बैंक धोखाधड़ी में ई-सिम का दुरुपयोग

प्रिलिम्स के लिये:

ई-सिम, 'ई-बात कार्यक्रम'

मेन्स के लिये:

सूचना प्रौद्योगिकी का विकास और साइबर सुरक्षा से जुड़ी चुनौतियाँ

चर्चा में क्यों?

हाल ही में हरियाणा पुलिस द्वारा 300 से अधिक बैंक खातों से जुड़े एक बहुराज्यीय बैंक धोखाधड़ी के मामले में 'ई-सिम' (e-SIM) के प्रयोग की बात कही गई है। इस मामले के सामने आने के बाद एक बार फिर इंटरनेट और साइबर सुरक्षा तंत्र पर प्रश्न उठने लगे हैं।

प्रमुख बिंदु:

- 300 से अधिक राष्ट्रीयकृत और निजी बैंक खातों में धोखाधड़ी के ये मामले देश के पाँच राज्यों (पंजाब, हरियाणा, बिहार, पश्चिम बंगाल और झारखंड) से संबंधित हैं।
- इन मामलों में पुलिस द्वारा गिरफ्तार किये गए पाँच आरोपियों में से 4 झारखंड के 'जमतारा' (Jamtara) ज़िले से हैं।
- बैंक धोखाधड़ी से जुड़े इन मामलों में आरोपियों द्वारा पीड़ितों के बैंक खातों से पैसे निकालने के लिये 'ई-सिम' का प्रयोग किया गया था।

बैंक धोखाधड़ी में ई-सिम का प्रयोग:

धोखाधड़ी के इन मामलों में अपराधी बड़ी संख्या में मोबाइल नंबरों को प्राप्त कर उनके माध्यम से बैंक खातों में लॉग-इन (Log-in) का प्रयास करते हैं।

- यदि किसी नंबर पर बैंक द्वारा ओटीपी (OTP) भेजने का संकेत प्राप्त होता है, तो वे उस नंबर पर ग्राहक सेवा अधिकारी होने का दिखावा करते हुए फोन करते हैं और संबंधित व्यक्ति से सिमकार्ड अपग्रेड करने या उसकी पहचान से जुड़ी जानकारी जानने का प्रयास करते हैं।

- इसके बाद अपराधी पीड़ित को एक इ-मेल भेजते हैं, जिसे आधिकारिक ग्राहक सेवा नंबर पर भेजना होता है।
- वास्तविकता में यह पीड़ित व्यक्ति के फोन नंबर से अपनी ईमेल आईडी (Email-id) जोड़ने का एक तरीका होता है, जिसके माध्यम से अपराधी पीड़ित के सिम को 'ई-सिम' में बदलने के लिये आधिकारिक आवेदन कर सकते हैं।
- यह प्रक्रिया पूरी होने के बाद पीड़ित के नंबर से जुड़ी सभी सेवाओं (बैंक खाते सहित) तक अपराधियों की पहुँच हो जाती है।

'ई-सिम' (e-SIM):

- 'ई-सिम' का पूरा नाम 'एंबेडेड सब्सक्राइबर आइडेंटिटी मॉड्यूल' (Embedded Subscriber Identity Module) है, इसे एंबेडेड सिम (Embedded SIM) के नाम से भी जाना जाता है।
- पारंपरिक सिम कार्ड की तरह मोबाइल फोन से अलग होने की बजाय, इसे निर्माता द्वारा फोन में ही स्थापित कर दिया जाता है।
- ई-सिम, पारंपरिक सिम के विपरीत फोन में अनावश्यक स्थान नहीं घेरता है, साथ ही इसका प्रयोग स्मार्टवाच (Smartwatch) जैसे छोटे उपकरणों में भी किया जा सकता है।

भारत में इंटरनेट से जुड़े बैंक धोखाधड़ी के मामले:

- भारतीय रिज़र्व बैंक (Reserve Bank of India-RBI) द्वारा जारी आँकड़ों के अनुसार, वित्तीय वर्ष 2019-20 में भारतीय बैंकों द्वारा कुल 195 करोड़ रुपए से संबंधित इंटरनेट और क्रेडिट अथवा डेबिट कार्ड धोखाधड़ी से जुड़े 2,678 मामले दर्ज किये गए थे।
- वित्तीय वर्ष 2019-20 में इंटरनेट से जुड़े बैंक धोखाधड़ी के मामलों में पिछले वर्ष की तुलना में दोगुने से अधिक वृद्धि (मूल्य के आधार पर) देखी गई है।
- वर्तमान वित्तीय वर्ष में अप्रैल से जून के बीच इंटरनेट और क्रेडिट या डेबिट कार्ड धोखाधड़ी से संबंधित 530 मामले दर्ज किये गए, इन मामलों में कुल 27 करोड़ रुपए की धोखाधड़ी देखी गई है।

बैंक धोखाधड़ी को रोकने के प्रयास:

- बैंक धोखाधड़ी की निगरानी और पहचान में सुधार हेतु RBI द्वारा विभिन्न डेटाबेस और सूचना प्रणालियों को जोड़ने का प्रयास किया जा रहा है।
- RBI द्वारा 'इलेक्ट्रॉनिक बैंकिंग जागरूकता और प्रशिक्षण' या 'ई-बात' (Electronic Banking Awareness And Training or e-BAAT) कार्यक्रम के माध्यम से जागरूकता बढ़ाने का प्रयास किया जा रहा है।
- साथ ही RBI के द्वारा डिजिटल भुगतान प्रणाली के सुरक्षित उपयोग, महत्त्वपूर्ण व्यक्तिगत जानकारी जैसे- पिन, ओटीपी, पासवर्ड, आदि को साझा करने से बचने हेतु जागरुकता अभियानों का आयोजन किया जाता है।

- RBI द्वारा सभी बैंकों और प्राधिकृत भुगतान प्रणाली ऑपरेटरों को डिजिटल भुगतान के सुरक्षित उपयोग के बारे में अपने उपयोगकर्ताओं को शिक्षित करने हेतु एसएमएस, प्रिंट और विज़ुअल मीडिया आदि के माध्यम से लक्षित बहुभाषी अभियान शुरू करने का निर्देश दिया गया है।
- हाल ही में महाराष्ट्र पुलिस द्वारा इस प्रकार की बैंक धोखाधड़ी से बचने के लिये कुछ आवश्यक दिशा निर्देश जारी किये गए थे।

आगे की राह:

- पुलिस के अनुसार, बैंकों और टेलीकॉम कंपनियों की ओर से प्रक्रियात्मक कमी और तत्परता का अभाव ऐसे मामलों में वृद्धि का एक बड़ा कारण है।
- ऐसे मामलों से बचने का सबसे प्रभावी ग्राहक जागरूकता को ही माना जाता है, अत: लोगों को किसी संदेहप्रद लिंक पर क्लिक करने तथा किसी के साथ अपनी निजी जानकारी साझा करने से बचना चाहिये।
- बैंकिंग क्षेत्र में तकनीकी के प्रयोग को बढ़ावा देने के साथ इससे जुड़ी सुरक्षा को मज़बूत बनाने पर विशेष ध्यान दिया जाना चाहिये।
- बैंकों द्वारा स्थानीय प्रशासन के सहयोग से नवीन तकनीकों और उससे जुड़ी सुरक्षा चुनौतियों के संदर्भ में जन-जागरूकता को बढ़ाने हेतु आवश्यक प्रयास जाना चाहिये।

स्रोत: इंडियन एक्सप्रेस