Cyber Crime Police Station Dhule

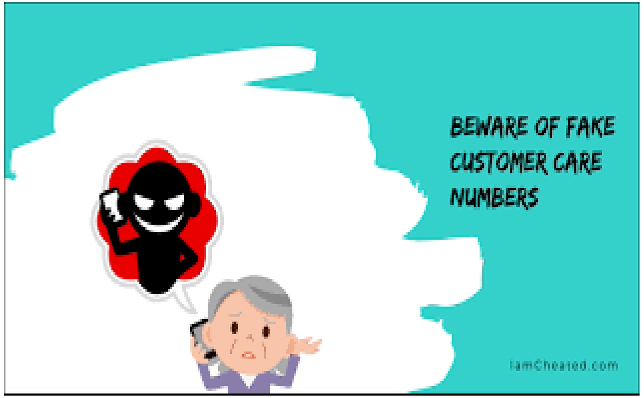
Types of Cyber Crimes

1. Online Debit/Credit cards & Bank frauds
2. Social Media offences
3. Job/VISA Frauds
4. Loan, Insurance & Lottery
5. Marketing Intelligence & OLX Frauds
6. Miscellaneous Frauds

Online Debit/Credit Cards and Bank Frauds

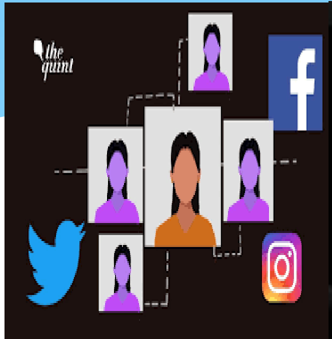
- Wishing calls to the victims in the name of bank officials
- Credit Card reward points
- Your Debit Card is being blocked, etc.,
- UPI frauds by installing remote desktop apps such as Any Desk/ Team viewer apps

- Sending UPI money request links and siphoning money
- Impersonating as customer care support (Google Pay, PhonePe Amazon, Snapdeal etc.,)
- PayTM and other E-commerce wallet's KYC updating frauds



Social Media Offences

- Fake id creation to defame the victim
- Circulating lascivious material of the victim over social media
- Keeping phone numbers of victims over dating websites
- Facebook friendship (gift) frauds
- Facebook friendship (Business) Frauds
- Sextortion through Facebook and other social media platforms



- Keeping morphed photos of victims over social media
- Circulating defamatory material over social media
- Hacking the mails of companies and sending fake invoices to clients
- Hacking of individual mails and sending money requests to friends
- Hacking of mail account and demanding money
- Ransomware Attacks

Job/VISA Offences

- Fake Job offers
- Visa processing on the name of abroad jobs
- Backdoor Jobs
- Impersonating as Job portal officials

LOAN, LOTTERY, INSURANCE OFFENCES

- Calls offering loan at unbelievable interest without sureties
- Calls offering bonus over the existing insurance policy
- Calls offering gift from shopping websites
- SMS and Mails about winning of Coca Cola lottery
- Calls regarding KBC lottery originated from Pakistan
- Instant loan apps fraud

Marketing Intelligence & OLX Frauds

- OLX and other social media advertising frauds
- Surveillance over Dating websites
- Surveillance over Locanto website
- Surveillance over news advertisements
- Male Escort Service Frauds

Miscellaneous Frauds

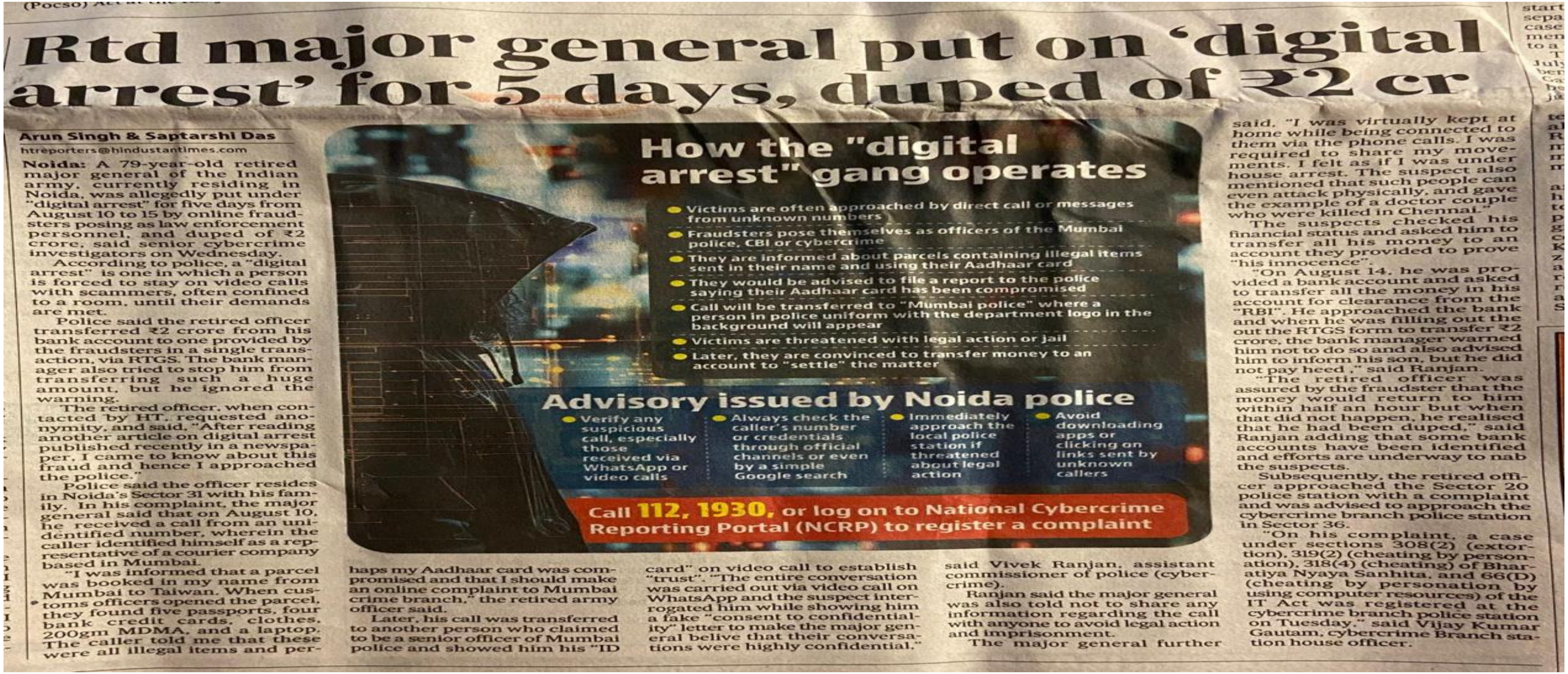
- Fake investment websites & Apps scam on the name of higher returns in Crypto currency
- Multi-level marketing scam on the pretext of higher returns in crypto currency.
- Matrimonial frauds, Nigerian frauds

Digital Arrest

The fraudsters pose as law enforcement officers and demand money from their targets by creating a panic situation

* **The Call:-**False Accusations: The callers falsely claim that the victim has committed significant crimes such as financial fraud, drug trafficking, or money laundering.
* **Creating Panic:-** The caller alleges fraudulent activity on the victim's account or a threat to their identity. They use urgency and fear tactics to pressure the victim into taking immediate action.
* **Isolation and intimidation:-** In order to keep things under control, victims are frequently told to spend a lot of time on the video call. This keeps them from asking for assistance or double-checking the information.

* **Demanding Compliance:-** The caller demands the victim take specific actions, such as transferring money, providing personal information, or downloading malware.



Rtd major general put on 'digital arrest' for 5 days, duped of ₹2 cr

Arun Singh & Saptarshi Das
htreporters@hindustantimes.com

Noida: A 79-year-old retired major general of the Indian army, currently residing in Noida, was allegedly put under "digital arrest" for five days from August 10 to 15 by online fraudsters posing as law enforcement personnel, and duped of ₹2 crore, said senior cybercrime investigators on Wednesday.

According to police, a "digital arrest" is one in which a person is forced to stay on video calls with scammers, often confined to a room, until their demands are met.

Police said the retired officer transferred ₹2 crore from his bank account to one provided by the fraudsters in a single transaction, via RTGS. The bank manager also tried to stop him from transferring such a huge amount, but he ignored the warning.

The retired officer, when contacted by HT, requested anonymity, and said, "After reading another article on digital arrest published recently in a newspaper, I came to know about this fraud and hence I approached the police."

Police said the officer resides in Noida's Sector 31 with his family. In his complaint, the major general said that on August 10, he received a call from an unidentified number, wherein the caller identified himself as a representative of a courier company based in Mumbai.

"I was informed that a parcel was booked in my name from Mumbai to Taiwan. When customs officers opened the parcel, they found five passports, four bank credit cards, clothes, 200gm MDMA, and a laptop. The caller told me that these were all illegal items and perhaps my Aadhaar card was compromised and that I should make an online complaint to Mumbai crime branch," the retired army officer said.

Later, his call was transferred to another person who claimed to be a senior officer of Mumbai police and showed him his "ID card" on video call to establish "trust". "The entire conversation was carried out via video call on WhatsApp and the suspect interrogated him while showing him a fake "consent to confidentiality" letter to make the major general belive that their conversations were highly confidential," said Vivek Ranjan, assistant commissioner of police (cybercrime).

Ranjan said the major general was also told not to share any information regarding the call with anyone to avoid legal action and imprisonment.

The major general further said, "I was virtually kept at home while being connected to them via the phone calls. I was required to share my movements. I felt as if I was under house arrest. The suspect also mentioned that such people can even attack physically, and gave the example of a doctor couple who were killed in Chennai."

The suspects checked his financial status and asked him to transfer all his money to an account they provided to prove "his innocence".

"On August 14, he was provided a bank account and asked to transfer all the money in his account for clearance from the "RBI". He approached the bank and when he was filling out the out the RTGS form to transfer ₹2 crore, the bank manager warned him not to do so and also advised him to inform his son, but he did not pay heed ," said Ranjan.

"The retired officer was assured by the fraudster that the money would return to him within half an hour but when that did not happen, he realised that he had been duped," said Ranjan adding that some bank accounts have been identified and efforts are underway to nab the suspects.

Subsequently, the retired officer approached the Sector 20 police station with a complaint and was advised to approach the cybercrime branch police station in Sector 36.

"On his complaint, a case under sections 308(2) (extortion), 319(2) (cheating by personation), 318(4) (cheating) of Bharatiya Nyaya Sanhita, and 66(D) (cheating by personation by using computer resources) of the IT Act was registered at the cybercrime branch police station on Tuesday," said Vijay Kumar Gautam, cybercrime Branch station house officer.

How the "digital arrest" gang operates

- Victims are often approached by direct call or messages from unknown numbers
- Fraudsters pose themselves as officers of the Mumbai police, CBI or cybercrime
- They are informed about parcels containing illegal items sent in their name and using their Aadhaar card
- They would be advised to file a report to the police saying their Aadhaar card has been compromised
- Call will be transferred to "Mumbai police" where a person in police uniform with the department logo in the background will appear
- Victims are threatened with legal action or jail
- Later, they are convinced to transfer money to an account to "settle" the matter

Advisory issued by Noida police

- Verify any suspicious call, especially those received via WhatsApp or video calls
- Always check the caller's number or credentials through official channels or even by a simple Google search
- Immediately approach the local police station if threatened about legal action
- Avoid downloading apps or clicking on links sent by unknown callers

Call 112, 1930, or log on to National Cybercrime Reporting Portal (NCRP) to register a complaint

- **Loan application.**

Latest cyber crime Trend

Safty Tips

* Use multi-factor authentication
* Share passwords carefully
* Backup your data
* Keep personal information private
* Keep your software updated
* Manage your social media settings
* Use secure internet connections
* Avoid clicking on links in emails
* Browse on authorized websites only
* Never share sensitive personal inform

MAHARASHTRA
CYBER

Thank You!