CENTRAL RESERVE POLICE FORCE

OCTOBER 2025

CYBER BYTE

Cyber Swachhta Kendra (CSK)

Sanchar Saathi Portal

New Development in IT DTE

WhatsApp 0-Click Vulnerability Exploited Using Malicious DNG File

Cyber Expert Urges Citizens to Stay Alert Against Frauds During This Festive Season

1. CYBER GEEKS NEWS

(A) Cyber Expert Urges Citizens to Stay Alert Against Frauds During This Festive Season: -

During the 2025 festive season, cybersecurity experts have urged citizens to be highly vigilant against a variety of online and digital frauds. Scammer exploit the festive rush and increased online activity through sophisticated and personalized attacks powered by AI. Both individual consumers and small businesses are at heightened risk. Festivals like Dussehra and Diwali, when 95% of Indians plan shopping, are prime targets. Phishing links in emails and SMS are the oldest trick in the playbook. But now, you have AI-generated celebrity endorsements with deals on top products, spreading through social media. It is observed that 40% increase in such scams during these months.

scammers are also exploiting festive greetings. People also share e -greeting cards during festivals, where an image or animation gets downloaded. But those are actually mobile trojans, which later hack apps like WhatsApp and send random messages to your contacts, posing as you, asking for money. If 100 people receive such messages, at least four or five end up sending money.

HAPPY
Diwali
FESTIVAL OF LIGHTS
On this beautiful occasion of Diwali, wish for new opportunities, new hopes, and new kinds of happiness for you.
I LOVE YOU SO MUCH.
From: Any Name Here

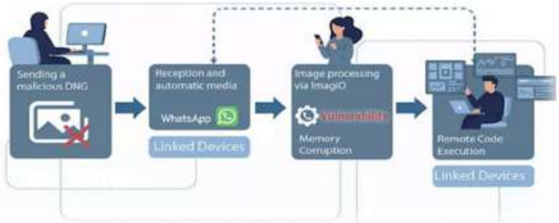
Cyber fraudsters trick common people through the messages of gaining more money in less time or attractive advertisements. The main element behind it is the greed of the people. Hence, not falling prey to any kind of lure of an unknown scheme is the only remedy to be safe from the cybercrimes.

- ✓ Cyber Expert said calls or messages from unknown numbers should not be responded to and unknown links should not be clicked, they can have viruses.
- ✓ Identity documents should not be shared with the unknown persons.
- ✓ The cyber frauds are generally done on Friday afternoon, as the banks are closed on Saturday and Sunday.

(B) WhatsApp 0-Click Vulnerability Exploited Using Malicious DNG File: -

WhatsApp 0-click remote code execution (RCE) vulnerability affecting **Apple's iOS, macOS, and iPadOS** platforms. The attack chain exploits two distinct vulnerabilities, identified as CVE-2025-55177 and CVE-2025-43300 to compromise a target device without requiring user interaction.

As a "zero-click" attack, the vulnerability is triggered automatically upon receipt of the malicious message, making it particularly dangerous as victims have no opportunity to prevent the compromise. successful exploit could grant an attacker complete control over a device, enabling them to access sensitive data, monitor communications, and deploy further malware. The stealthy nature of the attack means a device could be compromised without any visible indicators.



WhatsApp users are advised to ensure their applications and operating systems are always updated to the latest versions to receive security patches as soon as they become available. Both WhatsApp and Apple are expected to address these critical vulnerabilities in upcoming security updates.

Affected / Versions to update immediately

- ✓ WhatsApp for iOS before 2.25.21.73
- ✓ WhatsApp Business for iOS before 2.25.21.78
- ✓ WhatsApp for Mac before 2.25.21.78
- ✓ iOS/iPadOS 18.6.2, 17.7.10
- ✓ macOS Sequoia 15.6.1, Sonoma 14.7.8, Ventura 13.7.8

Suggested Actions

- ✓ Update WhatsApp on all devices.
- ✓ Update your iPhone, iPad, and Mac to the latest versions.
- ✓ Be extra cautious about suspicious messages or links

2. CYBER FRAUDS

(A) UIDAI Deactivates Crores of Aadhaar Numbers of Deceased to Prevent Welfare Fraud

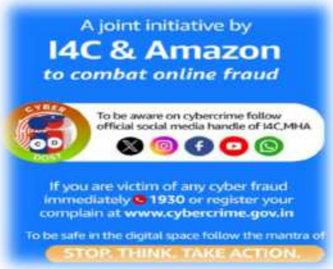
The Unique Identification Authority of India (UIDAI) has begun deactivating Aadhaar numbers linked to deceased individuals, in one of the largest clean-up operations in India's welfare system. The move is aimed at curbing Misuse of government schemes, where benefits were often issued in the names of the dead. In an effort to tighten India's welfare delivery system, the Unique Identification Authority of India (UIDAI) has deactivated more than 1.4 crore Aadhaar numbers belonging to deceased citizens.

Reporting of Death of a Family Member
Aadhaar Number Deactivation

Officials say this step is part of the government's plan to make sure benefits like subsidies and pensions only go to real, living people who have linked their Aadhaar ID to government programs. **This is important because, for years, some fake accounts have been using the names of dead people to get money.** The UIDAI and the government want to stop this cheating and save money.

(B) Cyber frauds surge past ₹4,200 crore, Amazon joins govt scam awareness push

Indians lost more than ₹4,245 crore to cybercrime in the first ten months of FY25. The country saw 2.4 million cases of digital payment fraud, according to government data. Unified Payments Interface (UPI), the backbone of India's payments revolution—has become a prime target. Losses from UPI-linked scams alone stood at ₹1,087 crore across 1.34 million cases in FY24. To address this, Amazon India has partnered with the Indian Cybercrime Coordination Centre (I4C) under the Ministry of Home Affairs to launch Scam Free Oct 2025, an initiative to raise awareness among students, first-time shoppers, and families.



A joint initiative by
I4C & Amazon
to combat online fraud

To be aware on cybercrime follow official social media handle of I4C,MHA

If you are victim of any cyber fraud immediately ☎ 1930 or register your complain at www.cybercrime.gov.in

To be safe in the digital space follow the mantra of
STOP. THINK. TAKE ACTION.

Shopping is a natural part of every Indian household in the festive season. It is also a time of heightened fraudulent activity by scamsters who try to dupe consumers, particularly vulnerable groups like first-time internet users and senior citizens. This partnership with Amazon will create awareness for consumers on how to detect frauds and avoid falling prey to them.

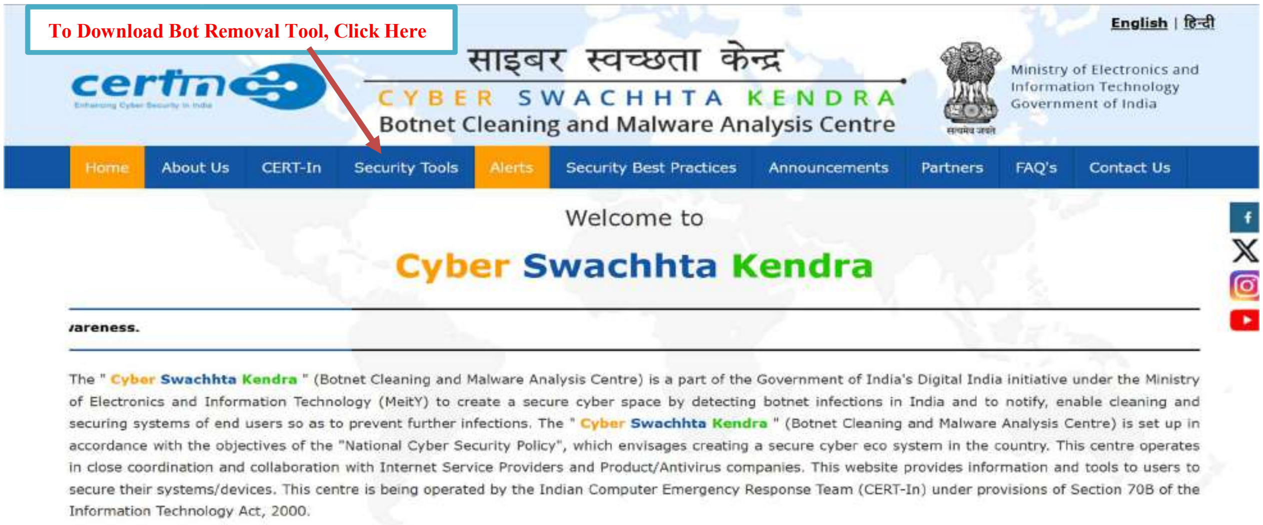
3. TIPS OF THE MONTH

(A) Cyber Swachhta Kendra (CSK)

https://www.csk.gov.in

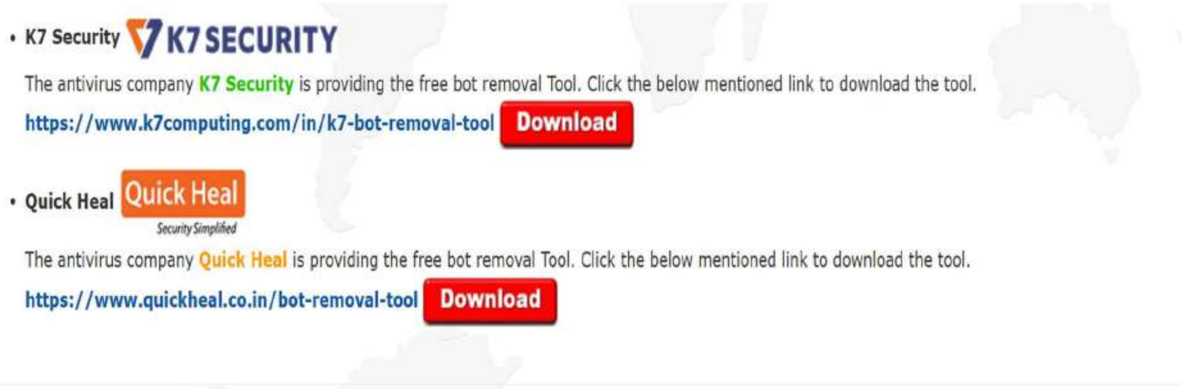
The "Cyber Swachhta Kendra" is a Botnet Cleaning and Malware Analysis Centre (BCMAC), operated by the Indian Computer Emergency Response Team (CERT-In) as part of the Government of India's Digital India initiative under the Ministry of Electronics and Information Technology (MeitY). **Its goal is to create a secure cyber space by detecting botnet infections in India.**

Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) **will provide free-of-cost bot removal tool for windows and android system.** It is a Government of India initiative to make a clean and secure Indian cyber space.



The " Cyber Swachhta Kendra " (Botnet Cleaning and Malware Analysis Centre) is a part of the Government of India's Digital India initiative under the Ministry of Electronics and Information Technology (MeitY) to create a secure cyber space by detecting botnet infections in India and to notify, enable cleaning and securing systems of end users so as to prevent further infections. The " Cyber Swachhta Kendra " (Botnet Cleaning and Malware Analysis Centre) is set up in accordance with the objectives of the "National Cyber Security Policy", which envisages creating a secure cyber eco system in the country. This centre operates in close coordination and collaboration with Internet Service Providers and Product/Antivirus companies. This website provides information and tools to users to secure their systems/devices. This centre is being operated by the Indian Computer Emergency Response Team (CERT-In) under provisions of Section 70B of the Information Technology Act, 2000.

Free Bot Removal Tool - For Microsoft Windows



- K7 Security

The antivirus company K7 Security is providing the free bot removal Tool. Click the below mentioned link to download the tool.

https://www.k7computing.com/in/k7-bot-removal-tool

- Quick Heal

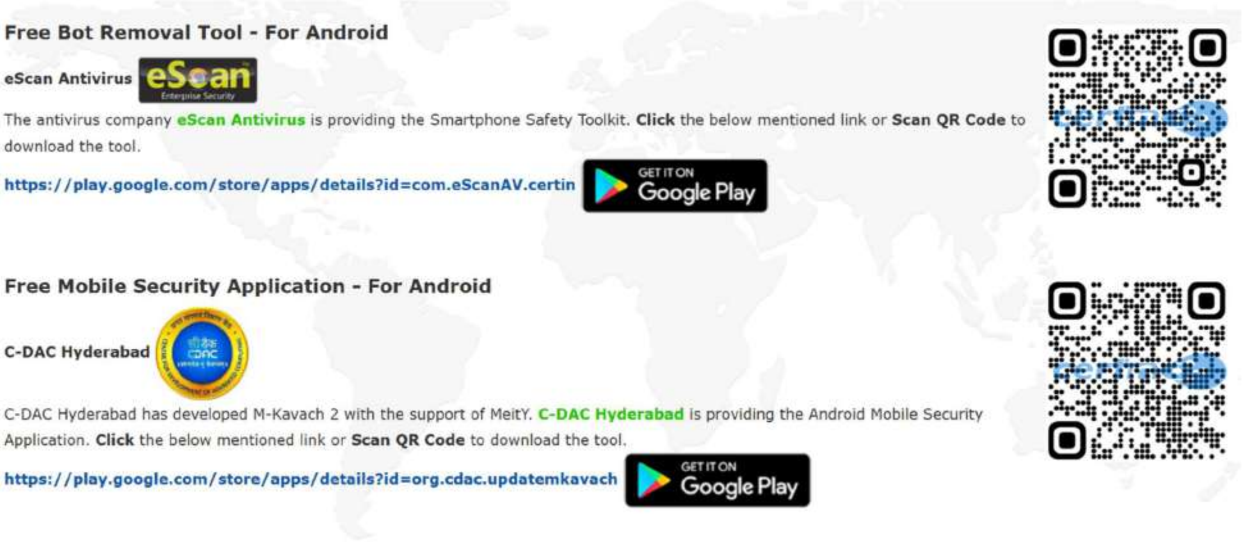
The antivirus company Quick Heal is providing the free bot removal Tool. Click the below mentioned link to download the tool.

https://www.quickheal.co.in/bot-removal-tool

➡ https://www.k7computing.com/in/k7-bot-removal-tool **(for K7 security)**

➡ https://www.quickheal.co.in/bot-removal-tool **(for quick heal)**

Free Bot Removal Tool - For Android



Free Bot Removal Tool - For Android

eScan Antivirus

The antivirus company **eScan Antivirus** is providing the Smartphone Safety Toolkit. **Click** the below mentioned link or **Scan QR Code** to download the tool.

https://play.google.com/store/apps/details?id=com.eScanAV.certin

Free Mobile Security Application - For Android

C-DAC Hyderabad

C-DAC Hyderabad has developed M-Kavach 2 with the support of MeitY. **C-DAC Hyderabad** is providing the Android Mobile Security Application. **Click** the below mentioned link or **Scan QR Code** to download the tool.

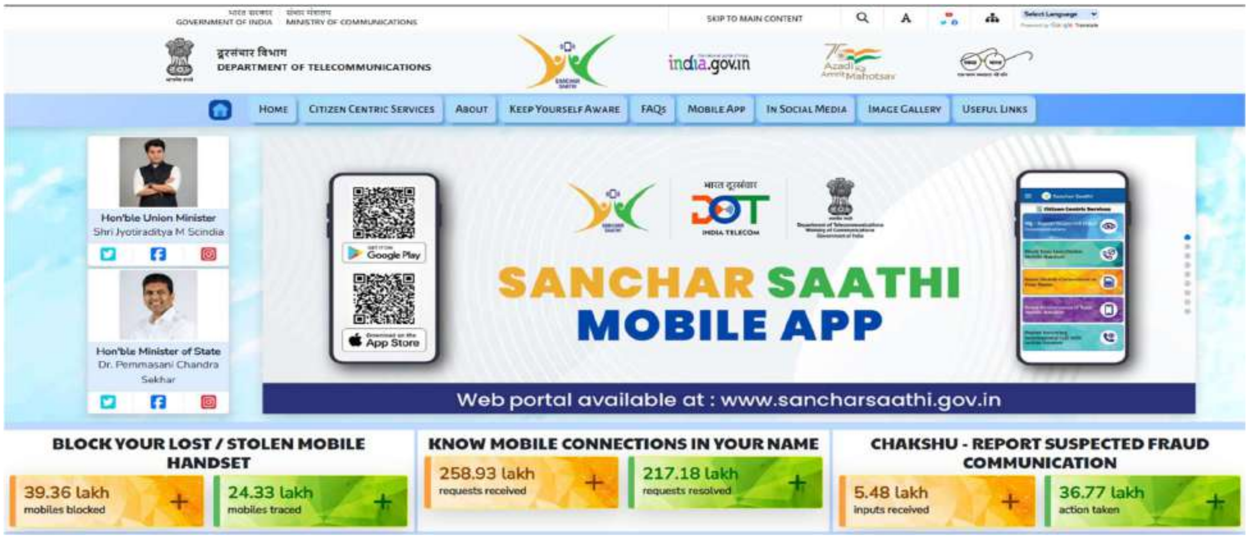
https://play.google.com/store/apps/details?id=org.cdac.updatemkavach

➡ https://play.google.com/store/apps/details?id=com.eScanAV.certin **(For escan)**

➡ https://play.google.com/store/apps/details?id=org.cdac.updatemkavach **(For mkavach)**

(B) Sanchar Saathi Portal (An Integrated Space for Citizen Centric Initiative)

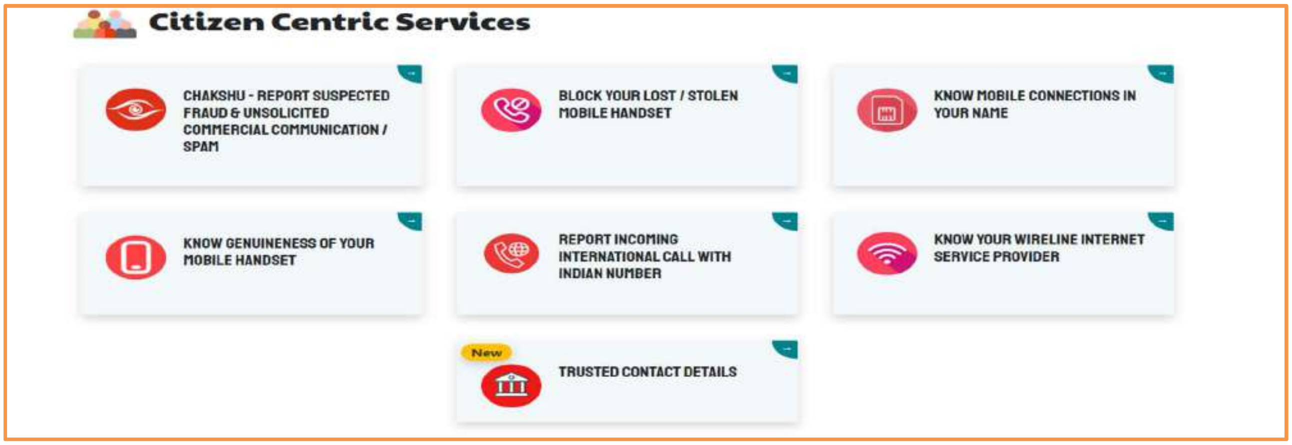
Sanchar Saathi is a citizen centric initiative of Department of Telecommunications (DoT) to empower mobile subscribers, strengthen their security and increase awareness about citizen centric initiatives of the Government. Sanchar Saathi is available in form of Mobile App and web portal (www.sancharsaathi.gov.in). Sanchar Saathi provides various citizen centric services.



भारत सरकार GOVERNMENT OF INDIA
संचार मंत्रालय MINISTRY OF COMMUNICATIONS
SKIP TO MAIN CONTENT
Select Language
दूरसंचार विभाग DEPARTMENT OF TELECOMMUNICATIONS
india.gov.in
Azadi Ka Amrit Mahotsav
HOME
CITIZEN CENTRIC SERVICES
ABOUT
KEEP YOURSELF AWARE
FAQs
MOBILE APP
IN SOCIAL MEDIA
IMAGE GALLERY
USEFUL LINKS
Hon'ble Union Minister
Shri Jyotiraditya M Scindia
Hon'ble Minister of State
Dr. Pemmasani Chandra Sekhar
Google Play
App Store
भारत दूरसंचार
DOT
SANCHAR SAATHI MOBILE APP
Web portal available at : www.sancharsaathi.gov.in

BLOCK YOUR LOST / STOLEN MOBILE HANDSET		KNOW MOBILE CONNECTIONS IN YOUR NAME		CHAKSHU - REPORT SUSPECTED FRAUD COMMUNICATION	
39.36 lakh mobiles blocked	24.33 lakh mobiles traced	258.93 lakh requests received	217.18 lakh requests resolved	5.48 lakh inputs received	36.77 lakh action taken

Citizen Centric Services



Citizen Centric Services

CHAKSHU - REPORT SUSPECTED FRAUD & UNSOLICITED COMMERCIAL COMMUNICATION / SPAM

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

KNOW YOUR WIRELINE INTERNET SERVICE PROVIDER

New

TRUSTED CONTACT DETAILS

A) Chakshu - Report Suspected Fraud Communication

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.

B) Block Your Lost/Stolen Mobile Handset

It facilitates tracing of the lost/stolen mobile devices. This also facilitates blocking of lost/stolen mobile devices in network of all telecom operators so that lost/stolen devices cannot be used in India. If anyone tries to use the blocked mobile phone, its traceability is generated. Once mobile phone is found it may be unblocked on the App or portal for its normal use by the citizens.

C) Know Mobile Connection in Your Name

It facilitates a mobile subscriber to check the number of mobile connections taken in his/her name. It also facilitates to report the mobile connection(s) which are either not required or not taken by the subscriber.

D) Know Genuineness of Your Mobile Handset

It facilitates a mobile subscriber to check the genuineness of mobile handset with the help of International Mobile Equipment Identity (IMEI) number.

E) Report Incoming International Call with Indian Number

It facilitates citizens to report about the international calls received by them with local Indian number (+91-xxxxxxxxxx) starting with +91 and having 10 digits excluding +91. Such international calls are received by illegal telecom setups over internet from foreign country and sent to Indian citizens disguising as domestic calls.

F) Know Your Wireline Internet Service Provider

Know Your Wireline Internet Service Provider facilitates citizens to check the details of Wireline Internet Service Providers (ISPs). The module enables the citizens to search for presence of any ISP across the length and breadth of the country by entering PIN code, address or name of the ISP.

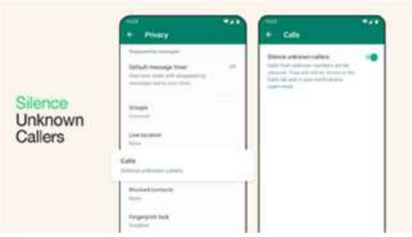
G) Trusted Contact Details

Trusted Contact Details helps citizens verify official contact information such as customer care numbers, toll-free numbers, email IDs, and genuine website links of important stakeholders, like banks and financial institutions. The module enables citizens to check whether a contact number they are calling -or receiving a call from- belongs to an authentic source. This empowers users to make informed decisions and prevent potential frauds.

4. Cyber Fraud Occurred With CRPF Personnel In Last Month

A constable GD of 30 BN has received a WhatsApp video call from an unknown person claiming as a HDFC bank staff for the renewal of expiry date of credit card. So, the jawan has shown both his SBI and AXIS bank credit card after that the fraudster diverted the call and also hacked or took control of both email and WhatsApp application etc. By doing this he(fraudster) made two deduction Rs 36000/- from SBI credit card and 1,50,000/- from Axis bank credit card amounting to total 1,86,000/- Rs.

After that jawan has complained to Imphal Cybercrime Branch as well as to his company commander.



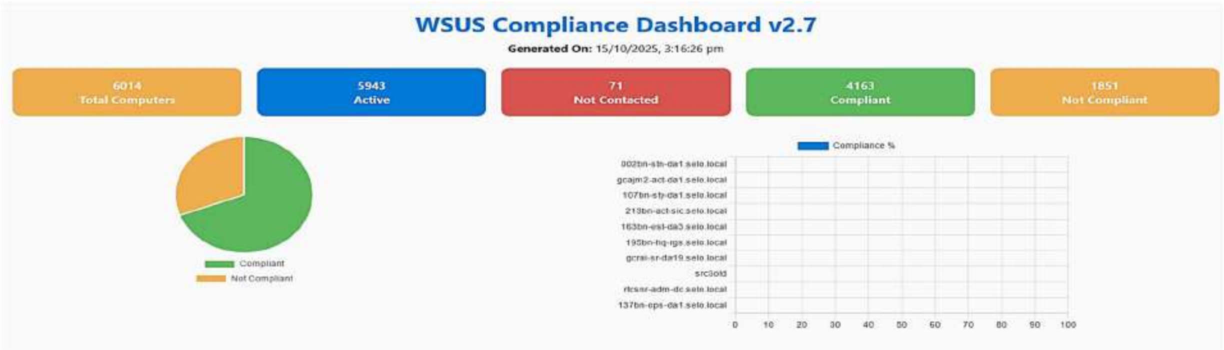
✓ Hence it is again advised to all to not receive any unknown video call from any messenger like WhatsApp, telegram, Facebook etc.

✓ Reduce/manage the credit card limit. If there had been a limit on the card, the fraudster wouldn't have been able to take such a big amount.

5. New Development in IT DTE

1.) ISERT (Information Security & Emergency Response Team)

A new WSUS (Windows Server Update Services) Compliance Dashboard has been developed for timely monitoring and for both SECTOR and DTE ISERT team to look out for available filters like computer name, IP Address, Operating System, compliance%, updation of patches, etc.



WSUS Compliance Dashboard v2.7

Generated On: 15/10/2025, 3:16:26 pm

6014 Total Computers	5943 Active	71 Not Contacted	4163 Compliant	1851 Not Compliant

2.) PPMS (Paperless Process Management System)

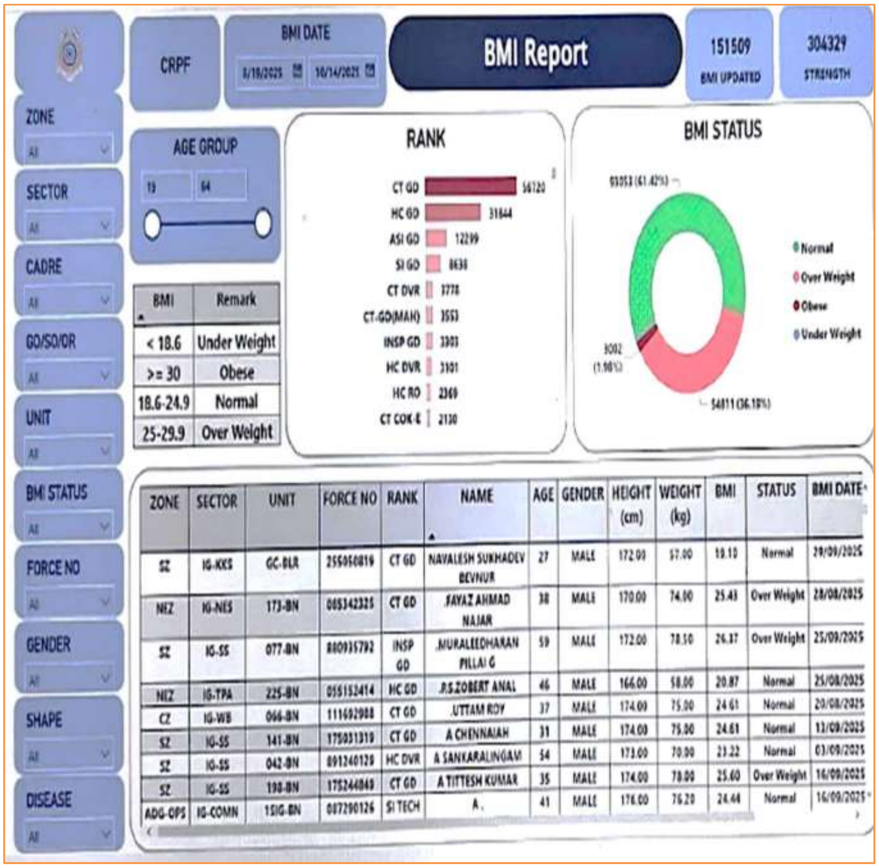
- Punishment order, Confirmation order, Medal / Reward order (Backlog Data), Education Entry Order, BMI

3.) Sambhav (SELO Application Mobile Availability)

- NGO can apply Apply for Deputation/Course/Attachment
- Application for CEA, Hostel subsidy and both
- Late reporting in case of leave extension

4.) POWER BI

- BMI (Body Mass Index) Dashboard
- CWS /AWS AOR Dashboard



BMI	Remark
< 18.6	Under Weight
>= 30	Obese
18.6-24.9	Normal
25-29.9	Over Weight

ZONE	SECTOR	UNIT	FORCE NO	RANK	NAME	AGE	GENDER	HEIGHT (cm)	WEIGHT (kg)	BMI	STATUS	BMI DATE
SZ	IG-KKS	GC-BLR	255050819	CT GD	NAVALESH SUKHADEV BEVNUR	27	MALE	172.00	57.00	19.10	Normal	29/09/2025
NEZ	IG-NES	173-BN	085342325	CT GD	FAYAZ AHMAD NAJAR	38	MALE	170.00	74.00	25.43	Over Weight	28/08/2025
SZ	IG-SS	077-BN	880935792	INSP GD	MURALEEDHARAN PILLAI G	59	MALE	172.00	78.50	26.37	Over Weight	25/09/2025
NEZ	IG-TPA	225-BN	055152414	HC GD	P.S.ZOBERT ANAL	46	MALE	166.00	58.00	20.87	Normal	25/08/2025
CZ	IG-WB	066-BN	111692988	CT GD	UTTAM ROY	37	MALE	174.00	75.00	24.61	Normal	20/08/2025
SZ	IG-SS	141-BN	175031319	CT GD	A CHENNAIAH	31	MALE	174.00	75.00	24.61	Normal	13/09/2025
SZ	IG-SS	042-BN	891240129	HC DVR	A SANKARALINGAM	54	MALE	173.00	70.00	23.22	Normal	03/09/2025
SZ	IG-SS	198-BN	175244849	CT GD	A TITTESH KUMAR	35	MALE	174.00	78.00	25.60	Over Weight	16/09/2025
ADG-OPS	IG-COMN	1SIG-BN	087290126	SI TECH	A.	41	MALE	176.00	76.20	24.44	Normal	16/09/2025

The DG, CRPF celebrating DEEPAWALI along with senior Officers and all ranks at CRPF Hqr. CGO Complex.

The DG, CRPF In Police Commemoration Day

The DG, CRPF visited the Vice President Enclave and interacted with troops.