PAREEKSHA BAAZ
Institute for CSE Examination

CURRENT AFFAIRS
2th DEC 2024

INDEX

Rising Digital Arrests

Why in News?

Digital arrests are the newest form of **cyber scam** that has affected more than **92,000 Indians** in 2024 in which **money is extracted** through online transfers under the guise of **resolving tax or legal dues.**

What are Key Facts About Digital Arrest?

- **About:** Digital arrest scams involve cybercriminals **impersonating law enforcement officials or government agencies** such as the State police, **CBI**, **ED**, and **Narcotics Bureau** defrauding gullible victims of their hard-earned money.

  o Scammers call **unsuspecting people,** claiming a case has been filed against them and even use a **fake police station** to give credence to their allegations.

- **Modus Operandi:** Cybercriminals contact victims by **phone or email,** starting with **audio calls and then video calls** from places like airports, police stations, or courts.

  o They use photos of **police officers, lawyers, and judges** as display pictures on their social media accounts to appear legitimate.

  o They may also send **fake arrest warrants, legal notices, or official-looking documents** via email or messaging apps.

- **Trapping Victims**: The cybercriminals typically accuse victims of serious crimes such as **money laundering, drug trafficking**, or cybercrime.

  o They may **fabricate evidence** to make their accusations seem credible.

- **Vulnerability of People:**

  o **Fear and Panic:** Fear of arrest threats push victims to comply **without rational thought.**

  o **Lack of Knowledge:** Unfamiliarity with law enforcement procedures makes it difficult for victims to distinguish legitimate claims from fraud.

  o **Social Stigma:** Fear of **social stigma** and impact on family motivates victims to comply to avoid embarrassment.

  o **Manipulative Techniques:** Use of **AI voices, professional logos, and simulated video calls** to appear credible and increase victim compliance.

  o **Isolation and Control:** Scammers isolate victims by preventing them from seeking verification, making it easier to control them.

  o **Increased Target Vulnerability:** Trusting, **less tech-savvy,** or stressed individuals are prime targets for easier deception.

What is the Status of Cyber Scams in India?

- **Overview:** According to the **Indian Cyber Crime Coordination Centre (I4C),** cyber scams in India have shown a significant rise in both **frequency and financial impact.**
  - This alarming trend indicates a **persistent and evolving** threat landscape in India's digital ecosystem.
- **Complaints and Losses:** The number of complaints increased significantly over the years, with **1,35,242 complaints in 2021, 5,14,741 in 2022, and 11,31,221 in 2023.**
  - The total **monetary loss** from cyber frauds has reached **Rs 27,914 crore** between **2021 and September 2024.**
- **Major Scams:**
  - **Stock Trading Scams:** It is the most significant source of loss with **Rs 4,636 crore** from **2,28,094** complaints.
    - Under it, scammers offer **unrealistic returns** trading stocks, foreign currencies, or cryptocurrencies but victims end up being **defrauded**.
  - **Ponzi Scheme Scam:** Caused **Rs 3,216 crore** in losses with **1,00,360** complaints.
  - **"Digital Arrest" Frauds:** Accounted for **Rs 1,616 crore** in losses from **63,481** complaints.
- **New Money Siphoning off Tactics:** Cybercriminals have adapted their strategies to siphon off money.
  - **Withdrawal Methods:** Stolen money is often withdrawn through various channels, including **cheques**, **CBDC, fintech cryptocurrencies, ATMs, merchant payments,** and **e-wallets.**
  - **Mule Accounts:** The I4C has identified and frozen around **4.5 lakh mule bank accounts**, used primarily for laundering funds from cybercrime.

Indian Cyber Crime Coordination Centre (I4C)

- **About:** I4C was launched by the **Ministry of Home Affairs in 2020** to deal with all types of **cyber crimes** including **cyber fraud** in a comprehensive and coordinated manner.
- **Objectives of I4C:**
  - To act as a **nodal point** to curb **Cybercrime** in the country.
  - To **strengthen the figh**t against Cybercrime committed against **women and children.**
  - Facilitate **easy filing Cybercrime related complaints** and identifying Cybercrime trends and patterns.

- o   To act as an **early warning system for Law Enforcement Agencies** for proactive Cybercrime prevention and detection.

- o   **Awareness creation** among the public about preventing Cybercrime.

- o   Assist States/UTs in **capacity building of Police Officers,** Public Prosecutors and Judicial Officers in the area of cyber forensic, investigation, cyber hygiene, cyber-criminology, etc

- ▪   **National Cyber Crime Reporting Portal:**

  - o   Under I4C, the **National Cyber Crime Reporting Portal** is a **citizen-centric initiative** which will enable citizens to **report cyber fraud online** and all the complaints will be accessed by the concerned law enforcement agencies for taking action as per law.

What are Challenges in Addressing Cyber Scams?

- ▪   **Anonymity and Privacy:** Cybercriminals use tools such as **virtual private networks (VPNs)** and **encrypted messaging** apps to **conceal their identity and location**, complicating efforts to trace and arrest them.

- ▪   **International Scope:** Cyber scams often span **multiple countries**, making it difficult for local law enforcement to take action.

  - o   A significant portion of scams originates from **Southeast Asia and China**.

- ▪   **Rapidly Evolving Tactics**: Phishing scams have advanced from simple emails to more sophisticated tactics, including **social engineering**, **text messages, and voice calls,** making fraud harder to detect.

- ▪   **Advanced Malware:** Cyber scams use advanced malware that can **bypass antivirus programs and firewalls** to steal data or gain unauthorized access.

- ▪   **Regulatory Fragmentation:** Different countries have different regulations, making it difficult to create cohesive international strategies for combating cybercrime.

  - o   Also, countries **lack comprehensive threat intelligence** to identify emerging cyber scam trends and tactics without sharing data.

- ▪   **Growing Digital Market**: The growth of **e-commerce** and **digital payment systems** has led to an increase in scams such as **fake online stores, card skimming, and fraudulent payment schemes.**

Types of Cyber Scams

- ▪   **Phishing Scams:** Fraudsters **send fake emails or messages** that mimic trusted organizations to trick victims into sharing sensitive information like **passwords or financial details.**

- ▪   **Lottery and Prize Scams:** Victims receive notifications claiming they have won a **significant prize** and are asked to pay a **processing fee or taxes** to claim it.

- **Emotional Manipulation Scams:** Scammers on **dating apps** build relationships with victims and later ask for money for emergencies, often demanding payments in **cryptocurrency.**

- **Job Scams:** Scammers post **fake job listings** on hiring platforms or social media to trick job seekers, especially fresh graduates, into giving **personal information or money.**

- **Investment Scams:** These scams appeal to a **victim's desire for quick money** by promising high, unrealistic returns through **Ponzi or pyramid schemes.**

- **Cash-on-Delivery (CoD) Scams:** Scammers set up **fake online stores** that accept CoD orders. When the product is delivered, it is either **counterfeit or not as advertised.**

- **Fake Charity Appeal Scams:** Scammers create **fake websites or social media pages** for bogus causes like **disaster relief or health initiatives,** using emotional stories or images to create **urgency and sympathy.**

- **Mistaken Money-Transfer Scams:** Scammers contact victims claiming money was **mistakenly sent** to their account and using fake transaction receipts to pressure them into returning it to avoid **legal trouble.**

- **Credit Card Scams**: Fraudsters offer loans at **low interest rates** with quick approval. After the victim pays an **upfront fee** to secure the loan, the scammers disappear.

What are the Key Government Initiatives Related to Cyber Scam in India?

- **National Cyber Security Policy**

- **Computer Emergency Response Team - India (CERT-In)**

- **Cyber Surakshit Bharat Initiative**

- **Cyber Swachhta Kendra**

- **National Critical Information Infrastructure Protection Centre (NCIIPC)**

- **Digital Personal Data Protection Act, 2023**

- **Cyber Crime Coordination Centre**

- **Citizen Financial Cyber Fraud Reporting and Management System**

Way Forward

- **Digital Safety:** India's PM outlined a simple **three-step safety protocol** to protect against digital arrests.
  - **Stop:** Remain calm and **avoid giving out personal information** immediately.
  - **Think:** Be aware that **legitimate agencies** don't conduct such inquiries over calls or demand payments through calls.

- o **Take Action**: Report incidents on the **National Cyber Crime Helpline (1930) or at National Cyber Crime Reporting Portal**, inform family members, and record evidence.
- **Cybersecurity Best Practices:** Use **firewalls** that act as the **first line of defence** for computers, monitoring and filtering network traffic to prevent unauthorised access.
  - o Keep all software and hardware systems **up-to-date to patch security vulnerabilities.**
- **Enhanced Security:** Implement **two-factor authentication** to add an extra layer of security. Use encryption to protect sensitive data, including financial records.
- **Heightened Alertness:** Banks should monitor **high-value transactions in low-balance or salaried accounts** and alert authorities, as **stolen money** is often moved to these accounts before being converted to **cryptocurrency and sent abroad.**
- **Awareness:** Don't give out any personal information (such as **Aadhaar or PAN card** details). Do not send any money.
  - o Always independently **verify the caller's identity** through official channels.
  - o Learn about **common scam tactics** and share this information with your family and friends to prevent such events.
- **International Cooperation:** Collaboration between nations to create **common laws, share intelligence, and coordinate response**s can help combat cross-border cybercrime.

Rise of Indian Tourism Sector

In News

- The Centre has approved ₹3,295 crore in interest-free loans for **tourism** infrastructure development across states.

About

- The Union Finance Ministry cleared the loans, which are being disbursed under the **Special Assistance to States for Capital Investment (SASCI) scheme.**
  - o The loans are long-term, interest-free, and will be repaid over 50 years.
  - o The aim is to develop iconic tourist centers, enhance global branding, and promote sustainable **tourism** that boosts local economies and creates jobs.
- States are encouraged to develop lesser-known tourist destinations like Bateshwar (Uttar Pradesh), Ponda (Goa), Gandikota (Andhra Pradesh), and Porbandar (Gujarat).
  - o 40 new tourism projects have been identified across 23 States.

India's Tourism Sector Growth:

- India, one of the oldest civilisations in the world, is a multicultural melting pot.
- India's tourism industry is becoming a global favorite due to its **rich heritage, cultural diversity, and beautiful destinations,** contributing significantly to **economic growth and job creation.**
  - o In 2022-23, 76.17 million direct and indirect jobs were created in the tourism sector, compared to 70.04 million in 2021-22.
- **Government Budget for Tourism:** For FY25, the government has allocated ₹2,479 crore to further develop the tourism sector.
- **Global Ranking**: India ranks **39th among 119 countrie**s in the **Travel and Tourism Development Index 2024 (TTDI)**, with improvements in:
  - o Prioritization of Travel & Tourism,Safety & Security,Health & Hygiene.
- **Foreign Tourist Arrivals (FTAs):** In 2023, India recorded 9.24 million FTAs, a 43.5% growth compared to 2022 (6.44 million).
  - o Foreign Exchange Earnings (FEEs) from FTAs grew by 65%, reaching ₹2.3 lakh crore in 2023.
  - o **Measures to Increase FTAs:** Promotion of adventure and niche tourism.
    - ▪ Easier access to e-visas.
    - ▪ Launch of a 24×7 multilingual helpline for tourists.
    - ▪ Launch of Paryatan Didi and Paryatan Mitra for a better tourist experience.

- o In 2023, 2,509.63 million Domestic Tourist Visits (DTVs) were recorded, up from 1,731.01 million in 2022.

Government's Initiatives

- The government is prioritizing adventure tourism and sustainable tourism along with technological integration to increase sector growth.
- **Infrastructure Investment**: India has invested around ₹7,000 crore (approximately $1 billion) in building tourism infrastructure to improve the tourist experience.
- Initiatives like **Dekho Apna Desh, PRASHAD, Vibrant Village Programme, SWADESH 2.0**, and Udaan aim to promote domestic tourism.

Challenges

- **Infrastructure Deficiencies**: Poor connectivity in remote areas, limited quality accommodation in rural destinations, and inadequate basic amenities.
- **Safety and Security Concerns:** Issues such as crime, health risks from disease outbreaks, and political instability in certain regions can deter tourists.
- **Environmental Impact**: Pollution in urban areas, overtourism leading to the degradation of popular destinations, and potential harm to wildlife and ecosystems due to tourism in sensitive areas.
- **Cultural Sensitivities:** Tourists may unintentionally disrespect local customs, and increased tourism can threaten the preservation of cultural and heritage sites.
- **Marketing and Promotion**: Inadequate awareness and ineffective branding campaigns, like "Incredible India," fail to highlight the country's diverse attractions.
- **Skill Development:** There is a lack of trained professionals in the tourism industry and language barriers for foreign tourists.

Conclusion and Way Forward

- India's tourism industry has shown remarkable growth due to government initiatives, infrastructure development, and global branding.
- The government sees tourism as a driver of social inclusion, employment, and economic progress, working towards making India a developed country by 2047.
- Continued focus on sustainable tourism and technological integration is expected to further boost the sector.

Odisha Public Examinations (Prevention of Unfair Means) Bill, 2024

Context

- The Odisha government is to enact a new law with **stringent penal provisions to check cheating and other discrepancies in public examinations of the state.**

About

- The law is known as the **Odisha Public Examination (Prevention of Unfair Means) Bill, 2024**.

- The law would be aimed at effectively and **legally deterring persons, organised groups, or institutions** that indulge in various unfair means and adversely impact the public examination systems for monetary or wrongful gains.

- Currently, there is **no specific law in Odisha** to prevent cheating in examinations.

Recent Cases of Discrepancies in Public Exams in India

- The National Crime Records Bureau (NCRB) revealed that there are about 2,000 cases of examination malpractices recorded in the year 2018 only.

- Four people were arrested in Bihar state for leaking the **question papers of the National Eligibility Cum Entrance Test (Undergraduate).**

- The **qualifying exams for the post of Review Officer/Assistant Review Officer in Uttar Pradesh**, was cancelled amid allegations of paper leak.

- These malpractices have severe financial and psychological tolls on the students, and the whole of the education system requires stronger measures to deal with them.

Impact of Examination Malpractices:

- **Undermines Educational Integrity:** When cheating and malpractices become widespread, it erodes the credibility of the examination system.

- **Devaluation of Qualifications:** When malpractices affect the credibility of exams, the value of the qualifications awarded by educational institutions diminishes, affecting the employability and future prospects of all students.

- **Loss of Trust in the System:** Parents and the public lose trust in the education system.

- **Psychological Impact on Students:** Students feel demotivated and discouraged by the prevalence of malpractices.

- **Delay in Exams:** Malpractices in public examinations lead to delays and cancellation of examinations, adversely impacting the prospects of millions of youth.

- **Additional Cost:** The government has to bear additional financial burden to reconduct the examination.

Public Examination (Prevention of Unfair Means) Act, 2024

– The Act broadly defines **"unfair means"** to include various malpractices, such as:

1. Leaking question papers or answer keys,

2. Assisting candidates during exams (unauthorized communication, providing solutions),

3. Tampering with computer networks or resources,

4. Impersonating candidates,Conducting fake examinations or issuing fake documents,Tampering with documents for merit lists or ranks.

– **Penalties and Punishments:**

1. Individuals:

1.1 Imprisonment ranges from 3 to 10 years depending on the offense's severity.

1.2 Fines up to Rs. 1 crore for organized crimes.

2. Service providers:

1.1 Fines up to Rs. 1 crore for involvement in malpractices.

1.2 Barring from conducting public examinations for 4 years.

1.3 Personal liability for directors/management involved.

3. Organized crimes:

1.1 Harsher penalties, with imprisonment between 5 and 10 years and a minimum fine of Rs. 1 crore

1.2 The institution involved can face property attachment and forfeiture

– **Investigation:**

1. All offences under the Act are cognisable, non-bailable, and non-compoundable.

2. An officer not below the rank Deputy Superintendent or Assistant Commissioner of Police will investigate the offences under the Act.

3. The Central Government may transfer the investigation to any Central Investigating Agency.

Accelerated Degree Programme (ADP) and Extended Degree Programme (EDP)

Context

- The University Grants Commission (UGC) has recently approved a Standard Operating Protocol (SOP) for Higher education institutions (HEIs) to offer the **Accelerated Degree Programme (ADP) and Extended Degree Programme (EDP).**

What are ADPs and EDPs?

- At the end of the **first or second semester**, but not beyond, undergraduate students will be allowed to opt for an **ADP or an EDP**.

- Students enrolled under an ADP will follow the same curriculum and must earn the same **number of credits** as required for a **three- or four-year undergraduate (UG) programme**. However, they can **complete their programme sooner** by earning additional credits starting from the semester they choose the ADP.

- **Under ADP**, a three-year UG programme can be completed in **five semesters** instead of the standard six (shortened by a maximum of one semester), while a four-year UG programme can be completed in **six or seven semesters** (shortened by a maximum of two semesters) rather than eight.

- On the other hand, **students who choose the EDP** will be allowed to earn **fewer credits per semester** compared to the standard programme, allowing them to take longer to complete their course.

- The government departments, private organisations, and recruiting agencies like **UPSC/State Service Commissions** and so on, will treat the ADPs and EDPs on a par with those of standard duration.

How will they be implemented?

- HEIs will set up the **committee** to scrutinise the applications they receive for ADP and EDP at the end of the first or second semester and select students accordingly.

- An institution can earmark **up to 10%** of the sanctioned intake for ADP students, while there will be **no cap** on the number of EDP students.

- HEIs can begin offering ADP or EDP from the **2025-26 academic year**, with the choice to implement these programs left to the institutions.

Significance

- ADP allows high-performing students to complete their degrees faster and allows them to enter the **workforce or pursue higher studies** sooner.

- The move was in line with the **National Credit Framework (NCrF)** released last year in accordance with the **National Education Policy (NEP) 2020.**

University Grants Commission (UGC)

– It came into existence on 28th December, 1953 and became a **statutory Organization** of the Government of India by an **Act of Parliament in 1956.**

– The UGC's **mandate** includes:

1. Promoting and coordinating university education.

2. Determining and maintaining standards of teaching, examination, and research in universities.

3. Disbursing grants to the Universities and Colleges.

4. Serving as a vital link between the Union and State Governments and institutions of higher learning.

5. Advising the Central and State Governments on the measures necessary to improve university education.

Government Proposed 100% FDI in Insurance Sector

Context

- The Union Finance Ministry released a consultation paper proposing to raise the Foreign Direct Investment (FDI) limit in the insurance sector from **74% to 100%.**

About

- The FDI limit in the insurance sector was previously increased from **49% to 74% in February 2021.**
- A comprehensive review of the legislative framework of the sector has been conducted in consultation with the Insurance Regulatory and Development Authority (IRDAI) and the industry.

Foreign Direct Investment (FDI)

– It refers to investments made by a company or individual from one country in assets, businesses, or production activities in another country.

Significance

– It boosts the economy by bringing in capital, technology, and management expertise, which enhances productivity and innovation in the host country.

– It generates employment opportunities, especially in sectors like manufacturing, services, and infrastructure.

– It facilitates the exchange of skills and technology, enhancing the competitiveness of domestic firms.

Proposed Amendment to Insurance Laws:

- It aims to **ensure accessibility and affordability** of insurance for citizens, foster the expansion and development of the insurance industry, and streamline business processes.
- Net Owned Funds for foreign reinsurers is also proposed to be reduced from Rs 5,000 crore to Rs 1,000 crore.
- IRDAI is being empowered to specify lower entry capital (not less than Rs 50 crore) for underserved or unserved segments on a special-case basis.
- Open architecture for insurance agents that will allow them to tie up with more than one life, general and health insurance player.
  - o Currently, the insurance agents are allowed to tie-up with only one life, general and health insurance company.

Need for the Amendments

- The sector regulator is making efforts **to attract more capital** to the capital-intensive industry.
- The insurance sector needs to infuse **approximately ₹50,000 crore** annually to **double insurance penetration in the country.**

- o Insurance penetration refers to the ratio of insurance premiums written in a particular year to the gross domestic product (GDP).

- India could save up to **USD 10 billion annually** by expanding insurance coverage to currently uninsured individuals and assets.

  - o With a large portion of India's population still without insurance, the country faces significant risks, including high out-of-pocket expenses.

- IRDA is determined to achieve its mission of **'Insurance for all by 2047'**, with aggressive plans to address the industry's challenges.

Insurance Sector in India

- India is the **fifth largest life insurance market** in the world's emerging insurance markets, growing at a rate of 32-34% each year.

- **Insurance Penetration:** As per the Economic Survey 2023-24, overall insurance penetration in the country moderated slightly to 4% in FY23, from 4.2% in FY22.

  - o During the same period, insurance penetration in the life insurance segment declined from 3.2% in FY22 to 3% in FY23, while it remained flat at 1% for the non-life insurance segment.

- **Insurance Companies:** At present, there are **25 life insurance companies, and 34 general insurers in the country.**

  - o Among the life insurers, Life Insurance Corporation (LIC) is the sole public sector company.

  - o In addition to these, there is a sole national re-insurer, namely General Insurance Corporation of India (GIC Re).

Challenges faced by the Sector

- **Low Penetration:** Insurance penetration remains low, with limited awareness among the population about the benefits and types of insurance.

- **Claims Settlement Issues:** Delays, rejections, and lack of transparency in the claims process create customer dissatisfaction.

- **Distribution Limitations:** There is limited reach in rural areas, and insurance distribution remains urban-centric, relying heavily on agents.

- **Affordability:** High premiums and the underpricing of certain products affect accessibility for low-income groups.

- **Fraud and Mis-selling:** Fraudulent claims and mis-selling by agents are common problems, damaging customer trust.

- **Health Insurance Gaps:** Limited coverage and high medical costs make health insurance inadequate.
- **Rising Costs:** Increasing medical and claims costs impact affordability and profitability for insurers.

Way Ahead

- **Increase Financial Literacy:** Conduct educational programs to enhance understanding of insurance products among the population.
- **Simplify Regulations:** Streamline regulatory processes to make product approvals faster and less complex, while ensuring consumer protection.
- **Improve Claims Settlement:** Ensure faster, transparent, and more efficient claims processing to build trust and reduce disputes.
- **Expand Distribution Networks:** Leverage digital platforms and mobile technology to reach underserved rural and semi-urban areas.
- **Enhance Health Coverage:** Expand coverage to include critical illnesses, hospitalization, and post-treatment care.