Vulnerability to Cyber Frauds

Mains: *GS-III – Cyber Security*

Why in news?

A recent study by Lokniti-Centre for the Study of Developing Societies (CSDS) and Common Cause surveyed 8,306 citizens across 16 States, examining how frequently citizens encounter fraud calls/messages, who is targeted, and the social profile of those most exposed.

What is cyber fraud and its types?

- **Cyber fraud** – It is any illegal activity using the internet and digital tools to steal your sensitive information, personal data or money through deception.
- **Common Types**
- **Digital Arrest** – Scammers pose as police or customs officials, claiming you are in a fake crime video and demanding money to avoid arrest.
- **Investment & Trading Scams** – Fake apps or social media groups promise huge profits on stock or crypto trading.
- **Phishing & Vishing** – Fraudulent texts, emails, or phone calls trick you into revealing passwords or One-Time Passwords (OTPs).
- **Task-Based Scams** – Offers for easy money in exchange for rating videos, liking posts, or doing small online tasks.
- **Customer Care Fraud** – Fake helplines offering cashbacks or refunds.
- **Malware/APK Scams** – Harmful apps that give criminals remote access to your phone.
- **National Crime Records Bureau (NCRB) Data** – Cybercrime cases rose 17.9% nationally, from 86,420 in 2023 to 1,01,928 in 2024, even as overall registered crime declined by 6% in the same period.
- Cybercrime as a crime category is moving sharply against the national trend.

What is the scale of cyber frauds and scams in India?

- **Widespread exposure to fraud calls –** Nearly 33% of the citizens reported frequently (‘many times’ and ‘sometimes’) receiving calls about deliveries they never ordered.
- Regularly encountered high-return investment scam calls (31%).
- More than 27% frequently received calls from bank officials asking for personal account details
- About 23% received calls about their phones being linked to illegal activities

- An unknown number claiming to be their friend urgently in need of money is 23%.
- 20% of the respondents frequently received calls from police or someone in authority claiming that their friend or relative is in danger or has committed some type of crime.
- However, it is important to note that a majority, roughly 50-60% of respondents, have never received these calls.
- **Internet usage and scam exposure** – Moreover, respondents who spend more time online were more likely to be targeted by fraudsters.
- **Heavy Internet Users** – 18% fall in the high scam-exposure category and 28% in the moderate category; together, over 46% report scam exposure.
- **Non-Internet Users** – In contrast, among those who do not use the internet, only 5% report high exposure and 14% report moderate exposure.

How do fraudsters exploit the digital footprint?

- **Growing digital footprint** – The common thread is deeper integration into the digital ecosystem, creating a larger footprint for fraudsters to exploit.
- **Exploiting digital participation** – Instead of relying solely on technical expertise, fraudsters target social relationships and institutional credibility.
- Investment scams appeal to the aspiration of getting rich quickly, delivery scams draw on trust in e-commerce, bank impersonation uses institutional credibility, and fake police calls exploit fear of authority.
- By manipulating familiar relationships and situations, fraudsters are able to effectively make deception appear legitimate.
- **From scam attempts to actual victims** – Not every scam attempt succeeds, but a significant number of people suffer real harm.
- Data shows that 13% of people were direct victims of cybercrime in the last two to three years.
- Among them, more than half (54%) of the people have experienced financial fraud, 13% said their devices were hacked, 11% reported personal data theft, 7% reported cyberbullying or abuse on social media, and four per cent reported online sexual harassment.

Who are the targets of financial fraud?

- **Financial fraud and social status** – Financial frauds are more layered around social and economic position.
- The wealthiest people (57%) are most vulnerable to financial fraud, though nearly half of economically disadvantaged respondents (47%) are victims of digital fraud too.
- **Higher education, higher risk** – Similarly, the more educated a respondent is, the more likely they are to be a victim of cybercrime.
- 40% of those without any formal education are victims of financial fraud, as compared to nearly three in five (59%) college graduates.
- **Significant financial loss** – The losses incurred due to cyber fraud are substantial. Over eight in ten victims of cybercrime reported some financial loss.
- **Target people with resources** – In essence, fraudsters in India, all the while exploiting ignorance and vulnerability, are also systematically tracking digital participation, aiming to catch those with resources.

- Fraud in this sense has become less a tax on carelessness than a tax on connectivity itself.

Table 1: Frequently reported cyber fraud attempts

Received a call/ text message for	Many times	Sometimes	Rarely	Never
Investment opportunity, guaranteeing a high return	10	21	20	45
Delivery of a product you never ordered	8	25	20	44
Bank official asking for personal account details	7	20	21	49
A phone number has been linked to illegal activities	6	17	16	56
An unknown number claiming to be your friend/ relative who is in urgent need of money	6	17	19	54
Call from police or someone in authority claiming that your friend/ relative is in danger or has committed some crime	5	15	18	59

Note: All figures are in percentages. Others did not respond.

Table 2: Online engagement and exposure to fraudulent calls

Online exposure	Likelihood of receiving fraudulent calls/messages			
	Did not receive any fraudulent calls/messages	Low likelihood	Moderate likelihood	High likelihood
Not active online	54	27	14	5
Low online exposure	45	33	19	3
Moderate online exposure	30	34	26	10
High online exposure	22	32	28	18

Note: All figures are in percentages. This is an index created using questions including those regarding frequency of use of social media, mobile banking apps and UPI; frequency of receiving suspicious/fraud-related calls or messages, including fake deliveries, bank scams, emergency money requests, illegal activity claims, and fraudulent investment offers.

Table 3: Nature of cybercrimes faced by people

Nature of crime	Victims (%)
Digital financial frauds	54
Hacking of devices	13
Personal data theft	11
Cyberbullying/abuse on social media	7
Online sexual harassment	4

Note: The rest did not respond.

Table 4: Socioeconomic profile of digital financial fraud victims

Economic class	Victims of digital financial frauds (%)
Poor	47
Lower	56
Middle	57
Rich	57
Level of education	
Non-Literate	40
Upto Primary	44
Upto Matric	53
College and above	59

Note: The figures are only among financial fraud victims.

Table 5: Financial losses incurred by victims of digital fraud

Amount of financial loss suffered	Digital financial fraud victims (%)
No financial loss*	9
Up to ₹1,000	8
₹1,001 to 5000	25
₹5,001 to 10,000	16
₹10,001 to 20,000	13
Above ₹20,000	23

Note: The rest did not respond.
*Since not all digital fraud resulted in loss of money, some people have reported no financial loss.

How are cyber frauds administered and reported in India?

- **Legal framework** – When an FIR is filed by law enforcement, the offences are booked under a combination of two major legal codes -
- **Information Technology (IT) Act, 2000** –
  - **Section 66D** – Cheating by personation using a computer resource (e.g., fake profiles, impersonating officials).
  - **Section 66C** – Identity theft (stealing passwords, OTPs, digital signatures, or biometrics).
  - **Section 66** – Fraudulent or dishonest damage to a computer or network.
- **Bharatiya Nyaya Sanhita (BNS), 2023** (Formerly the Indian Penal Code) – Sections covering Cheating & Forgery – Traditional criminal aspects of the fraud, such as financial cheating, extortion, and forging electronic documents.
- **Designated Reporting Systems**
- **National Cybercrime Reporting Portal (NCRP) –** All online frauds can be registered digitally at cybercrime.gov.in.
- **Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS)**

– Financial online frauds (like UPI, banking, or credit card scams) reported through the 1930 National Helpline are processed under this dedicated system to freeze stolen funds in real-time.

Reference

The Hindu | Who is the most vulnerable to cyber frauds?