GMR

BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

Delhi Police bust cyber scam network with Chinese links, 3 held from Jaipur

Incident
A cyber fraud network was uncovered involving individuals who deceived people through offers related to hotel reviews. The incident came to light following investigations by law enforcement agencies in Delhi, with coordinated operations conducted across multiple states.

Modus Operandi
The perpetrators used Telegram to approach individuals with offers of monetary rewards in exchange for posting hotel reviews. After gaining the victims' trust, they were asked to transfer small amounts under the guise of processing fees. These amounts were quickly converted into USDT (a cryptocurrency) and transferred to a foreign crypto wallet, reportedly operated by an unidentified individual.

Action Taken
Authorities conducted raids in Rajasthan and Uttar Pradesh, leading to the arrest of three individuals. Investigations revealed the use of encrypted messaging platforms and cryptocurrency transactions to avoid detection and facilitate cross-border fund transfers.

Key Concern
The case underscores the growing trend of cyber frauds leveraging encrypted communication platforms and cryptocurrencies, making tracking and enforcement more complex. It also raises concerns about the vulnerability of individuals to seemingly legitimate online offers and the urgent need for digital awareness.

Former IAF Officer Duped of ₹1 Crore Through 'Digital Arrest' Scam in Noida

Incident
A retired individual was defrauded of approximately Rs 1 crore in a sophisticated cyber scam involving impersonation of government officials and threats of a so-called "digital arrest."

Modus Operandi
The victim received a call from someone claiming to be affiliated with a regulatory authority, alleging that the victim's personal credentials were linked to a money laundering case. The call was escalated to others impersonating law enforcement personnel who confirmed the false charges. The victim was coerced into believing he was under government surveillance and was offered a video interrogation as part of a fabricated investigation. Under pressure, the victim transferred funds to multiple bank accounts, believing it was necessary to avoid arrest and asset seizure.

Action Taken
Upon realizing the fraud, the victim filed a complaint through the national cybercrime reporting portal. A formal FIR was lodged the following day under relevant provisions of the Information Technology Act. Investigations are currently underway.

Key Concern
The case highlights a growing trend of psychological manipulation in cyber frauds, where scammers exploit public trust in government institutions. It also brings attention to the evolving concept of "digital arrest" used to instil fear and extract money, emphasizing the need for increased public awareness and vigilance.

Ahmedabad trader loses ₹1.42 lakh in overseas credit-card fraud, cyber cell probes

Incident
A businessman based in Ahmedabad reported unauthorized international transactions amounting to ₹1.42 lakh on his RBL Bank credit card. The transactions were carried out without any OTP or verification being shared by the cardholder."

Modus Operandi
According to the complaint, the credit card was used for three transactions in the name of an international merchant based in Hong Kong. The cardholder received an alert from the bank's customer care regarding the suspicious activity during the early hours. Despite not disclosing any OTP or security credentials, the transactions had already been processed.

Action Taken
The cardholder immediately blocked the credit card and filed a complaint with the bank's vigilance team. Although the bank initially withheld the amount as disputed, it later informed the cardholder that the liability of payment rested with him. Subsequently, a police complaint was lodged at the local police station for further legal recourse.

Key Concern
This case highlights vulnerabilities in international payment processing systems, particularly the potential bypassing of OTP-based authentication mechanisms. It also raises questions around customer liability and the protections available for victims of cross-border cyber fraud.

Powered by
GRAMAX
A GMR GROUP ENTERPRISE

Mumbai woman duped of ₹22 lakh by cyber fraudsters over spying for Pakistan.

Incident
An elderly woman from Mumbai was defrauded of ₹22 lakh by cybercriminals impersonating law enforcement officials. The accused falsely alleged her involvement in espionage activities to extort money.

Modus Operandi
The victim received multiple calls from unidentified numbers. The caller introduced himself as a member of Delhi's Anti-Terrorism Squad and claimed to be posted at a police station near the Jammu and Kashmir border. The woman was falsely informed that a case had been registered against her for allegedly leaking sensitive information to a foreign nation. Using intimidation and the threat of legal action, the perpetrators manipulated her into transferring the money.

Action Taken
The victim reported the incident to the South Region Cyber Police Station in Mumbai. A formal investigation has been initiated based on the complaint, and efforts are underway to identify the individuals behind the scam.

Key Concern
This case reflects a new and alarming trend in cybercrime where scammers impersonate national security agencies and use fabricated charges of espionage to intimidate and financially exploit victims. It also underscores the urgent need for public education on verifying the identity of callers and recognizing pressure tactics used in social engineering scams.

Mining engineer held from Jharkhand in KYC fraud

Incident
An individual was arrested for impersonating a bank official and defrauding people under the pretext of KYC verification. The accused gained unauthorized access to victims' mobile devices and misused the access to transfer funds and make high-value purchases.

Modus Operandi
The accused contacted individuals posing as a bank representative, requesting them to complete KYC formalities. Under this guise, victims were manipulated into installing a remote access application. Once control over the device was obtained, the accused transferred funds from victims' accounts and used them to purchase electronic items, including multiple high-end Apple products. Digital vouchers were used during transactions to avoid direct traceability.

Action Taken
Law enforcement officials arrested the accused, a mining engineer by profession, from Jharkhand. Several electronic devices purchased with the defrauded money were recovered. The case was brought to light following a complaint from a Delhi-based victim, leading to the investigation and subsequent arrest.

Key Concern
The incident highlights the growing misuse of remote access tools in cyber frauds, especially those disguised as routine banking processes like KYC verification. It emphasizes the importance of public awareness regarding unsolicited technical support or verification calls and the risks associated with granting remote access to mobile devices.