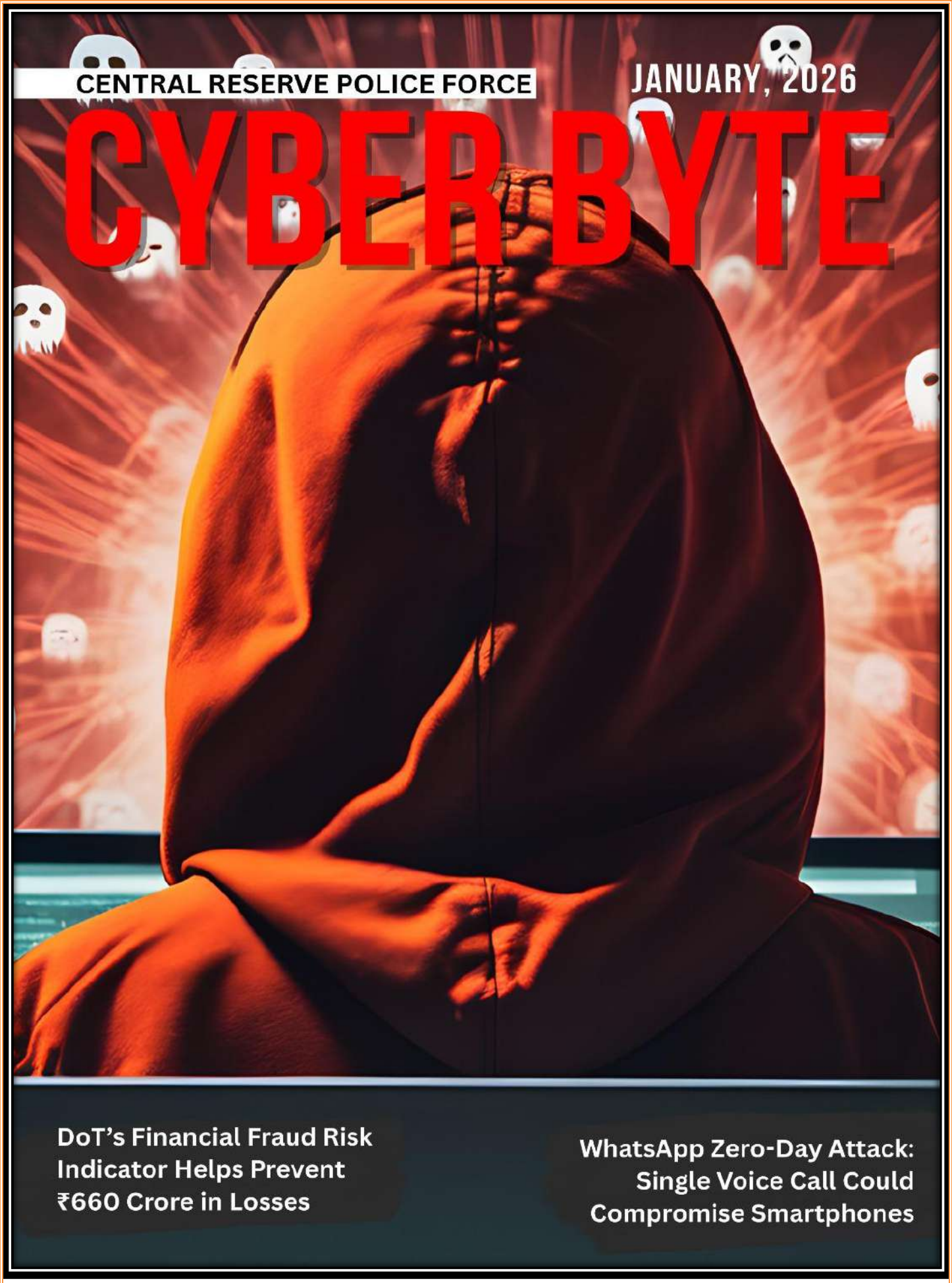
CENTRAL RESERVE POLICE FORCE

JANUARY, 2026

CYBER BYTE



DoT's Financial Fraud Risk Indicator Helps Prevent ₹660 Crore in Losses

WhatsApp Zero-Day Attack: Single Voice Call Could Compromise Smartphones

IG (COMN & IT) Dte. CRPF

1. CYBER GEEKS NEWS

(A) Fake New Year Greeting Links Trigger Cyber Crime Alert

The Cybercrime Expert, has issued a public advisory warning of a sharp rise in cyber fraud cases involving fake New Year greeting links and malicious APK files circulating across digital platforms. Cybercriminals are exploiting the festive season by sending deceptive messages through SMS, WhatsApp, social media, and emails, claiming to offer New Year wishes, gifts, or video cards. These messages often contain suspicious links or APK files with names such as "NewYear.apk," which, once clicked or installed, can compromise mobile phones and applications, including messaging apps. This may lead to theft of personal data, banking credentials, and unauthorized access to financial and social media accounts.

The advisory urges people to remain cautious and watch out for red flags such as messages demanding urgent action or threatening penalties, requests to download APK files or enable installation from unknown sources, and receiving one-time passwords without initiating any transaction or request.

- Do not click on unknown or suspicious links.
- Never install APK files sent via messages or social media
- Disable "Install from unknown sources" on your phone
- Do not share OTPs, PINs, or banking details
- Be wary of links asking for permissions like SMS access or OTPs.
- Enable two-step verification and strong security settings on messaging apps.

- Report suspicious messages to cybercrime authorities
  - 1930 (Immediate reporting)
  - cybercrime.gov.in

(B) DoT's Financial Fraud Risk Indicator Helps Prevent ₹660 Crore in Losses

In a major boost to India's fight against rising digital financial fraud, the Department of Telecommunications (DoT) has revealed that its **Financial Fraud Risk Indicator** (FRI) has helped prevent potential losses of nearly ₹660 crore within just six months of its launch. The initiative reflects growing coordination between telecom authorities, banks, and digital payment platforms to safeguard citizens in an increasingly digital economy.

The FRI system was launched on May 22, 2025, as part of the government's broader strategy to curb cyber-enabled financial crimes, including phishing, fake calls, identity theft, and UPI-related frauds. Since its rollout, the tool has played a key role in detecting and disrupting suspicious transactions before money could be siphoned off by fraudsters.

How the Financial Fraud Risk Indicator Works

The Financial Fraud Risk Indicator is an intelligence-driven mechanism that identifies mobile numbers linked to potential financial fraud. Using inputs from telecom service providers, cybercrime complaint databases, and financial institutions, the system assigns risk levels such as medium, high, or very high to mobile numbers suspected of being used for fraudulent activities.

These risk indicators are then shared in real time with banks, UPI platforms, and payment system operators. Based on the alert level, financial institutions can take preventive action such as delaying transactions, blocking payments, seeking additional verification, or issuing warnings to customers. This proactive approach has significantly reduced the chances of successful fraud attempts.

Citizen Participation

Citizen engagement via platforms like **Sanchar Saathi** helps feed ground-level reports of suspicious activity into the system, strengthening the FRI's intelligence base.

Why FRI System Is Important

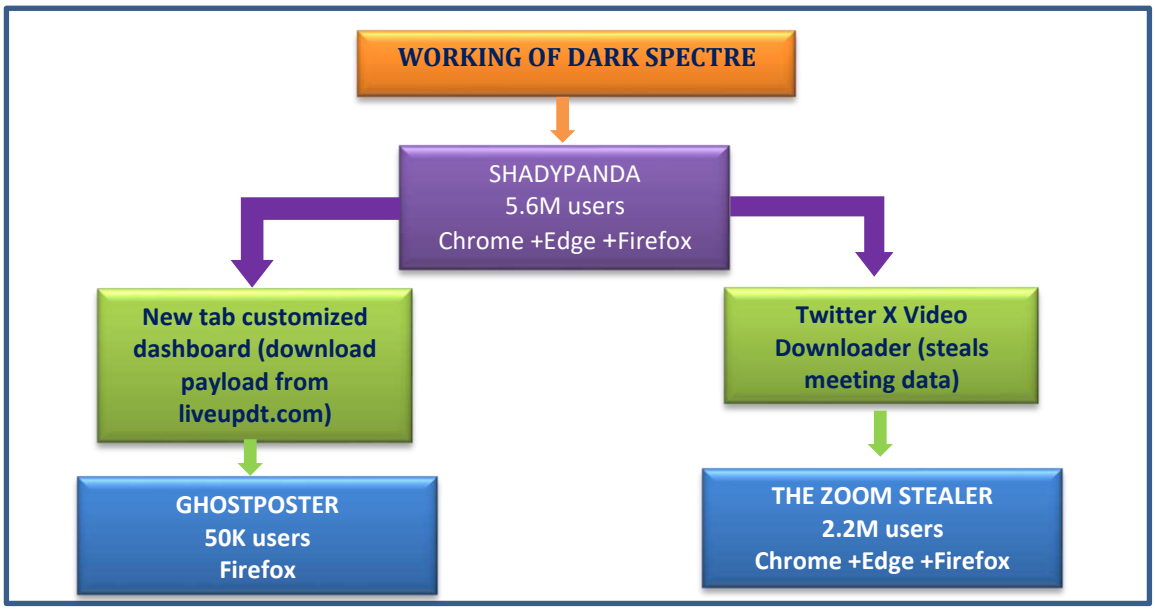
As digital payments and mobile banking grow rapidly in India, cyber-enabled financial fraud has been a major concern. FRI complements other safeguards by providing early warnings and actionable risk scores that financial entities can use to prevent fraud proactively.

- Works before money is lost
- Integrates telecom + banking + law enforcement
- Scalable model for national cyber security

2. CYBER FRAUDS

(A) DarkSpectre Hackers Infected 8.8 Million Chrome, Edge, and Firefox Users with Malware:

DarkSpectre refers to a sophisticated, long-running malware operation in which threat actors compromised an estimated **8.8 million users** by distributing malicious browser extensions through official extension stores for **Google Chrome, Microsoft Edge, and Mozilla Firefox**. These extensions appeared legitimate and often provided real functionality at first, allowing them to gain high download counts and positive reviews, but they secretly contained hidden or dormant code that was activated later through updates or remote commands. Once active, the malware enabled extensive surveillance capabilities, including tracking browsing activity, harvesting cookies and session data, injecting advertisements, redirecting traffic, and in some campaigns collecting sensitive information such as online meeting URLs, IDs, participant details, and embedded credentials. The attackers used advanced evasion techniques such as code obfuscation, delayed execution, and command-and-control infrastructure hosted on legitimate cloud services, which allowed the campaign to remain undetected for years. Researchers identified multiple coordinated sub-campaigns under the DarkSpectre umbrella, indicating an organized and well-resourced threat actor, with evidence suggesting possible links to China based on infrastructure and development patterns. The incident underscores a major security risk in the browser extension ecosystem, demonstrating how excessive permissions and user trust can be exploited at massive scale, and highlights the need for stricter extension vetting, continuous monitoring, and greater user caution when installing or updating browser add-ons.



How to check if you might be affected

- **Review installed extensions**

  - Chrome / Edge: Settings → Extensions
  - Firefox: Add-ons and themes → Extensions
  - Remove anything you don't clearly recognize or no longer use.

- **Check permissions carefully**

  - Be suspicious of extensions that request full website access without a strong reason.
  - Productivity or utility tools rarely need access to all browsing data.

- **Look for warning signs**

  - Browser slowdowns, unexpected redirects, new ads, or changed search results
  - Extensions updating frequently without clear feature changes
  - Background activity even when the browser is idle

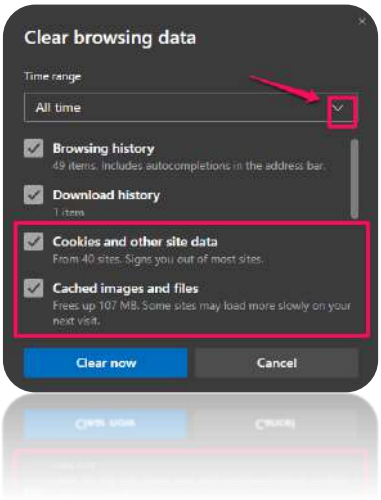
- **Check extension update history**

  - Some DarkSpectre extensions were benign at first and became malicious later through updates.

- **Run a security scan**

  - Use a reputable antivirus or endpoint protection tool that includes browser extension scanning.

- **Reset browser data (if suspicious)**



  - Clear cookies and site data
  - Log out of important accounts and change passwords, especially work-related ones

(B) WhatsApp Zero-Day Attack: Single Voice Call Could Compromise Smartphones

Cybersecurity researchers and government agencies have raised serious concerns over a newly reported **WhatsApp zero-day vulnerability** that could allow attackers to compromise a smartphone through **a single incoming voice call**, without the victim answering or interacting in any way. The flaw is believed to reside in WhatsApp's voice-calling mechanism, enabling a **zero-click attack** in which malicious code may execute silently in the background as soon as the call is received. Because it is zero-day vulnerability attackers may have had a window of opportunity to target users undetected. Experts warn that successful exploitation could lead to **remote code execution**, unauthorized access to private chats, photos, contacts, and even the installation of spyware capable of long-term surveillance. Financial institutions and cybersecurity authorities, particularly in the Middle East, have issued "high alert" warnings, emphasizing the heightened risk to banking customers, journalists, executives, and other high-value targets. Until an official patch is fully deployed, users are advised to immediately install any available WhatsApp and operating system updates.

What is zero-day vulnerability?

A **zero-day vulnerability** is a hidden weakness in software or a system that the company who made it does not know about yet. Because they don't know it exists, there is no fix or update available. Hackers can take advantage of this weakness to attack systems before anyone can stop it. It is called "zero-day" because the developer has had zero days to fix the problem.

- install updates from the App Store or Google Play as soon as they appear (security patches are likely forthcoming)
- Keep your phone's operating system updated
- Silence or block calls from unknown numbers
- Enable two-step verification in WhatsApp
- Be cautious with unrecognized numbers and unsolicited calls

3. TIPS OF THE MONTH

(a) QR Codes Can Be Risky: -

QR codes can be risky because they hide their destination, making it easy for attackers to direct users to phishing websites, malware downloads, or fake payment pages without obvious warning. Scammers often place malicious QR codes on posters, parking meters, menus, or even over legitimate codes, tricking people into entering personal information or financial details. Since users cannot see the full web address before scanning, it is harder to judge whether the link is trustworthy.

- To reduce risk, people should avoid scanning QR codes from unknown or suspicious sources.
- carefully review the URL before interacting with a site, and never enter sensitive information unless they are confident the source is legitimate.

(b) Limit Social Media Footprint: -

Limiting your social media footprint is one of the most effective ways to protect your personal information and prevent cyberattacks. Cybercriminals often gather small pieces of publicly available information such as birthdays, pet names, vacation plans, or work details to craft personalized phishing attacks, guess passwords, or even commit identity theft.

- Regularly review your privacy settings and make your posts, friend lists, and personal details visible only to trusted contacts.
- Be mindful of what you share, avoiding sensitive information like your home address, travel plans, birthday or anything that reveals your daily routines.
- Use unique usernames across platforms to make it harder for attackers to track you.
- Be selective with friend requests, accepting only people you know personally

(c) Log Out at the End of the Day

Logging out at the end of the day is an important security practice that helps protect sensitive information and systems from unauthorized access. Leaving accounts signed in, especially on shared or workplace devices, increases the risk of someone accessing data, sending messages, or making changes without permission. Logging out ensures that sessions are properly closed, reduces exposure to insider threats, and supports overall cybersecurity hygiene. Making it a daily habit to log out before leaving helps safeguard both personal and organizational information.

- Set a daily reminder to log out before leaving work or shutting down your device.
- Log out of all applications, not just email - include messaging tools, databases, and cloud platforms.
- Avoid saving passwords on workplace or public systems.
- Sign out of VPNs and remote access tools when you're done working.
- Enable automatic logout or session timeouts where available.

4. New Development in IT DTE

1.) E-bill

- Tour TA/DA Adjustment

2.) PPMS

- Appointment Correction Order (PIS Photo Update)
- PT/Parade Order

Dr. Srinivas M, Director, AIIMS New Delhi. Delivered enlightening talk on the critical role of healthy dietary practices in preventing lifestyle diseases.

DG CRPF At SDG ground during a friendly match

National voter's day pledge at CGO 2026