CENTRAL RESERVE POLICE FORCE

JUNE-2025

CYBER BYTE

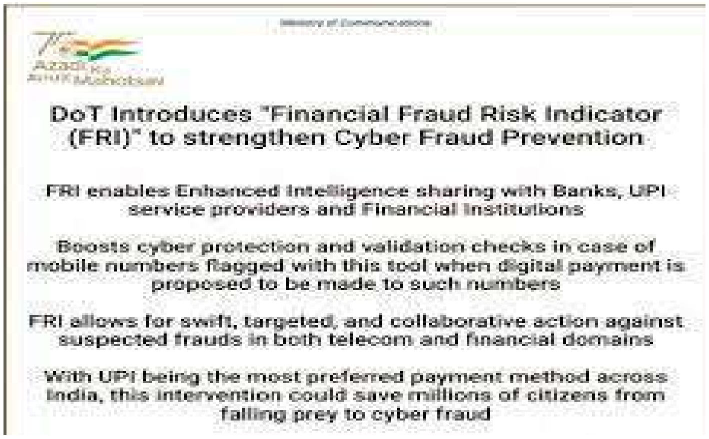
DoT Unveils Cyber Fraud and Risk Indicator

NCSC issues alert against more ransomware attacks on retailers

Kedarnath Yatra Cyber Scam Busted: Fake Sites, Fraud Ads, 100+ Accounts Blocked

1. CYBER GEEKS NEWS

A. DoT Unveils Cyber Fraud and Risk Indicator: -



Ministry of Communications

Azadi Ka Amrit Mahotsav

DoT Introduces "Financial Fraud Risk Indicator (FRI)" to strengthen Cyber Fraud Prevention

FRI enables Enhanced Intelligence sharing with Banks, UPI service providers and Financial Institutions

Boosts cyber protection and validation checks in case of mobile numbers flagged with this tool when digital payment is proposed to be made to such numbers

FRI allows for swift, targeted, and collaborative action against suspected frauds in both telecom and financial domains

With UPI being the most preferred payment method across India, this intervention could save millions of citizens from falling prey to cyber fraud

To combat the rising threat of cyber fraud, the Department of Telecommunications (DoT) has launched the Financial **Fraud Risk Indicator** (FRI)—a core feature of the **Digital Intelligence Platform** (DIP). This tool enhances digital payment security by enabling real-time intelligence sharing with banks, UPI service providers, and other financial institutions.

The FRI is a multi-dimensional tool that categorizes mobile numbers based on their potential involvement in financial fraud. It assigns risk levels—Medium, High, or Very High—based on data sourced from the National Cybercrime Reporting Portal (NCRP), DoT's Chakshu platform, and inputs from financial institutions.

By serving as an early warning system, the FRI empowers stakeholders to proactively verify flagged mobile numbers before authorizing financial transactions. When a digital payment is initiated to a flagged number, additional validation checks can be triggered to prevent potential fraud.

The initiative aims to build a resilient, technology-driven security infrastructure that evolves with emerging fraud techniques. Parallel efforts are underway to run public awareness campaigns, equipping users with the knowledge to identify and avoid digital payment fraud.

B. NCSC issues alert against more ransomware attacks on retailers: -

Following recent cyber-attacks on major UK retailers like Harrods and Marks & Spencer, the National Cyber Security Centre (NCSC) has issued an urgent warning about rising ransomware threats, especially in the retail sector. In response, it has released detailed guidelines to help businesses strengthen defenses and reduce financial risk.

Anticipating further attacks as digital threats continue to evolve, the NCSC has expressed concern over the increasing frequency and sophistication of ransomware incidents, which typically encrypt critical business data and demand payment for its release. The retail industry remains a high-risk target due to its vast repositories of customer data and sensitive transactional information.

The NCSC strongly urges businesses to adopt immediate and proactive defense measures, stressing that preparedness is crucial for maintaining business continuity and mitigating the impact of cyber incidents.

Key Guidelines to Protect Against Ransomware Attacks:

- **Isolate and contain the threat immediately** to prevent lateral spread.
- **Utilize secure and up-to-date backup systems** to restore operations quickly.
- **Report the incident to relevant authorities** without delay for coordinated response and support.

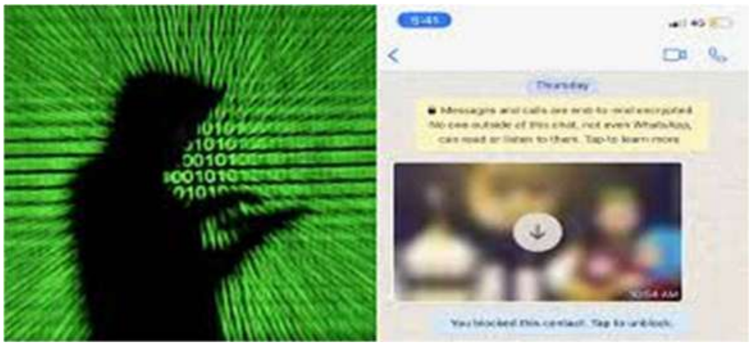
2. CYBER FRAUDS

Kedarnath Yatra Cyber Scam Busted: Fake Sites, Fraud Ads, 100+ Accounts Blocked: -

As the Char Dham Yatra begins, cybercriminals are targeting devotees by creating fake websites and social media pages offering fraudulent helicopter ticket bookings to Kedarnath Dham.

In response, the Uttarakhand Police's Special Task Force (STF) has launched an aggressive crackdown on the growing cybercrime menace. The STF is conducting round-the-clock surveillance and taking decisive legal action against cybercriminal infrastructure through continuous daily monitoring.Leveraging close coordination with the Ministry of Home Affairs' Indian Cyber Crime Coordination Centre (I4C), the operation has successfully blocked hundreds of digital assets exploited by fraudsters.As technology evolves, so too must law enforcement strategies. The success of this initiative lies in its proactive leadership, inter-agency coordination, platform collaboration, and active public participation—a powerful combination that could serve as a national benchmark for cybercrime prevention.

(B) No OTP, No Link—Hackers Just Need One WhatsApp Image Now: -



Thursday

Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more

You blocked this contact. Tap to unblock.

In the digital age, where phishing links and OTP frauds are common threats, a new danger has emerged—one that hides in plain sight. Hackers are now weaponizing WhatsApp images as Trojan horses to deliver malware directly to users' devices. Unlike traditional scams, this sophisticated method uses **steganography**—a technique where malicious code is stealthily embedded within seemingly harmless image files.

Once the infected image is opened, the malware silently installs itself on the victim's phone. It can then exfiltrate sensitive information such as banking credentials, OTPs, and even perform unauthorized financial transactions—all without the user's awareness. This makes detection and prevention particularly challenging.

The gravity of this threat came into sharp focus when a resident of Jabalpur, Madhya Pradesh, lost nearly ₹2 lakh after opening an image received from an unknown WhatsApp number. The malware had infiltrated his device, granting cybercriminals access to his financial apps and personal data.

In response, the Department of Telecommunications (DoT) issued an urgent advisory, warning users not to download image files from unknown sources. Cybersecurity experts have since labeled this tactic "**more dangerous than traditional phishing**" due to its covert execution and lack of obvious red flags.

3. TIPS OF THE MONTH

A.) How to protect yourself from digital arrest.

Verify information: Never share personal information or financial details with anyone over the phone or online unless you are absolutely certain of their identity and the legitimacy of their request.

Be wary of unfamiliar numbers: Avoid answering calls from unknown numbers, especially those with foreign area codes.

Cross-check information: If you receive a suspicious call or message, try to verify the information with a trusted source, such as a government website or a known law enforcement agency.

Stay calm: Scammers often rely on fear and intimidation to manipulate their victims. Stay calm and avoid making impulsive decisions.

Report the scam: If you believe you have been targeted by a digital arrest scam, report it to the local police or cybercrime authorities. You can also report it to your internet service provider or mobile carrier.

B) How to protect yourself from lottery scam:

In this type of scam, the sender requests assistance in facilitating the transfer of a substantial sum of money, typically via email. In return, the sender promises a commission, usually amounting to several million dollars. The scammers then ask the recipient to send money to cover costs associated with the transfer, such as processing fees or taxes. If money is sent, the scammers either disappear immediately or continue requesting additional funds, citing ongoing issues with the transfer.

Protection from the lottery scam

- **Never Respond, ignoring messages** or calls about the fake lottery wins is the smart move to avoid falling into the trap.

- **Take time to research** the organization supposedly running the lottery and ask probing questions to anyone reaching out with the offers.

- **Never share sensitive personal details** as scammers often request such information. Be cautious, as reputable organizations do not ask for such data.

- **It is essential to approach any unexpected windfalls** with skepticism, as genuine lottery wins typically require participation.

- **Refrain from paying any fees to claim supposed winnings**; legitimate lotteries do not ask for money upfront.

- **Be wary of urgent demands for payment from scammers;** they often pressure victims to act quickly, aiming to exploit their sense of urgency.

C) Windows Sandbox Usage Guidelines for Phishing Email:

1. Enable Windows Sandbox (if not already enabled)

- Go to Control Panel > Programs > Turn Windows features on or off.
- Check Windows Sandbox.
- Click OK, then restart your PC.

⚠ **Requires Windows 10/11 Pro, Enterprise, or Education.**

2. Prepare the Phishing Email Artifacts for Investigation

- Do NOT open links or attachments on your main system.
- Save suspicious attachments (e.g., .docx, .exe, .pdf, etc.) or copy URLs without clicking.
- Store these files in a secure location (e.g., a dedicated folder on your desktop).

3. Launch Windows Sandbox

- Press Start and search for Windows Sandbox.
- Launch it — a clean, isolated Windows environment will open.

4. Transfer the File or Link into the Sandbox

- Copy the suspicious file/link from your host OS.
- Paste it inside the sandbox environment.

5. Open and Analyze the Suspicious Content.

- Open attachments or click on suspicious links inside the Sandbox only.
- Observe behavior:
  - Does it try to install software?
  - Does it redirect to a shady site?
  - Is there a request for credentials?

🛑 **Do NOT enter personal information or real credentials**.

6. Discard the Sandbox Session

- **Close the Sandbox** window when you're done.
- All contents and changes will be **permanently deleted**.

☑ **This ensures any malware or phishing attempts cannot affect your host system.**

7. Report and Delete the Phishing Email

- Report the email to ISERT Dte. or email provider.
- Delete the original phishing email from your inbox and trash.

Additional Tips

- Keep your OS and antivirus updated.
- Use email filters and spam protection.
- Avoid interacting with emails from unknown senders, even in the sandbox.
- Use multi-factor authentication (MFA) to protect accounts.

Golden Jubilee Celebration official language

Career Counselling Session at

International Yoga Day 2025

30th Raising Day Celebrations of CWA

Silver medal winner L. Nirupama Devi, AC
(World Police and Fire Games in Birmingham)

Inspection of Data Center by IG (Comn&IT)