CENTRAL RESERVE POLICE FORCE

MARCH, 2026

CYBER BYTE

Cybercrime expert issues alert on AI-based biometric scam

Inside the SIM Box Scam: Gurugram Arrest Exposes China-Linked Cyber Network

IG (COMN & IT) Dte. CRPF

1. CYBER GEEKS NEWS

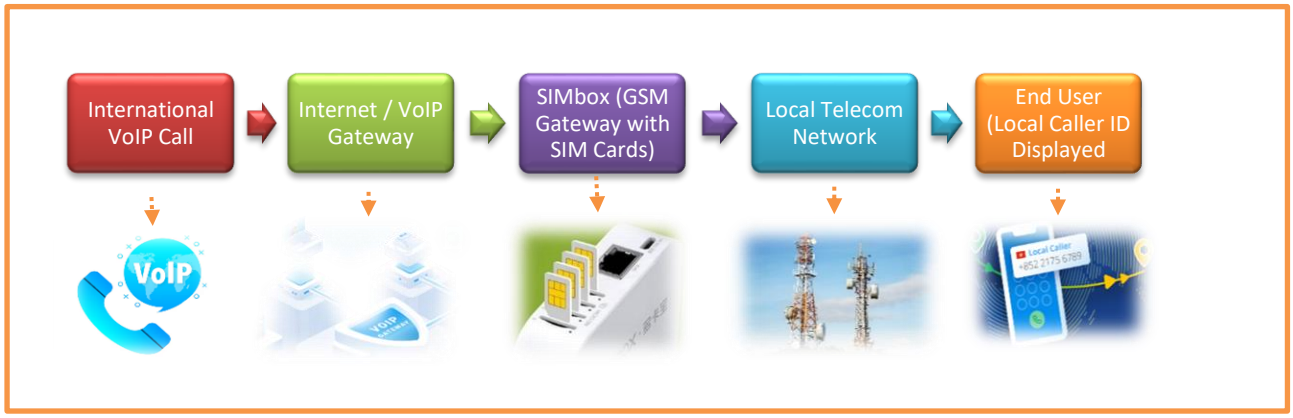
(A) Inside the SIM Box Scam: Gurugram Arrest Exposes China-Linked Cyber Network

A 30-year-old woman from Nagaland was arrested by the Gurugram Police in a joint operation with the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs ,for allegedly helping a cyber fraud network linked to China. The arrest has uncovered a cross-border scam operation that was reportedly being run from a rented apartment in the city, raising fresh concerns about the growing reach of international cybercrime in India.

According to police officials, The police allege the woman, along with her husband, had installed a virtual SIM box system in their rented flat that converted international VoIP calls into Indian local calls.This process makes it appear as though the calls are coming from within India, making it harder for authorities to trace the original source. Such systems are commonly used by cybercriminals to avoid detection while targeting victims across the country.

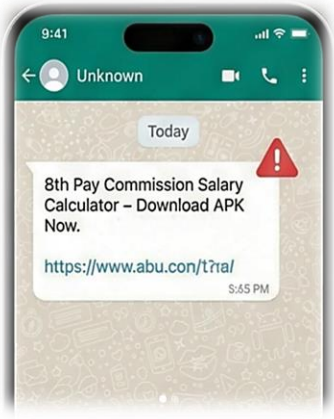
Investigators revealed that the setup included multiple phones and SIM cards making automated calls using an app known as “VDMS Apk,” a typical tool used in fraud operations. The accused allegedly helped maintain the devices by keeping them powered and connected, allowing overseas fraudsters to make bulk calls to Indian citizens. These calls were reportedly used for various scams, including fake investment schemes, digital arrest threats, and other online financial frauds.

Working of SIM-Box Device



(B) I4C alerts employees against the Eighth Pay Commission app scam

The Indian Cyber Crime Coordination Centre (I4C) has issued an alert warning government employee about a new scam related to the proposed 8th Central Pay Commission. The warning was released under the Union Ministry of Home Affairs after reports emerged that fraudsters are targeting employees with a fake mobile application.



? According to officials, scammers are spreading links through WhatsApp, claiming that the app provides a salary calculator for revised pay under the upcoming pay commission. The messages are designed to look official and may create a sense of urgency to encourage people to download the app quickly. However, authorities have clarified that no official salary calculator or mobile app has been launched in connection with the 8th Pay Commission. The fake app is intended to steal sensitive personal and financial information, including bank details, Aadhaar numbers, PAN information, passwords, and OTPs. In some cases, it may also install malware on the device, putting users at further risk of financial loss or identity theft.

Employees have been strongly advised not to click on unknown links or download applications from unofficial sources. They should verify any updates about the pay commission only through official government websites (**8cpc.gov.in**) and report suspicious messages to the national cybercrime portal (**cybercrime.gov.in**). Authorities have urged everyone to remain alert, as cybercriminals often take advantage of public interest in major government announcements.

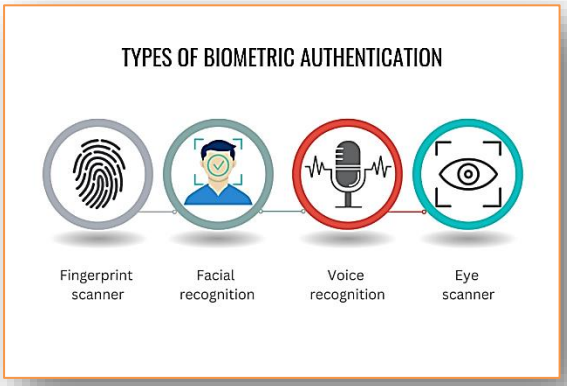
If You Already installed the app : -

- Immediately turn on airplane mode
- Uninstall the app
- Run a security/antivirus scan
- Change banking & email passwords
- Inform your bank
- Report at 1930 (India's cybercrime helpline) or cybercrime.gov.in

2. CYBER FRAUDS

(A) cybercrime expert issues alert on AI-based biometric scam:

The Cybercrime expert has warned people about a new type of scam that uses artificial intelligence (AI) to steal biometric data. Unlike conventional scams that focus primarily on stealing money through phishing or financial deception, this new threat is aimed at capturing sensitive biometric information such as facial features and voice samples data that, once compromised, cannot be changed like a password or OTP.



According to Cybercrime expert, scammers are using smart and secret methods to collect people's biometric details like their face and voice without them knowing.He said the scam has been noticed in busy places, such as shopping malls, metro stations, and other crowded areas. In these places, people are usually busy and less likely to realize that someone might be secretly recording or collecting their information.

How the AI-Based Biometric Scam Works?

The scammers often pretend to be elderly or middle-aged people so that no one suspects them. By looking harmless and behaving normally in public places, they are able to move around without attracting attention. They may start simple, friendly conversations to secretly record a person's voice. They might also use hidden cameras or mobile phones to capture clear pictures or videos of someone's face. Sometimes, they act like they are doing a survey, asking for directions, or just making small talk while quietly collecting voice and facial details.

Later, they use advanced AI tools to copy or recreate this information. Artificial intelligence today can carefully study a person's face, voice, and expressions. With enough data, criminals can create fake videos (deepfakes) or cloned voice recordings that sound and look very real, making it easier for them to pretend to be someone else.

Why This Is Dangerous

Today, many apps and online services use face recognition or voice verification to confirm who you are. But unlike a password, you cannot easily change your face or voice. If someone steals your biometric data, it can be misused for a long time.

Criminals may use this stolen information to pretend to be you online, try to access your bank accounts or digital wallets, create fake videos or voice recordings in your name, or commit identity theft.

- Avoid talking unnecessarily with strangers.
- Be careful if someone is recording near you.
- Do not share personal details loudly in public.
- Report any suspicious activity to cybercrime authorities immediately

(B) Global Phishing-as-a-Service Platform "Tycoon 2FA" Disrupted in International Cybercrime Operation

A major phishing-as-a-service platform known as **Tycoon 2FA** has been taken down in a coordinated international operation supported by **Europol**. The platform was widely used by cybercriminals to launch phishing attacks that could bypass multi-factor authentication (MFA) and gain unauthorized access to online accounts. Authorities say the disruption is part of a broader effort to combat organized cybercrime networks that provide ready-to-use hacking tools to criminals around the world. Tycoon 2FA operated as a subscription-based service that allowed attackers to run sophisticated phishing campaigns without needing advanced technical knowledge. Users of the platform could access ready-made phishing pages designed to look like legitimate login portals, tools to host malicious websites, and dashboards to track stolen credentials. By lowering the technical barrier for cybercrime, the service enabled many attackers to carry out large-scale phishing operations targeting individuals and organizations.

One of the most dangerous features of Tycoon 2FA was its ability to bypass MFA protections using a technique known as an adversary-in-the-middle attack. In these attacks, victims are tricked into clicking a phishing link that leads to a fake login page that closely resembles a legitimate website. When the victim enters their username, password, and MFA code, the platform intercepts the information in real time and captures the authenticated session. This allows attackers to access the victim's account without needing to enter the credentials again.

Security experts say accounts connected to major cloud services from companies such as Microsoft and Google were among the common targets because gaining access to these accounts can expose corporate emails, sensitive documents, and internal systems. Such compromises can lead to data theft, financial fraud, and further cyberattacks within organizations.

- Always Check the Website URL Carefully
  - Look for misspelled domains (e.g., **micros0ft.com** instead of microsoft.com)
  - Ensure the URL starts with **https://**
  - Avoid logging in from links in emails or SMS
- Use Strong and Unique Passwords
- Check the Sender's Email Address
  - **Fake**: support@micr0soft-security.com
  - **Real**: support@microsoft.com
- Keep Devices Updated
  - Operating system
  - Browser
  - Security software

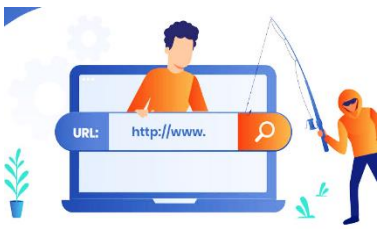
- Check the Login Page Behavior (A real site behaves differently from a phishing page)

✔ Real site:

- Password manager auto-fills login
- Domain matches the official website
- HTTPS certificate belongs to the company

✘ Phishing site:

- Password manager does not autofill
- Page looks real but URL is strange
- Login page opens from a random link



3. TIPS OF THE MONTH

(a) **Check for System and Software Updates: -**

Regularly checking for system and software updates is one of the easiest and most effective ways to protect your devices from cyber threats like phishing kits, malware, and account-stealing tools. Keep OS, browsers, and apps updated, for example: Windows 11, Kali Linux, and Google Chrome regularly release security patches.

(b) **Monitor Login Activity: -**

Monitoring login activity helps you quickly detect if someone else is trying to access your accounts. Many major services provide security dashboards where you can see devices, locations, and times of recent logins. If you see an unknown device or location, immediately sign out and change your password.

(c) **Enable Multi-Factor Authentication (MFA): -**

Enabling Multi-Factor Authentication (MFA) adds an extra security layer to your accounts. Even if someone steals your password through phishing or malware, they cannot log in without the second verification step. This protects accounts from attacks like phishing and password leaks.

(d) **Scan Devices for Malware :-**

Regularly scanning your devices for malware helps detect and remove harmful software that could steal passwords, monitor your activity, or enable phishing attacks. These threats can target computers and smartphones running systems like Microsoft Windows, Android, and macOS.

4. New Development in IT DTE

1.) PPMS

- DCPS Recovery

2.) power BI

- Signal Personal Report
- CRPF Strength Report w.r.t Posted Unit

DG CRPF Shri G.P. Singh (IPS) donating blood at Blood Donation Camp.

DG CRPF Shri G.P. Singh (IPS) at 26th All India Police Shooting Competition.

DG CRPF Shri G.P. Singh (IPS) at IIM, Pune releasing BDD guide for all field formation.