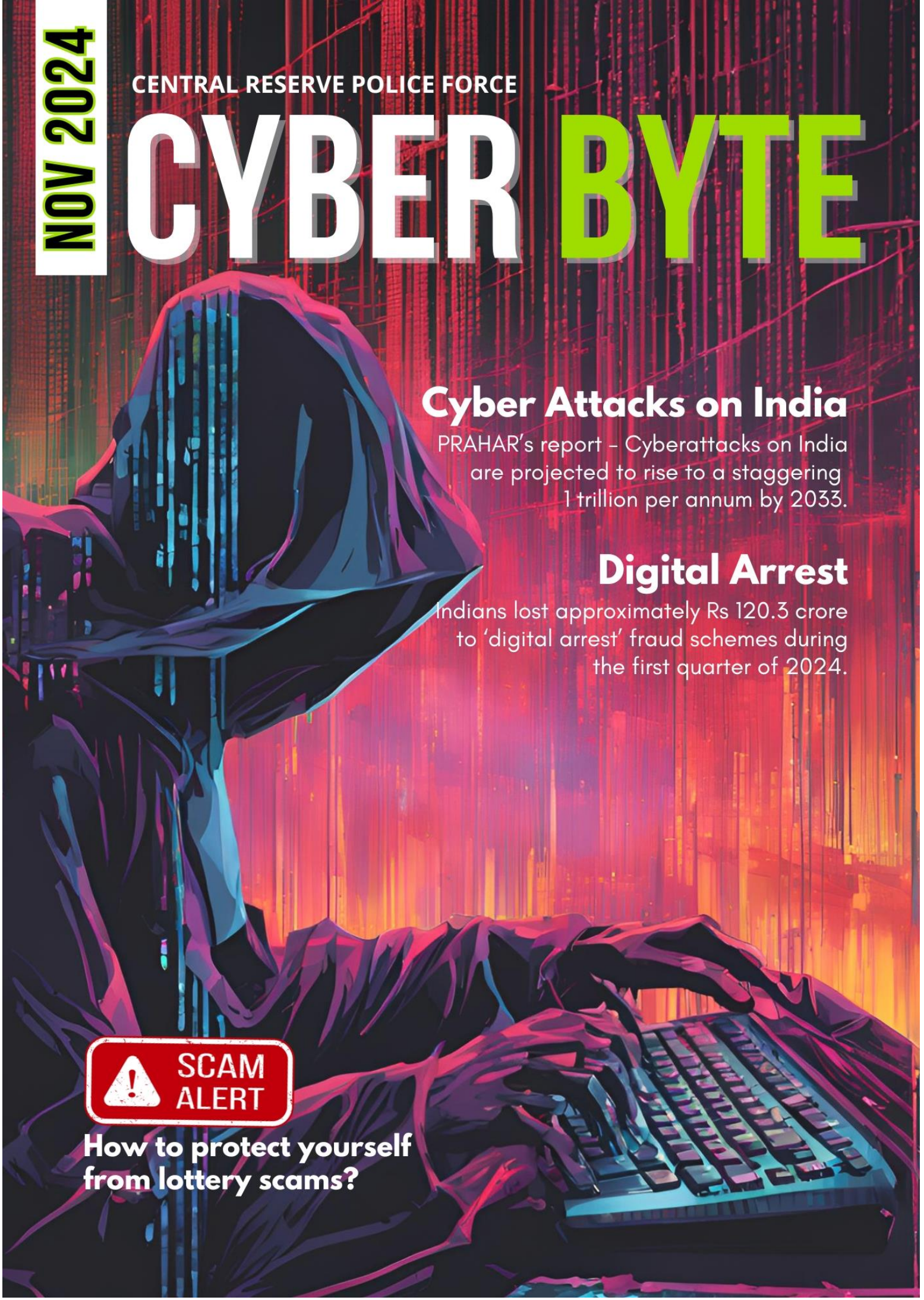
NOV 2024

CENTRAL RESERVE POLICE FORCE

CYBER BYTE



Cyber Attacks on India

PRAHAR's report – Cyberattacks on India are projected to rise to a staggering 1 trillion per annum by 2033.

Digital Arrest

Indians lost approximately Rs 120.3 crore to 'digital arrest' fraud schemes during the first quarter of 2024.

SCAM ALERT

How to protect yourself from lottery scams?

1.CYBER GEEKS NEWS

A) Cyber attacks on India are projected to rise to a staggering 1 trillion per annum by 2033

Cyber attacks on India are projected to rise to a staggering 1 trillion per annum by 2033, reaching 17 trillion by 2047, when the country turns 100, said a study by PRAHAR (Public Response against Helplessness & Action for Redressal), a not for profit organisation that takes up pressing issues where common citizen often feel helpless in dealing with them.

This alarming outlook indicated that the country's rise as a global power was being threatened by a steady, well-coordinated effort from adversaries aiming to destabilise its growth, both from within and outside its borders, cautioned the report.

Globally, cyberattacks increased by 76% in Q1 2024, with India among the most affected countries. This surge highlights a growing need for stronger cybersecurity measures across industries, particularly in sectors increasingly targeted by cybercriminals, as per the report.

In 2023, the country experienced over 79 million cyberattacks, ranking it third globally in terms of the number of such incidents. This marked a 15% increase from the previous year. The escalation continued into 2024. In the first quarter, reports indicated a sharp rise in cyberattacks, with over 500 million incidents blocked in just three months, it reported.

PRAHAR's report also observed that citizens' growing appetite for digital entertainment and gaming pushed them to illegal offshore betting and gambling platforms, making them vulnerable to sophisticated cyber manipulation, and turning them into tools for attacks on the state.

B) Crackdown on PAN details unauthorized use

Big crackdown on PAN details unauthorised use! The Indian Cybercrime Coordination Centre (I4C), operating under the Union home ministry, has directed the cessation of unauthorized usage of Indian citizens' Permanent Account Numbers (PAN) by financial technology companies and other consumer tech firms.

The government is taking stringent action against technology companies' unauthorized handling of personal data as it moves forward with implementing the Digital Private Data Protection Act, 2023 (DPDP).

2.CYBER FRAUDS

A) DIGITAL ARREST

Indians lost approximately Rs 120.3 crore to 'digital arrest' fraud schemes during the first quarter of 2024, as per recent government data. This fraud, among other scams, was highlighted by Prime Minister Narendra Modi during his monthly radio address 'Mann Ki Baat' on Sunday (October 27)

Understanding digital arrest fraud

Digital arrest fraud involves scammers posing as officials from investigative agencies or law enforcement bodies, such as the CBI, Narcotics Bureau, RBI, TRAI, customs, or tax authorities. These fraudsters reach out to targets via audio or video calls, using intimidation to extort money while keeping them confined — often in their own homes

B) Cyber Crime Branch of Ahmedabad in Gujarat busted an international gang

The Cyber Crime Branch of Ahmedabad in Gujarat busted an international gang involved in a ₹79,34,639 fraud case where the accused posed as officials from TRAI, Mumbai Cyber Crime, and the CBI. The gang tricked a local resident by falsely claiming that their mobile phone was involved in illegal activities.

Using intimidation tactics, including threats of an arrest warrant, the criminals continuously monitored the complainant through WhatsApp calls. They pressured the victim to transfer ₹79,34,639 to a bank account under the guise of verification, promising to refund the money after the process was complete.

A joint operation by the Cyber Crime Branch in Delhi and Bengaluru led to the arrest of two Taiwanese nationals, Mu Chi Sang and Chang Hao Yun (also known as Mark), who were key players in the scam.

Over 120 mobile devices were linked to this setup, with operations spread across Delhi, Bengaluru, and Mumbai. The gang was using rented bank accounts in exchange for commissions, provided by the locals in Gujarat, Rajasthan, Delhi, and Odisha, eight of whom were arrested during the raids.

3. TIP 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 help in facilitating the transfer of a substantial sum of money, generally in the form of an email. In return, the sender offers a commission, usually in the range of several million dollars. The scammers then request to send some money to pay for some of the costs associated with the transfer/processing fee or tax. If money is sent to the scammers, they will either disappear immediately or try to get more money with claims of continued problems 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 organisation 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 organisations do not ask for such data.
- It is essential to approach any unexpected windfalls with scepticism, 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.


NATIONAL
POLICE
MEMORIAL