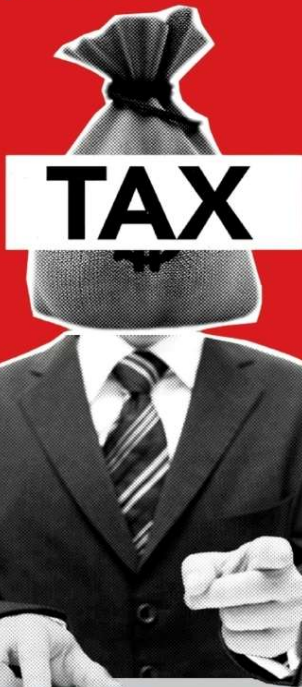


CYBER BYTE

FAKE TAX NOTICE SCAMS

Think before
you click



Supreme Court Issues 13-Point Directions to
Combat Digital Arrest Scams

1. LATEST CYBER THREAT

1. Fake Tax Notice Scams

Cybercriminals are increasingly impersonating government agencies such as the Income Tax Department (ITD) to trick people into downloading malicious files. A common scam involves WhatsApp or SMS messages claiming that the recipient has tax irregularities and must respond within 72 hours to avoid penalties or legal action. These messages often contain attachments such as ITD.zip or suspicious links that install malware on the victim's device.



How the Scam Works

Once the ZIP file is opened, malicious software is installed, allowing attackers to steal banking credentials, passwords, personal information, and one-time passwords (OTPs). Victims may also lose control of their devices, leading to financial fraud and identity theft.

How to Stay Safe

Always verify tax-related communications through the official Income Tax portal or email. Never download attachments or click links received through unsolicited WhatsApp or SMS messages. If a message creates urgency or threatens legal action, treat it as suspicious and report it immediately.

Key Message: *"Think before you click—official government notices are never delivered through suspicious WhatsApp attachments."*

2. Agentic & Machine-Speed Exploits

Cyberattacks are entering a new era where Artificial Intelligence (AI) can act with little or no human intervention. Threat actors are increasingly using **autonomous AI agents** to identify vulnerabilities, generate exploit code, and launch attacks at machine speed. This automation enables attackers to compromise systems in minutes rather than hours or days, dramatically increasing the scale and efficiency of cybercrime.



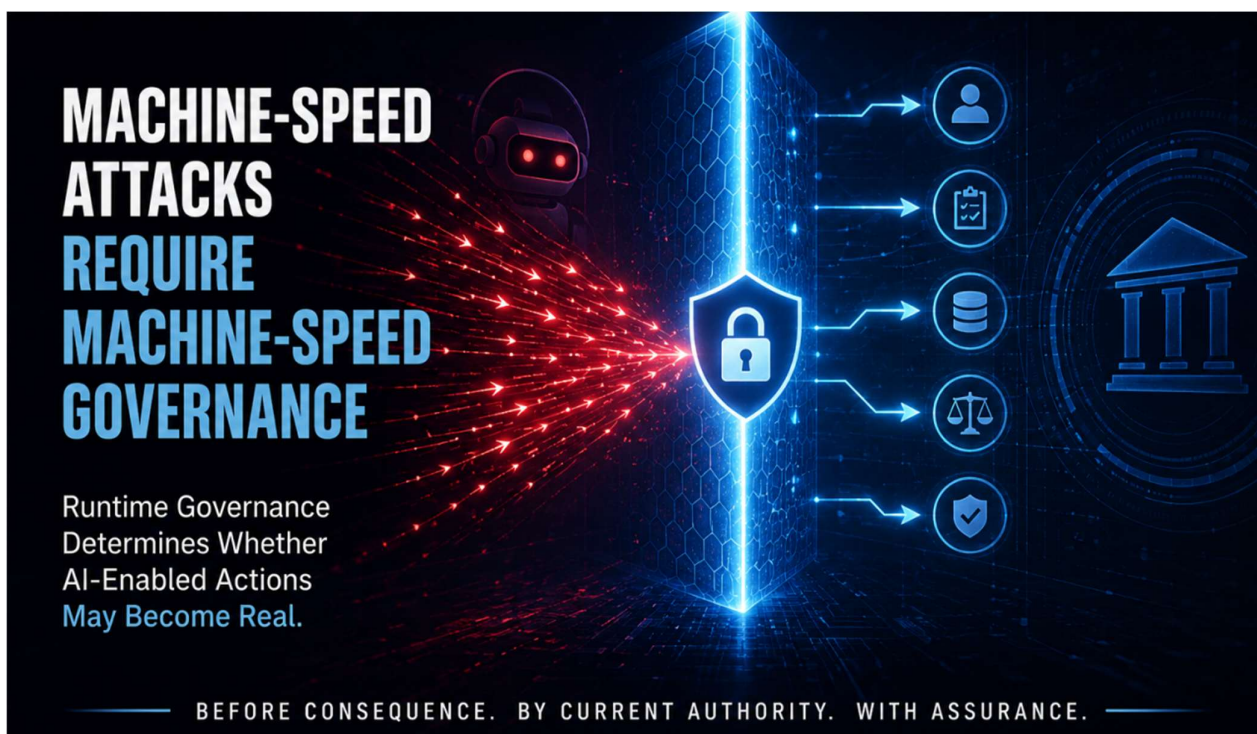
How the Threat Works

AI-powered agents continuously scan public-facing applications, cloud environments, and enterprise networks for security weaknesses. Once vulnerability is found, the AI can generate attack code, exploit the flaw, move laterally across connected systems, and establish persistence—all with minimal human involvement. According to recent cybersecurity reports, the average **breakout time**—the time attackers take to move from the initial breach to other systems—has dropped to **just 29 minutes**, leaving organizations with very little time to respond.

Why It Matters

Machine-speed exploits can lead to rapid data theft, ransomware deployment, and widespread disruption before security teams can react. To defend against these evolving threats, organizations must adopt AI-powered threat detection, continuously monitor their networks, patch vulnerabilities quickly, and implement a **Zero Trust** security model.

***Key Message:** "In the age of autonomous AI, every minute matters—because cyberattacks now move at the speed of machines, not humans."*



2. KNOWLEDGE BANK

1. Trellix Endpoint Security: Protecting Devices Against Modern Cyber Threats.

A Smarter Approach to Endpoint Protection

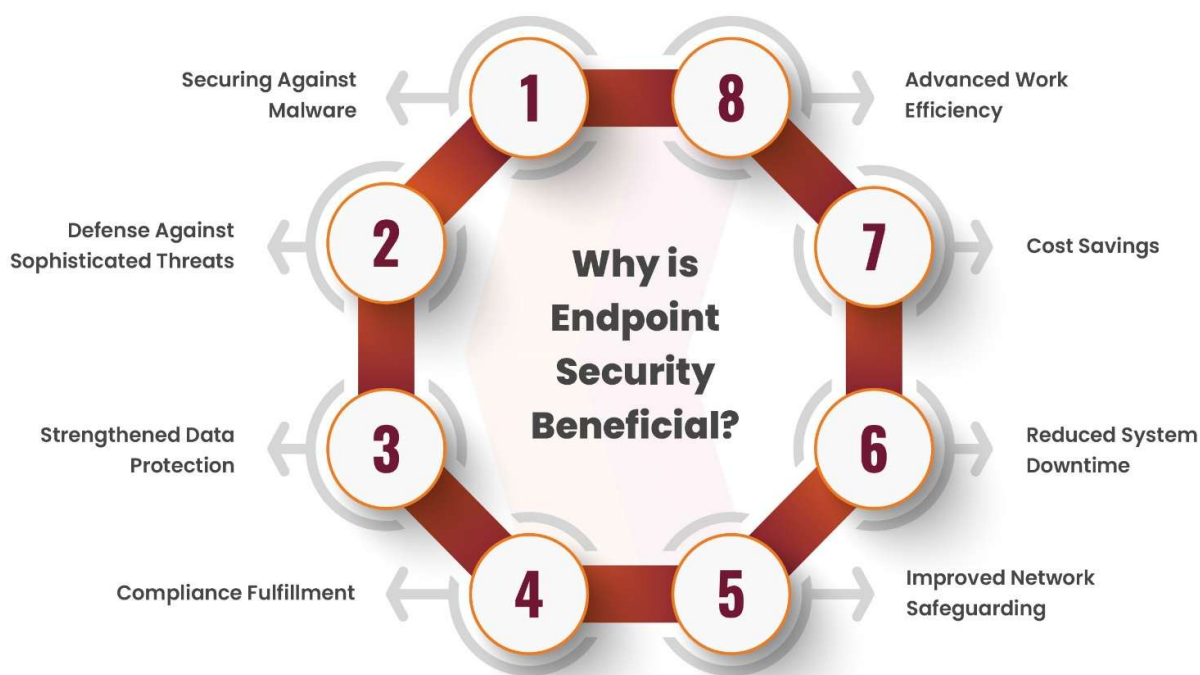
With employees working across offices, homes, and remote locations, laptops, desktops, and servers have become prime targets for cybercriminals. **Trellix Endpoint Security (ENS)** is an advanced endpoint protection platform designed to safeguard these devices from malware, ransomware, fileless attacks, and other sophisticated cyber threats. By combining multiple security technologies into a single solution, it helps organizations detect, prevent, and respond to attacks before they can impact business operations.



Trellix Endpoint Security uses **real-time threat detection**, **behavior-based analysis**, and **machine learning** to identify both known and unknown threats. Its integrated modules—including Threat Prevention, Firewall, Web Control, Adaptive Threat Protection, and Endpoint Detection and Response (EDR)—provide multiple layers of defence against cyberattacks. The platform also offers centralized security management, enabling IT teams to monitor endpoints, deploy security policies, and investigate incidents from a single console.

Why It Matters

As ransomware, phishing, and AI-driven attacks continue to evolve, endpoint security has become a critical component of every organization's cybersecurity strategy. Solutions like Trellix Endpoint Security help reduce attack surfaces, improve threat visibility, and strengthen an organization's overall cyber resilience. By continuously monitoring endpoint activity and responding quickly to suspicious behaviour, organizations can better protect sensitive data, maintain business continuity, and defend against today's rapidly changing threat landscape.



2. Supreme Court Issues 13-Point Directions to Combat Digital Arrest Scams

The **Supreme Court of India** has issued **13 interim directions** to strengthen the country's response to the growing menace of "**digital arrest**" scams, where fraudsters impersonate police officers, CBI officials, or other government authorities to intimidate victims into transferring money or revealing sensitive information. As part of its directions, the Court instructed the **Reserve Bank of India (RBI)** to develop a **Standard Operating Procedure (SOP)** within four weeks for the nationwide implementation of grievance redressal and fund restoration mechanisms. The Court emphasized the need for faster coordination among banks, law enforcement agencies, telecom operators, and digital platforms to improve the recovery of defrauded funds.

DIGITAL ARREST SCAMS: SUPREME COURT ORDERS STRONGER SAFEGUARDS, SEEKS COMPENSATION PLAN FOR VICTIMS

KEY DIRECTIONS

- RBI TO ISSUE SOP FOR BANKS**
RBI to adopt and circulate SOP within 4 weeks for debit holds, grievance redressal and money restoration
- STATES TO STRENGTHEN CYBER RESPONSE**
Operationalise State Cyber Crime Centres, adopt e-Zero FIR and ensure speedy disposal of account freezing matters
- COMPENSATION FRAMEWORK**
Inter-departmental committee to examine shared liability and compensation plan for scam victims
- CBI THRESHOLD & TELECOM CURBS**
Committee to review CBI monetary threshold and telecom curbs on audio/video calls
- AWARENESS & COORDINATION**
Wide public awareness campaigns on prevention, grievance redressal and fund recovery

FOCUS ON VICTIM PROTECTION AND JUSTICE

Mechanism requires wide adoption, faster disposal and continued follow-up. **99**

Matter to be next taken up in **September**

The Court also called for wider adoption of existing cyber fraud reporting systems, including the **1930 Cyber Helpline** and the **National Cyber Crime Reporting Portal (NCRP)**, to ensure quicker reporting and response to cybercrime complaints. The directions aim to strengthen India's cyber fraud ecosystem by improving public awareness, accelerating investigation processes, and enhancing cooperation between financial institutions and government agencies. The move is expected to provide better protection to citizens against rapidly increasing online financial fraud and impersonation scams, reinforcing the importance of timely reporting and digital vigilance.

3. How to protect IT infrastructure

1. Prepare an Incident Response Plan

No organization is completely immune to cyberattacks, making an Incident Response Plan (IRP) an essential part of cybersecurity. An incident response plan is a documented set of procedures that guides an organization on how to detect, report, contain, investigate, and recover from cyber incidents such as ransomware attacks, data breaches, or malware infections. A well-prepared plan helps reduce downtime, minimize financial losses, and protect sensitive information.



The plan should clearly define the roles and responsibilities of employees, IT teams, management, and external partners. Organizations should regularly conduct cyberattack simulations and tabletop exercises to ensure everyone understands their responsibilities during an incident. Keeping emergency contact lists updated, maintaining secure backups, and documenting recovery procedures can significantly improve response time. A fast and well-coordinated response not only limits the impact of an attack but also helps restore business operations and customer trust more quickly.

2.Limit User Access

Restricting user access is one of the most effective ways to protect an organization's IT infrastructure from cyber threats. Employees should be given access **only to the data, applications, and systems required to perform their specific job responsibilities**. This security practice, known as the **Principle of Least Privilege (PoLP)**, helps reduce the risk of unauthorized access, accidental data leaks, and insider threats. If a user's account is compromised through phishing or malware, limited access prevents attackers from moving freely across the network and reaching critical business systems.



Organizations should also regularly review user permissions to ensure employees do not retain unnecessary access after changing roles or leaving the company. Inactive accounts should be disabled immediately, and administrator privileges should be granted only to authorized personnel. Access to sensitive information should be monitored through regular audits, and critical systems should be protected with additional approval mechanisms. By implementing proper access controls and continuously reviewing user permissions, organizations can significantly reduce the impact of cyberattacks, protect confidential information, and maintain a secure and resilient IT environment.

4. CYBER GUPSHUP

1. Centre rules out separate cyberbullying law, strengthens AI content safeguards

The Central Government has clarified that it is **not planning a separate law for cyberbullying**, stating that existing provisions under the **Information Technology Act** and the strengthened **IT Rules** are considered adequate to address online abuse, deepfakes, and AI-generated harmful content. The government informed Parliament that its current focus is on enforcing existing laws more effectively while strengthening safeguards for digital platforms. As AI-generated content becomes more sophisticated, the emphasis remains on faster detection, improved platform accountability, and enhanced protection for internet users against online harassment and misinformation.

2. Police Intercept Cyber Mule Network in Jharkhand, Rescuing 40 Vulnerable Youth

In a significant action against organized cybercrime, police in Jharkhand dismantled a network that allegedly recruited unemployed youth as "**money mules**" to transfer illegally obtained funds through their bank accounts. Acting on intelligence, authorities conducted raids at several hotels and lodges in the Adityapur industrial area, rescuing around **40 young men** from Jharkhand, Bihar, and West Bengal. The incident highlights how cybercriminals exploit vulnerable individuals by offering easy money in exchange for access to their bank accounts. Citizens are advised never to share or rent out their bank accounts, debit cards, or digital payment credentials, as they could unknowingly become part of a cybercrime operation.

3. CBI Charge Sheets Bank Officer, Firm Owner In Rs 1.6 Crore Digital Arrest Scam

The Central Bureau of Investigation (CBI) has filed a charge sheet against the owner of a Kashmir-based firm and a Deputy Manager of Axis Bank in connection with a digital arrest scam in which a Delhi senior citizen was defrauded of Rs 1.6 crore, an official statement said on Wednesday. The accused named in the charge sheet are Umer Iqbal, proprietor of M/s Himalayan Enterprises, Pulwama, and Umer Ahmad Dar, Deputy Manager at Axis Bank.

5. CYBER HYGIENE

- Review your bank accounts and online accounts regularly for suspicious activity.
- Verify investment offers, job opportunities, and government notices before taking any action.
- Keep your operating system, applications, and antivirus software updated with the latest security patches.
- Verify emails, messages, and QR codes before clicking links or downloading attachments.
- Download apps and software only from trusted or official sources.
- Lock your devices with a PIN, password, or biometric authentication.
- Avoid using public Wi-Fi for banking or accessing sensitive information without a trusted VPN.
- Check and limit app permissions, especially access to your camera, microphone, contacts, and location.
- Log out of accounts after using shared or public computers.
- Stay informed about the latest cyber threats through trusted government and cybersecurity advisories.

6. New development in IT WING

Guest Management System - "Satkar Portal":

The application enabled systematic management of transportation, food arrangements, accommodation, dissemination of timely event-related updates and other essential requirements of the participating guests, thereby significantly enhancing the efficiency and coordination of guest management.



DG CRPF Shri G.P. Singh (IPS) reviewed the progress of the construction of new CRPF HQ building and interacting with all key stakeholders.



DG CRPF Shri G.P. Singh (IPS) kickstarted BMI 2.0 - 2026 by undergoing the assessment along with officers and men at CRPF's Northern Sector Hospital, New Delhi.



DG CRPF Shri G.P. Singh (IPS) reviewed the prestigious Valediction Parade of the 77th Regular Recruits (RR) batch of IPS officer at the Sardar Vallabhbhai Patel National Police Academy, Hyderabad.