshot. He subsequently received a fabricated invoice carrying a forged CRPF logo and reflecting a remaining due amount of ₹50,000/-.

At about 1500 hrs, the Head Constable received another WhatsApp call from the same fraudster, claiming that the luggage had been dispatched and pressuring him to pay an additional ₹41,000/- as “transport charges,” with a false assurance of instant refund within 10 minutes. The Head Constable refused further payment.

Recognizing the fraudulent activity, the Head Constable immediately informed his Company Commander, 182 Bn, and promptly lodged a complaint with Cyber Crime authorities for necessary investigation and action.



- ✚ If someone claims to be a senior officer, call them on their official number from the directory.
- ✚ Never trust unknown WhatsApp, Facebook, Telegram or messenger calls claiming to be senior officials.
- ✚ Never transfer money based on messages or calls.
- ✚ Do not share transaction proofs, personal documents, ID cards on social media apps.

## 5. New Development in IT DTE

### 1.) SAMBHAV

#### Ticket Based Helpdesk System

New ticket-based helpdesk system has been developed and integrated into the SAMBHAV mobile app to address technical issues faced by forced personnel in various modules such as SANTOS, APAR/IPR, CLMS, e-bill, Ayushman, E-office, NFMS, NIC Mail, pay, PPMS and SAMBHAV etc.





**DG, CRPF Celebrating New Year-2026 with Officers, SOs and Jawans at Directorate premises.**



**DG, CRPF Visited Bawana Camp CRPF**



**DG, CRPF along with President of CWA at Ashray shelter camp at AIIMS.**

**COMN & IT DTE, CRPF**