Securing India's Digital Future

Why in News?

Gujarat Police recently uncovered a large-scale cyber fraud operation, who were running a nationwide “digital arrest” scam.

What is the need for cyber financial security?

- **Digital India** - India is one of the largest global consumer markets, with shoppers going more digital every single day.
- **Expanding FinTech Inclusion** - India is leading in fintech inclusion, with an fintech adoption rate of 87%, significantly higher than the global average of 64%.
- **Growing Digital Lending** - Digital lending market valued at $270 billion in 2022, expected to grow at a CAGR of 22% to reach $1.3 trillion by 2030.
- **Increasing Digital Payments** - India currently leads the world in digital payments with more than 40% of payments made digitally amounting to Rs.10 billion in January 2023.
- **Digital Shift** - The affinity to shop and pay online has created an immense shift in Indian retail, most noticeable with the rise of D2C businesses nationwide.
- **Cyber Fraud** - Digital payment frauds in India saw a more than fivefold jump to Rs 14.57 billion (Rs 1,457 crore) in the year that ended in March 2024.
- **Public Trust** – Increased cyber fraud could lead to an erosion of public trust in digital businesses.

What are the types of cyber financial fraud?

- As the Financial Services sector continues to advance technological innovations, scammers employ various deceptive tactics to obtain sensitive information and money from individuals.
- **KYC Fraud** - Scammers impersonate as Bank officials or government representatives, target customers through deceptive text messages or calls to lure into providing personal / sensitive / financial information.
- **Customer Care Fraud** - Scammers manipulate search engine results to display fake customer care numbers or call as customer care representatives and ask sensitive information.
- **Lottery Fraud** - Victims receive Fake notifications claiming they've won a lottery, but they need to pay fees or provide personal details to claim the prize, resulting in financial loss.
- **Card Fraud** - Fraudster posing as Bank representative, may call & ask for sharing Card Number, Expiry Date, CVV, PIN, OTP etc. under false pretext or fabricated scenarios.
- **UPI Fraud -** Fraudsters persuade users to make fund transfers or payments to

unknown UPI IDs or disclose sensitive UPI credentials such as UPI ID, PIN, OTP, etc., enabling them to carry out fraudulent transactions.

- **Electricity Bill Scam** - Fraudster sends fake message threatening disconnection of services due to unpaid bills.
- **Task Based Job Fraud** - Scammers approach individuals, with lucrative work-from-home opportunities and convince them to invest.
- **Digital Arrest Fraud** - Cybercriminals coerce victims into paying large sums to avoid fake criminal charges investigation for money laundering or drug smuggling.

How fintech can make businesses safer?

Fintech refers to the integration of information communication technology into financial services to improve and automate the delivery and use of financial services.

- **Identity verification -** Fintech is leveraging advancements in biometric security, such as face recognition software, to make the opening of digital accounts safer through accurate identity verification.
- **Risk Management -** By leveraging AI-backed algorithms, fintech products can scan thousands of transactions in real time to identify payments and accounts linked to fraudulent activities.
- **Proactive Risk Profiling -** Fintech products can create risk profiles for accounts with a high chance of fraudulent activity.
- **Data Encryption** - Fintech companies use advanced encryption techniques to protect sensitive financial data, ensuring that information is secure during transmission and storage.
- **Secure Payment Processing** - Fintech companies provide secure and efficient payment processing solutions, reducing the risk of payment fraud and ensuring that transactions are processed safely.
- **Compliance and Regulatory Support** - Fintech firms help businesses stay compliant with regulatory requirements, ensuring that they adhere to industry standards and best practices for security

What are the government initiatives to counter cybersecurity in Indian financial services sector?

- **National Cyber Security Policy -** Established in 2013, this policy provides a framework for protecting critical information infrastructure and enhancing cybersecurity awareness.
- **CERT-Fin (Computer Emergency Response Team for Financial Sector)** - Launched in 2017, this specialized unit works towards strengthening cyber security in the financial sector.
- **RBI Cybersecurity Framework -** The Reserve Bank of India (RBI) issued comprehensive guidelines for financial institutions to enhance their cybersecurity posture.
- **Cyber Swachhta Kendra**: A botnet cleaning and malware analysis centre that

provides free tools to citizens and organizations to secure their systems.

- **National Critical Information Infrastructure Protection Centre (NCIIPC)** - Established to protect critical information infrastructure in various sectors, including banking and finance.
- **Information Technology Act, 2000** - Provides legal framework for addressing cybercrime and electronic commerce.
- **Cyber Surakshit Bharat Initiative** - A programme to educate & enable the Chief Information Security Officers (CISO) & broader IT community to address the challenge of cybersecurity.
- **Indian Computer Emergency Response Team (CERT-In)** -The national agency for responding to computer security incidents.
- **Digital Personal Data Protection (DPDP) Act 2023** - The DPDP Act provides for the processing of digital personal data in a manner that recognizes both the rights of the individuals to protect their personal data.
- **National Cybercrime Reporting Portal (NCRP)** - To facilitate victims/ complainants to report cybercrime complaints online.
- **Chakshu facility on Sanchar Saathi portal** - It facilitates citizens to report the suspected fraud communications with the intention of defrauding telecom service users.

What lies ahead?

- With better security products, fintech can enhance public trust in digital India to catalyse the country's economic growth further.
- By building on this foundation, fintech has the potential to emerge as the anchor of India's digital safety.

References

[Business Today | Securing India's Digital Future]