Digital Financial Frauds

written by iasexam.com | 29/03/2024

Context

A recent report by the Indian Cyber Crime Coordination Centre has stated that **digital financial frauds** in India accounted for ₹1.25 lakh crore over the last three years.

Rise in Digital Frauds

- According to the **National Crime Records Bureau (NCRB)**, cybercrimes in India in 2023 led to a loss of ₹66.66 crore, with 4,850 reported cases.
- According to the National Cybercrime Reporting Portal (NCRP), in 2023, as a minimum ₹10,319 crore was mentioned to be lost by digital financial fraud.

How Digital Frauds Work?

- Convincing the victim to send money, either by impersonation (fake WhatsApp/FB/Insta, social media profiles) or by giving them a fake promise of higher return.
- By taking credentials including **Unified Payments Interface ID (UPI)**, **Personal Identification Number (PIN)**, **One-Time Password (OTP)** or Internet banking ID/password from the victim and then the use of the same on different apps/websites and shifting cash without the knowledge of the victim.
- By taking card information and convincing the victim to share OTP.

How can Frauds be Prevented?

- Just as Google money does not allow logging in from a new tool unless permission is

granted by using the former, financial establishments need to be mandated to replicate this selection of their apps.
- The display proportion facility should be disabled. Banking and financial apps should disable display screen-sharing to run on top of them.
- In the bank statement, all banks/NBFCs/SEs must be mandated to offer understandable statistics.
    - Currently only partially printed numbers are proven which even informed customers are not able to recognize.
- The International Mobile Equipment Identity (IMEI) must be recorded.
    - All banking and financial apps must be mandated to shop IMEI details of the tool being used.
    - Fraudsters use fake mobile numbers and pretend bank debts which span across different States with the purpose of adding layers to increase anonymity and preventing businesses from prosecuting them.

Government Initiatives

- The **Digital Intelligence Platform (DIP)** is an initiative evolved by the Department of Telecommunications to function as a strong and incorporated platform for real-time intelligence sharing, information exchange, and coordination amongst diverse stakeholders.
- **Chakshu Facility:** It is a newly introduced function at the Sanchar Saathi portal that encourages residents to proactively record suspected fraudulent communications acquired by call, SMS, or WhatsApp.
- The Central Government has additionally launched the **National Cyber Crime Reporting Portal**, to enable complainants to report lawsuits concerning all types of cyber crimes, which include internet and online frauds.
- Reserve Bank of India has issued several circulars/ guidelines related to security and risk mitigation measures for securing electronic / digital payment transactions.

Conclusion

- The fintech and telecom industries should be mandated to take certain preventive steps in their technology and offer statistics in a manner which enables quicker investigation, the prevention, detection, recuperation and conviction will be much more effective.
- Faster availability of data will make it simpler to be aware of and convict pan-Indian gangs.

Source: **The Hindu**

UPSC Prelims Practice Question

Q.With reference to the Non-banking Financial Companies (NBFCs) in India, consider the following statements: (2010)

1. They cannot engage in the acquisition of securities issued by the government.

2. They cannot accept demand deposits like Savings Account.

Which of the statements given above is/are correct?

a. 1 only
b. Both 1 and 2
c. 2 only
d. Neither 1 nor 2

Ans – “b”