मोबाइल बैंकिंग को साइबर खतरा

प्रिलिम्स के लिये:

डिजिटल भुगतान, साइबर सुरक्षा खतरा, कंप्यूटर वायरस, डेटा उल्लंघन, डिनायल ऑफ़ सर्विस (Denial of Service- DoS), ट्रोजन, मैलवेयर।

मेन्स के लिये:

साइबर हमले और उसके प्रभाव।

चर्चा में क्यों?

हाल के एक अध्ययन के अनुसार **बड़ी संख्या में लोग** डिजिटल रूप में भुगतान कर रहे हैं इसी क्रम में **स्मार्टफोन के माध्यम से उनके बैंक या बैंक खातों के मध्य अंतःक्रिया (Interactions) में वृद्धि** हुई है।

- डिजिटल भुगतान में वृद्धि, मोबाइल उपकरणों पर साइबर हमलों **के खतरे के बढ़ने की आशंका** को भी जन्म देता है।

साइबर खतरे:

- **परिचय:**
  - साइबर या साइबर सुरक्षा खतरा एक दुर्भावनापूर्ण कार्य है जो डेटा को व्यक्तिगत डेटा के साथ छेड़छाड़ करता है, उसकी चोरी करता है या सामान्य रूप से डिजिटल प्रक्रिया को बाधित करने का प्रयास करता है। इसमें कंप्यूटर वायरस, डेटा ब्रीच, डिनायल ऑफ सर्विस (DoS) अटैक और अन्य कारक शामिल हैं।
- **विभिन्न प्रकार:**
  - **मैलवेयर:** दुर्भावनापूर्ण सॉफ़्टवेयर के लिये प्रयोग किया जाने वाला संक्षिप्त शब्द 'मैलवेयर' किसी भी प्रकार के सॉफ़्टवेयर को संदर्भित करता है जिसे किसी एकल कंप्यूटर, सर्वर या कंप्यूटर नेटवर्क को हानि पहुँचाने के लिये डिज़ाइन किया गया है। **रैंसमवेयर, स्पाई वेयर, वर्म्स, वायरस और ट्रोजन मैलवेयर का प्रमुख प्रकार हैं।**
  - **फिशिंग:** यह भ्रामक ई-मेल और वेबसाइटों का उपयोग करके **व्यक्तिगत जानकारी एकत्र करने का का एक तरीका है।**
  - **डिनायल ऑफ सर्विस अटैक:** एक डिनायल-ऑफ-सर्विस (DoS) अटैक एक मशीन या नेटवर्क को बंद करने के लिये किया जाने वाला अटैक है, जिससे इच्छित उपयोगकर्त्ताओं के लिये उस सेवा तक पहुँच बाधित हो जाती है। DoS हमले लक्षित सेवा पर नेटवर्क/सर्वर ट्रैफिक को दिखाकर या प्रेरित करने वाली जानकारी भेजकर किये जाते हैं।
  - **मैन-इन-द-मिडिल (Man-in-the-middle-MitM) अटैक,** जिसे ईव्सड्रॉपिंग अटैक के रूप में भी जाना जाता है, ऐसा तब होता हैं जब हमलावर खुद को दो-पक्षीय लेनदेन में सम्मिलित करते हैं इस क्रम में जब हमलावर नेटवर्क/सर्वर में बाधा डालते हैं, इसी दौरान **डेटा को फिल्टर और उसकी चोरी कर सकते** हैं।
  - **सोशल इंजीनियरिंग** एक ऐसा हमला है जो आम तौर पर संरक्षित संवेदनशील जानकारी प्राप्त करने के लिये उपयोगकर्त्ताओं की सुरक्षा प्रक्रियाओं को तोड़ने के लिये अप्रत्यक्ष रूप से मानव संपर्क पर निर्भर करता है।

मोबाइल बैंकिंग पर साइबर खतरों से संबंधित मुद्दे:

- **साइबर हमलों में वृद्धि:**
  - साइबर सुरक्षा फर्म **कास्परस्की (Kaspersky)** का एक अध्ययन **एशिया प्रशांत क्षेत्र** में एंड्रॉयड और iOS उपकरणों पर साइबर हमले में वृद्धि की चेतावनी देता है, क्योंकि इस क्षेत्र में बड़ी संख्या में लोग **मोबाइल बैंकिंग सुविधाओं** का उपयोग करते हैं।
  - **ट्रोजन और मैलवेयर का उपयोग:**
    - कास्परस्की के अनुसार, **मोबाइल बैंकिंग ट्रोजन खतरनाक मैलवेयर हैं जो लोगों को मैलवेयर इंस्टॉल करने के लिये लुभाते** हैं तथा एप्लीकेशन को वैध ऐप के रूप में दिखाकर इसके द्वारा मोबाइल उपयोगकर्त्ताओं के **बैंक खातों से पैसे चुराये जा सकते** हैं।
    - उदाहरण के लिये मोबाइल बैंकिंग ट्रोजन, जिसे **एनबीस (Anubis)** कहा जाता है, वर्ष 2017 से उपयोगकर्त्ताओं को लक्षित

कर रहा है।
    - इसने **रूस, तुर्की, भारत, चीन, कोलंबिया, फ्राँस, जर्मनी, अमेरिका, डेनमार्क और वियतनाम** में उपयोगकर्त्ताओं को प्रभावित किया है।
- **क्रियाविधि:**
  - अपराधी **गूगल प्ले** पर वैध दिखने वाले और उच्च-रैंकिंग वाले दुर्भावनापूर्ण**ऐप्स, स्मिशिंग (एसएमएस के माध्यम से भेजे गए फिशिंग संदेश) एवं एक अन्य मोबाइल बैंकिंग ट्रोजन बियानलियन मैलवेयर** के माध्यम से डिवाइस को प्रभावित कर सकते हैं।
    - **रोमिंग मेंटिस (Roaming Mantis)** मोबाइल बैंकिंग उपयोगकर्त्ताओं को लक्षित करने वाला एक अन्य मैलवेयर है।
      - यह एंड्रॉयड उपकरणों पर हमला करता है और स्मिशिंग के माध्यम से डोमेन नेम सिस्टम (Domain Name Systems-DNS) को दुर्भावनापूर्ण कोड प्रसारित है।

- **पारस्परिकता (Interoperability) का मुद्दा:**
  - चूंकि गूगल पे, पेटीएम, फोन पे, स्क्वायर, पेपैल और अली पे जैसे विभिन्न भुगतान प्लेटफार्मों ने मोबाइल बैंकिंग को अपनाकर उपभोक्ता के बैंकिंग व्यवहार में बदलाव लाया है।
    - परिणामस्वरूप, **उन्होंने अपने लाभ के लिये भुगतान विधि को स्थायी रूप** से बदल दिया है।
  - **क्लोज्ड लूप पेमेंट सिस्टम (Closed Loop Payment System-CLPS):**
    - ये प्लेटफॉर्म एक क्लोज्ड लूप पेमेंट सिस्टम के आधार पर कार्य कर रहे हैं, जहाँ एक गूगल पे उपयोगकर्त्ता भुगतान प्लेटफॉर्म के माध्यम से दूसरे बैंक खाते में पैसा भेज सकता है।
      - इसका संचालन वीज़ा और मास्टरकार्ड के संचालन के समान हैं क्योंकि वे भुगतान लेनदेन को केवल अपने नेटवर्क में ही संचालित करतें हैं।
  - **व्यापार मॉडल में परिवर्तन:**
    - यह आंशिक रूप से नियामकों द्वारा संचालित होता है जो**खुले, मानकीकृत प्लेटफार्म का उपयोग करते हैं, ये मंच बाधाओं को कम करते हैं।**
    - कुछ देश पहले से ही भुगतान मंच प्रदाताओं को अपने व्यवसाय मॉडल बदलने के लिये प्रोत्साहित कर रहे हैं।
      - उदाहरण के लिये, चीन ने अपनी **इंटरनेट कंपनियों को अपनी प्रतिद्विंद्वी फर्मों को अपने प्लेटफॉर्म/मंच पर लिंक और भुगतान सेवाओं की पेशकश करने का आदेश दिया है।**
      - भारत में **सभी लाइसेंस प्राप्त मोबाइल भुगतान प्लेटफॉर्म वॉलेट के बीच अंतर-संचालन प्रदान करने में सक्षम एक** नए कानून की आवश्यकता है।
    - नियामकों द्वारा भुगतान प्लेटफॉर्म को अंतर-संचालन को बढ़ावा ऐसे समय में दिया जा रहा है जब तकनीकी विशेषज्ञों की मांग बैंकिंग उद्योग में गंभीर चिंता का विषय है।
- **सुरक्षा विशेषज्ञों की कमी:**
  - अपनी डिजिटल आकांक्षाओं को पूरा करने के लिये बैंकों द्वारा आवश्यक प्रौद्योगिकी, इंजीनियरिंग, डेटा और सुरक्षा विशेषज्ञों की कमी को छिपाया जाता हैं।
- **पर्याप्त साइबर सुरक्षा नीति का अभाव**:
  - पर्याप्त साइबर सुरक्षा की कमी और बैंकिंग में प्रतिभा की कमी संभावित रूप से उपयोगकर्त्ता उपकरणों पर साइबर हमलों में और वृद्धि का कारण बन सकती है।
    - जब तक इस समस्या का समाधान नहीं किया जाता है, तब तक भुगतान करने के लिये मोबाइल डिवाइस का उपयोग करते समय सतर्क रहने की आवश्यकता है।

आगे की राह

- **फोन को अप-टू-डेट रखने और नियमित रूप से रीबूट करने जैसी डिजिटल तरीकों का उपयोग किया जा सकता है।**
- इसके अलावा, उपभोक्ता यह सुनिश्चित कर सकते हैं कि वे अपने फोन का उपयोग बैंकिंग के लिये तभी करें जब डिवाइस सुरक्षित VPN से जुड़ा हो (VPN "वर्चुअल प्राइवेट नेटवर्क" को संदर्भित करता है और सार्वजनिक नेटवर्क का उपयोग करते समय संरक्षित नेटवर्क कनेक्शन स्थापित करने के अवसर प्रदान करता है) और iOS 16 उपयोगकर्त्ता लॉकडाउन मोड को चालू कर सकते हैं क्योंकि यह डिवाइस की कार्यक्षमता को सीमित करता है एवं इसे किसी भी संभावित मैलवेयर से बचाता है।

यूपीएससी सिविल सेवा परीक्षा, विगत वर्षों के प्रश्न (PYQs):

प्रीलिम्स

प्रश्न. हाल ही में कभी-कभी समाचारों में आने वाले शब्द 'वानाक्राई, पेट्या और इंटर्नलब्लू' निम्नलिखित में से किससे संबंधित हैं (2018)

(a) एक्सोप्लैनेट
(b) क्रिप्टोकरेंसी
(c) साइबर हमले
(d) मिनी उपग्रह

उत्तर: (c)

व्याख्या:

- रैंसमवेयर दुर्भावनापूर्ण सॉफ्टवेयर (या मैलवेयर) का एक रूप है। एक बार जब यह कंप्यूटर में प्रवेश कर लेता है, तो यह आमतौर पर डेटा तक पहुँच कर उपयोगकर्त्ताओं को नुकसान पहुँचाता है। भुगतान करने पर डेटा तक पहुँच बहाल करने का वादा करते हुए हमलावर पीड़ित से फिरौती की मांग करते है।
- **'वानाक्राई, पेट्या और इंटरनलब्लू'** कुछ रैनसम वेयर हैं, जिन्होंने बिटकॉइन (क्रिप्टोकरेंसी) में फिरौती के भुगतान की मांग की थी।**अतः विकल्प (c) सही है।**

मैन्स

प्रश्न. साइबर हमले के संभावित खतरों की एवं इसे रोकने के लिये सुरक्षा ढाँचे की विवेचना कीजिये। (मेन्स-2017)

स्रोत: द हिंदू

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/cyber-threat-to-mobile-banking