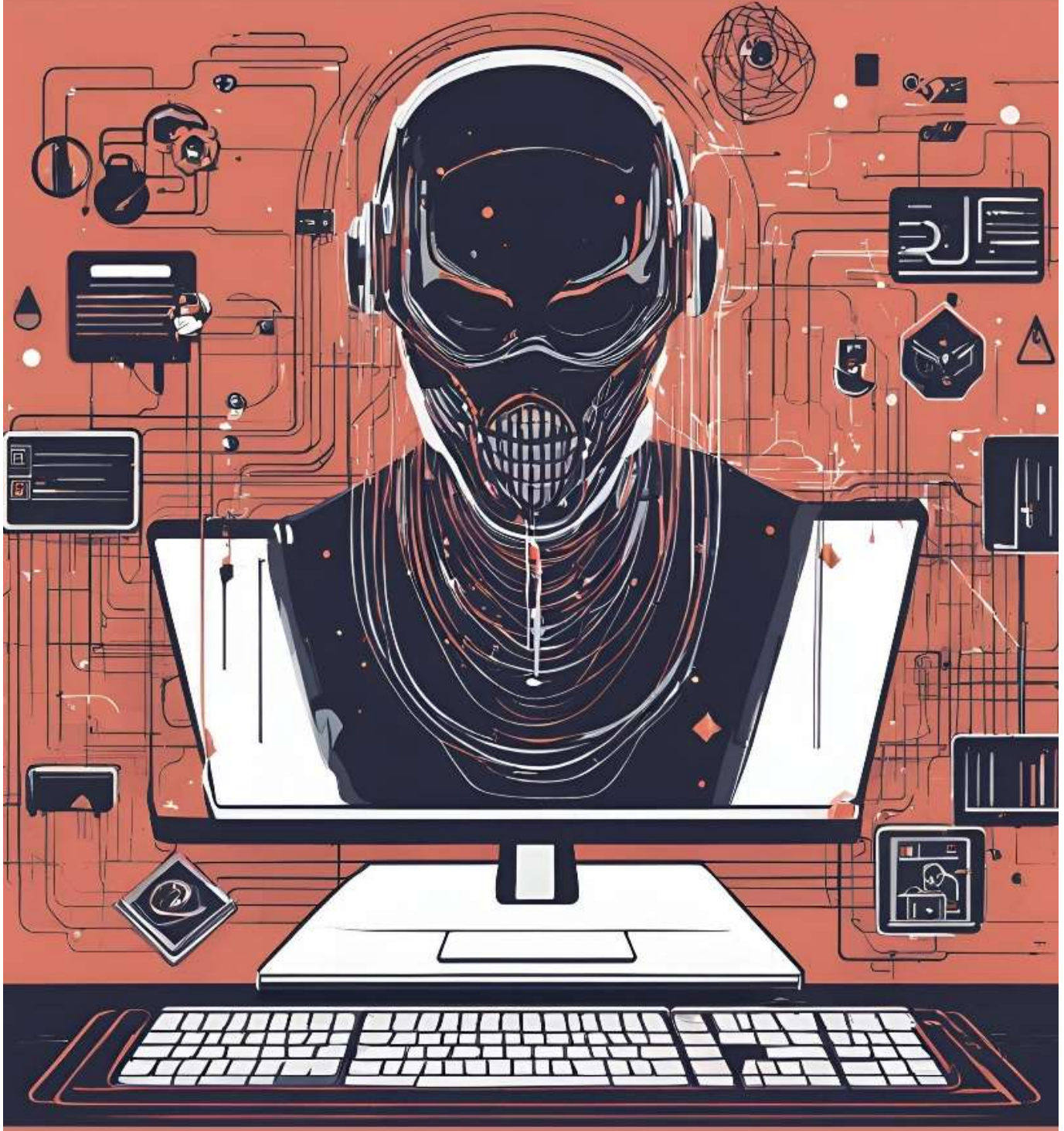


CENTRAL RESERVE POLICE FORCE

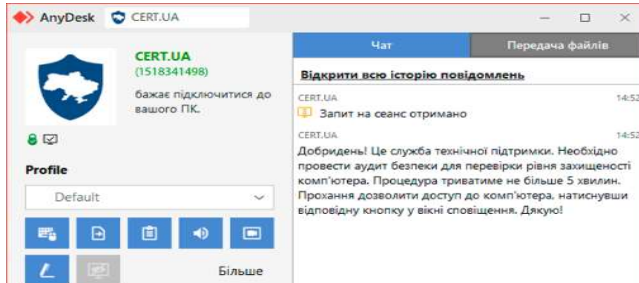
FEB, 2025

CYBER BYTE



1. CYBER GEEKS NEWS

A) (CERT-UA) Warns of Cyber Scams Using Fake AnyDesk Requests for Fraudulent Security Audits.



The Computer Emergency Response team of Ukraine (CERT-UA) is warning of ongoing attempts by unknown threat actors to impersonate the cybersecurity agency by sending AnyDesk connection requests.

The AnyDesk requests claim to be for conducting an audit to assess the "level of security," CERT-UA added, cautioning organizations to be on the lookout for such social engineering attempts that seek to exploit user trust.

"It is important to note that CERT-UA may, under certain circumstances, use remote access software such as AnyDesk," CERT-UA said. "However, such actions are taken only after prior agreement with the owners of objects of cyber defense through officially approved communication channels."

However, for this attack to succeed, it's necessary that the AnyDesk remote access software is installed and operational on the target's computer.

It also requires the attacker to be in possession of the target's AnyDesk identifier, suggesting that they may have to first obtain the identifier through other methods.

To mitigate the risk posed by these attacks, it's essential that remote access programs are enabled only for the duration of their use and the remote access is coordinated through official communication channels.

B) Cyber police warn people against sharing hateful content in J&K.



A day after police detained six persons for allegedly inciting sectarian unrest through derogatory remarks, the Cyber Police Kashmir on Thursday warned people against sharing hateful content on social media.

It further stated that several offenders have already been summoned to the Cyber Police Kashmir and strict legal action is being taken. "We urge everyone who has downloaded or shared this harmful content to stop immediately." Sharing hateful content is a punishable offence. Legal action will be enforced against violators.

"WE ARE WATCHING", the message from Cyber Police Kashmir had been circulated also.

Police had detained six persons and charged them under **sections 126 and 170** of the Bhartiya Nagarik Suraksha Samhita (BNSS) for allegedly inciting unrest through derogatory remarks. The two sections of BNSS empower police to take preventive measures in situations where there is credible information about a potential breach of peace or disturbance to public tranquility.

2. CYBER FRAUDS

(A) UP Police Rescued a Doctor Held Under Digital Arrest for 7 Hours in a Hotel.



A doctor in Bareilly found himself in the clutches of cyber fraudsters who trapped him in a web of threats and manipulation for over seven hours. The incident highlights the growing sophistication of cybercrime and the importance of quick thinking and timely intervention.

The trouble began when the doctor received a call from scammers who falsely claimed that his Aadhaar card was involved in fraudulent activities across multiple states. Posing as officials, the **fraudsters threatened him** with a “digital arrest” and warned that **if he disconnected the call, officers from the Central Bureau of Investigation (CBI) would immediately raid his residence.** Paralyzed by fear, the doctor chose not to alert his family. Instead, he scribbled a note stating, **“I am trapped,”** and discreetly passed it to his relatives.

Recognizing the gravity of the situation, his family promptly contacted the police. Police officers, under the guidance of SP City Bareilly, quickly traced the doctor’s location to a local hotel. They discovered that he had been coerced into bringing **sensitive banking documents** with him to the hotel room.

The scammers had **forced him to stay under their control** via continuous phone communication, demanding critical financial information.

(B) AI-Powered Scams: Voice Cloning and Fake Couriers Fuel Bengaluru’s Cybercrime Surge.



Bengaluru has witnessed a staggering loss of Rs 1,788 crore to cybercrimes between 2021 and September 2024, accounting for 78.7% of the total Rs 2,270 crore siphoned off during this period. Police data highlights that these losses were concentrated across six major fraud categories, with scammers increasingly leveraging Artificial Intelligence

(AI) to enhance their schemes.

Investigators have managed to recover only 20% of the stolen funds, leaving the majority of victims without redress. The largest chunk of losses was attributed to investment frauds, amounting to Rs 1,187.2 crore, followed by job frauds (Rs 601.23 crore), courier scams (Rs 165.57 crore), debit or credit card scams (Rs 116 crore), phishing (Rs 96.98 crore), and loan app frauds (Rs 32.25 crore).

A senior police official identified delayed scam reporting and sluggish responses from banks as critical factors hampering recovery efforts. Until August, banks— including nationalized ones—took an average of eight days to respond to investigators’ requests for account details related to cyber frauds. “Victims rarely report fraud within the crucial golden hour, which is vital for freezing stolen funds. Coupled with banks’ delayed responses, recovering the money becomes almost impossible,” the officer explained.

3. TIP OF THE MONTH

A. How to differentiate between fake and real.

1. Analyze the Face and Expressions:



- **Unnatural Facial Movements:** Deepfake videos often struggle with mimicking natural facial expressions. Look for unnatural blinking (either too much or not enough) or a lack of facial muscle movements.
- **Lip Syncing:** In some fake videos, the lips may not perfectly sync with the audio, especially during complex sentences or fast speech.

2. Look for Audio-Visual Mismatches:

- **Audio Quality:** Fake videos may have audio that doesn't match the visual environment, such as a sudden change in tone, volume, or background noise.
- **Background Inconsistencies:** Watch the background and how it interacts with the subject. If shadows, reflections, or background objects seem to move unnaturally, it could be a sign of manipulation.

3. Check for Video Artifacts:

- **Blurriness or Glitches:** Deepfake or edited videos might have glitches, distortions, or blurry spots, especially around edges like hair or glasses.
- **Skin Texture Issues:** Fake videos often fail to replicate fine details, like skin pores or subtle lighting variations, especially in low-light conditions.

4. Lighting and Shadows:

- **Inconsistent Lighting:** Look for unnatural lighting on the person's face or body. If the lighting doesn't match the environment or changes suddenly, it may be a sign of tampering.
- **Shadows and Reflections:** Check whether the shadows or reflections match the lighting source and the person's movement.

5. Frame-by-Frame Analysis:

- **Motion Irregularities:** Break down the video frame by frame to catch irregularities. Fake videos may have unrealistic transitions between frames, jerky movements, or distortions that are less noticeable in real-time playback.

6. Use Deepfake Detection Tools:

- There are online tools and software designed to analyze videos for signs of tampering. Some of these tools use AI

to detect deep fake artifacts that may be invisible to the human eye.

7. Investigate Metadata:

- **File Metadata:** Inspect the video file's metadata for any signs of editing. Metadata may reveal inconsistencies like unusual compression methods or software used to edit the video.
- **Source Verification:** Always verify the source of the video. Videos that come from unverified or suspicious sources are more likely to be fake.

8. Use Reverse Video Search:

- Similar to reverse image search, you can try using a reverse video search to see if the video has been posted elsewhere, especially in a different context or with different audio.

9. Trust Your Intuition:

- If something seems too good (or bad) to be true or appears oddly sensational, it's worth investigating further. Fake videos often play on emotional responses to manipulate viewers.

By combining these techniques and remaining skeptical of unverified sources, you can better differentiate between fake and real videos.

(B) How the lost phones can remotely be locked to protect data and prevent unauthorized access.



Depending on whether you're using an **Android** or an **iPhone**:

For Android Phones:

1. Use Google's Find My Device:

- Go to Find My Device on a web browser.
- Sign in using the Google account linked to your lost phone.
- After signing in, you'll see a list of devices associated with your account. Select your lost phone from the list.

You'll have several options:

Play Sound: If your phone is nearby, you can make it ring to help find it.

Secure Device (Lock): Choose this option to lock your phone. You can set a new password, PIN, or pattern to lock the device and prevent others from accessing it. You can also display a message on the lock screen with your contact information (like a phone number or email) in case someone finds it.

Erase Device: As a last resort, if you're sure you can't recover your phone, you can erase all its data remotely. However, this should only be done if locking the device is not an option and you want to protect your data.

Alternative: Use Samsung's Find My Mobile (Samsung Phones):

If you're using a Samsung phone, you can also use Find My Mobile.

Log in with your Samsung account.

Choose your lost device and select the "Lock" option to secure your phone remotely.

For iPhones:

1. Use Apple's Find My iPhone:

- Open iCloud.com on a web browser or use the **Find My** app on another Apple device.

Sign in with your Apple ID.

Select your lost iPhone from the list of devices.

Choose **Mark as Lost**. This will lock your phone with your existing passcode and display a custom message (you can enter your contact information in case someone finds it).

Apple Pay will also be disabled when you enable "Mark as Lost."

Play Sound: You can make the phone play a sound if it's nearby.

Erase iPhone: If you believe you won't recover the phone and want to protect your personal data, you can choose the "Erase iPhone" option, which will erase all data on your device remotely. Note that once you erase it, you won't be able to track the phone anymore.

2. **Activation Lock:** If you have "Find My" enabled, **Activation Lock** will prevent anyone from using your iPhone even if they erase it. It will require your Apple ID and password to reactivate the device.

General Tips:

- **Report to your carrier:** You can inform your mobile carrier about the lost phone. They can disable your SIM card to prevent unauthorized use of your mobile number and may also help track the device.
- **Change passwords:** If you think your phone is lost permanently or contains sensitive data, change the passwords for important accounts, such as your Google, Apple ID, email, and banking apps.
- **File a police report:** In case of theft, report the phone as stolen with the police, especially if it contains valuable or sensitive information.

By following these steps, you can lock your lost phone and secure your personal information remotely.

