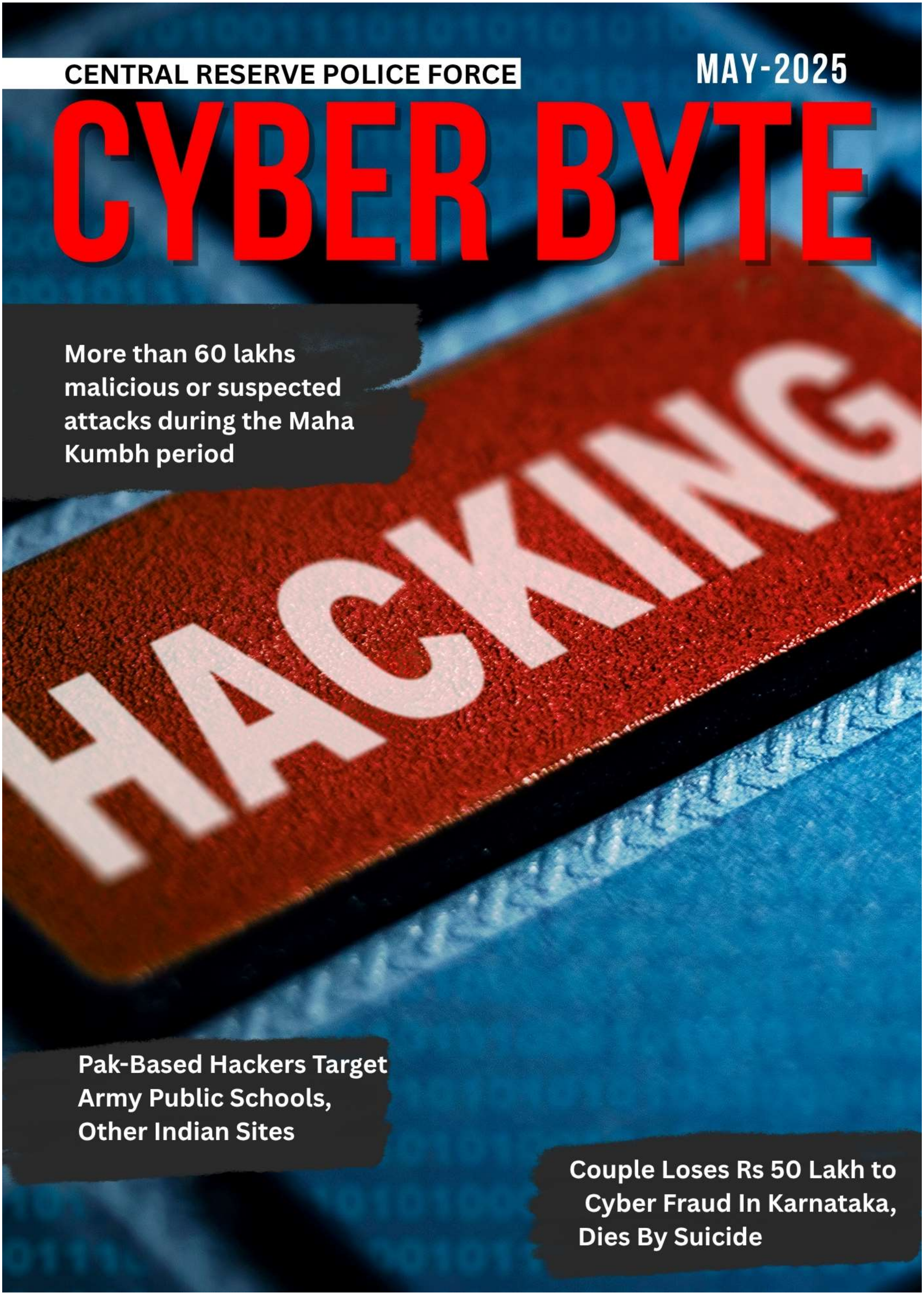
CENTRAL RESERVE POLICE FORCE

MAY-2025

CYBER BYTE



More than 60 lakhs malicious or suspected attacks during the Maha Kumbh period

Pak-Based Hackers Target Army Public Schools, Other Indian Sites

Couple Loses Rs 50 Lakh to Cyber Fraud In Karnataka, Dies By Suicide

1.CYBER GEEKS NEWS

A) More than 60 lakhs malicious or suspected attacks during the Maha Kumbh period

Cyberattacks aimed at disrupting the technological infrastructure deployed for the smooth functioning of the 45-day-long Maha Kumbh were foiled by a dedicated team of men in khaki who kept a close watch on such attacks, most of which originated from overseas IP addresses.

According to police, these attacks were related to ransomware, DNS poisoning, DDoS attacks, hacking, SQL injection, spoofing, brute force, web app attacks, many connection attempts over specific ports akin to trojans, malware and huge traffic from malicious IPs to name a few.

However, all these attacks were thwarted due to timely alerts by central agencies and prompt action by state police in coordination with various system integrators. Additional director general (Prayagraj zone) Bhanu Bhaskar said, “There were more than 60 lakhs malicious or suspected attacks during the Maha Kumbh period and these IPs were traced to more than 25 countries. The essence of Digital Maha Kumbh 2025 was preserved by ensuring the cyber security of the digital infrastructure of Maha Kumbh.”

B) Pak-Based Hackers Target Army Public Schools, Other Indian Sites

Pak based hackers target many Indian sites included Army Public School (APS) Srinagar, APS Ranikhet, the Army Welfare Housing Organization (AWHO) database, and the Indian Air Force Placement Organisation portal.

The provocation continues. Attempts to hack Indian websites by Pakistan-based cyber actors are on the rise since last week's Pahalgam terror attack that claimed 26 lives, the deadliest attack on civilians in Jammu and Kashmir in decades.

The attacks involved efforts to deface pages, disrupt services with a denial-of-service assault on APS Srinagar, and access personal information.

A Pakistan flag was visible right in the centre of the website pages, declaring "SITE HACKED", followed by a provocative message about Kashmir. A person in the centre with a Guy Fawkes mask (also known as the V for Vendetta mask or Anonymous mask) sits there pointing a finger at the viewer.

There have been multiple hacking attempts from Pakistan in the last few days, largely to autonomous institutions associated with the armed forces.

2. CYBER CRIME

A) Couple Loses Rs 50 Lakh to Cyber Fraud In Karnataka, Dies By Suicide

An elderly couple in Khanapur taluk, Belagavi district, died by suicide after falling victim to cyber fraud and alleged harassment, Diogjeron Santan Nazareth (82) and his wife Flaviana (79), residents of Beedi village in Khanapur, A two-page handwritten death note left behind by victim.

Victim named two individuals-Sumit Birra and Anil Yadav. He wrote that Birra, who claimed to be a telecom department official from New Delhi, informed him that a SIM card had been fraudulently purchased in his name and was being used for harassment and illegal advertisements. Birra later transferred the call to Yadav, who claimed to be from the Crime Branch. Yadav demanded details of victim's property and finances, threatening legal consequences over the alleged SIM card misuse.

Falling prey to the scam, victim transferred over Rs 50 lakh to them, but they continued to demand more, victim further stated that he had borrowed money from friends and requested that the loans be repaid by selling his wife's gold bangles and earrings.

B) Odisha MLA and former information technology minister has lost Rs 1.4 crore to cyber fraud

An Odisha MLA and former information technology minister has lost Rs 1.4 to cyber fraud in around one-and-a-half months, a senior police officer said here on Monday. The police arrested seven people - four from Karnataka and three from Tamil Nadu - in connection with the case.

The former minister, who lodged a police complaint in this regard in January, however, claimed that a friend of his had been using his trading account and lost the money.

The accused and their associates used to pose as trade analysts and persuade people to invest money into initial public offerings (IPOs), shares, and other forms of trading, promising them high returns, the police officer said. During the investigation, the cybercrime unit of the Crime Branch found that the accused people fraudulently obtained Rs 1.40 crore from the complainant.

3. TIP OF THE MONTH

A. Investment Scam

An Investment Scam involves fraudulent schemes that promise high returns, often too good to be true. These scams pay earlier investors with the money of new investors instead of generating profits through legitimate economic activity. It is also known as Ponzi scheme.

DO'S

- Invest with Registered Entities: Deal only with SEBI-registered intermediaries for investments.
- Verify Investment Products: Always invest through regulated financial entities.
- Stay Informed: Follow trusted information sources of regulated entities and financial products.
- Report Suspicious Activity: Call 1930 or cybercrime.gov.in

DON'T

- Don't Panic: Stay calm and verify the offer.
- Don't Trust Unbelievable Returns: Avoid schemes promising high returns with no risk.
- Don't Join Dubious Groups: Stay away from social media groups promoting suspicious trading apps.
- Don't Ignore Red Flags: Be cautious if the returns seem too consistent or too high over time.

B) Online Gaming

Online Gaming has become a hotspot for cybercriminals, with threats ranging from virtual theft and account breaches to real-world financial fraud and identity theft. Attackers exploit platform shortcomings and target players through phishing scams, malware, and social engineering.

DOS

- Supervise Access: If you are a parent, provide access to online games under supervision.
- Be Cautious with Real Money Apps: Many real money gaming apps may be fraudulent. Stay cautious and avoid apps that seem suspicious.
- Judicious App Permissions: Be careful before granting permissions like Contacts, Storage, and Location to the app.
- Protect Personal Information: Keep safe your sensitive personal information, such as your full name, address, or bank account details, etc.

DON'T

- Avoid Suspicious Sources: Do not download gaming apps from unreliable sources.
- Beware of Assured Returns: Do not install gaming apps that promise assured returns on social media or through advertisements.
- Keep Information Private: Do not share confidential information with unknown fellow players.
- Limit Social Media Sharing: Avoid oversharing your gaming achievements on social media to prevent becoming a target of harassment or cyberattacks.

C) Search Engine Fraud

Search Engine Fraud occurs when fraudsters manipulate search results to display fake contact information, posing as legitimate entities. Victims who unknowingly call these numbers may reveal sensitive information, such as passwords and account details, leading to financial loss, identity theft, and other severe consequences.

DOS

- Visit Official Websites: Always check the official website for contact details, rather than relying on search results.
- Verify Contacts: Double-check phone numbers and websites using caller ID or trusted directories before sharing personal info.
- Watch for Red Flags: Be wary of urgency, scare tactics, or suspicious offers. Legitimate companies don't pressure immediate action.

DON'T

- Don't Trust Search Results: Never call numbers listed in search engine results; fraudsters often disguise themselves as an illegitimate entity.
- Don't Share Info Unprompted: Only share personal details over the phone if you've initiated the contact

भौति

Shri Akash Garg and his parents felicitated by DG CRPF

Farewell Function of IG Communication

Veteran Shri Munshi Ram felicitated by DG CRPF

MOU Signing Ceremony Physics Wallah Foundation and CRPF Family Welfare Association