CENTRAL TRAINING COLLEGE
(TELECOM & INFORMATION TECHNOLOGY)

AUGUST, 2025

e-Newsletter

https://crpf.gov.in/Training/Central-Training-College/CTC-(T-&IT)

Let's explore technology together
to live in the future

ctcit@crpf.gov.in @ctctitranchi CTC(T&IT)_CRPF_RANCHI ctctitcrpfranchi

INDEX

Contents

Published By:
CTC(T&IT),RANCHI

Cyber Security

The first quarter of 2025 saw a significant surge in cyberattacks, particularly ransomware attacks, with a record number of victims and active threat groups. Ransomware attacks increased by 126% compared to the same period in the previous year, according to Check Point. There was also a notable increase in the number of reported vulnerabilities and actively exploited flaws. A record-breaking 2,063 ransomware victims were recorded, marking the highest number in a single quarter, according to Zero Threat. There were 74 active ransomware groups, a 56% increase year-over-year. In 2025, cybercrime continues to be a major global issue, with costs projected to reach $10.5 trillion, according to Cybersecurity Ventures. India is also facing a surge in cyber threats, with a significant increase in malware detections and a growing sophistication of attacks. These attacks are targeting both individuals and organizations, highlighting the need for enhanced cybersecurity measures and awareness. The recent cyber attacks that came into limelight are as under.

Cambodia hosts slave camps: Criminals advertise well-paid jobs in Asia, and those who travel to take them up are often enslaved in camps and forced to spend their days running romance and investment scams. The United Nations thinks over 100,000 people may toil in such camps, which human rights group Amnesty International describes as "hellish scamming compounds" that operate "with the apparent consent of the Cambodian government.

Maritime Sector Faces Surge in APT and Hacktivist Cyber Threats: The maritime industry, responsible for as much as 90% of global trade, is increasingly becoming a target of cyber threat actors. A recent Cyble report documented more than a hundred cyberattacks by advanced persistent threat (APT) groups, financially motivated threat actors, ransomware groups, and hacktivists, as the maritime and shipping industry has become a prime target amid growing geopolitical conflict.

In one notable incident in March 2025, in concert with U.S. attacks on Houthi rebels in Yemen, the anti-Iranian group Lab Dookhtegan launched a well-orchestrated cyberattack that allegedly disrupted communications (VSAT) on 116 Iranian vessels. The operation reportedly severed inter-ship and ship-to-port links, targeting entities accused of supplying arms to Houthi forces. Electronic interference, including GPS jamming and spoofing, is escalating in critical maritime chokepoints like the Persian Gulf and Strait of Hormuz, posing a serious threat to vessel safety and operational reliability.

Russian Pharmacies Hit by Coordinated Cyberattacks, Shutting Services Nationwide : Several of Russia's largest pharmacy chains, including Rigla, A5, and ASNA, were forced to suspend operations following what officials described as a coordinated wave of cyberattacks targeting their IT infrastructure. The disruption affected hundreds of retail locations and online medicine delivery services, leaving consumers scrambling for essential medications.

Son squanders Rs 3cr in online gaming; cyber crime steps in to help: The case came to light when a retired government employee approached the State Cybercrime Office after losing a substantial chunk of his Provident Fund and savings that he got following his retirement. He lost the money after his unemployed son blew it away playing online games via apps. Initially, the son lost a few lakhs, which resulted in family disputes. But matters took a turn when the losses mounted to Rs 3 crore. Soon, the staff working at the 1930 Cybercrime Control Room sprang into action and technical experts, including the mobile forensics team, pooled their efforts to trace the transactions and freeze the remaining funds. The State Cybercrime team reassured the distraught father and promised all possible assistance. A formal complaint has also been registered, but the father has sought anonymity out of fear of social stigma and to protect his son.

₹1550 crore cyber fraud busted in Gujarat:8 RBL bank employees accused of opening fake current accounts;

linked to 50 lakh transactions: In a massive cyber fraud case involving transactions worth ₹1550 crore, Udhana Police in Surat have arrested eight employees from three RBL Bank branches—Sahara Darwaja, Besu, and Varachha. The arrests have uncovered a wide-reaching fraud network involving over 50 lakh bank accounts nationwide. According to DCP Bhagirath Gadhvi, the arrested bank staff were directly involved in opening 164 fake current accounts that facilitated fraudulent transactions. Investigations revealed they received illegal commissions ranging from ₹20,000 to ₹2 lakh for opening fraudulent accounts. The 164 current accounts were used for transactions linked to online betting, gaming, and cyber fraud. These accounts received money from more than 50 lakh savings and current accounts across India, with amounts ranging from ₹100 to several lakhs.

Social media misuse' constitutes bulk of cybercrime cases in MP, youngsters most affected:

Social media misuse forms the bulk of cybercrime cases in Madhya Pradesh, particularly affecting the young and most productive section of the State. Out of the 1021 total cybercrime cases reported across the central Indian State in 2022, as many as 542 cases, which accounted for more than 53 per cent of the total cases, pertained to misuse of social media. In 2023, when the total number of cybercrime cases declined to 927 (a dip of 9%), the cases related to social media abuse comprised 46% or 428 cases out of the total cases. In 2024, as many as 1082 cases of cybercrime (which was the highest in three years) were registered by police in the State, out of which 37% or 396 cases were related to social media abuse. Out of the 511 cybercrime cases reported this year, more than 47% cases (242 cases) are related to social media misuse.

Raids Underway Across 4 Cities In Rs 260 Crore Global Cyber Fraud Case:
In a major crackdown on an international cyber fraud racket, the Enforcement Directorate (ED) is conducting extensive search operations at 11 locations across Delhi, Noida, Gurugram, and Dehradun. The raids are part of an ongoing investigation into a massive scam involving extortion, impersonation, and cryptocurrency laundering under the provisions of the Prevention of Money Laundering Act (PMLA), 2002. The ED's probe stems from multiple FIRs registered by the Central Bureau of Investigation (CBI) and Delhi Police. Investigations have so far revealed that both foreign and Indian nationals were targeted and defrauded by cybercriminals posing as police officers, law enforcement agents, or tech support executives from major companies like Microsoft and Amazon. Using fear tactics, the fraudsters threatened victims with arrest or legal consequences, coercing them into transferring large sums of money.

Emerging Cybersecurity Trends to Watch Out in 2025:

- The Emergence of Automotive Cybersecurity Threats.
- Harnessing the Power of Artificial Intelligence in Cybersecurity.
- Mobile Devices: A Growing Target for Cyber Attacks.
- Cloud Security Challenges and Solutions.
- Data Breaches: A Persistent Concern.
- IoT Security in the Era of 5G.
- Targeted Ransomware Attacks.
- Escalating State-Sponsored Cyber Warfare.
- Mitigating Insider Threats Through Awareness.
- Combating Social Engineering Attacks.
- Enhancing Security with Multi-Factor Authentication.
- Strengthening Identity and Access Management.

******** "Be proactive, not reactive: Take charge of your cybersecurity."*********

AI Replay of the Browser Wars.

(Bloomberg Opinion) -- A quarter of a century ago, when Microsoft Corp. used its dominance of the personal computer market to force people to use Internet Explorer, it famously led to a devastating antitrust lawsuit loss that some believe held the company back for more than a decade. Only now, revitalized by Chief Executive Officer Satya Nadella's quick moves in artificial intelligence, is the Windows-maker back on top. As AI rivalries intensify, Google is now trying to put Microsoft through its '90s nightmare again.

The search giant is funding the Browser Choice Alliance, an industry group involving Google and a number of smaller browser makers, such as Opera, Vivaldi and others, set up to put pressure on Microsoft. The complaint, as it was back then, is that Microsoft is once again using its ownership of the Windows operating system to give its own browser an unfair leg up — at a moment that some feel is as pivotal as the emergence of the internet.

The new “Browser War” is brewing thanks to the desktop or laptop computer’s position as one of the biggest early battlegrounds in AI. While the smartphone has become people’s most frequently used computing platform, the desktop (or laptop) has retained its place for accomplishing real work — the kind of tasks AI makers say they can help with the most. As such, we’re seeing a slew of new or improved browsers hit the market, with new entrants such as the Browser Company’s Dia browser or Perplexity’s Comet. OpenAI is said to be working on its own. Winning the browser is seen as critically important as it can help forge new habits. Perplexity, for instance, told me that users who installed Comet were making three times more AI queries every day than they had been previously.

Microsoft recently announced that Edge — the default browser for Windows users — had received a significant AI upgrade. The company’s CoPilot assistant is now embedded in the browser and can take control of a user’s tabs to carry out tasks such as making a booking, much like a human might.