CENTRAL RESERVE POLICE FORCE

JUNE, 2026

CYBER BYTE

Zero Trust Security follows a simple principle: "Never Trust, Always Verify.

Boss Scam: MHA Warns Citizens Against Cybercriminals' New Modus Operandi

(COMN & IT) DTE. CRPF

1. LATEST CYBER THREAT

Boss Scam: MHA Warns Citizens Against Cybercriminals' New Modus Operandi

'Boss scam', I4C – the Indian Cyber Crime Coordination Centre, MHA, has issued an advisory warning citizens about fraudulent emails and WhatsApp messages which could impersonate RBI officials and target CEOs of companies. Through CEOs, subordinate employees could be compromised to carry out high-value financial frauds.

How the Scam Operates

Cybercriminals are targeting high-ranking officials and executives by delivering malicious archives via email or WhatsApp under the guise of urgent regulatory compliance.

The same modus operandi has been observed in CRPF. The fraudster first calls the Control Room of Unit, Office, or Establishment and falsely identifies himself as an IT Officer or a senior officer. He then requests the mobile number of the DBA. After obtaining the DBA's contact number, the fraudster calls the DBA and instructs them to install an application that is sent via WhatsApp. The intention is to deceive the DBA into installing a malicious application, potentially compromising official systems and sensitive information.

How to escape: -

Aware all employee about the Cyber Hygiene and Cyber Security.

2. Third-Party Vendor Attacks (Supply Chain Attacks)

In recent years, cybercriminals have increasingly targeted third-party vendors and service providers instead of attacking organizations directly. Rather than trying to break through a well-protected organization's security, attackers look for weaker vendors who already have access to the organization's systems.

Today's organizations rely on many external vendors, cloud services, software applications, APIs, and open-source software. If any one of these is compromised, attackers may use it as a gateway to gain unauthorized access to the organization's network.

For example, if a computer maintenance company, software vendor, or cloud service provider has access to an organization's systems and their own security is weak, attackers can misuse that access to enter the organization's network without raising suspicion.

Our organization also engages third-party vendors for activities such as the repair and maintenance of computers, servers, network devices, and other IT equipment. During such work, vendors may require access to systems, administrator accounts, passwords, or other sensitive information.

Therefore, before awarding any contract or assigning work to a third-party vendor, a Third-Party Vendor Cybersecurity Policy should be implemented to ensure that the organization's information and IT assets remain secure.

All vendors must:

- Use their access only for authorized work.
- Keep all official information confidential.
- Follow the organization's cybersecurity guidelines and security procedures.
- Return or delete any official data after completion of the assigned work.
- Be monitored throughout the engagement to ensure that organizational data and systems remain protected.

Key Message:

Even if an organization's own security is strong, a poorly secured vendor can become the weakest link. Therefore, every third-party vendor must be treated as a potential cyber security risk and should be granted only the minimum access required to perform the assigned task.

2. KNOWLEDGE BANK

1. Agentic AI Attacks

Hackers are now using Artificial Intelligence (AI) to attack computer systems automatically. Instead of a person manually searching for weak points, AI can quickly scan networks, find security gaps, break into systems, and move from one computer to another with little or no human involvement. This makes cyberattacks much faster and more difficult to stop..

2. Deepfakes & Identity Deception

Cybercriminals are using AI to create fake voices and realistic-looking videos that closely imitate real people. They can pretend to be your boss, a senior officer, or a trusted colleague and ask you to transfer money, share confidential information, or perform urgent tasks. Because these fake audio and video messages appear genuine, it has become much harder to verify a person's identity

3.Malware-Free Infiltrations

Modern hackers do not always use viruses or malware to break into systems. Instead, they steal usernames and passwords or misuse legitimate tools already available in the operating system (such as Windows administrative utilities). Since these are genuine tools used by system administrators, their malicious activities are much harder to detect using traditional antivirus software.

For enhanced security, regularly monitor your system's behavior using process analysis tools to identify any abnormal or unauthorized activities. Keep your antivirus software up to date and perform regular system scans. Additionally, verify that your system has not been altered or modified without proper authorization.

3. How to protect IT infrastructure

Zero Trust Security – Trust No One by Default:

Earlier, once a user logged into an organization's network, they were generally trusted and could access many systems. However, cyber threats have become much more advanced, and stolen usernames and passwords are frequently used by attackers to gain unauthorized access.

Zero Trust Security follows a simple principle: **"Never Trust, Always Verify."** Every user, device, and application must be verified before being allowed to access any system or data, even if they are already inside the organization's network.

Under this approach:

- Users are given access **only to the systems and information required for their official duties**.
- Different parts of the network are separated so that, even if one system is compromised, the attacker cannot easily move to other systems.
- All user activities are continuously monitored, and suspicious actions, such as repeated failed login attempts or access from unusual locations or devices, are immediately investigated.

This approach is particularly important today because employees access official systems from different locations, networks, and devices. Therefore, security should depend on **continuous verification** rather than simply trusting a user because they are connected to the organization's network.

Action Required

It has been observed that several Units/Establishments are providing unrestricted Internet access to users without proper access controls, which increases the risk of cyberattacks and unauthorized access.

Accordingly, all DBAs/Technical Officers should ensure that:

- Every user is provided **Role-Based Access Control (RBAC)**, allowing access only to the systems and applications required for official duties.
- Administrative privileges are granted only to authorized personnel.
- All Internet traffic is routed through the **centralized firewall** to enable uniform security monitoring, filtering, logging, and enforcement of cybersecurity policies across the organization.

Key Message:

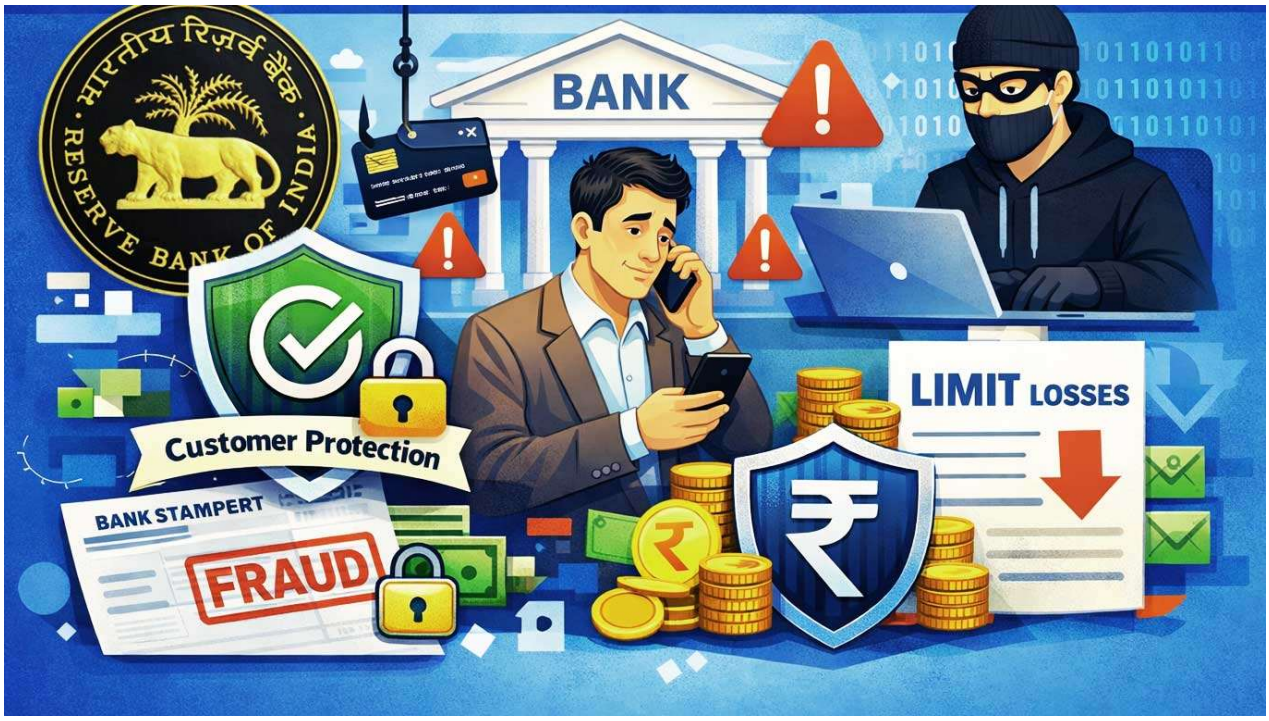
Do not trust any user or device automatically. Verify every access request, provide only the minimum permissions required, and monitor all activities continuously to minimize the impact of cyber threats.

.

4. CYBER GUPSHUP

10 Arrested in Delhi for online banking frauds worth Rs 26 lakh"

New Delhi, Police arrested 10 people of an interstate cyber fraud racket operating from Jharkhand's Jamtara and Deoghar regions and Delhi-NCR, who were allegedly involved in online banking fraud worth over Rs 26 lakh,



According to the police, the syndicate used sophisticated APK malware, impersonation scams and remote access techniques to target gullible victims. The accused allegedly posed as bank officials, persuaded victims to install malicious APK files through WhatsApp, gained unauthorized access to their mobile phones, stole internet banking credentials, intercepted OTPs and siphoned money from their bank accounts.

2. Anatomy of Rs 7.8 crore cyber fraud: WhatsApp 'Boss' Scam

According to police sources, the IFSO unit, which is probing the case, found that the scammers had initially sent the malicious message to one of the company's directors. Perceiving it as urgent, the director forwarded it to the accountant for further action. As soon as the accountant clicked on the ZIP file, his WhatsApp account was allegedly compromised. The alleged fraudsters then gained control of

the account, altered company contact details on WhatsApp, and began sending messages impersonating him. They instructed the accountant to transfer funds through Real-Time Gross Settlement (RTGS), a system used for urgent, high-value bank transactions. Sources said the scammers are targeting high-ranking officials and corporate executives by sending malicious ZIP archives through email or WhatsApp under the guise of urgent regulatory compliance requirements. In some cases, they impersonate officials from the Reserve Bank of India (RBI). The messages typically create a false sense of urgency by providing only a short time window for compliance.

Once the malicious file is executed, malware infects the executive's Windows device and active WhatsApp Web sessions. This enables the scammers to communicate with subordinate employees while posing as senior executives and to orchestrate fraudulent financial transfers.

5. CYBER HYGIENE

1) Ensure your operating system Windows 11 up to date.

2) Trellix antivirus installed and updated.

3) Don’t click on short links.

4) Don’t open the images, pdf files, zip files received from unknown sources.

5) Don’t open the email which is received from unknown sources.

6) Scan the USB drive while using in network.

6. New Development in IT DTE

1 Sambhav

GMS has been successfully integrated into the Sambhav App. CRPF personnel can now conveniently lodge complaints through the Sambhav App.

2. E-bill

i) The Newspaper Bill Claim functionality has been made available in the e-Bill module, enabling users to submit their Newspaper bill claims electronically.

ii) The Mobile and Telephone Bill Claim feature has been introduced in the e-Bill module.

3. Power BI Report

i) The Signal Stock Position has been made available in the Power BI Report.

ii) The Signal Personnel Strength dashboard is now available in Power BI for monitoring and analysis.

iii) The CRD OPS Report has been made available in Power BI, offering a comprehensive view of the working profiles of all CRPF personnel.

DG CRPF Shri G.P. Singh (IPS) joined the trainers, recruits, and administrative staff for a 'Bada Khana' at RTC Peringome.

DG CRPF Shri G.P. Singh (IPS) planting a sapling, reinforcing the Force's deep commitment to environmental conservation at RTC Peringome.

DG CRPF Shri G.P. Singh (IPS) presenting Memento to superannuating officers at a grand farewell party at Dte. Genl.