CENTRAL RESERVE POLICE FORCE

APRIL, 2026

CYBER BYTE

Iranian hackers target US critical infrastructure through ransomware proxies

STF Launches Major Crackdown On Cyber Fraud, Blocks Fake Websites And Social Media Links

COMN & IT Dte. CRPF

1. CYBER GEEKS NEWS

(A) North Korea targets Mac OS users in latest heist: -

North Korean criminals set on stealing Apple users' credentials and cryptocurrency are using a combination of social engineering and a fake Zoom software update to trick people into manually running malware on their own computers, according to Microsoft.

Redmond's threat intelligence team tracks the Pyongyang-backed crew as Sapphire Sleet (aka APT38). The Lazarus Group offshoot has been in business since at least 2020, and primarily targets the finance sector to steal cryptocurrency wallets and intellectual property related to cryptocurrency trading and blockchain platforms.

These attacks begin with social engineering. The crew creates fake recruiter profiles on social media and networking platforms like LinkedIn and then reaches out to finance professionals with phony job opportunities before scheduling a technical interview - that's the delivery mechanism for the malware. And they follow a rash of other social-engineering-enabled intrusions, including one in which North Korea-linked attackers socially engineered an Axios maintainer, compromised his account, and published malicious versions of the open source JavaScript library containing a remote-access trojan.

One thing organization can do to protect their users and themselves from falling victim to this and other social-engineering campaigns is to educate people about threats originating from LinkedIn and other social media sites, especially unsolicited communications asking users to download software or install virtual meeting tools.

.

For Individual Users

1. Be skeptical of "urgent help" requests

- Unsolicited messages on LinkedIn, email, or chat asking you to:
  - join a meeting
  - install software

  ☞ Treat them as suspicious by default.

Never run unknown scripts or files

- Files like `.scpt`, `.bat`, `.sh`, `.exe` = **high risk**
- Especially if sent during a "support session"

For Organizations

1. Conduct regular security awareness training

- Focus on:
  - social engineering
  - fake support scams
- Use real scenarios (like fake meeting invites)

2. Enforce "no script execution" policy

- Block or restrict:
  - AppleScript (.scpt)
  - PowerShell / shell scripts
- Especially from untrusted sources

(B) Char Dham Yatra Ahead: STF Launches Major Crackdown On Cyber Fraud, Blocks Fake Websites And Social Media Links

In addition, authorities have identified 52 mobile numbers suspected of being involved in the cyber fraud network. A request has been sent to the Department of Telecommunications (DoT) for blocking these numbers to prevent further misuse. Investigations have also revealed 10 websites operating fraudulent helicopter booking services in the name of Char Dham travel arrangements. These websites have been reported to their respective domain registrars for immediate deactivation.

Cyber criminals often use misleading advertisements and terms such as "official booking portal" to create a false sense of authenticity. In many cases, pilgrims are unable to distinguish between genuine and fake platforms and end up losing significant amounts of money.

Authorities have urged pilgrims to use only official government websites and authorized booking channels for any travel-related services. They have also advised people to avoid clicking on unknown links or trusting social media advertisements offering discounted pilgrimage packages.

Cybersecurity experts have noted that religious events often see a spike in online fraud cases, as people tend to act quickly due to faith and urgency, making them more vulnerable to scams. They emphasized that real-time monitoring and rapid response mechanisms are crucial to preventing financial losses.

☑ DO's (What you should do)

✔ Use only official platforms

- Book travel, darshan, or helicopter services through verified government portals
- Cross-check links from trusted sources (state tourism / official announcements)

✔ Verify before payment

- Confirm website authenticity (HTTPS, correct spelling, contact details)
- Call official helpline numbers if unsure

✔ Check domain carefully

- Look for minor spelling tricks (e.g., ".in.net", ".org.in")
- Prefer well-known domains over newly created ones

✔ Use secure payment methods

- Pay via trusted gateways (net banking, cards)
- Keep transaction receipts/screenshots

DON'Ts (What you should avoid)

✕ Don't trust "too good to be true" offers

- Cheap helicopter bookings or VIP darshan claims are major red flags

✕ Don't click unknown links

- Avoid links from SMS, WhatsApp, or social media ads

✕ Don't rely on social media pages

- Fake pages often copy logos and photos of real services

✕ Don't make advance payments blindly

- Especially via UPI IDs or personal numbers

2. CYBER FRAUDS

(A) Iranian hackers target US critical infrastructure through ransomware proxies, KELA warns

New data from KELA recognizes that Iranian state-sponsored threat actors have moved well beyond traditional espionage, increasingly blurring the line between nation-state operations and financially motivated cybercrime. Rather than running large-scale ransomware cartels of their own, these groups have embedded themselves into the existing criminal ecosystem, acting as initial access brokers, collaborating with ransomware affiliates, and deploying pseudo-ransomware to mask destructive attacks as extortion campaigns.

A key example is Pay2Key, an Iran-linked ransomware operation that has resurfaced as a professionalized RaaS platform operating on the anonymous I2P network, actively recruiting affiliates from Russian cybercrime forums and offering an elevated profit share, bumping the affiliate cut from 70% to 80%, for attacks on U.S. and Israeli targets. The model creates a significant compliance risk for victim organizations: paying what appears to be a routine ransom demand could unknowingly funnel money to OFAC-sanctioned Iranian entities, exposing companies to severe legal and financial penalties.
The KELA Cyber Intelligence Center identified in its Monday post that one of the more concerning developments is the growing collaboration between Iranian state-linked actors and the broader ransomware ecosystem.

A joint advisory from the Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, and Department of Defense Cyber Crime Center in August 2024 highlighted groups such as Pioneer Kitten, also known as UNC757 or Fox Kitten. Rather than deploying their own ransomware, these actors focus on exploiting vulnerabilities in internet-facing edge devices, including VPNs and firewalls, to gain initial access. Once inside, they collaborate directly with ransomware affiliates such as NoEscape, RansomHouse, and ALPHV/BlackCat, effectively handing off compromised networks in exchange for a share of ransom payments.

(B) LPG Booking Scam Alert: Cybercriminals Exploit Panic Amid Supply Concerns, I4C Issues Warning

Amid rising tensions in the Middle East involving Iran, Israel, and the United States, concerns over LPG supply disruptions have begun affecting consumers in India. As panic-driven demand surges, cybercriminals are exploiting the situation by launching fake LPG booking scams targeting unsuspecting users.

What is the LPG booking scam?

Experts describe the LPG booking scam as a form of cyber fraud where scammers impersonate gas agencies or service providers. Victims are contacted through fake websites, calls, or messages and are asked to share sensitive details such as OTPs, bank information, or payment credentials.

Once these details are shared, fraudsters gain access to victims' bank accounts and siphon off money, often within minutes.

How scammers trap victims?

Cybercriminals take advantage of urgency and fear, especially during times when supply disruptions are being reported. Posing as officials or representatives of gas agencies, they offer instant or priority LPG bookings.

Victims are lured into making quick decisions and are redirected to fake platforms or asked to make payments via suspicious links. In many cases, they are also asked to verify bookings through OTPs, which are then misused to complete fraudulent transactions.

Panic and urgency fuel the fraud

The current environment of uncertainty around LPG availability has made people more vulnerable. Many consumers, worried about delays or shortages, are booking cylinders in haste, often without verifying the authenticity of the source.

This urgency creates the perfect opportunity for scammers, who rely on psychological pressure rather than technical sophistication. Cyber experts, including officials from law enforcement, have urged citizens to remain cautious and avoid sharing any personal or banking details with unknown callers or websites.

They emphasise that genuine LPG providers never ask for OTPs or confidential financial information for booking services. Any such request should be treated as a red flag.

Authorities have advised users to rely only on official apps, websites, or registered distributors for LPG bookings. In case of suspicious activity, citizens should immediately report the matter to the national cybercrime helpline or online portal.

The rise of such scams highlights a broader pattern where cybercriminals exploit real-world crises to launch targeted fraud campaigns. Awareness and vigilance remain the most effective defence against such evolving threats.

Cyber experts, including officials from law enforcement, have urged citizens to remain cautious and avoid sharing any personal or banking details with unknown callers or websites. They emphasise that genuine LPG providers never ask for OTPs or confidential financial information for booking services. Any such request should be treated as a red flag. Authorities have advised users to rely only on official apps, websites, or registered distributors for LPG bookings. In case of suspicious activity, citizens should immediately report the matter to the national cybercrime helpline or online portal.

The rise of such scams highlights a broader pattern where cybercriminals exploit real-world crises to launch targeted fraud campaigns. Awareness and vigilance remain the most effective defence against such evolving threats.

3. TIPS OF THE MONTH

April is a high-risk month for cyber fraud in India—tax filing, new financial year activities, and events like the Char Dham Yatra 2026 create urgency that scammers exploit. Here's a practical April Cyber Security Do's & Don'ts guide:

☑ DO's (April Cyber Safety Tips)

✔ Verify tax-related communications

- Use only the official Income Tax Department of India portal
- Double-check emails/SMS claiming refunds or notices

✔ Secure financial accounts

- Enable **2-factor authentication (2FA)**
- Regularly check bank and UPI transactions

✔ Update devices and apps

- Install latest security patches on phone/laptop
- Update banking and payment apps

✔ Use official booking platforms

- For travel/pilgrimage (like Char Dham), rely only on government-authorized websites

✔ Verify job or offer messages

- Many fake "new financial year hiring" scams circulate in April
- Cross-check company details (e.g., Infosys, TCS)

✔ Backup important data

- Store copies of important documents securely (cloud or external drive)

✕ DON'Ts (Avoid These Common Mistakes)

✕ Don't click on refund/offer links blindly

- "Income tax refund" or "financial bonus" links are often phishing

✕ Don't share OTPs or banking details

- No legitimate authority asks for OTPs

❌ Don't trust social media ads

- Fake travel deals, job offers, and investment schemes increase in April

❌ Don't download unknown apps/APKs

- Especially those claiming "fast booking", "easy tax filing"

❌ Don't reuse passwords

- Avoid same password for banking, email, and social media

❌ Don't ignore small suspicious transactions

- Even ₹1 debit can indicate fraud testing

⚠ April-Specific Cyber Threats

- **Tax phishing scams** (fake refunds/penalties)
- **Pilgrimage booking frauds** (Char Dham, etc.)
- **Job scams** (new financial year hiring)
- **UPI collect request scams**
- **Fake investment schemes ("new year high returns")**

Quick Safety Formula

👉 **Think → Verify → Act**

If something feels urgent + financial + unexpected → **pause and check**

4. New Development in IT DTE

1.) PPMS

- Individual Achievement /Skill Entry Order
  - Pay Fixation Order
  - DCPS Recovery Order

DG CRPF Shri G.P. Singh (IPS) at inauguration of school (SAKSHYAM) for Differently Abled Children at GC, Jharoda Kalan.

DG CRPF Shri G.P. Singh (IPS) at GC, Jharoda Kalan interacting with Differently Abled Children and their parents.

DG CRPF Shri G.P. Singh (IPS) at CRPF HQr on the occasion of Gallantry Medal Recipient award ceremony on Shaurya Diwas-2026.