Gaps in AePS Exploited by Cybercriminals

For Prelims: Aadhaar-enabled Payment System (AePS), Aadhar Lock, Silicone thumbs

For Mains: Vulnerabilities associated with the AePS, Challenges of using biometric authentication in financial transactions, Role of financial literacy and digital skills in preventing AePS frauds

Why in News?

The **Aadhaar-enabled Payment System (AePS)** in India has recently faced exploitation by **cybercriminals**, leading to **unauthorized access to users' bank accounts.**

- Scammers have been **using leaked biometric details to bypass the need for One Time Passwords (OTPs)** and drain funds from unsuspecting victims.
- A series of recent scams have exposed the **vulnerabilities of the AePS** and how cybercriminals are exploiting the loopholes in the system to defraud unsuspecting customers.

What is AePS?

- **About:**
  - Th AePS is a bank-led model that allows **online interoperable financial transactions at Point of Sale (PoS) or micro-ATMs** through the **Business Correspondent (BC)** of any bank using the **Aadhaar authentication.**
  - It was taken up by the **National Payments Corporation of India (NPCI)** - a joint initiative of Reserve Bank of India (RBI) **and Indian Banks' Association (IBA).**
  - The AePS is meant to provide **easy and secure access to banking services** for the poor and marginalized sections of society, especially in rural and remote areas.
  - It **eliminates the need for OTPs, bank account details,** and other financial information.
  - Transactions can be carried out with only the **bank name, Aadhaar number, and captured fingerprint during Aadhaar enrollment.**
- **Benefits:**
  - **Deepening Social Security:**
    - The AePS helps in deepening social security by facilitating cash **transfers from various government schemes such as** PM-KISAN**,** MGNREGA, etc., directly into the beneficiaries' bank accounts.
  - **Enabling Interoperability:**
    - The AePS enables interoperability among different banks and financial institutions, **allowing customers to access their bank accounts through any BC or micro-ATM** of any bank.
- **Drawbacks:**
  - Neither Unique Identification Authority of India (UIDAI) **nor NPCI mentions clearly whether AePS is enabled by default.**

How is AePS Exploited?

- **Leaked Biometric Details:**
  - **Cybercriminals obtain leaked biometric information,** which includes fingerprints captured during Aadhaar enrollment.
    - They use this stolen data to **operate biometric POS devices and ATMs** without the need for **two-factor authentication or OTPs.** By bypassing these security measures, they can transfer money from users' bank accounts.
- **Silicone Thumbs:**
  - Scammers have been known to use silicone thumbs to deceive biometric devices.
    - They **place the artificial thumb on the fingerprint sensor,** tricking the system into authenticating their fraudulent transactions.
    - This method allows them to perform unauthorized financial activities on behalf of the account holder.
- **Lack of Transaction Notifications:**
  - In some cases, victims of AePS scams **do not receive any notification** from their banks **regarding unauthorized transactions.**
  - They remain **unaware of the fraudulent activity until they notice discrepancies** in their bank account balance.
    - This lack of immediate alerts enables scammers to continue draining funds undetected.
- **Exploiting Weak Security Measures:**
  - Gaps in the AePS system's security protocols, such as **inadequate identity verification or authentication processes,** provide opportunities for cybercriminals to carry out their fraudulent activities. They take advantage of these weaknesses to exploit the system and access users' bank accounts.
- **Systemic Issues:**
  - The AePS also faces issues such as **biometric mismatches,** poor connectivity, weaker systems of certain banking partners, etc., that affect its performance and reliability.
    - Sometimes, the **transactions fail** due to these reasons but the money gets debited from the customers’ accounts without their knowledge.

How to Prevent AePS Frauds?

- **Amendments to Aadhar Regulations 2016:**
  - UIDAI proposes an amendment to the **Aadhaar (Sharing of Information) Regulations, 2016.**
    - The amendment requires entities in possession of an Aadhaar number to not share details unless Aadhaar numbers have been redacted or blacked out.
- **Aadhaar Lock:**
  - Users are advised to **lock their Aadhaar information** using the **UIDAI website or mobile app.**
  - Locking Aadhaar prevents the **unauthorized use of biometric information** for financial transactions.
  - Aadhaar can be unlocked when **biometric authentication is required,** such as for property registration or passport renewals.
    - After the necessary authentication, Aadhaar can be locked again for security purposes.
- **Other Preventive Measures:**
  - It is advisable **to avoid scanning QR codes or clicking on links** sent by unknown or suspicious sources.
  - Exercise caution and **refrain from trusting individuals who offer assistance in withdrawing money** from locations other than authorized bank branches or ATMs.
  - Prior to providing a fingerprint on a PoS machine, it is recommended **to verify the displayed amount and request a receipt for every transaction.**
  - Regularly **check the balance and transaction alerts of the bank account** linked to the mobile number.
  - In the event of any suspicious or fraudulent activity, promptly report it to both the bank and the police.
    - According to the **RBI**, customers are entitled to **zero liability for unauthorized**

transactions if promptly reported within three working days.

What are the Challenges of AePS?

- **Lack of Awareness and Literacy:**
  - Many customers are not aware of the benefits and features of the AePS or how to use it safely and securely. They also lack financial literacy and digital skills, which makes them vulnerable to fraud and errors.
- **Inadequate Infrastructure and Connectivity:**
  - The AePS depends on the availability and quality of infrastructure and connectivity, such as biometric devices, PoS machines, internet, power supply, etc. However, these are often lacking or unreliable in rural and remote areas, where the AePS is most needed.
- **Regulatory and Policy Issues:**
  - The AePS also faces some regulatory and policy issues, such as **the legal validity of Aadhaar authentication, the privacy and security of biometric data,** the MDR charges for transactions, the grievance redressal mechanism for customers, etc.

Way forward

- **Strengthening the Security and Authentication of AePS Transactions:**
  - **Implement encryption** and digital signatures to protect transaction data.
  - Incorporate **biometric liveness detection to prevent cloning or spoofing** of biometric data.
  - **Certify devices used for AePS transactions** and monitor transactions for suspicious activity.
- **Raising Awareness:**
  - **Educate users about the risks associated** with sharing Aadhaar number and biometrics.
  - Utilize the **Aadhaar lock/unlock feature to control access to biometrics.**
  - **Ensure service providers follow guidelines** and standards issued by authorities and comply with data protection laws.
- **Enhancing Coordination and Cooperation among Stakeholders:**
  - Facilitate information sharing among UIDAI, **NPCI**, RBI, banks, **fintech companies**, law enforcement agencies, and civil society organizations.
  - Develop joint strategies and action plans to address cybercrime challenges.
  - Provide technical assistance and capacity building to stakeholders.
  - Establish a platform for reporting and resolving grievances related to AePS.

UPSC Civil Services Examination, Previous Year Questions (PYQs)

Prelims

Q1. In India, under cyber insurance for individuals, which of the following benefits are generally covered, in addition to payment for the loss of funds and other benefits? (2020)

1. Cost of restoration of the computer system in case of malware disrupting access to one’s computer
2. Cost of a new computer if some miscreant wilfully damages it, if proved so
3. Cost of hiring a specialised consultant to minimise the loss in case of cyber extortion
4. Cost of defence in the Court of Law if any third party files a suit

Select the correct answer using the code given below:

(a) 1, 2 and 4 only
(b) 1, 3 and 4 only
(c) 2 and 3 only
(d) 1, 2, 3 and 4

Ans: (b)

Q2. In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centres
3. Body corporate

Select the correct answer using the code given below:

(a) 1 only
(b) 1 and 2 only
(c) 3 only
(d) 1, 2 and 3

Ans: (d)

Q3. Consider the following statements: (2018)

1. Aadhaar card can be used as a proof of citizenship or domicile.
2. Once issued, Aadhaar number cannot be deactivated or omitted by the Issuing Authority.

Which of the statements given above is/are correct?

(a) 1 only
(b) 2 only
(c) Both 1 and 2
(d) Neither 1 nor 2

Ans: (d)

Mains

Q. What are the different elements of cyber security ? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. **(2022)**

Source: TH