CENTRAL RESERVE POLICE FORCE

FEBRUARY, 2026

CYBER BYTE

MHA asks agencies to verify complaints before freezing bank accounts in online fraud cases

Hugging Face Infra abused to spread Android RAT in a large-scale malware campaign

IG (COMN & IT) Dte. CRPF

1. CYBER GEEKS NEWS

(A) C-Mitra Initiative Gives Hope to Cybercrime Victims, 100 FIRs Filed in 10 Days: -

The C-Mitra initiative was launched by the Hyderabad Police in Hyderabad, Telangana. In a significant boost to cybercrime victims, the C-Mitra Initiative has successfully facilitated the registration of 100 First Information Reports (FIRs) within just 10 days, marking a major step forward in improving access to justice and timely police action in cyber fraud cases. The C-Mitra Launched with the objective of assisting citizens affected by cybercrime, C-Mitra acts as a bridge between victims and law enforcement agencies. The initiative helps individuals navigate the often complex and intimidating process of filing cybercrime complaints, ensuring that cases are formally registered and acted upon without unnecessary delays.

Officials associated with the initiative stated that many cybercrime victims struggle to get FIRs registered due to lack of awareness, technical complexities, or procedural hurdles. C-Mitra addresses these challenges by providing guidance, documentation support, and coordination with concerned police stations, resulting in faster and more efficient case registration.

Beneficiaries of the initiative have expressed relief and appreciation, noting that timely FIR registration is crucial for freezing fraudulent transactions, initiating investigations, and improving chances of recovery. Several victims reported that they had earlier faced difficulties in getting their complaints acknowledged before approaching C-Mitra. Law enforcement officials have also welcomed the initiative, noting that properly documented complaints help speed up investigations and improve coordination between cybercrime cells and local police stations.

- If you're a victim of cyber fraud, report it immediately. Early reporting increases chances of freezing fraudulent transactions.
- File complaints through the cybercrime helpline **1930** or the official cybercrime portal (**cybercrime.gov.in**).
- An FIR is crucial for investigation and legal action. Initiatives like **C-Mitra** help ensure FIRs are registered smoothly.
- Keep screenshots of messages, transaction details, call logs, URLs, and emails related to the fraud.
- Banks and police never ask for confidential details over calls or messages.

(B) MHA asks agencies to verify complaints before freezing bank accounts in online fraud cases: -

The Ministry of Home Affairs (MHA) has asked law-enforcement agencies and cybercrime units to properly check complaints and confirm a clear connection to online fraud before freezing bank accounts. This decision was taken after concerns that accounts of innocent people and businesses were being frozen due to wrong identification, disputed transactions, or poor verification, causing serious financial problems such as blocked salaries, halted business activities, and difficulty in meeting daily expenses. Under the new approach, agencies must verify complaints or FIRs before ordering a freeze and follow clearer and better-documented procedures under updated cyber fraud rules. The MHA is also improving processes under the National Cybercrime Reporting Portal (NCRP) to ensure better investigations while protecting people from unnecessary financial hardship.

How the process worked earlier (the problem)

Earlier, in many cyber-fraud cases:

- A single complaint on the National Cybercrime Reporting Portal (NCRP)
- or a suspicion-based FIR

(was often enough for police to)

- ask banks to freeze entire accounts, sometimes within hours.
- even if the account holder was only a pass-through or wrongly tagged.

What changes under the MHA's new directions

i. Verification BEFORE freezing

- Verify the complaint (not just accept it at face value)
- Establish a clear link between the account and the fraud
- Check transaction trails, timing, and beneficiary details
- No more freezing just because your account appeared somewhere in the chain

ii. No more "blanket" freezes

(Instead of freezing the entire account, agencies are expected to)

- Freeze only the suspected amount
- Avoid blocking unrelated funds like:
  - Salary
  - Pension
  - business working capital

iii. Stronger paperwork from police

(Before banks act, police instructions should now include)

- FIR / complaint reference
- Reasoned justification for the freeze
- Specific transaction details (amount, date, trail)
- Banks are no longer expected to act on vague emails or oral requests

iv. Swift Refunds for Small-Value Frauds

- Frauds involving amounts below Rs 50,000 can be refunded quickly without a court order.
- Banks must lift holds on such amounts within 90 days if no court or restoration order exists.

If you're affected, what you should keep ready (very important)

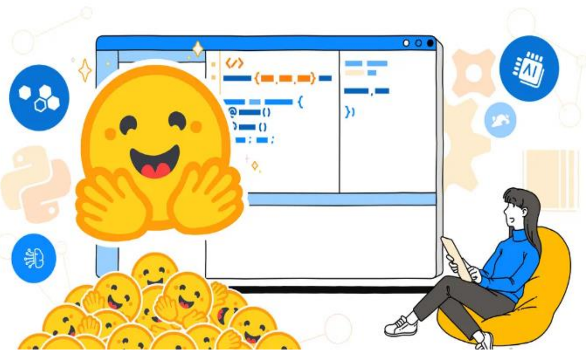
- Bank statements showing legitimate source of funds
- Salary slips / invoices / GST returns (if business account)
- Written request to:
  - ➢ Investigating Officer (IO)
  - ➢ Bank grievance cell
- If police delay, High Court writ petitions have proven effective in many cases

2. CYBER FRAUDS

(A) Hugging Face infra abused to spread Android RAT in a large-scale malware campaign

Cybersecurity researchers at **Bitdefender** have found a new Android malware campaign that uses a fake security app called **TrustBastion** to infect phones. The attack starts with ads or pop-up warnings that falsely claim a user's device is infected and needs protection. When users install TrustBastion, it looks like a real security app, but it is actually a dropper designed to secretly download more harmful malware. After installation, the app shows a fake system or Google Play update message. If the user accepts it, the app downloads **a second malicious app** that gives attackers remote access to the device.

This malware is hosted on **Hugging Face** a popular platform normally used by developers to share AI models and data. By using a trusted service, the attackers make the malicious downloads harder to detect and easier to hide among normal traffic. Bitdefender found that the attackers automatically created thousands of slightly different versions of the malware, sometimes a new one every 15 minutes, to avoid antivirus detection. One malicious Hugging Face repository collected more than 6,000 updates in under a month before it was removed. Even after that, the campaign quickly reappeared elsewhere with only small changes, showing that it is highly automated and persistent. Researchers warn users to be cautious of unexpected security alerts and apps claiming to "fix" infections, as these are often used to spread malware.



- Real Android or Google Play security alerts do not appear in ads, browsers, or random pop-ups. If a message pressures you to install an app immediately, it's a red flag.
- Avoid downloading apps from links in ads, SMS messages, or websites. Even on Google Play, check the developer name, reviews, and download count before installing.
- Android system updates come through device settings, not through third-party apps. If an app asks you to install an "update," decline it.
- Be cautious if a security or utility app asks for excessive permissions, especially accessibility access, device admin rights, or permission to install other apps.
- Be cautious if a security or utility app asks for excessive permissions, especially accessibility access, device admin rights, or permission to install other apps.
- Keep Play Protect enabled, it scans apps and can warn you about known malicious behavior.

- If your phone starts showing strange pop-ups, overheating, or unusual battery drain, uninstall recently added apps and run a security scan.

Urgency + Fear + "Security App" = Slow Down and Double-Check

(B) Cyber Police Bust Cryptocurrency Trading Scam, Including Two Bank Staff

Cyber police arrested three men in a fake USDT (Tether) trading scam after a victim was tricked through WhatsApp messages into investing money in what looked like a real cryptocurrency opportunity. Police said two of the accused were bank employees who allegedly misused their jobs to help open bank accounts using fake documents. These accounts were then used to move stolen money. About ₹50 lakh was transferred through one such account under a shell company called Dinesh Enterprises, which was reportedly reused within the fraud network. The accused are believed to have received commissions for helping set up these accounts, and more arrests may follow.

Cyber Police explained that this type of scam is common. Fraudsters create fake trading websites or apps that look professional and trustworthy. They contact people on WhatsApp, Telegram, social media, or email and promise very high or guaranteed profits in a short time. To gain trust, they may show fake screenshots or dashboards displaying profits. Once victims invest larger amounts, the money is quickly moved to other accounts or converted into cryptocurrency, making it hard to recover. Scammers may also pretend to be company representatives or use fake office details to make everything look real.

- If someone promises fixed or unusually high returns, it's almost always a scam. Crypto markets are volatile, no one can guarantee profits.
- Fraudsters often approach victims through messaging apps or social media. Legitimate financial institutions do not randomly message people with investment opportunities.
- Even if someone claims to be a bank employee, verify directly through the bank's official customer care number. Internal staff can also be involved in fraud cases.
- Check account names before transferring money, If the account name doesn't match the company, stop immediate

Pressure + Promise of high returns + Urgency to transfer money = Likely Scam

3. TIPS OF THE MONTH

(a) Valentine Week Fraud: -

During Valentine Week (Feb 7–14), cybercriminals become more active because many people are shopping online, using dating apps, and sending gifts. Scammers take advantage of emotions, urgency, and special offers to cheat victims. Here are the most common Valentine Week frauds:

1) Romance Scams ♡

Fraudsters create fake profiles on dating apps or social media. They quickly build emotional trust and then ask for money, gift cards, medical help, travel expenses, or cryptocurrency.

2) Fake Gift & Flower Websites 🌹

Scammers create fake online stores offering heavy discounts on flowers, chocolates, and jewelry. After payment, the gift never arrives.

3) Phishing Offers & Discount Links 📩

You may receive SMS, WhatsApp, or email messages with "Valentine special offers." Clicking the link can steal your banking details or OTP.

4) Fake Event & Dinner Reservations 🍽

Fraudsters promote fake hotel, restaurant, or concert bookings at discounted prices and disappear after receiving payment.

5) Sextortion & Blackmail 💻

Scammers may lure victims into sharing private photos or engaging in video chats, then threaten to leak recordings unless money is paid.

4. New Development in IT DTE

1.) PPMS

- Individual Achievement /Skill Entry Order
- Pay Fixation Order
- DCPS Recovery Order

DG CRPF Shri G.P. Singh (IPS) at the 87th CRPF Day Parade in Guwahati with Hon'ble Home Minister and Minister of Cooperation Shri Amit Shah.

DG CRPF Shri G.P. Singh (IPS) interacting with trainees at Guwahati during the 87th CRPF Day Parade.

DG CRPF Shri G.P. Singh (IPS) interacting with Jawans at Badakhana in Guwahati during the 87th CRPF Day.