भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

प्रेस विज्ञप्ति
PRESS RELEASE

संपर्क प्रभाग, सेबी भवन, बांद्रा कुर्ला कॉम्प्लेक्स, बांद्रा (पूर्व), मुंबई - 400 051
Communications Division, SEBI Bhavan, Bandra Kurla Complex, Bandra (E), Mumbai – 400 051
दूरभाष / Tel: +91-22-26449000 ईमेल / email:press@sebi.gov.in वेबसाइट /website: www.sebi.gov.in

PR No. 40/2026

Caution to Regulated entities and listed companies- Boss Scam

The Indian Cyber Crime Coordination Centre (I4C) has intimated SEBI about an emerging trend in cybercrime referred to as the "Boss Scam" or CEO/ MD impersonation fraud.

The modus operandi of the Boss Scam is stated below:
Target and initiation of fraud: Fraudsters are targeting CEO or high ranking official via email or WhatsApp by impersonating them. The communication through email/ WhatsApp/Microsoft Teams/other social media platforms with their subordinates or counterparts, directs them to carry out instructions given to them resulting in transfer of funds to fraudsters.

Impersonation through Deep-fakes/ Malicious Zip Archive: The fraudsters have been observed to be employing either of the following strategies:

a. Strategy A: Impersonation of MDs/ CEOs through deep-fake methodologies like voice cloning, use of AI on video calls impersonating MDs/CEOs, false groups on Social Media Platforms impersonating high ranking officials.
b. Strategy B: Sending a compressed .zip archive through the message. This archive comprises of a malicious executable (.exe) accompanied by a Dynamic Link Library (.dll) file. As observed by I4C, the CEO forwards the message to his finance officers.

Instructions to transfer funds: Through Strategy A stated above, the finance officer is instructed to transfer funds to a specified mule account which may/ may not be accompanied with directions to not share the transaction as it may be Unpublished Price Sensitive Information. All the instructions are observed to have been shared through messages/ fake calls on Social Media Platforms

Hijacking of Whatsapp Web: Through Strategy B stated above, when the finance officer extracts and executes the file on a Windows desktop or laptop, a Trojan dropper is initiated. The malware hacks the system and hijacks the active Web

WhatsApp session tokens. The fraudster gets access to the finance officer's WhatsApp account and then contacts accounts or finance employees, instructing them to make immediate payments to specified mule bank accounts. Alternatively, if the fraudster achieves complete device takeover, they secretly alter the contact list on the device, and saves the fraudster's phone number under the name of the CEO/MD and use that secondary number to instruct finance officer into transferring funds.

Regulated entities and listed companies are advised to:

- Remain cautious and cross-check requests received through WhatApp/ email/ social media platforms, by calling their seniors.
- Do not transfer funds solely on the basis of instructions received on any social media platforms.
- Not install executables without verifying the identity of the sender or verifying through call, if received from a known sender
- Log out any Web WhatsApp sessions that are not being actively used.
- Report any fraudulent applications or any scam incident immediately on 1930 or www.cybercrime.gov.in.

SEBI is issuing this Press Release as I4C has observed an emerging trend in cybercrime referred to as the "**Boss Scam**" or CEO/MD impersonation fraud whereby fraudsters are targeting high-ranking officials/finance executives which compels them to transfer of funds to fraudsters.

Mumbai
July 17, 2026