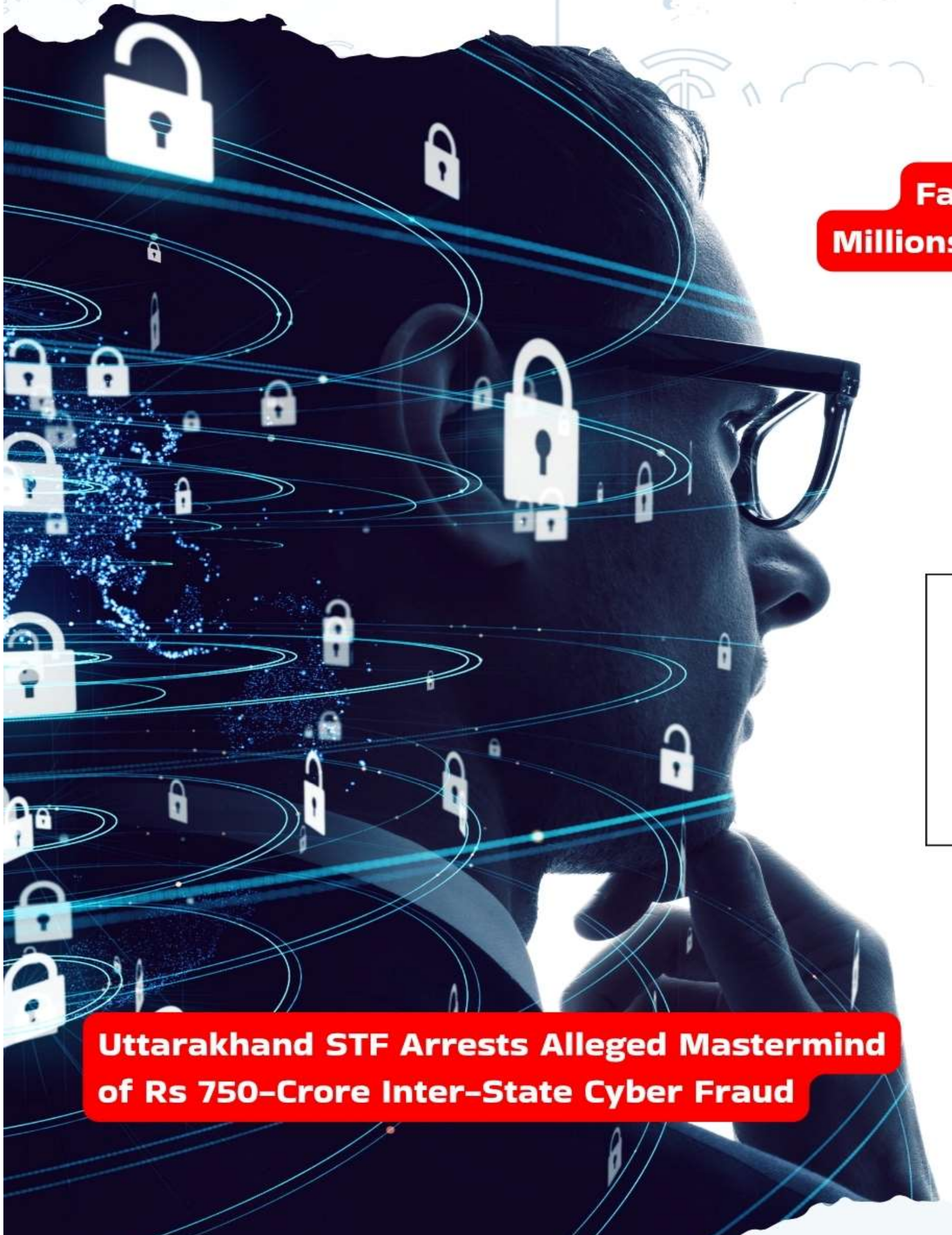
CENTRAL RESERVE POLICE FORCE

CYBER BYTE

JULY-2025



Fake "e-PAN" Emails Target Millions with Identity Theft Scam

QUICK TIPS!

Protect Your Mobile from Unnecessary Applications

How to Detect Malware in PDF Files

Uttarakhand STF Arrests Alleged Mastermind of Rs 750-Crore Inter-State Cyber Fraud

1. CYBER GEEKS NEWS

A) McDonald’s AI hiring tool’s password ‘123456’ exposed data of 64M applicants

A security oversight in McDonald’s AI-powered hiring platform “McHire” was found exposing sensitive applicant data belonging to as many as 64 million job seekers.

Discovered in late June 2025 by security researchers Ian Carroll and Sam Curry, the issue was a default admin login and an insecure direct object reference (IDOR) in an internal API that allowed access to applicants’ chat histories with ‘Olivia’, McHire’s automated recruiter bot.

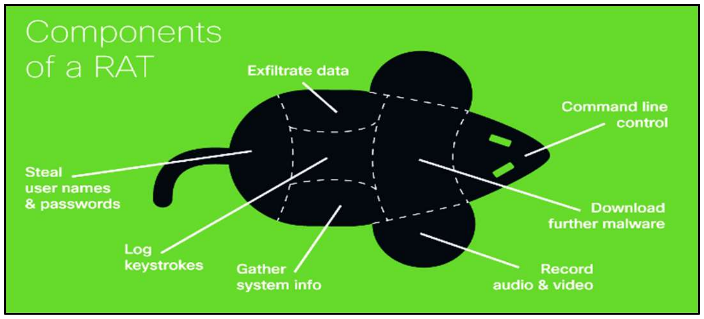
McDonald's acknowledged the report within an hour, and the default admin credentials were disabled soon after.

"We're disappointed by this unacceptable vulnerability from a third-party provider, Paradox.ai. As soon as we learned of the issue, we mandated Paradox.ai to remediate the issue immediately, and it was resolved on the same day it was reported to us," McDonald's told Wired in a statement about the research.

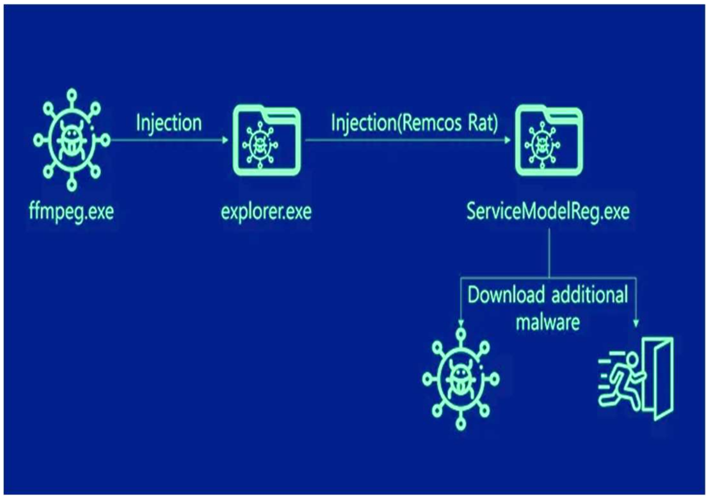
Paradox deployed a fix to address the IDOR flaw and confirmed that the vulnerability was mitigated. Paradox.ai has since stated that it is conducting a review of its systems to prevent similar big issues from recurring.

B) Remcos RAT (Remote Control and Surveillance Trojan)

It is reported that a malware dubbed as Remcos RAT (Remote Control and Surveillance Trojan) which is a sophisticated Remote Access Trojan (RAT), is being escalated by the threat actors for espionage, credential theft, and system takeover. Remcos (Remote Control and Surveillance) is a Remote Access Trojan (RAT) created by Breaking Security and initially promoted as a legitimate tool for remote system management. However, it has since been extensively used by cybercriminals and Advanced Persistent Threat (APT) groups for malicious activities.



In a recent campaign observed, cybercriminals used a stealthy, fileless method to deliver Remcos. Attackers use a specially crafted PowerShell loader that runs entirely in memory and performs further advanced activities. This technique helps the malware avoid being detected by antivirus software and allows attackers to remain hidden while maintaining access to the infected system.



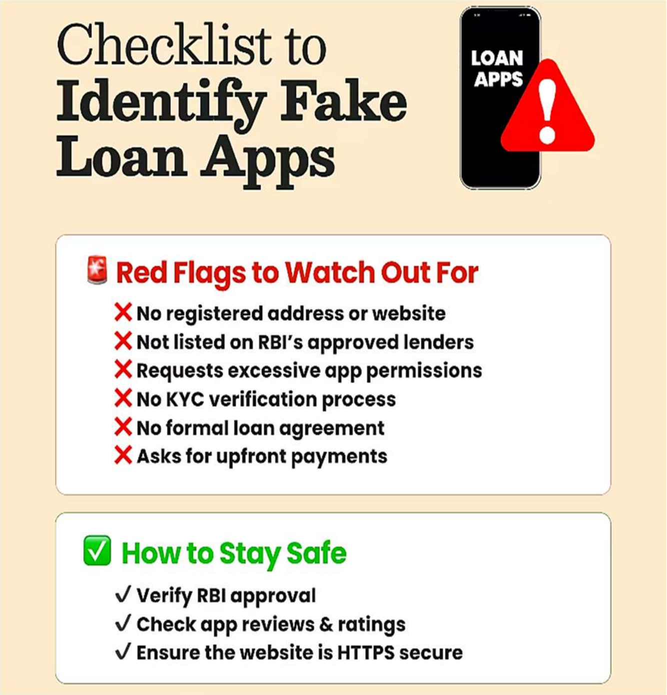
2. CYBER FRAUDS

(A) Uttarakhand STF Arrests Alleged Mastermind of Rs 750-Crore Inter-State Cyber Fraud: -

The Uttarakhand Special Task Force (STF) claimed to have arrested the alleged mastermind in a Rs 750 crore interstate cyber fraud at Delhi Airport.

Officials alleged that the accused, who is a chartered accountant, had created about 35 to 40 shell companies, about 13 companies in his name and 28 in the name of his wife, for Chinese operatives and to trap people **using fake loan apps.**

The accused reportedly harassed individuals by posing as representatives of companies and extorted money through fraudulent loan apps such as **Inst Loan, Maxi Loan, KK Cash, RupeeGo, Lendkar, and others**. After investigating the case, a police team identified the accused, a resident of West Delhi, as the mastermind behind the scheme. The cyber team initiated a search for the accused under legal provisions, and since he was abroad, a Look Out Circular (LOC) was issued against him.



Checklist to **Identify Fake Loan Apps**

Red Flags to Watch Out For

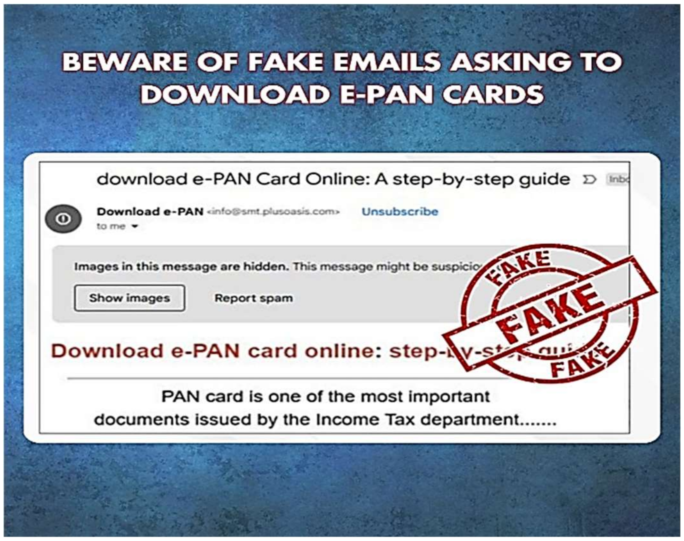
- ✗ No registered address or website
- ✗ Not listed on RBI's approved lenders
- ✗ Requests excessive app permissions
- ✗ No KYC verification process
- ✗ No formal loan agreement
- ✗ Asks for upfront payments

How to Stay Safe

- ✓ Verify RBI approval
- ✓ Check app reviews & ratings
- ✓ Ensure the website is HTTPS secure

(B) Fake "e-PAN" Emails Target Millions with Identity Theft Scam:-

The Press Information Bureau's Fact Check unit has issued a red alert over a surge in fraudulent emails that lure recipients into downloading counterfeit e-PAN cards. These emails are not from the Income Tax Department and are engineered to extract bank, Aadhaar, and personal credentials via malicious links. Recipients are strongly urged to delete these messages and report them to the official authorities.



download e-PAN Card Online: A step-by-step guide

Download e-PAN <info@smt.plusoasis.com>
to me

Images in this message are hidden. This message might be suspicio

Download e-PAN card online: step-by-step gui

PAN card is one of the most important
documents issued by the Income Tax department.......

The phishing messages typically carry subject lines such as **"Download e-PAN Card Online: A step-by-step guide"**, claiming the Income Tax Department sent them.

In reality, they redirect users to spoofed websites controlled by cybercriminals. Clicking links or opening attachments risks exposure to malware or identity theft. The department emphatically advises: it never requests personal PINs, passwords, or OTPs via email.

Cybersecurity experts explain that once victims engage with the fake emails, they're prompted to enter sensitive data. This information enables the scammers to hijack bank and government accounts, then deploy malware remotely.

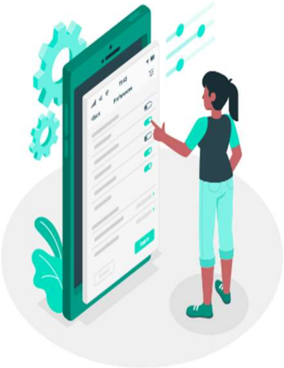
3. TIPS OF THE MONTH

(A) How to Protect Your Mobile from Unnecessary Applications

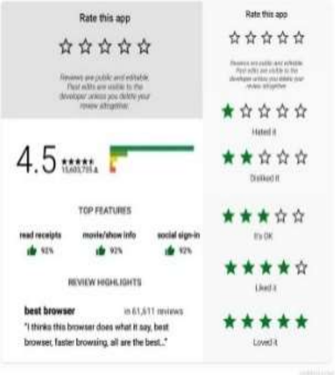
1. **Download Apps Only from Trusted Sources.**

Stick to official app stores like Google Play Store or Apple App Store. Avoid downloading apps from unknown websites or third-party stores.

2. **Review App Permissions Carefully** Before installing or updating an app, check what permissions it requests. If an app asks for more access than it needs (like a calculator app requesting your contacts), that's a red flag.



3. **Read App Reviews and Ratings.** Check user feedback before installing. Poor reviews or reports of suspicious behaviour can warn you off.



Rate this app

☆☆☆☆☆

Reviews are public and editable. Past edits are visible to the developer unless you delete your review altogether.

4.5 ★★★★★

TOP FEATURES

read receipts 92%

movie/show info 92%

social sign-in 92%

REVIEW HIGHLIGHTS

best browser in 61,611 reviews

"I thinks this browser does what it say, best browser, faster browsing, all are the best..."

Rate this app

☆☆☆☆☆

★☆☆☆☆ Hated it

★★☆☆☆ Disliked it

★★★☆☆ It's OK

★★★★☆ Liked it

★★★★★ Loved it

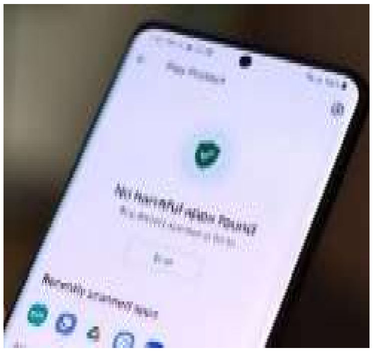
4. **Avoid Clicking on Suspicious Links or Ads** Don't install apps promoted by random pop-ups, spam messages, or shady ads.

5. **Uninstall Unused Apps Regularly.** Review your installed apps and delete those you no longer use. This helps keep your device secure and frees up space.

6. **Use Mobile Security Apps** Install reputable antivirus or security apps that scan for and block harmful or unnecessary apps.

7. **Keep Your Device and Apps Updated.** Updates patch security holes that could be exploited by malicious or unnecessary apps.

8. Google Play Protect should be enabled on Android device.



B) How to Detect Malware in PDF Files

1. Look for Suspicious Signs in the PDF

- **Unexpected prompts or pop-ups** when opening the PDF.
- The PDF asks you to enable macros, JavaScript, or other active content.
- The file size is unusually large or very small compared to what you expect.
- The PDF contains links or buttons leading to unknown websites.
- The PDF requests personal information or login credentials.

2. Check the Source

- Only open PDFs from trusted senders or websites.
- Be cautious of unexpected email attachments or downloads, especially from unknown contacts.

3. Use Antivirus or Anti-Malware Software.

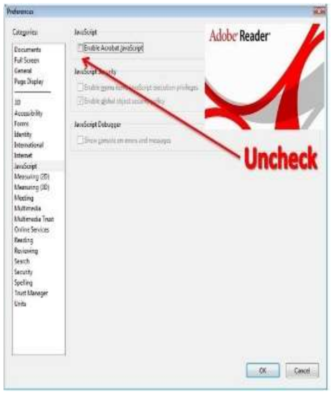
- Scan the PDF file with updated antivirus software before opening.
- Many security suites can detect malicious code embedded in PDFs.

4. Use Online PDF Scanners.

- Upload the PDF to services like Virus Total to scan it with multiple antivirus engines.
- These tools analyse the file and report if malware is detected.

5. Disable Java Script in PDF Readers.

- Most malware embedded in PDFs relies on JavaScript.
- Disable JavaScript in your PDF reader settings unless you absolutely trust the file.



6. Open PDFs in a Sandbox or Virtual Machine.

- If you must open a suspicious PDF, do it in a sandboxed environment or a VM to avoid infecting your main system.

World Police & Fire Games 2025, felicitation ceremony at Shaurya, New Delhi.

CWA hosted a mental health special session in collaboration with Aditya Birla's Project M-Power.

DG CRPF met pilgrims on Shri Amarnath Ji Yatra route and checked their well-being.

CRPF dedicated teams to assisting pilgrims during SANJAY- 2025.

DG CRPF chaired GCOs Conference at Shaurya, New Delhi

DG CRPF visited Veer Balidani ASI/GD Satyvan Kumar Singh's native village in Rampur, Sohrouna, UP.