

# **Unmasking Deception: Social Engineering & Phishing Threats in India**

Presentation for ITU DFS Security Webinar

---

Amol Kulkarni | CUTS International (amk@cuts.org)

17 July 2025

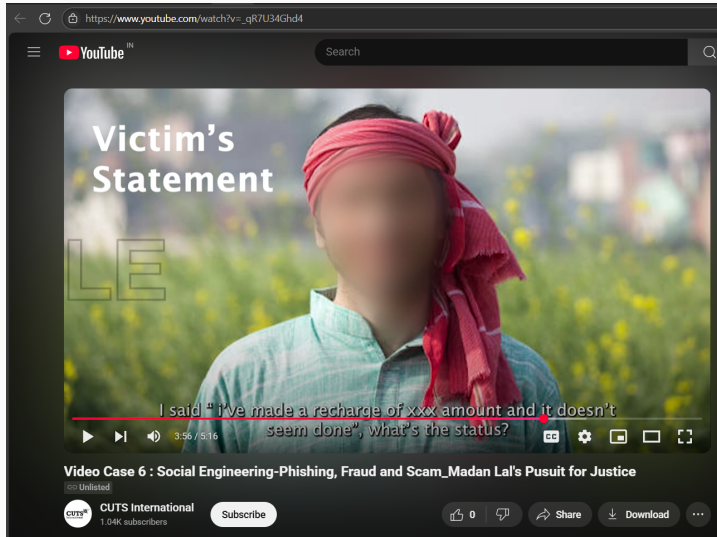
## Different forms of social engineering & phishing threats

**Actors** pose as government officials, customs officers, bank managers, army personnel, vendors, recruiters, police, office colleagues, utility providers, grievance handlers, relatives, or friends in distress

**Modes** resemble calls, sms, whatsapp, signal, popular bank websites, mobile apps, e-commerce platforms, govt portals, trusted brands, job links, customer care numbers, emails and QR codes

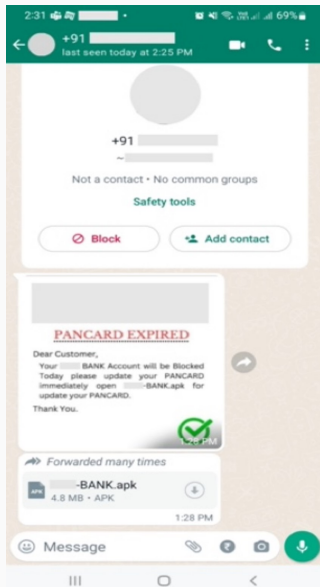
**Key targets** are senior citizens, women, children, uneducated, low income and vulnerable groups

**Money transfer mechanisms** include wallets, cryptocurrency, mules, dormant accounts, cheques, cash-outs

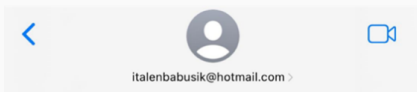


Source: <https://www.youtube.com/watch?v=qR7U34Ghd4>

# Whatsapp attack



# SMS attack



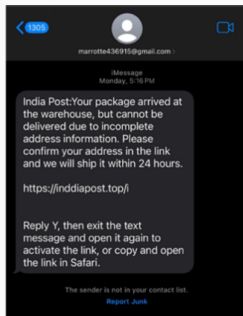
iMessage  
Yesterday, 7:14 PM

India Post:

Your package has arrived at the warehouse and we attempted delivery twice but were unable to due to incomplete address information. Please update your address details within 48 hours, otherwise your package will be returned. Please update the address in the link:<https://qrco.de/bfDaNQ>  
After the update is completed we will re-deliver within 24 hours, India Post!

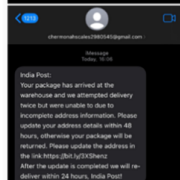
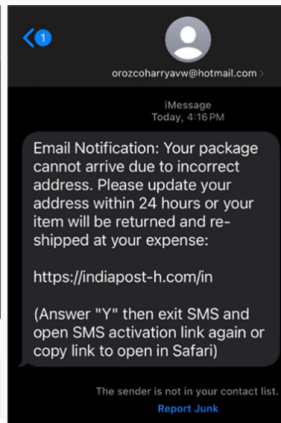
The sender is not in your contact list.

[Report Junk](#)



iMessage  
Today, 12:36 PM

India Post:  
Your package has arrived at the warehouse and we attempted delivery twice but were unable to due to incomplete address information. Please update your address details within 48 hours, otherwise your package will be returned. Please update the address in the link:<https://qrco.de/bfDGRE>  
After the update is completed we will



## The rise in social engineering & phishing threats

USD 2.78 billion lost to digital frauds in 2024 alone, nearly 3x the losses in 2023 and almost 10x that of 2022. These are just recorded numbers

Over 1.91 million complaints in 2024

Increasing trend of cyber slavery, wherein people are forced to participate in digital fraud

THE TIMES OF INDIA

# 73-year-old woman loses Rs 1.3 crore to cyber cons after five-day digital interrogation

TNN | Jun 22, 2024, 09:45 AM IST



NOIDA: A 73-year-old woman was allegedly coerced and defrauded of Rs 1.3 crore by cyber criminals, who told her that the crime branch had intercepted a package bearing her name and details, which supposedly contained drugs.

They also said that her name was linked to six accounts used for money laundering and that she would need to cough up money to clear her name. Consequently, the woman paid the amount and was subjected to digital interrogation for five days between June 13 and 18. A case has been registered

Sector 49 resident Shuchi Agrawal registered a complaint at Noida cyber crime police station in Sector 36 on Friday. She said in her complaint that a person posing as an employee of the Mumbai branch of FedEx Courier Services claimed that a parcel containing drugs, an LCD, an expired passport, an Apple iPad, and clothes weighing 5 kg was seized, which was in her name.

MONEY OFTEN WITHDRAWN USING CHEQUES, CENTRAL BANK DIGITAL CURRENCY

# Indians lost ₹11.3K cr to cyber fraud in nine months of 2024

MAHENDER SINGH MANRAL  
New Delhi, November 27

**INDIA LOST APPROXIMATELY** ₹11,333 crore to cyber fraud in the first nine months of 2024, according to data compiled by the Indian Cyber Crime Coordination Centre (I4C), a division of the ministry of home affairs (MHA).

Stock trading scams accounted for the largest share, with losses of ₹4,636 crore from 228,094 complaints. Investment-based scams caused losses of ₹3,216 crore from 100,360 complaints, while ₹1,616 crore was lost to 'digital arrest' frauds across 63,481 complaints.

Data from the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS), showed nearly 1.2 million cyber fraud complaints

## SCAM 2024

■ Stock trading scams accounted for losses of **₹4,636 cr** from 228,094 complaints

**₹1,616 cr** was lost to 'digital arrest' frauds across **63,481 complaints**

Prime Minister Narendra Modi recently cautioned citizens about 'digital arrest' frauds



Nearly **1.2 million** cyber fraud complaints were received in 2024, with 45% of these originating from Cambodia, Myanmar and Laos

were received in 2024, with 45% of these originating from South-east Asian countries—Cambodia, Myanmar, and Laos. Since 2021, the CFCFRMS has recorded 3 million complaints, leading to losses amounting to ₹27,914 crore. Of these, 1.13 million complaints were registered in 2023; 514,741 in 2022,

and 135,242 in 2021.

Prime Minister Narendra Modi recently cautioned citizens about 'digital arrest' frauds during the 115th edition of his 'Mann Ki Baat' radio programme. Stressing that no government agency contacts individuals via phone or video calls for investigations, Modi

urged the public to remain alert. "There is no system like digital arrest under the law," he said, emphasising the importance of awareness to combat such scams.

An analysis of cyber frauds this year revealed that stolen money is often withdrawn using cheques, central bank digital

currency (CBDC), fintech crypto, ATMs, merchant payments, and e-wallets. Over the past year, the I4C has frozen around 450,000 mule bank accounts, typically used to launder the proceeds of cyber crime.

At a recent anti-terror conference, the I4C flagged challenges faced by investigators in cyber fraud cases, including the anonymity of digital wallets, foreign money exchanges, lack of KYC protocols, VPN access, and cryptocurrency frauds originating from abroad.

In collaboration with the telecom ministry, the I4C has also blocked 17,000 WhatsApp accounts linked to cybercriminals operating out of Southeast Asia, as part of efforts to disrupt offshore criminal networks and strengthen India's digital security.



# Use of AI in social engineering & phishing threats


AI in over 80% of phishing threats

Creation of realistic dashboards, dynamic, interactive phishing pages


Replication of voices and faces for advanced social engineering and identity spoofing

Real time adaptation to avoid detection

Difficulty in differentiating real from fraudulent cases



## Cyber Security Awareness



### Beware of FraudGPT Scam

FraudGPT, an AI-powered Chatbot is used by Cyber criminals to craft fraudulent content for cyber frauds and crimes.

#### Modus Operandi

- FraudGPT can generate authentic-looking phishing emails, text messages, or websites that trick users to reveal sensitive information, such as login credentials, financial details, or personal data.
- It can create deceptive messages to trick users to click on malicious links/attachments leading to malware infections.
- It can imitate human conversation with users to share sensitive information or to perform harmful actions.
- It can help hackers create fraudulent documents, invoices, or payment requests for financial scams.

#### Safety Tips

- Avoid clicking on links/ attachments from unknown sources.
- Always verify the authenticity of calls, emails or messages, especially those asking for sensitive information or financial transactions.
- Contact the organization directly through their official channels to validate such requests.
- Regularly update security software, install patches, and use genuine antivirus programs to protect against potential threats.

For more safety tips visit: <https://www.cert-in.org.in> and <https://www.csk.gov.in>

## Industry efforts in curbing social engineering & phishing threats

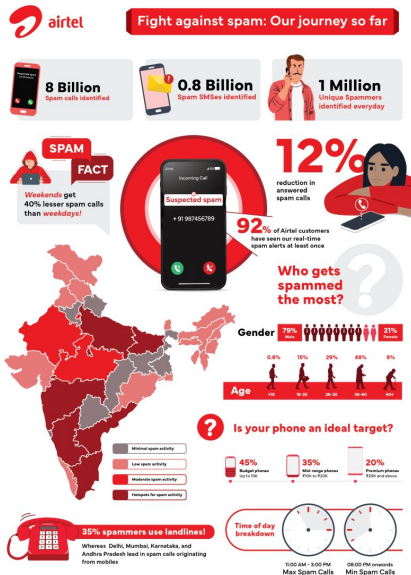
Flagging of suspicious callers

Use of AI to scan and filter links across sms, whatsapp, telegram, facebook, instagram, email, leveraging real time threat intelligence to examine over 1 billion urls daily and block access to harmful sites

Adoption of safety charters and internal standards

Dedicated programmes to raise awareness of cybercrimes through sms, radio, social media

# Industry efforts



## Govt efforts in curbing social engineering & phishing threats

Regulations around cyber and digital payment security

Limited liability frameworks to protect consumers

Tools like mulehunter.ai

Launch of dedicated number series and prefixes for promotional calls and smses

Dedicated cybercrime helpline

Device binding and transaction limits

Behavioural nudges like "I am not a fool" adverts

## Dedicated helpline

The advertisement features a dark blue background with a futuristic, glowing blue and red digital interface on the right side, showing a globe and various data points. At the top left, there is a logo for the Central Bank of India with the text 'श्रीमद्दत्तत्रयचक्रम्' and 'Central Bank of India'. To its right is the Indian national flag and the Reserve Bank of India logo. Further right is the text 'सर्वोच्च न्यायालय' and 'Supreme Court of India'. The main text in the center-left reads 'DIAL **1930** FOR ONLINE FINANCIAL FRAUD'. Below this, it says 'Report for any cybercrime at [WWW.CYBERCRIME.GOV.IN](http://WWW.CYBERCRIME.GOV.IN)'. At the bottom left, it says 'Follow cyberdost for updates on cyber hygiene'. At the bottom center, there is a red bar with the text 'www.centralbankofindia.co.in'. At the bottom right, there are five small red icons representing different services or features.

श्रीमद्दत्तत्रयचक्रम्  
Central Bank of India

भारत  
Reserve Bank of India

सर्वोच्च न्यायालय  
Supreme Court of India

**DIAL 1930**  
FOR ONLINE  
FINANCIAL FRAUD

Report for  
any cybercrime at  
[WWW.CYBERCRIME.GOV.IN](http://WWW.CYBERCRIME.GOV.IN)

Follow cyberdost for  
updates on cyber hygiene


[www.centralbankofindia.co.in](http://www.centralbankofindia.co.in)

## How does MuleHunter.AI work?

- ✓ Recognizing Patterns
- ✓ Cross-Border Tracking
- ✓ Machine Learning
- ✓ Real-Time Alerts
- ✓ Continuous Improvement
- ✓ Success Rate




# I am not a fool campaign

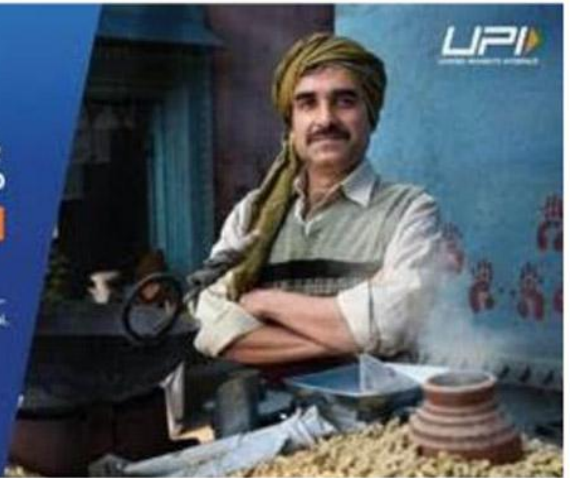



KOI LAALACH DE KAR  
LINK CLICK KARWAYE AUR  
UPI PIN MAANGE TOH KAHO  
**MAIN MOORKH  
NAHI HOON**

Dhyan rahe, kisi bhi anjaan link par click nahi karna hai.



Scan to watch the video.





## Limitations of existing approaches

Implementation and enforcement of regulatory frameworks

Sub-optimal coordination between govt departments, regulators, and states leading to limited accountability

Unreliable helplines and grievance redress mechanisms

Absence of compensation when fraud is deemed to be contributory

Privacy and data protection risks

Exclusion of genuine consumers in the name of stringent access and security protocols

Making customers responsible for falling for social engineering and phishing threats, resulting in shame and guilt

Costs on small businesses which are eventually passed on to consumers

## Too much expectations from consumers?

Stopping and thinking before proceeding with transactions

Not sharing OTPs

Use of strong passwords and 2FA

Avoiding unverified links and public wi-fi

Shifting the burden of stopping frauds on consumers

***Are we putting too much burden on already stressed consumers?***



Karthik    
@beastoftraal

I'm adequately baffled! The guy is an engineer... shouldn't his internal alarm stop him right after the first 'Send Rs. 5 so I can Rs. 10 back' in the long charade? 🙄

## Techie trying to sell used bed online shares OTPs with 'buyer', loses ₹68L

### Biggest Loss In Such A Fraud In City: Police

Chaitanya Swamy  
@timesgroup.com

**Bengaluru:** A 39-year-old engineer trying to sell a used bed by posting an advertisement on online marketplace OLX lost Rs 68 lakh to cyber-crooks over three days.

According to police, this is the biggest amount siphoned off by crooks in this manner in the city so far.

Acting on a complaint filed by Aadish (name changed), a resident of HSR Layout, on December 9, police registered a case under the Information Technology Act and IPC sections 419 (cheating by personation) and 420 (cheating and dishonestly inducing delivery of property). "We've written to the banks to freeze the accounts of the fraudsters," a police officer said.



Aadish recently posted an advertisement on OLX along with photographs of his bed that he wanted to sell, quoting a price of Rs 15,000. Around 7pm on December 6, he got a call from a person claiming to be Rohit Mishra, owner of a furniture store in Indiranagar. He told Aadish he had seen the post on OLX and was interested in buying the bed.

After discussing the price, Sharma told Aadish he would send the money to his account through a digital payment app. After a minute, Sharma said he wasn't able to send the money to his UPI ID. He asked Aadish to send him Rs 5 so he could send back the

money. Accordingly, Aadish sent Rs 5 to the UPI ID given by Sharma. In return, Sharma sent him Rs 10. Later, Sharma once again told Aadish he was unable to make the payment and asked him to send Rs 5,000. After receiving money, Sharma sent back Rs 30,000. Sharma then asked Aadish to send Rs 7,500 and said he would send him back Rs 15,000. Aadish sent the money. After that, Sharma claimed he had accidentally sent him Rs 30,000 to his account and asked Aadish to return the money by clicking on a link and sharing the OTP.

Thereafter, Aadish started losing money from his account. Aadish told TOI Sharma kept sending links and asking him to send money to his account, citing some technical problems preventing him from sending money. "I assumed he was a trader with little knowledge of making online payments," Aadish said.

"The next links he shared was in the lakhs. As I started losing money through IMPS

transfer from my account, I asked him to return the same. Sharma managed to keep me engaged, saying he was making all efforts to return my money, and I continued to send money to him. Sharma then gave me another account number in the name of one Rajesh Mishra. Twice I sent Rs 15 lakh and once Rs 30 lakh. In all, I lost Rs 68.6 lakh

between 9pm on December 6 and 9pm on December 8. As Sharma continued to ask for more money, I realised it was a fraud," he narrated.

A cop said usually victims of such fraudsters lose up to Rs 5 lakh. "But this is a huge amount... Aadish clicked on the links sent by the fraudsters and also shared OTPs, thus losing money," he said.

THE TIMES OF INDIA, BENGALURU  
FRIDAY, DECEMBER 15, 2023

## Reforms required: Bringing trust back in digital ecosystem

Unified coordinated approach to tackle threats

A dedicated sector neutral techno-legal public-private bureau to identify emerging threats and modus operandi

Collect and disseminate data among regulators, help them create appropriate regulations, fix responsibility, and redress grievances

Collect and disseminate data among industry, help them create frameworks and standards, audit preparedness, respond and combat threats

Insurance and liability pools to help stakeholders operate confidently in a world where threats are minimized, implications are contained, and consumers are compensated

User friendly mechanisms for consumers to obtain refunds and restitution

Empowering consumer groups to ensure consumer voices are heard and feedback loops work

## About CUTS

Global public policy research advocacy and capacity building group, headquartered in India, with presence in Africa, South-East Asia, Europe and USA

Began as consumer group in 1983, now working on regulation, trade, and governance reforms

Regular engagement with govt, industry and other consumer groups

More about CUTS work in digital economy: <https://cuts-ccier.org/digital-economy/>

Recent study on digital fraud: <https://cuts-cart.org/frauds-and-grievance-redress-in-digital-payments-and-digital-credit-services-in-rajasthan/>