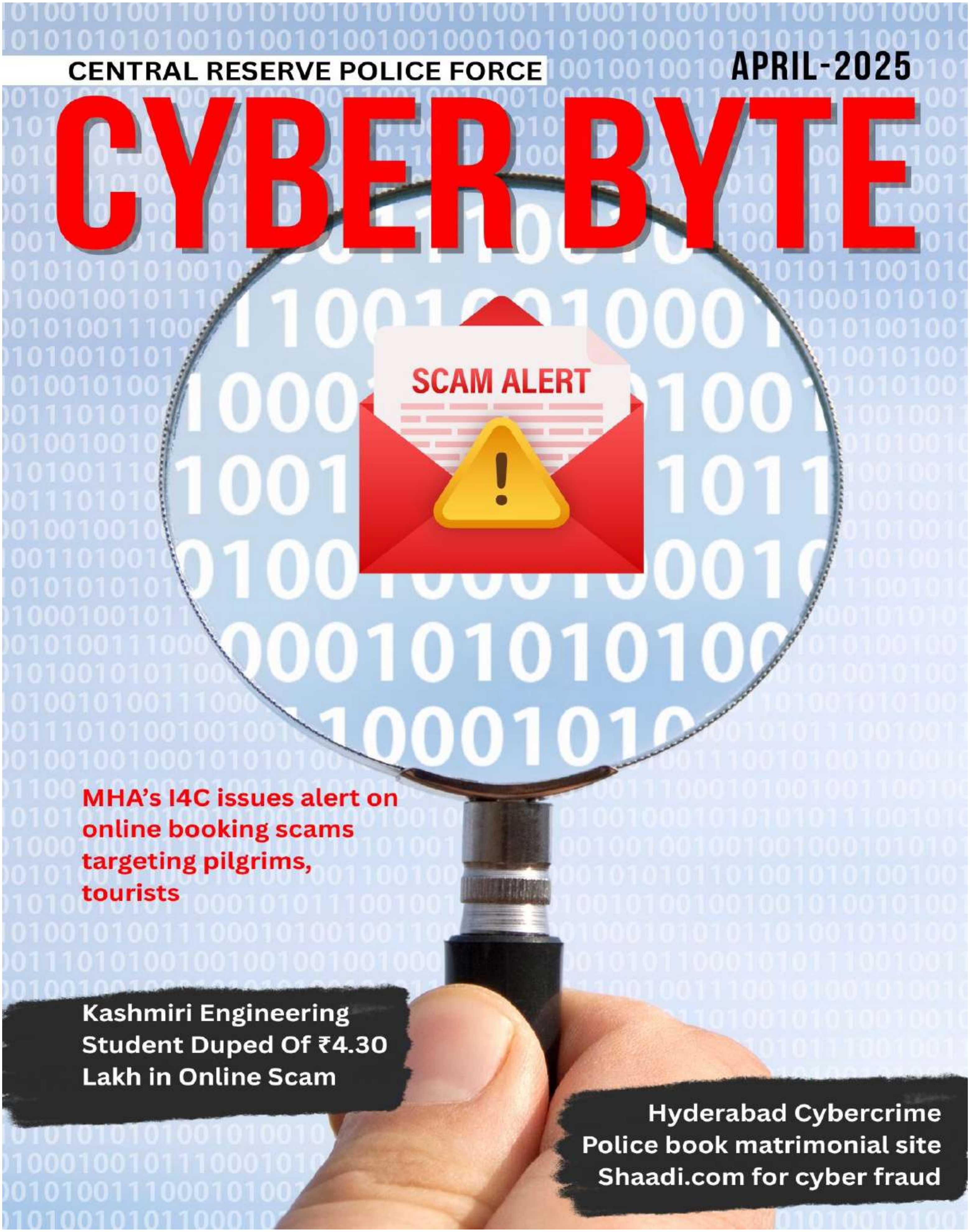
CENTRAL RESERVE POLICE FORCE

APRIL-2025

# CYBER BYTE



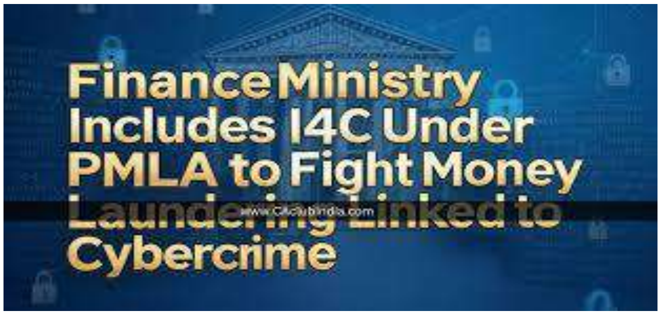
**MHA's I4C issues alert on online booking scams targeting pilgrims, tourists**

**Kashmiri Engineering Student Duped Of ₹4.30 Lakh in Online Scam**

**Hyderabad Cybercrime Police book matrimonial site Shaadi.com for cyber fraud**

## 1. CYBER GEEKS NEWS

### A. Govt. brings cybercrime centre I4C under PMLA: -


Finance Ministry Includes I4C Under PMLA to Fight Money Laundering Linked to Cybercrime
www.CAclubindia.com

The government has authorized Indian Cyber Crime Coordination Centre (I4C) **to share and receive information from the Enforcement Directorate** under the anti-money laundering law, a move aimed at detecting money trail and combating cyber frauds.

In a notification, the Revenue Department under the Finance Ministry included I4C under Section 66 of the Prevention of Money Laundering Act. **This would help I4C to share and receive information from the Enforcement Directorate and other law enforcement agencies.**

Amid growing instances of cyber frauds targeting common man, this **information sharing would help identify the masterminds** behind such frauds which are mostly trans-national.

### B. MHA's I4C issues alert on online booking scams targeting pilgrims, tourists: -

The Union Ministry of Home Affairs' (MHA) cyber security arm I4C on Saturday issued a nationwide alert cautioning people about a sharp rise in online booking frauds. The victims are mostly found to be religious pilgrims and unsuspecting tourists.

The Indian Cyber Crime Coordination Centre (I4C) in alert said that **cyber frauds are noticed to be executed through fake websites, social media pages, WhatsApp accounts and even sponsored advertisements on major platforms like Google and Facebook.**

The I4C has alerted the public about online booking frauds, **especially those targeting religious pilgrims and tourists across the country.** These frauds are being perpetrated through fake websites, deceptive social media pages, Facebook posts, and paid advertisements on search engines like Google.

According to I4C, these scams typically lure victims with offers like helicopter bookings for Kedarnath and the Char Dham yatra, guest house and hotel accommodations, online cab or taxi services, and religious tourism packages.

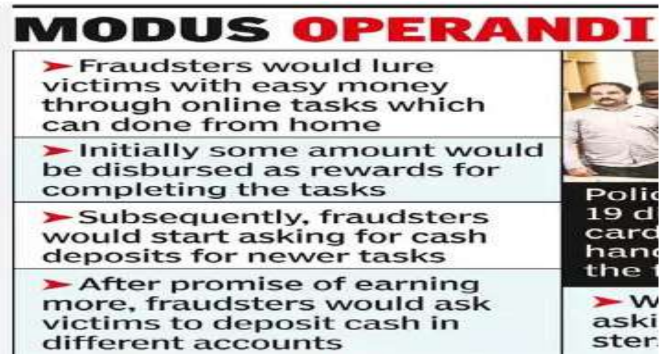
## 2. CYBER FRAUDS

### (A) Hyderabad Cybercrime Police book matrimonial site Shaadi.com for cyber fraud: -

The Hyderabad Cybercrime Police have uncovered a serious case of cyber fraud involving the matrimonial platform Shaadi.com, where a fake profile was used to cheat a woman doctor from the city to the tune of Rs 11 lakh, along with threats of extortion and blackmail.

The suspect who has been recently arrested, had created a fake profile under a different name and exploited the **platform's premium service to contact the victim, promising marriage.** "Claiming financial distress, he induced the victim to transfer large sums of money and later issued threats and blackmailed her using personal content," said a cybercrime official.

### (B) Kashmiri Engineering Student Duped Of ₹4.30 Lakh in Online Scam: -



**MODUS OPERANDI**

➤ Fraudsters would lure victims with easy money through online tasks which can done from home

➤ Initially some amount would be disbursed as rewards for completing the tasks

➤ Subsequently, fraudsters would start asking for cash deposits for newer tasks

➤ After promise of earning more, fraudsters would ask victims to deposit cash in different accounts

Polic
19 d
card
hand
the t

➤ W
aski
ster

A 20-year-old engineering student from Jammu and Kashmir fell victim to a cyber fraud and lost Rs 4.30 lakh in a "task fraud" scam, according to officials from the Matunga
police station on Wednesday.

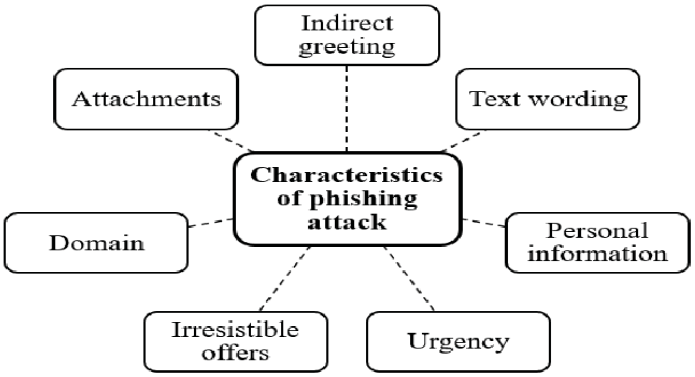
The student, currently residing in a college hostel in Mumbai's Matunga area, was approached **via WhatsApp** by a woman fraudster. She offered him a part-time opportunity to earn between Rs 2,000 and Rs 8,000 daily by posting online reviews.

Initially enticed by the quick earnings, the student agreed to participate. He was then added to a **Telegram channel** where he was assigned small tasks and even received some initial payments, which encouraged him to continue, according to PTI report. As the tasks progressed, he was asked to deposit money as a "**security measure**" for larger assignments. Over time, the victim deposited a total of Rs 4.30 lakh in multiple transactions. When demands for more money persisted without further payment or a clear explanation, the student grew suspicious and realized he had been defrauded.

The case adds to the growing number of cyber fraud incidents in India, with scammers increasingly using **social media and messaging apps to target unsuspecting individuals, particularly students and job seekers**. Authorities have advised the public to be cautious and verify any online job offers or financial schemes before participating.

## 3. TIPS OF THE MONTH

**1). Regarding phishing mail: -** It has been observed that cyber threats, particularly phishing attacks conducted through NIC email accounts, have seen a noticeable increase in the aftermath of the recent situation in Kashmir.



These attackers often involve deceptive emails that appear legitimate, attempting to extract sensitive information, install malware, or gain unauthorized access to official systems. All users are advised to follow below mention steps if such type of phishing mail received.

**To avoid falling victim to phishing domains:**

1. Be cautious of unsolicited emails or messages: Legitimate organizations rarely ask for **sensitive information** via email or message.

2. **Verify the domain name: Check the URL** carefully, looking for misspellings, extra characters, or variations in the domain name.

3. **Watch for poor grammar and spelling**: Legitimate websites usually have professional content.

4. Be wary of urgent or threatening messages: Phishing domains often try to create a sense of urgency to prompt users into taking the action.

5. Check for HTTPS and a valid SSL certificate: Legitimate websites usually have a valid SSL Certificate and use HTTPS.

## To protect from phishing domains:

1. Use strong, unique passwords: Avoid using the same password across multiple sites.

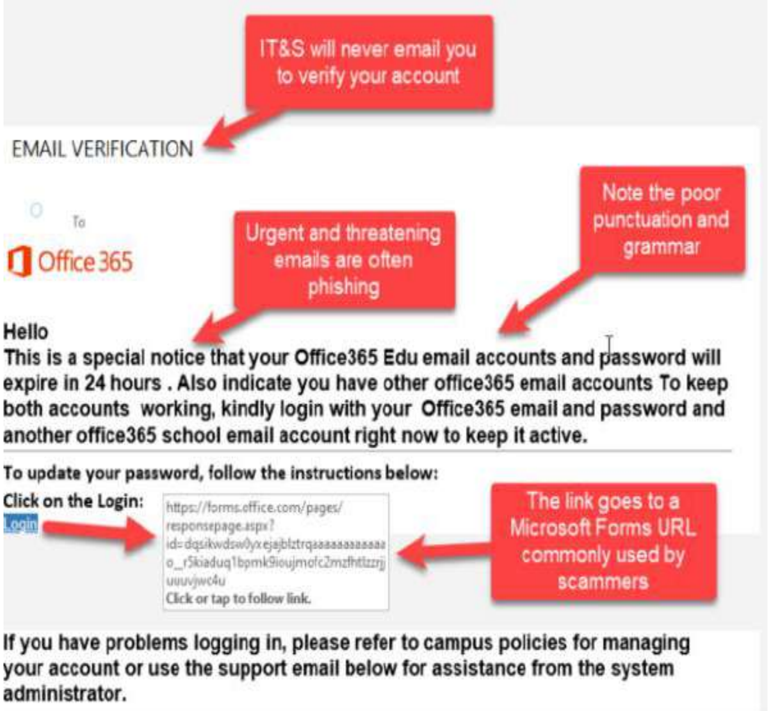
2. Enable two-factor authentication (2FA): 2FA adds an extra layer of security to prevent unauthorized access.

3. Keep your software and operating system up to date: Ensure you have the latest security patches and updates.

4. Use anti-virus software and a firewall: Protect your device from malware and unauthorized access.

By following above steps, you can effectively sanitize your system and mitigate the potential risks associated with clicking on a phishing mail.

## A. Some stances to identify the traits of fake mails:



IT&S will never email you to verify your account

EMAIL VERIFICATION

To

Office 365

Urgent and threatening emails are often phishing

Note the poor punctuation and grammar

Hello

This is a special notice that your Office365 Edu email accounts and password will expire in 24 hours . Also indicate you have other office365 email accounts To keep both accounts working, kindly login with your Office365 email and password and another office365 school email account right now to keep it active.

To update your password, follow the instructions below:

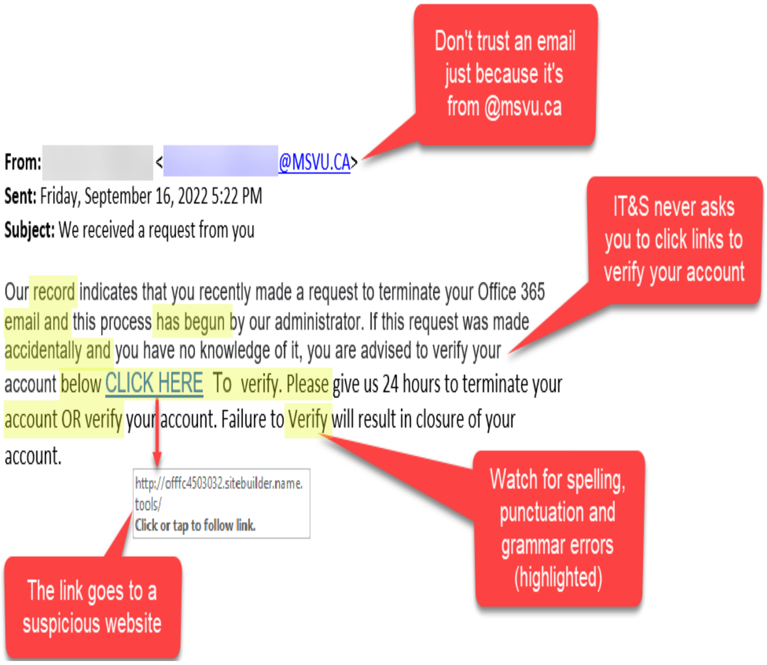
Click on the Login:

Login

https://forms.office.com/pages/responsepage.aspx?id=dqsikwdsw0yxejajblztrqaaaaaaaaaaaao__r5kiaduq1bpmk9ioujmofc2mzfhttlzzrjuuuvjwc4u
Click or tap to follow link.

The link goes to a Microsoft Forms URL commonly used by scammers

If you have problems logging in, please refer to campus policies for managing your account or use the support email below for assistance from the system administrator.



Don't trust an email just because it's from @msvu.ca

**From:** [redacted] <[redacted]@MSVU.CA>
**Sent:** Friday, September 16, 2022 5:22 PM
**Subject:** We received a request from you

Our record indicates that you recently made a request to terminate your Office 365 email and this process has begun by our administrator. If this request was made accidentally and you have no knowledge of it, you are advised to verify your account below CLICK HERE To verify. Please give us 24 hours to terminate your account OR verify your account. Failure to Verify will result in closure of your account.

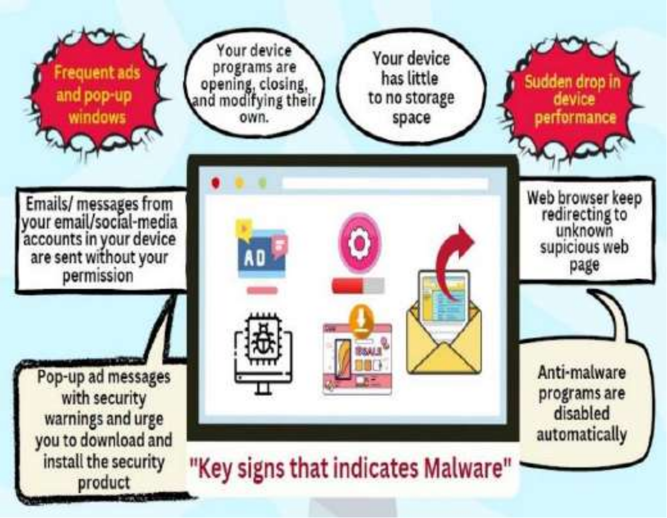
http://offfc4503032.sitebuilder.name.tools/
Click or tap to follow link.

IT&S never asks you to click links to verify your account

Watch for spelling, punctuation and grammar errors (highlighted)

The link goes to a suspicious website

## B). Malware key signs & protective measures: -


Frequent ads and pop-up windows
Your device programs are opening, closing, and modifying their own.
Your device has little to no storage space
Sudden drop in device performance
Emails/ messages from your email/social-media accounts in your device are sent without your permission
Web browser keep redirecting to unknown supicious web page
AD
Pop-up ad messages with security warnings and urge you to download and install the security product
Anti-malware programs are disabled automatically
"Key signs that indicates Malware"

- Avoid clicking on suspicious emails, links, and sites from unknown source.
- As soon as you click on any malicious link, your mobile can be hacked or your data can be stolen.
- Browse only secure and authorized websites.
- Always keep your computer software/browser up to date.
- Maintain backup of your data regularly.
- Install software like pop-up/ ad-blocker to block the malicious advertisements appearing on websites.
- Install antivirus and antimalware solutions in your devices and keep them updated.
- Hover over the images/links to find the actual link.
- Do not install any apps through links received on chats or social media posts.

## C). Ransomware crooks now SIM swap executives' kids to pressure their parents: -

**RSAC Ransomware** infections have morphed into "a psychological attack against the victim organization," as criminals use increasingly personal and aggressive tactics to force victims to pay up, according to Google-owned **Mandiant** (a cybersecurity company, now a subsidiary of Google).

We saw situations where threat actors essentially SIM swap the phones of children of executives, and start making phone calls to executives, from the phone numbers of their children. The psychological dilemma that the executive goes through – seeing a phone call from the children, picking up the phone and hearing that it's somebody else's voice?

Sometimes, **it's caller ID spoofing.** Other times, we see demonstrated SIM swapping family members." Either way, it's horrifying. Seeing a phone call from the children, picking up the phone, and hearing that it's somebody else's voice.

### Suggestion

- Enable SIM card locks.
- Use strong, unique passwords.
- Implement multi-factor authentication (MFA).
- Educate executives and their families.
- Regularly review and update security settings.
- Monitor accounts for suspicious activity.
- Limit exposure of personal information.
- Secure devices with up-to-date software.
- Establish communication protocols.
- Report suspicious activity.

Valour Day Gallantry Medal Ceremony 2025

86वीं के.रि.पु.बल दिवस परेड-2025
सांस्कृतिक संध्या
मुख्य अतिथि
श्री ज्ञानेन्द्र प्रताप सिंह, भा.पु.से.
महानिदेशक के.रि.पु.बल
Nikon Z 7_2, 64mm, f/4, 1/125s

DG CRPF in Cultural Program at GC, Neemuch

72nd ALL INDIA POLICE AQUATICS CLUSTER (AQUATICS & CROSS COUNTRY)
CHAMPIONSHIP - 24th to 28th March, 2025
CRPF, Gandhinagar, Gujarat

72nd All India Police Aquatics & Cross-country Championship at Gandhinagar

Honorable Home Minister at 86th CRPF Day Parade

Demonstration of K9 on the Occasion of 86th CRPF Day Parade