Executive Summary

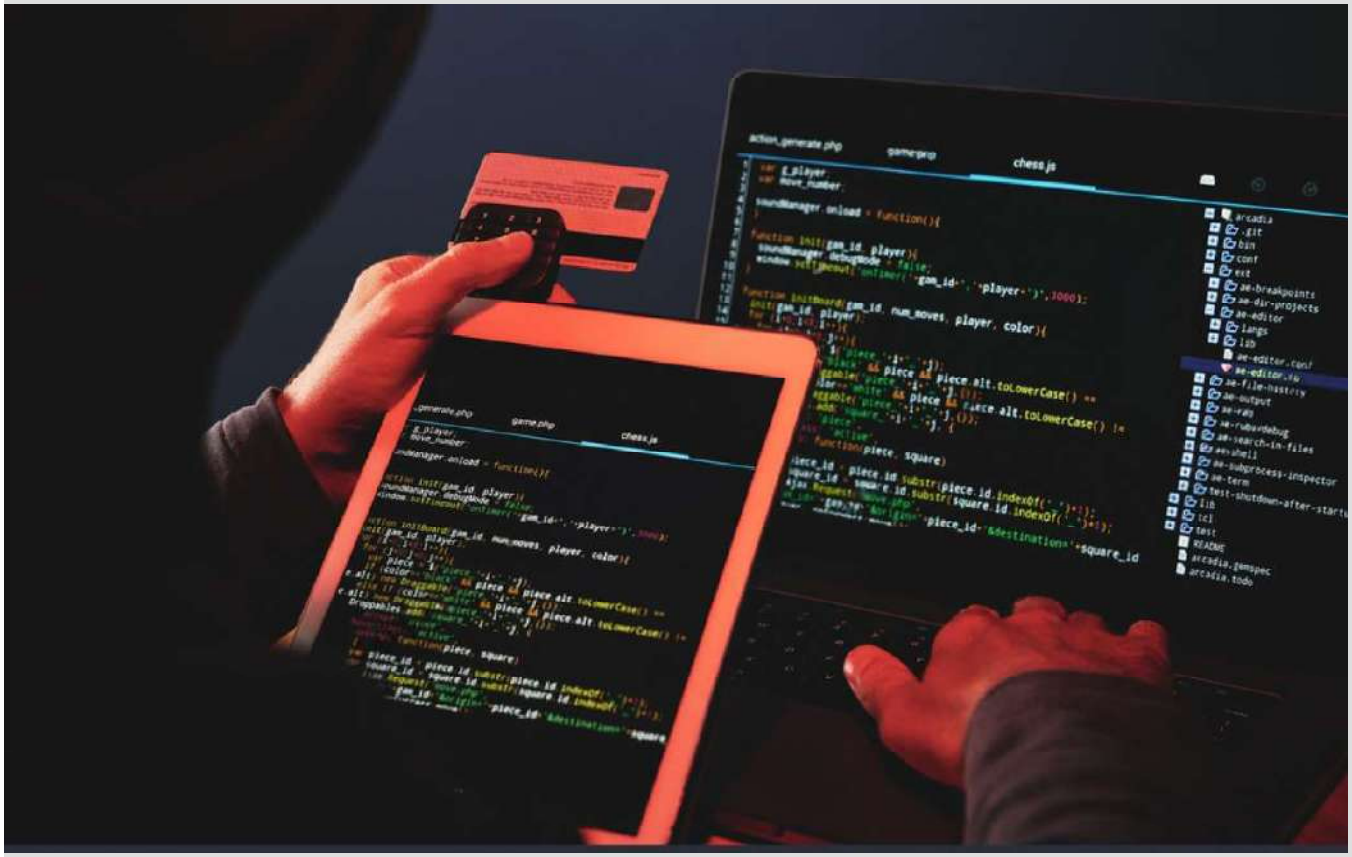
Fraudulent emails impersonating cyber cell authorities are on the rise, targeting individuals, businesses, and government entities. Scammers exploit fear and deception, disguising emails as official communications from cyber crime units to falsely accuse recipients of illegal activities or demand sensitive financial and personal information.

To appear legitimate, these fraudsters use forged letterheads, fake case numbers, and intimidating legal jargon, making their messages look like authentic government notices. Some emails even contain malicious links or attachments designed to install malware and compromise devices. In many cases, victims are pressured into making financial payments under threats of legal action.

This advisory aims to empower citizens and organizations with the knowledge and tools to recognize and resist cyber cell impersonation scams. Strengthening cybersecurity awareness, verifying official communications, and reporting suspicious activity are crucial steps in safeguarding trust in legitimate law enforcement efforts.

PUBLIC ADVSIROY

Introduction



PUBLIC ADVSIROY

There's a rising wave of cyber scams across India where fraudsters pose as Cyber Cell officials, sending fake emails that accuse recipients of crimes like child pornography, financial fraud, or data theft. These emails use official-looking logos, case numbers, and names of senior law enforcement officers to create panic and extract money or personal data.

Scammers often demand immediate action—threatening arrest or legal consequences unless the recipient responds, pays a fee, or clicks malicious links. These tactics aim to exploit fear and lack of public awareness.

According to **CERT-In** and the **Indian Cyber Crime Coordination Centre (I4C)**, phishing and impersonation remain among the top-reported cyber threats in India. Law enforcement does **not issue legal threats via email or WhatsApp without due process**.

Real Incident

- Navi Mumbai: 51-Year-Old Woman Duped of ₹32 Lakh by Cyber Crooks Posing as ED Officials
- Fake cyber cell email used to freeze bank accounts, case registered in Navi Mumbai
- Retired Punjab DGP Loses ₹2.5 Lakh to CBI Impersonators
- Tamil Nadu Police Dismantle Fake Cybercrime Reporting Portal
- Phishing Emails Alleging Sexual Offenses Circulate
- Fake Bank Alert Email Leads to ₹10 Lakh Theft
- Fake Tech Support Email Installs Malware on Corporate Systems

PUBLIC ADVSIROY

Key Indicators of Scam Email

Recognizing the signs early can help prevent falling victim. Here are some **red flags**:

Indicator	Details
Suspicious Sender Email	Not from official domains (e.g., @gov.in)
Unrealistic Threats	Claims of immediate arrest or legal action
Requests for Personal/Financial Info	Asking for PAN, Aadhaar, bank details, or payments
Grammatical Errors & Poor Formatting	Common in fake notices
Attachments or Links	Contain malware or phishing websites

Example Scam Subject Lines:

- "Immediate Action Required: FIR Registered Against You"
- "Cyber Crime Investigation Notice"

"Legal Summons from CBI Office"

Impact and Consequences

Falling victim to these scams can lead to:

Financial Loss:

Victims risk financial losses from fraud, hacked accounts, and deceptive investments—falling prey to phishing, fake tech support, and scam deals.

Identity Theft:

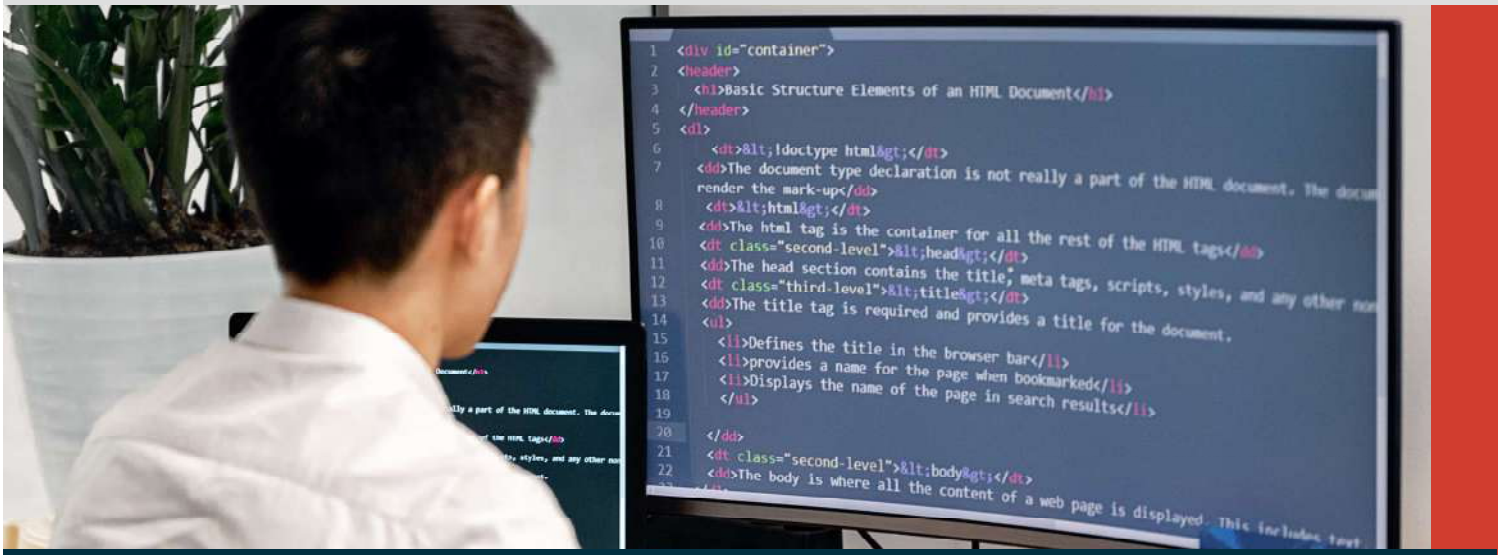
Scammers steal Aadhaar, passport details, and login credentials to commit identity fraud—opening fake accounts, filing false tax returns, and ruining financial credibility.

Reputational Damage:

Scammers steal Aadhaar, passport details, and login credentials to commit identity fraud—opening fake accounts, filing false tax returns, and ruining financial credibility.

Operational Disruption:

A hacked business system can lead to downtime, data breaches, and ransomware demands—crippling operations and exposing client data.



PUBLIC ADVSIROY

Preventive Measures

PUBLIC ADVSIROY

For Individuals:

- Do not respond to suspicious emails.
- Do not click on unknown links or download attachments.
- Verify legal notices through official sources to avoid scams.
- Enable spam filters and regularly update security software.
- Educate family members, especially senior citizens and teenagers.

For Organizations:

- Train employees on phishing and impersonation threats.
- Implement email authentication mechanisms (SPF, DKIM, DMARC).
- Conduct regular cybersecurity awareness sessions.
- Monitor email traffic for suspicious or spoofed domains.