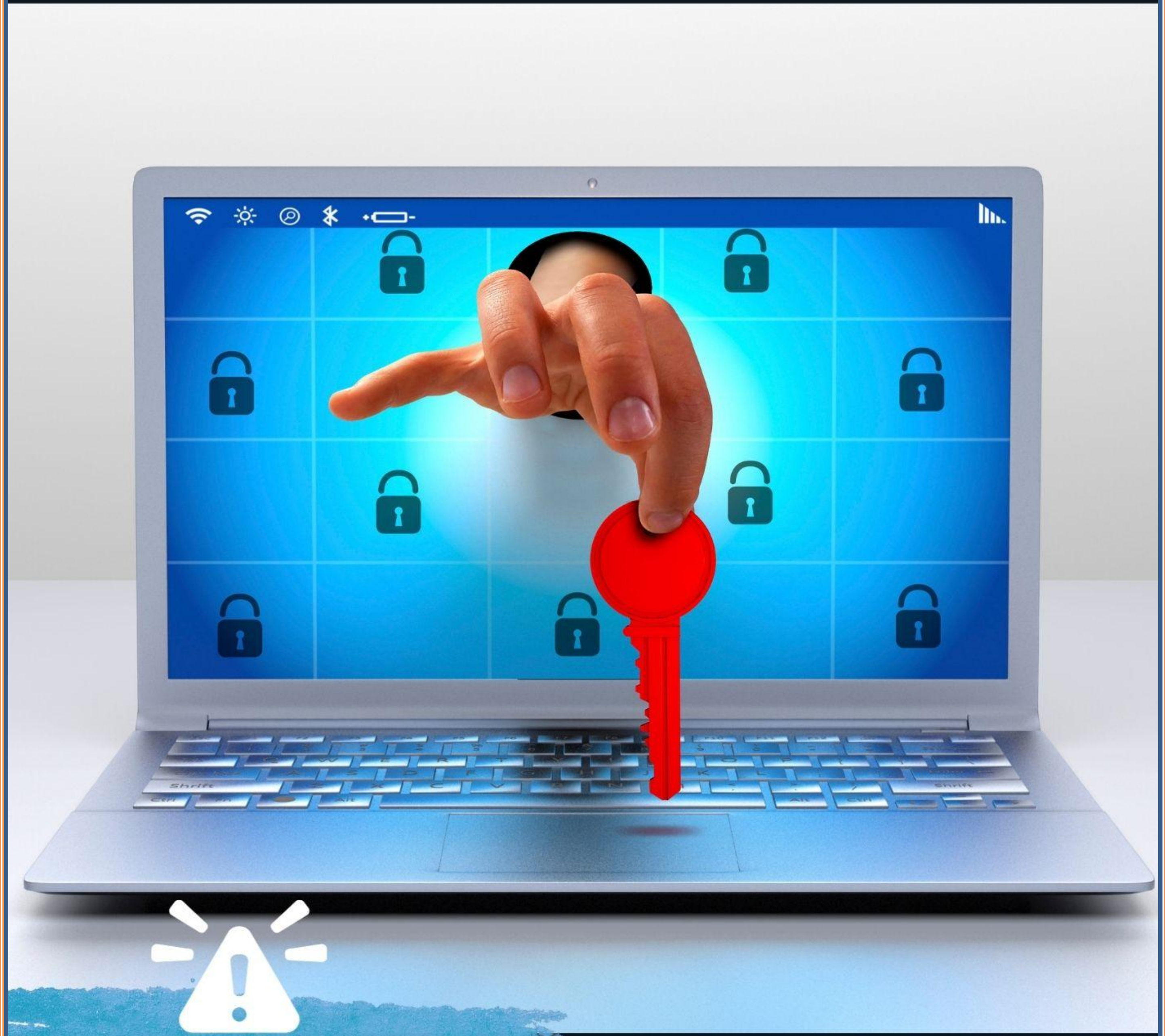
CENTRAL RESERVE POLICE FORCE

MAY, 2026

CYBER BYTE



RTO/e-Challan Android Malware Campaign

AI-Powered Phishing & Deepfake Scams

COMN & IT Dte. CRPF

1. LATEST CYBER THREAT

(A) RTO/e-Challan Android Malware Campaign

The scam involves fraudsters sending SMS, WhatsApp messages, or emails claiming you have a pending traffic fine. These messages include malicious payment links designed to steal user's bank or card details. Such fraudulent messages are crafted to mimic official government notices and lure victims into clicking immediately.

In multiple reported cases, victim clicked on these links only to face large unauthorized international transactions. For example, a Delhi resident recently lost over ₹2.49 lakh after attempting to pay a "₹500 pending challan" via a fake link.

How the Scam Operates
Cybercriminals uses several tactics to make their messages seem legitimate:

1. Fake SMS/WhatsApp Alerts

Messages often claim:
- Pending challan detected
- Pay immediately to avoid license suspension
- Court notice issued for non-payment

These alerts often come from regular 10-digit mobile numbers, not verified sender IDs.

2. Fraudulent Payment Links

The URLs mimic official government portals but redirect the victim to phishing sites designed to steal data.
Many fake domains closely resemble the Parivahan website and use shortened URLs.
Security researchers have also found 36+ fake domains impersonating RTO e-Challan sites.

3. Browser-Based Phishing Pages

Unlike older scams involving malware, cybercriminals now use cloned government portals that:

- Display fake violation details
- Look identical to real Parivahan pages
- Accept card-only payments (a major red flag)

How to Safely Check Your Challan

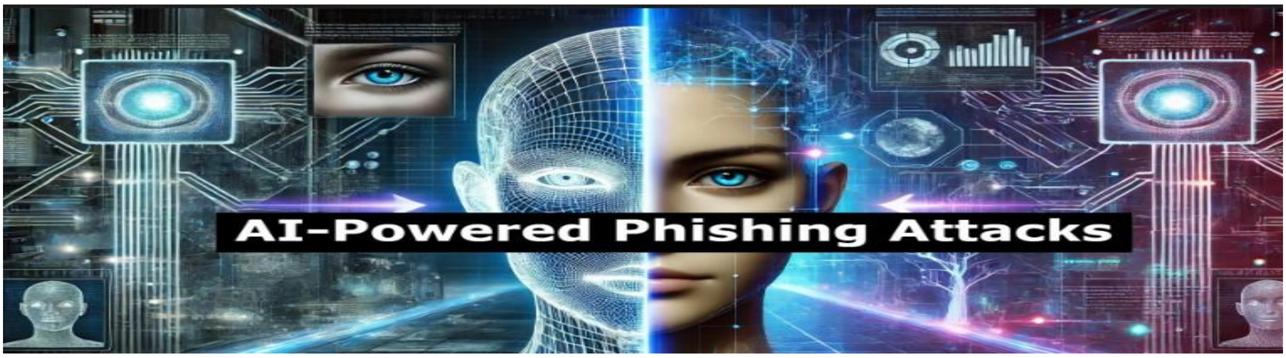
Use only official government portals:
Parivahan: https://echallan.parivahan.gov.in

State Traffic Police Websites
Steps to verify:
- Type the URL manually in your browser (never click links in messages).
- Go to "Check Challan Status."
- Enter the vehicle number + last 5 digits of the chassis/engine number.

If the system shows "No Challan Found," the message was fake.

2. AI-Powered Phishing & Deepfake Scams

Cybercriminals are using AI-generated voice calls, fake **HR emails, and deepfake video messages** impersonating banks, police, and company executives to steal credentials and funds. Indian enterprises are seeing increased business email compromise (BEC) attempts powered by AI.



The Two Main Threats:

AI Phishing: Scammers use AI (like ChatGPT) to write perfect emails or texts. They can study your social media to mention real details about your life, making the message look 100% real.

Deepfakes: This is "digital kidnapping" of a face or voice. A scammer can call you using a computer-generated version of your boss's face or your child's voice to ask for money.

Simple Rules to Stay Safe:
The "Safe Word" Strategy: Tell your family or coworkers a secret word (like "Blue Pineapple"). If someone calls claiming to be in trouble, ask for the word. If they don't know it, it's a fake.
- Hang Up and Call Back: If you get a suspicious "emergency" call, hang up immediately. Call that person back using the phone number already saved in your contacts—not the one that just called you.
- Watch for "The Rush": Scammers always want you to act fast so you don't have time to think. If a message makes you feel panicked or rushed to send money, it is almost certainly a scam.

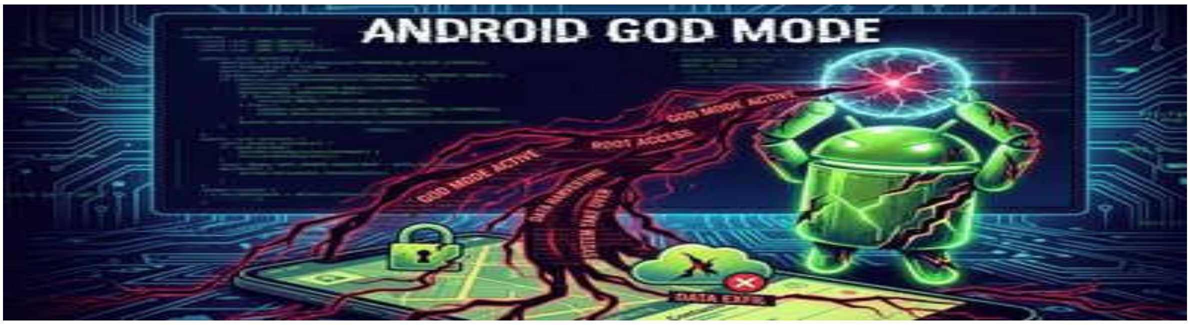
2. LATEST FINANCIAL FRAUD TRENDS THREAT

A) Android God Mode malware

"Android God Mode" is a dangerous new malware strain threatening Android users. It grants attackers full remote control over devices, enabling them to steal banking data, intercept OTPs, and spy on activities. It spreads via malicious APKs/phishing links, often bypassing standard uninstallation, necessitating Safe Mode removal.

How the malware reinstalls itself?

The malware relies on advanced persistence methods. In many cases, it requests accessibility permissions, which allow it to control parts of the device. Once granted, it can reinstall itself or trigger hidden processes that bring it back.



Steps to remove the malware permanently:

- Start by disconnecting the device from the internet to stop further communication with external servers.
- Boot the phone into Safe Mode, which prevents third-party apps from running.
- Next, review installed apps and remove any unfamiliar or suspicious ones.
- Check accessibility settings and revoke permissions from apps that do not require them.
- It is also important to disable device administrator access for unknown apps.
- Clear backup data linked to suspicious apps and turn off automatic restore temporarily. Running a trusted mobile security scan can help identify hidden components.
- If the issue persists, performing a factory reset may be necessary. Before resetting, ensure important data is backed up safely, excluding apps and system settings that may carry the malware.

B) Advance payment fraud

Although traditional, this type of fraud remains relevant and has adapted to digital environments. INTERPOL highlights its persistence in several regions, especially when combined with more sophisticated schemes, including fake job offers, prizes, or services that require an upfront payment.

Impact on banking:

- High volume of fraudulent microtransactions
- Use of digital channels and instant payments
- Increase in retail fraud

How to respond to advance payment fraud:
In these cases, **scalability is ke**y. Financial institutions need systems capable of analyzing large volumes of transactions in real time, identifying suspicious patterns without creating unnecessary friction.

The use of **dynamic risk models and multichannel** analysis allows institutions to correlate signals from different touchpoints, detect anomalous behavior, and act proactively without affecting the user experience.

3. CYBER GUPSHUP

Cyber fraud racket by opening a bank account

A 35-year-old bank employee was arrested by the Delhi Police Crime Branch for allegedly facilitating a cyber fraud racket by opening a bank account using forged documents, which was later used to siphon money from multiple victims.

Police said that the accused was working as a Relationship Manager with a private bank.

Hyderabad Police have busted a large cyber fraud network

Hyderabad Police have busted a large cyber fraud network under Operation Octopus 2.0, arresting 52 suspects, including 32 bank employees, across nine states.

Police said the operation targeted bank officials, who were helping cybercriminals open and operate fake (mule) accounts to transfer illegal money. Those arrested include managers, clerks, and KYC staff from banks like Bank of Baroda, Bandhan Bank, and IndusInd Bank.

4. CYBER HYGIENE

How Can You Improve Your Passwords?

Passwords are like keys to your online home. You want them to be strong. Here are some tips:

- ✓ Use Long Passwords Longer passwords are harder to guess.
- ✓ Try using a sentence. For example, “I love eating pizza on Fridays!” is a good password.
- ✓ Mix it Up Use different types of characters. Mix in numbers, symbols, and both big and small letters. “I<3EatingPizza0nFridays!” is even better.
- ✓ Don’t Reuse Passwords Use a unique password for each account. If someone steals one, the others stay safe.

Why Should You Update Your Software?

- ➢ Updating your software is like getting a flu shot. It protects you from new threats. Here’s why it’s important:
- ➢ Fix Security Holes Updates usually fix problems in your software. These are holes that bad guys can use to get in. Updating closes these holes.
- ➢ Get New Features Updates can also give you new cool stuff. Your apps may work better or do more things.
- ➢ Set Automatic Updates Turn on automatic updates when you can. Then you don’t have to remember to do it.

How Does Two-Factor Authentication Work?

Two-factor authentication is like putting two locks on your door. It makes it harder for bad guys to break in. Here’s how it works:

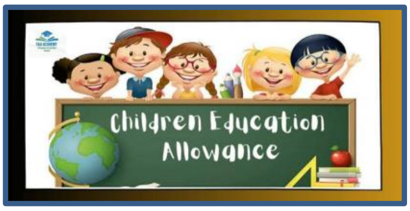
- ❖ 2FA needs two things to prove it’s you. Usually, one thing is your password. The second thing might be a code sent to your phone or your biomatrix.

- ❖ Why Use 2FA? If someone steals your password, they still can’t get in. They don’t have the second thing. It’s much safer.

- ❖ Where to Use 2FA Use 2FA on all your important accounts. These include email, banking, and even social media.

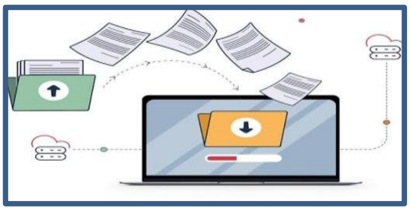
5. New Development in IT DTE

SAMBHAV

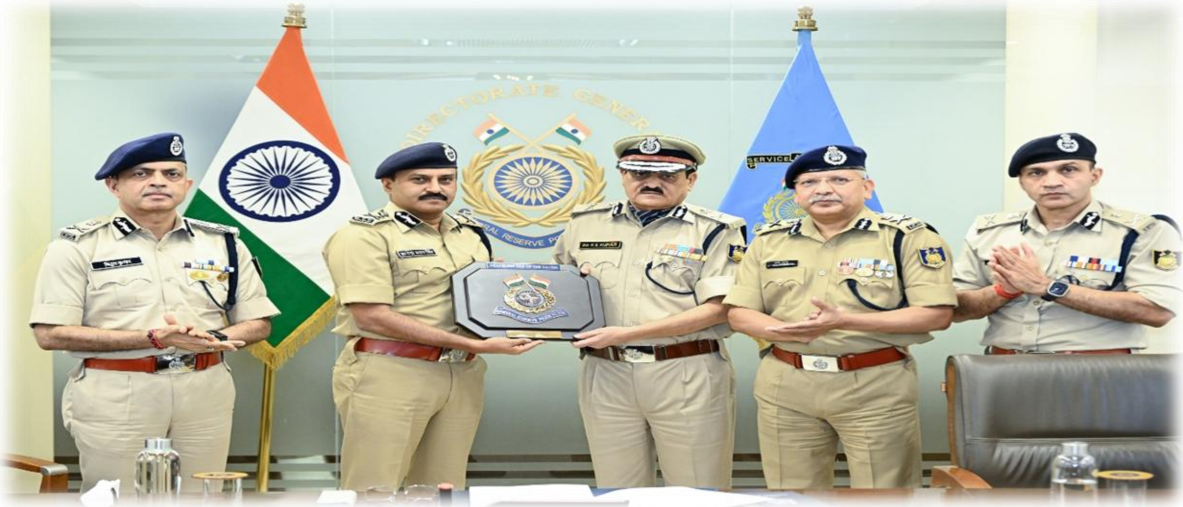


- Automation of CEA through SAMBAV app via PPMS.

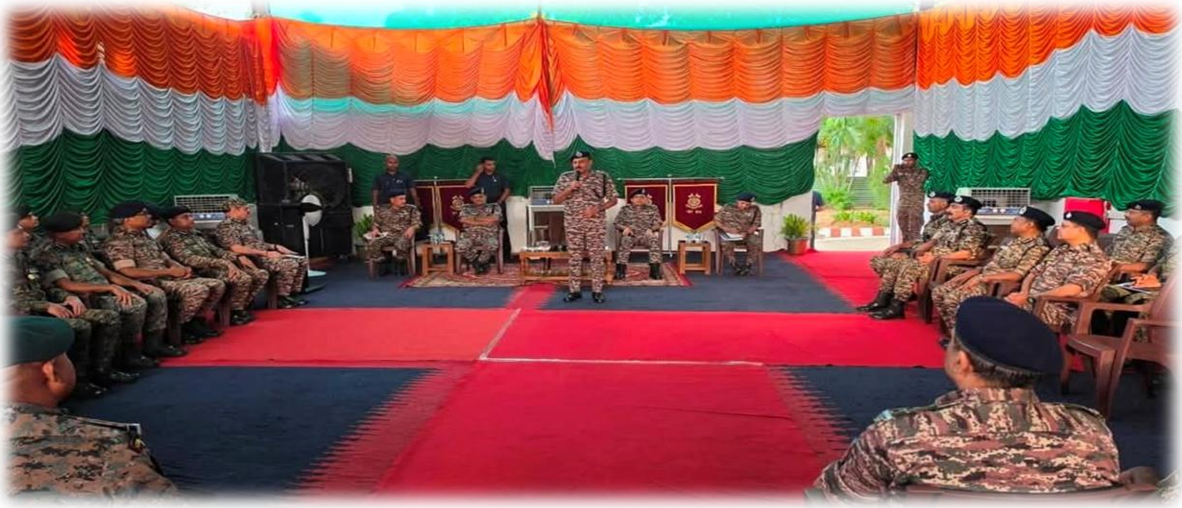
PPMS



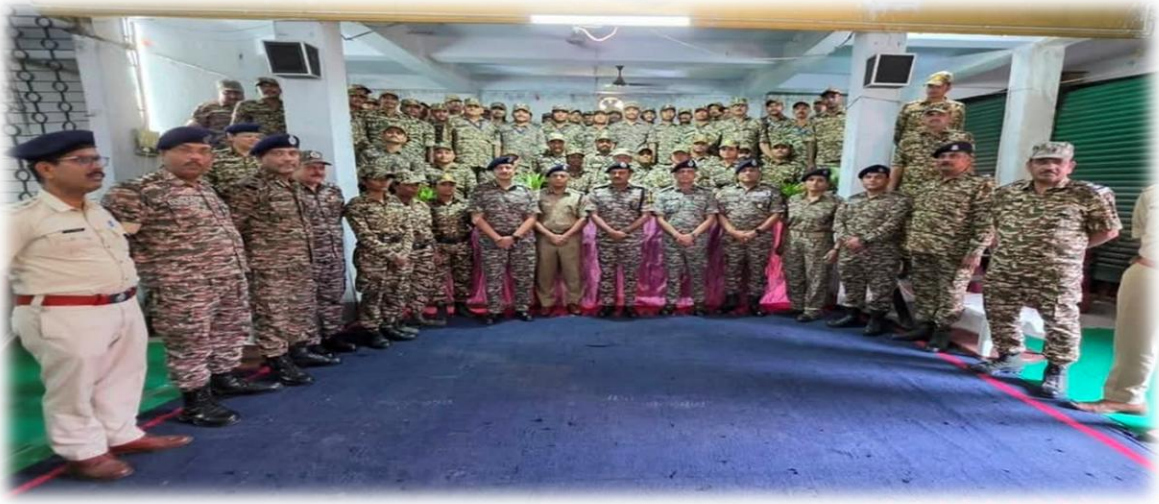
- Migration of Force Order (FO) publication process from SELO app to PPMS.
- Migration of risk fund final sanction process from SELO to PPMS.



DG CRPF Shri G.P. Singh (IPS) presenting a memento to senior officers on the occasion of their farewell ceremony held upon their superannuation.



DG CRPF Shri G.P. Singh (IPS) at Chaibasa, West Singhbhum, interacting with troops.



DG CRPF Shri G.P. Singh (IPS) at briefing troops of Adhoc 315 and WB police at Belur Girls High School, Howrah reg. maintaining law and order in West Bengal.