AePS की खामियों का साइबर अपराधियों द्वारा दुरुपयोग

प्रिलिम्स के लिये:

आधार-सक्षम भुगतान प्रणाली (AePS), आधार लॉक, सिलिकॉन थम्ब्स

मेन्स के लिये:

AePS से संबंधित खामियाँ, वित्तीय लेन-देन में बायोमेट्रिक प्रमाणीकरण का उपयोग करने की चुनौतियाँ, AePS धोखाधड़ी को रोकने में वित्तीय साक्षरता और डिजिटल कौशल की भूमिका

चर्चा में क्यों?

हाल ही में भारत में साइबर अपराधियों द्वारा आधार-सक्षम भुगतान प्रणाली (AePS) की खामियों के दुरुपयोग का मामला देखा गया और उन्होंने **उपयोगकर्त्ताओं के बैंक खातों तक अनधिकृत पहुँच** प्राप्त कर ली।

- स्कैमर्स द्वारा लीक हुए बायोमेट्रिक विवरणों का उपयोग पीड़ितों के खातों से धन निकालने के लिये किया गया जिसमें वन टाइम पासवर्ड (OTP) की आवश्यकता नहीं पड़ती है।
- हाल ही में **AePS में कई खामियाँ** देखने को मिली हैं जिस कारण साइबर अपराधी ग्राहकों को धोखा देने के लिये सिस्टम की खामियों का फायदा उठा रहे हैं।

AePS:

- **परिचय:**
  - AePS एक बैंक-आधारित मॉडल है जो **आधार प्रमाणीकरण** का उपयोग करके किसी भी बैंक के **बिज़नेस कॉरेस्पोंडेंट (BC)** के माध्यम से **पॉइंट ऑफ सेल (PoS) या माइक्रो-एटीएम पर ऑनलाइन इंटरऑपरेबल** वित्तीय लेन-देन की अनुमति देता है।
  - इसे भारतीय राष्ट्रीय भुगतान निगम (NPCI), **भारतीय बैंक संघ (IBA) और** भारतीय रिज़र्व बैंक **(RBI)** की एक संयुक्त परियोजना द्वारा अपनाया गया था।
  - AePS का उद्देश्य समाज के गरीब और सीमांत वर्गों, विशेषकर ग्रामीण व दूरवर्ती क्षेत्रों में **बैंकिंग सेवाओं तक आसान और सुरक्षित पहुँच** प्रदान करना है।
  - यह **OTP, बैंक खाता विवरण** और अन्य वित्तीय जानकारी की आवश्यकता को **समाप्त करता है।**
  - **आधार नामांकन के दौरान केवल बैंक का नाम, आधार संख्या और कैप्चर किये गए फिंगरप्रिंट** के साथ लेन-देन किया जा सकता है।
- **लाभ:**
  - **मज़बूत सामाजिक सुरक्षा:**
    - AePS **विभिन्न सरकारी योजनाओं जैसे** PM-KISAN, MGNREGA**,** आदि से सीधे लाभार्थियों के बैंक खातों में नकद हस्तांतरण की सुविधा प्रदान कर सामाजिक सुरक्षा को मज़बूत करने में मदद करता है।
  - **इंटरऑपरेबिलिटी को सक्षम करना:**
    - AePS विभिन्न बैंकों और वित्तीय संस्थानों के बीच इंटरऑपरेबिलिटी को सक्षम बनाता है,**जिससे ग्राहक** किसी भी बैंक **के बिज़नेस कॉरेस्पोंडेंट (BC) या माइक्रो-एटीएम के माध्यम से अपने बैंक खातों तक पहुँच प्राप्त कर सकते हैं।**
- **कमियाँ:**
  - न तो भारतीय विशिष्ट पहचान प्राधिकरण (UIDAI) और **न ही NPCI स्पष्ट रूप से उल्लेख करते हैं कि AePS डिफॉल्ट रूप से सक्षम है या नहीं।**

AePS की खामियाँ:

- **लीक बायोमेट्रिक विवरण:**

        - **साइबर अपराधी लीक बायोमेट्रिक जानकारी प्राप्त करते हैं**, जिसमें आधार नामांकन के दौरान कैप्चर किये गए फिंगरप्रिंट शामिल हैं।
            - वे **द्वि-कारक प्रमाणीकरण या OTP** की आवश्यकता के बिना **बायोमेट्रिक POS डिवाइस और एटीएम संचालित** करने के लिये इस चोरी किये गए डेटा का उपयोग करते हैं। इन सुरक्षा उपायों की उपेक्षा कर वे यूज़र्स के बैंक खातों से धनराशि ट्रांसफर कर सकते हैं।
- **सिलिकॉन थम्ब्स:**
    - स्कैमर्स बायोमेट्रिक उपकरणों को धोखा देने हेतु सिलिकॉन थम्ब्स का उपयोग करने के लिये जाने जाते हैं।
        - वे **फिंगरप्रिंट सेंसर पर कृत्रिम थम्स लगाते हैं,** जिससे सिस्टम को उनके धोखाधड़ी वाले लेन-देन को प्रमाणित करने में मदद मिलती है।
        - यह तरीका उन्हें खाताधारक की ओर से अनधिकृत वित्तीय गतिविधियों को करने की अनुमति देता है।
- **लेन-देन संबंधी सूचना का अभाव:**
    - कुछ मामलों में **AePS घोटालों के पीड़ितों को अनधिकृत लेन-देन** के संबंध में उनके **बैंकों से कोई सूचना प्राप्त नहीं** होती है।
    - जब तक वे अपने **बैंक खाते की शेष राशि में विसंगतियों को नोटिस नहीं करते तब तक वे धोखाधड़ी की गतिविधि से अनजान** रहते हैं।
        - तत्काल अलर्ट करने की यह कमी स्कैमर को धन की निकासी जारी रखने में सक्षम बनाती है।
- **कमज़ोर सुरक्षा उपायों का फायदा उठाना:**
    - AePS सिस्टम के सुरक्षा प्रोटोकॉल में खामियाँ जैसे- **अपर्याप्त पहचान सत्यापन या प्रमाणीकरण प्रक्रिया**, साइबर अपराधियों को अपनी धोखाधड़ी गतिविधियों को अंजाम देने के अवसर प्रदान करते हैं। वे इन कमज़ोरियों का फायदा उठाकर सिस्टम का दुरुपयोग करते हैं और यूज़र्स के बैंक खातों तक पहुँच बनाते हैं।
- **प्रणालीगत मुद्दे:**
    - AePS को **बायोमेट्रिक बेमेल**, खराब कनेक्टिविटी कुछ बैंकिंग भागीदारों की कमज़ोर प्रणाली आदि जैसे मुद्दों का भी सामना करना पड़ता है, जो इसके प्रदर्शन और विश्वसनीयता को प्रभावित करते हैं।
        - कभी-कभी इन कारणों से **लेन-देन विफल** हो जाता है, लेकिन धनराशि ग्राहकों के खातों से बिना उनकी जानकारी के डेबिट हो जाती है।

AePS धोखाधड़ी को कैसे रोकें?

- **आधार विनियम 2016 में संशोधन:**
    - UIDAI ने [आधार (सूचना साझा करना) विनियम, 2016]() में संशोधन का प्रस्ताव दिया है।
        - संशोधन में आधार संख्या रखने वाली संस्थाओं को विवरण साझा नहीं करने की आवश्यकता है जब तक कि आधार संख्या को संपादित या ब्लैक आउट नहीं किया गया हो।
- **आधार लॉक:**
    - **उपयोगकर्त्ताओं को सलाह दी जाती है कि वे UIDAI की वेबसाइट या मोबाइल एप** का उपयोग करके अपनी आधार जानकारी को लॉक करें।
    - आधार को लॉक करने से वित्तीय लेन-देन के लिये **बायोमेट्रिक** जानकारी के अनधिकृत उपयोग को रोका जा सकता है।
    - **बायोमेट्रिक प्रमाणीकरण की आवश्यकता** होने पर आधार को अनलॉक किया जा सकता है, जैसे कि संपत्ति पंजीकरण या पासपोर्ट नवीनीकरण के लिये।
        - आवश्यक प्रमाणीकरण के बाद सुरक्षा उद्देश्यों के लिये आधार को फिर से लॉक किया जा सकता है।
- **अन्य निवारक उपाय:**
    - **QR कोड को स्कैन करने या अज्ञात या संदिग्ध स्रोतों द्वारा भेजे गए लिंक** पर क्लिक करने से बचने की सलाह दी जाती है।
    - **अधिकृत बैंक शाखाओं या ATM के अलावा अन्य** स्थानों से पैसे निकालने में **सहायता करने वाले व्यक्तियों पर भरोसा करने से सावधान** रहें और उन पर भरोसा करने से बचें।
    - PoS मशीन पर फिंगरप्रिंट प्रदान करने से पहले, प्रदर्शित राशि को सत्यापित करने और **प्रत्येक लेन-देन के लिये रसीद का अनुरोध करने की सिफारिश की** जाती है।
    - मोबाइल नंबर से जुड़े बैंक खाते के बैलेंस और ट्रांजेक्शन अलर्ट की नियमित जाँच करना।
    - संदेह अथवा धोखाधड़ी की स्थिति में तुरंत ही बैंक और पुलिस दोनों को सूचना देनी चाहिये।
        - **भारतीय रिज़र्व बैंक** के अनुसार, किसी भी धोखाधड़ी और अनधिकृत लेन-देन के विषय में तीन कार्यदिवसों के भीतर सूचित करना उपभोक्ता के लिये अनिवार्य है।

AePS से संबंधित चुनौतियाँ:

- **जागरूकता और साक्षरता का अभाव:**
    - बहुत से ग्राहकों को AePS के लाभों और विशेषताओं अथवा इसे सुरक्षित रूप से उपयोग करने के तरीके के बारे में जानकारी नहीं है। उनके पास वित्तीय साक्षरता और डिजिटल कौशल की भी कमी है जिस कारण वे धोखाधड़ी और लेन-देन संबंधी त्रुटियों के प्रति संवेदनशील होते हैं।
- **अपर्याप्त बुनियादी ढाँचा और कनेक्टिविटी:**
    - AePS बायोमेट्रिक डिवाइस, PoS मशीन, इंटरनेट, विद्युत आपूर्ति जैसे बुनियादी ढाँचे और कनेक्टिविटी की उपलब्धता तथा गुणवत्ता पर निर्भर करता है। हालाँकि ग्रामीण और दूरदराज़ के क्षेत्रों में जहाँ AePS की सबसे अधिक आवश्यकता होती है, अक्सर इनकी कमी अथवा इन प्रणालियों के प्रति अविश्वसनीयता देखी गई है।
- **विनियामक और नीतिगत मुद्दे:**

- AePS को आधार प्रमाणीकरण की कानूनी वैधता, बायोमेट्रिक डेटा की गोपनीयता और सुरक्षा, लेन-देन के लिये MDR शुल्क, ग्राहकों के लिये शिकायत निवारण तंत्र जैसे विनियामक एवं नीतिगत मुद्दों का भी सामना करना पड़ता है।

आगे की राह

- **AePS लेन-देन की सुरक्षा और प्रमाणीकरण को मज़बूत बनाना:**
  - लेन-देन डेटा की सुरक्षा के लिये एन्क्रिप्शन और डिजिटल हस्ताक्षर लागू किया जाना।
  - बायोमेट्रिक डेटा की क्लोनिंग अथवा स्पूफिंग को रोकने के लिये बायोमेट्रिक लाइवनेस डिटेक्शन को शामिल करना चाहिये।
  - AePS लेन-देन के लिये उपयोग किये जाने वाले उपकरणों का प्रमाणीकरण और संदिग्ध गतिविधियों के लेन-देन की निगरानी करना।
- **जागरूकता का प्रसार करना:**
  - उपयोगकर्त्ताओं को आधार संख्या और बायोमेट्रिक्स साझा करने से जुड़े जोखिमों के बारे में शिक्षित करना।
  - बायोमेट्रिक्स तक पहुँच को नियंत्रित करने के लिये आधार लॉक/अनलॉक सुविधा का उपयोग करना।
  - सेवा प्रदाता अधिकारियों द्वारा जारी दिशा-निर्देशों और मानकों का पालन तथा डेटा सुरक्षा कानूनों का अनुपालन सुनिश्चित करना।
- **हितधारकों के बीच समन्वय और सहयोग को बढ़ावा देना:**
  - UIDAI, NPCI, RBI, बैंकों, फिनटेक कंपनियों, कानून प्रवर्तन एजेंसियों और नागरिक समाज संगठनों के बीच सूचना साझा करने की सुविधा प्रदान करना।
  - साइबर अपराध की चुनौतियों से निपटने के लिये संयुक्त रणनीति और कार्ययोजना विकसित करना।
  - हितधारकों को तकनीकी सहायता प्रदान करना और उनकी क्षमता बढ़ाना।
  - AePSसे संबंधित शिकायतों की रिपोर्टिंग और समाधान के लिये तंत्र स्थापित करना।

UPSC सिविल सेवा परीक्षा, विगत वर्ष के प्रश्न

प्रश्न. भारत में किसी व्यक्ति को साइबर बीमा कराने पर निधि की हानि की भरपाई एवं अन्य लाभों के अतिरिक्त सामान्यतः निम्नलिखित में से कौन-कौन से लाभ दिये जाते हैं? (वर्ष 2020)

1. यदि कोई मैलवेयर कंप्यूटर तक उसकी पहुँच बाधित कर देता है तो कंप्यूटर प्रणाली को पुनः प्रचलित करने में लगने वाली लागत।
2. यदि यह प्रमाणित हो जाता है कि शिरारती तत्त्व द्वारा जान-बूझकर कंप्यूटर को नुकसान पहुँचाया गया है तो नए कंप्यूटर की लागत।
3. यदि साइबर बलात ग्रहण होता है तो इस हानि को न्यूनतम करने के लिये विशेषज्ञ परामर्शदाता की सेवाएँ लेने पर लगने वाली लागत।
4. यदि कोई तीसरा पक्ष मुकदमा दायर करता है तो न्यायालय में बचाव करने में लगने वाली लागत

नीचे दिये गए कूट का प्रयोग कर सही उत्तर चुनिये:

(a) केवल 1, 2 और 4
(b) केवल 1, 3 और 4
(c) केवल 2 और 3
(d) 1, 2, 3 और 4

उत्तर: (b)

प्रश्न. भारत में निम्नलिखित में से किसके लिये साइबर सुरक्षा घटनाओं पर रिपोर्ट करना कानूनी रूप से अनिवार्य है? (2017)

1. सेवा प्रदाताओं
2. डेटा केंद्र
3. कॉर्पोरेट निकाय

नीचे दिये गए कूट का प्रयोग कर सही उत्तर चुनिये:

(a) केवल 1
(b) केवल 1 और 2
(c) केवल 3
(d) 1, 2 और 3

उत्तर: (d)

प्रश्न: निम्नलिखित कथनों पर विचार कीजिये: (2018)

1. आधार कार्ड का उपयोग नागरिकता या अधिवास के प्रमाण के रूप में किया जा सकता है।
2. एक बार जारी होने के बाद आधार संख्या को जारीकर्त्ता प्राधिकारी द्वारा समाप्त या छोड़ा नहीं जा सकता है।

उपर्युक्त कथनों में से कौन-सा/से सही है/हैं?

(a) केवल 1
(b) केवल 2
(c) 1 और 2 दोनों
(d) न तो 1 और न ही 2

उत्तर: (d)

प्रश्न. साइबर सुरक्षा के विभिन्न घटक क्या हैं? साइबर सुरक्षा में चुनौतियों को ध्यान में रखते हुए जाँच कीजिये कि भारत ने व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति को किस हद तक सफलतापूर्वक विकसित किया है? (मुख्य परीक्षा, 2022)

स्रोत: द हिंदू

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/gaps-in-aeps-exploited-by-cybercriminals