इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

www.isea.gov.in

certin
Enhancing Cyber Security in India

NATIONAL CYBERSECURITY AWARENESS MONTH 2024
Cyber Surakshit Bharat

# Beware! Scam Alert

## Frauds in the name of INDIA POST


Cybercrimes pose significant risks to vulnerable groups like senior citizens and women, who are often targeted by fraudsters due to their perceived lack of familiarity with complex digital scams. These crimes can result in financial exploitation, identity theft, and emotional distress, further threatening their personal safety and security.

## About India Post fraud

Cyber criminals are now using India Post to scam unsuspecting individuals. A recent case involved a retired government employee losing 23.26 lakh. Though only few cases have been reported so far, this can become a worrying trend, caution experts.

*Recent incident:*

**Scamsters using India Post for online fraud**


A 75-year-old retired central government employee from West Marredpally area in Hyderabad city of Telangana State, was defrauded of Rs 23.26 lakh by cyber fraudsters pretending to be officials from India Post.

In this case the fraudsters posing as India Post officials had contacted the victim claiming that a suspicious parcel has been booked with his name and ask him to immediately file complaint with police. Later they connect him to a conman pretending to be police officer who uses deceptive tactics and also entice him with a commission amount and in the process loot large sum of money on some or other pretext.

# Dangers

## Financial loss

Victims may lose large sums of money by transferring funds to fraudulent accounts under false pretenses.

## Identity theft

Fraudsters may misuse personal details like Aadhaar credentials for illegal activities, including money laundering.

## Emotional distress

Victims, especially senior citizens, may experience severe emotional distress due to fear, confusion, and anxiety caused by the scam.

## Bank account compromise

Sensitive payment information provided to the scammers can lead to full access to bank accounts, resulting in drained savings or credit limits.

## Legal and credit issues

Scammers may use stolen identities to commit crimes or take loans, leading to legal complications and damage to the victim's credit score.

## Involvement in criminal activity

They may implicate victims in criminal activities like money laundering, drawing them into legal and financial issues, often enticing them with false promises of commissions or rewards.

# Modus Operandi

## Initial Contact via SMS


Victims receive an SMS, supposedly from India Post, about a parcel booked in their name, containing a link for detail updates.

## Follow-up Phone Call

A scammer calls, posing as an India Post official, to further engage the victim.

## Pressure Tactics

The scammer creates a sense of urgency, pressuring the victim to act quickly.

## Fake Website and Verification Process


Victims are directed to a counterfeit website that resembles the official India Post site, where they're coerced into paying large sums to “clear” their names with authorities.

## Sensitive Information Theft

The fake site prompts victims to enter sensitive information (credit/debit card details, PINs, CVVs, OTPs), leading to financial theft through unauthorized transactions.

# Warning Signs

## Unsolicited SMS


Receiving an unexpected message from "India Post" about a parcel you did not book or are unaware of.

## Urgency and pressure

The message or caller emphasizes the need to act quickly, pressuring you to avoid penalties or order cancellations.

## Suspicious links


The SMS contains a link that redirects to a website that may look similar to India Post's official site, but with a different URL.

## Follow-up phone Call

Receiving a call from someone posing as an India Post official immediately to reinforce urgency.

## Requests for Personal Information

Being asked to provide sensitive details such as Aadhaar, PAN, or bank account information over the phone or through a website.

## Suspicious Payment Requests

Being asked to enter sensitive financial details like credit/debit card numbers, CVVs, OTPs, and PINs, which should never be required for parcel redelivery.

# Security Tips

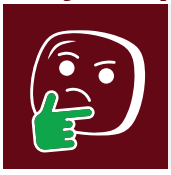
## Verify authenticity of the caller

Always cross-check with official India Post customer service or law enforcement if you receive suspicious calls.

## Do not share personal information

Never disclose sensitive information like Aadhaar, PAN, or bank details over the phone to unknown callers.

## Stay skeptical



Be cautious of unsolicited calls that demand immediate action, especially if they involve large sums of money.

## Consult authorities

If you receive such calls, report them to the cybercrime division or your local police before making any transactions.

India Post online fraud is a growing threat, targeting vulnerable individuals using deceit and manipulation. Awareness, care and caution needs to be exercised to remain safe against such frauds and imposters.

*References:*
*https://economictimes.indiatimes.com/news/how-to/beware-cybercriminals-are-now-using-india-post-for-online-fraud/articleshow/113412935.cms*
*https://cionews.co.in/criminals-target-victims-using-india-post-for-scam/*
*https://www.business-standard.com/india-news/new-india-post-scam-targets-citizens-what-is-it-and-how-to-be-safe-124091700490_1.html*

Supported by :

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Digital India
Power To Empower

mygov
मेरी सरकार

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

सी-डैक
CDAC