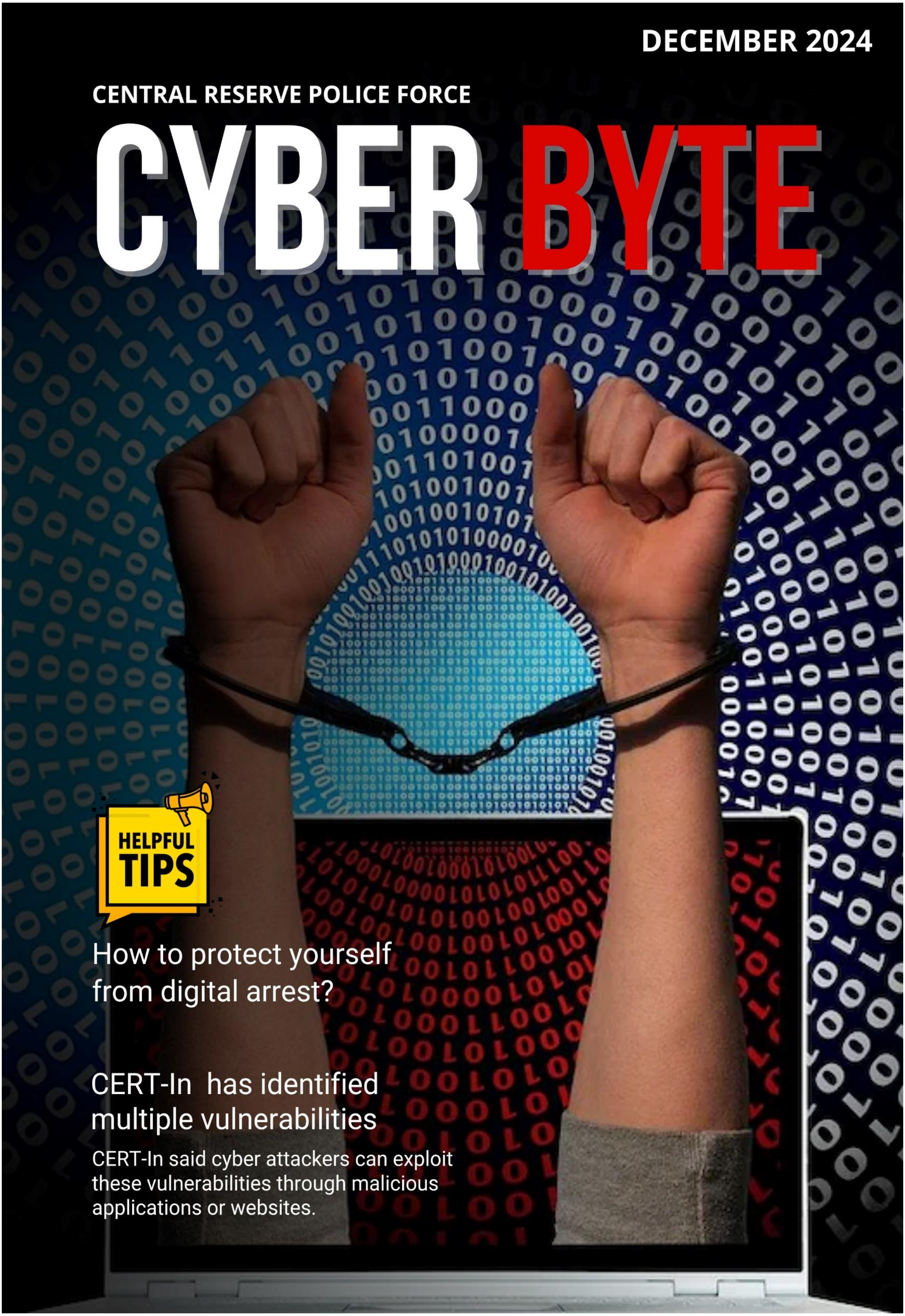
DECEMBER 2024

CENTRAL RESERVE POLICE FORCE

CYBER BYTE



HELPFUL TIPS

How to protect yourself from digital arrest?

CERT-In has identified multiple vulnerabilities

CERT-In said cyber attackers can exploit these vulnerabilities through malicious applications or websites.

1.CYBER GEEKS NEWS

A) Indian Computer Emergency Response Team (CERT-In) has identified multiple vulnerabilities in Android phones.

Phones with Android versions 15, 14, 13, 12 and 12L (for foldable phones) that could be exploited by hackers. These concerns have for both Android and Google Chrome users could potentially expose millions of devices at risk. Rated as "high-risk," CERT-In said that cyber attackers could exploit these vulnerabilities through applications or malicious websites to execute code and gain access to the system.

CERT-In advised users to update their Android devices as soon they were released by Google and Chrome. Users should ensure that they are running the latest version of the browser. Google has already acknowledged the issue and released security patches for these identified vulnerabilities, 129.0.6668.100 for Windows and Mac, and 129.0.6668.89 for Linux.

B) Razorpay Joins MHA To Boost Cyber Security Around Digital Payments Ecosystem

The Fintech major Razorpay on Monday said it has partnered with the Ministry of Home Affairs (MHA) and the Indian Cyber Crime Coordination Centre (I4C) to boost cyber security around the digital payments ecosystem in the country. The collaboration aims to empower businesses and end-customers with critical knowledge to protect themselves while driving widespread awareness about cybersecurity across the country. Recent data from the National Cybercrime Reporting Portal revealed a sharp increase in digital fraud incidents across India, with over **7,000** complaints reported daily

Strategic initiatives of I4C,

Alarmingly, 85 per cent of cyber complaints involve financial fraud, demonstrating the growing vulnerability of online transactions. From January to April, victims have lost more than $21.2 million to cybercrimes. "This partnership with Razor pay is a step towards strengthening our digital economy by combining the technological approach of Razor pay with the strategic initiatives of I4C," Director of Indian Cybercrime Coordination Centre, MHA.

Razor pay, in addition to its ongoing initiatives, will lead an extensive awareness campaign to educate businesses and consumers on critical topics concerning cybersecurity. The fintech platform has connected with over **1,600 cybercrime stations across 25 states and union territories**, enabling seamless.

2.CYBER FRAUDS

(A)NIA Raids 22 locations Across Six States in Human Trafficking, Cyber Fraud Probe

In a major crackdown on human trafficking and cyber fraud, the National Investigation Agency (NIA) conducted extensive raids at 22 locations across six states on Thursday. The operation targeted a large-scale trafficking syndicate involved in luring young Indians to Southeast Asia, particularly Cambodia, under the guise of well-paying jobs.

The raids focused on the premises of 17 suspects, including those in Vashi and Ghansoli in Navi Mumbai, as well as several districts across Maharashtra. In addition to Maharashtra, searches were also carried out in Bihar, Uttar Pradesh, Madhya Pradesh, Delhi, and Punjab.

The NIA's investigation focuses on individuals accused of facilitating the trafficking of Indian youth to Cambodia and other Southeast Asian countries. The searches were conducted on suspects including sub-agents, associates, and relatives of Indian agents based in Cambodia, who are allegedly managing the logistics and financial transactions of the trafficking network.

During the raids, NIA officials seized multiple digital devices, including mobile phones, laptops, hard drives, and memory cards. The agency also recovered a total of Rs 34,80,800 (Thirty-Four Lakh Eighty Thousand and Eight Hundred Rupees) in cash from the suspects' premises. Several individuals have been summoned for further questioning as the investigation progresses.

(B) Cyber fraudsters posing as doctors loot money from pregnant women in Odisha

In a disturbing and shocking incident of cyber fraud, several pregnant women have fallen victim to a new online scam, losing money to frauds posing as doctors and officials of the **Women and Child Development Department.**

The cybercriminals have been exploiting expectant mothers of their money given under ‘**Mamata Yojana**’ by posing as doctors and officials from the Women and Child Development Department. The matter came to the fore after an Anganwadi worker and expectant mother lodged a written complaint with Mohana police in Gajapati district.

According to sources, an Anganwadi worker received a call from the fraudster who claimed to be a doctor and a member of Women and Child Development Department. He enquired about all the pregnant women who had got money under Mamata Yojana and asked for their phone numbers.

3. TIP OF THE MONTH

(A) How to protect yourself from digital arrest

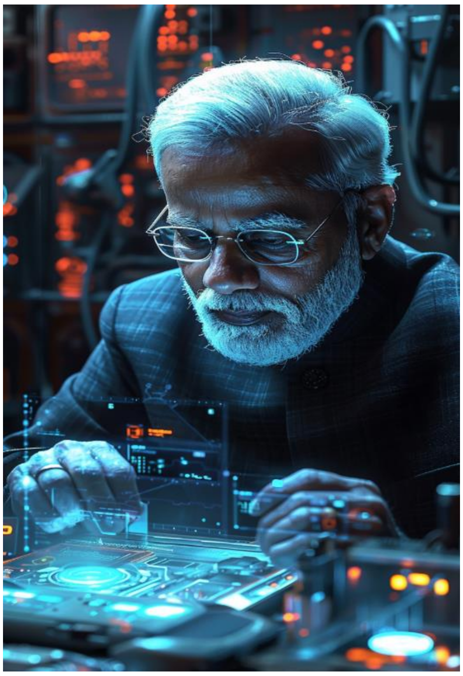
1. **Verify information**: Never share personal information or financial details with anyone over the phone or online unless you are absolutely certain of their identity and the legitimacy of their request.

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

3. **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.

4. **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) PM Modi expresses concern over threats emanating from digital frauds, cybercrimes, AI technology



Prime Minister Narendra Modi expressed his concern over the potential threats generated on account of digital frauds, cybercrimes and AI technology, particularly the potential of deep fake to disrupt social and familial relations.

Addressing the concluding session of the 59th All India Conference of Director Generals/Inspector Generals of Police, the prime minister also called for the use of technology to reduce the workload of the police constabulary and suggested that the police station be made the focal point for resource allocation.

Deliberations were held on **emerging security concerns** along the border with Bangladesh and Myanmar, trends in urban policing and strategies for countering malicious narratives, according to an official statement. In-depth discussions were held on existing and emerging challenges to national security, including counter-terrorism, left wing extremism, cybercrime, economic security, immigration, coastal security and narco-trafficking.

PM noted that wide-ranging discussions were held on national and international dimensions of security challenges and expressed satisfaction on the counter strategies that emerged during the conference, the statement said.

लावण्या
Salon and Beauty Parlour
inaugurated by
Smt. Rimjhim Singh
President
CRPF Welfare Association
on 19th November 2024

.