STUDY NOTES · BASIC CONCEPT

All about Digital Arrest, Social engineering, Money Mule accounts, Money laundering and Related laws in India

Defence & Security

09 Oct 2026

A. Digital Arrest

1. A cyber-fraud technique involving impersonation of police officers, CBI officials, judges or other authorities.
2. Victims are threatened with arrest, investigation or reputational damage.
3. Fraudsters may demand money under the pretext of verification, bail or settlement.
4. Key fact: Digital arrest is not a legally recognised form of arrest.

BECOME IAS
AI-Powered UPSC Preparation by ZINKPOT

B. Cybercrime and Social Engineering

1. Cybercrime refers to unlawful activities involving computers, digital devices, networks or electronic communication.
2. Social engineering involves manipulating people into revealing confidential information, transferring money or taking actions that benefit criminals.
3. Common techniques include:
4. Impersonation of government officials.
5. Phishing emails and fraudulent messages.
6. Fake video calls and forged documents.
7. Threats, urgency and psychological intimidation.

C. Money Mule Accounts

1. A money mule is a person whose bank account is used to receive, transfer or conceal proceeds of crime.
2. Some account holders knowingly assist criminals.
3. Others may be deceived, recruited under false pretences or have their accounts misused.
4. Investigators examine transaction records, beneficiaries and the movement of funds to establish the facts.

D. Money Laundering

Money laundering involves concealing the illicit origin of criminal proceeds to make them appear legitimate.

The traditional stages are:

1. Placement: Introducing illicit money into the financial system.
2. Layering: Moving money through multiple transactions to obscure its origin.
3. Integration: Reintroducing illicit proceeds into the economy in an apparently legitimate form.

Not every cyber-fraud transaction automatically constitutes money laundering; the applicable legal elements must be established.

E. Bank Account Freezing and Due Process

1. A bank account may be frozen or transactions restricted under applicable legal powers during an investigation.
2. Aspirants should understand the distinction between:
3. Suspicion and proven guilt.
4. Preventive or investigative action and punishment.
5. Temporary restrictions on an account and final confiscation of property.
6. Evidence of receiving funds and proof of knowing participation in a crime.
7. The accused retains applicable legal rights, including access to judicial remedies.

BECOME IAS
AI-Powered UPSC Preparation by VINKPOT

F. Important Laws and Institutions

Law or institution	Relevance
Information Technology Act, 2000	Addresses specified offences involving electronic records, identity theft and online impersonation-related conduct.
Bharatiya Nyaya Sanhita, 2023	Provides criminal-law provisions applicable to cheating, forgery and related offences, depending on the facts.
Prevention of Money Laundering Act, 2002	Applies where the statutory requirements concerning proceeds of crime and money laundering are satisfied.
Bharatiya Nagarik Suraksha Sanhita, 2023	Governs criminal procedure, including applicable investigative and seizure-related processes.
Indian Cyber Crime Coordination Centre (I4C)	Coordinates efforts to combat cybercrime.
National Cyber Crime Reporting Portal	Enables reporting of cybercrime complaints.
Indian Cyber Crime Helpline 1930	Provides a channel for promptly reporting financial cyber fraud.
Reserve Bank of India	Regulates banks and issues relevant directions on customer protection and banking operations.

BECOME IAS
AI Powered UPSC Preparation by ZINKPOT

G. Challenges for Internal Security

1. Cross-border cybercriminal networks.
2. Rapid transfer of stolen money across multiple accounts.
3. Use of fake identities, SIM cards and digital communication tools.
4. Limited cyber awareness among vulnerable citizens.
5. Difficulties in collecting and preserving digital evidence.

6. Coordination gaps among banks, police forces and other agencies.
7. Risk of innocent account holders being caught in investigations.

H. Way Forward

-

1. Promote public awareness about impersonation-based fraud.
2. Encourage immediate reporting through helpline 1930 and official cybercrime reporting channels.
3. Strengthen real-time fraud detection and transaction monitoring.
4. Improve coordination between banks, police and cybercrime units.
5. Build specialised digital-forensics capabilities.
6. Ensure prompt investigation and lawful handling of frozen accounts.
7. Protect victims and provide accessible grievance-redressal mechanisms.
8. Strengthen international cooperation against cross-border cybercrime.
9.

BECOME IAS
AI-Powered UPSC Preparation by ZINKPOT