drishti

Multi-State Phishing Scam

drishtiias.com/printpdf/multi-state-phishing-scam

Why in News

Recently, Haryana Police has **identified** a phishing racket which accessed over 300 nationalized and private bank accounts across many states.

Key Points

- Frauds were done with **Phishing** and use of **e-SIMs** as the **main conduit.**
  - **Phishing:** It is a cybercrime in which a target or targets are **contacted by email, telephone, or text message.**

    This is done by someone **posing as a legitimate institution** to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.
  - **e-SIM:** It is the **Subscriber Identification Module (SIM)** embedded in the phone.
    - It **can not be removed** as opposed to physical SIM cards, which can be removed.
    - The e-SIMs enable users to change service providers through a **simple process.**
    - **Multiple networks and numbers** can be stored on a single e-SIM too, so one can have more than one number.
- **Online Monetary Frauds in India:**
  - According to the **Reserve Bank of India (RBI)**, in 2019-20, banks reported 2,678 card and internet-related fraud, totalling Rs. 195 crore in value, which was more than double the value of such frauds reported by banks in 2018-19.
  - In the current fiscal (2020-21), between April and June, banks reported 530 fraudulent transactions involving debit and credit cards, or techniques such as phishing done over the internet.

- **Steps taken:**
    - **RBI** is taking measures to improve awareness related to **cybersafety** among people through:
        - **e-BAAT** (Electronic Banking Awareness And Training) programmes.
        - **Organising campaigns** on safe use of digital payment modes, to avoid sharing critical personal information like PIN, OTP, passwords, etc.
    - RBI has also directed all **banks and authorised payment system operators** to undertake **targeted multi-lingual campaigns** by way of SMS, advertisements in print and visual media to **educate their users** on safe and secure use of digital payments.
    - The **Computer Emergency Response Team (CERT-in)** functions as the **nodal agency** for **coordination** of all cyber security efforts, **emergency responses, and crisis management.**

Source IE