



"कम -नकदी" के दौर में बढ़ता हैकरों का खतरा

drishtias.com/hindi/printpdf/less-cash-grows-in-rounds-risk-of-hackers

हाल ही में विमुद्रीकरण के कारण उपजे "कम-नकदी" के माहौल ने लेन-देन के स्वरूप का डिजिटलीकरण करके निर्विवाद रूप से देश की अर्थव्यवस्था को एक महत्वपूर्ण लाभ पहुँचाया है। अर्थव्यवस्था के इस बदलते स्वरूप ने जहाँ एक ओर डिजिटल उपकरणों के प्रयोग को बढ़ावा प्रदान किया है वहीं दूसरी ओर तकनीकी रूप से अनपढ़ तथा अनुभवहीन लोगों के लिये चुनौती भी उत्पन्न की है। लेन-देन के इस बदलते स्वरूप ने जहाँ एक ओर अर्थव्यवस्था को विकास के एक नए दौर में पहुँचा दिया है वहीं दूसरी ओर ऑनलाइन भुगतान के सन्दर्भ में उत्पन्न होने वाले हैकरों के खौफ को भी बढ़ावा देने का काम किया है।

मोबाइल-आधारित व्यवस्था

- अर्थव्यवस्था के इस बदलते स्वरूप के साथ तालमेल बैठाने के लिये देश के कई प्रतिष्ठित बैंकों ने मोबाइल बैंकिंग एवं एप के प्रयोग को बढ़ावा प्रदान किया है।
- हाल ही में कुछ बैंकों ने अपने ग्राहकों को लेन-देन के सम्बन्ध में होने वाली असुविधा से राहत प्रदान करने के उद्देश्य से बहुत सी सुविधाओं से युक्त नई मोबाइल एपों का भी विकास किया है।
- इसी दिशा में आगे बढ़ते हुए हाल ही में भारत सरकार के भारतीय राष्ट्रीय भुगतान निगम (National Payments Corporation of India - NPCI) विभाग द्वारा भी एप (Bharat Interface for Money – BHIM) का विकास किया गया है।
- इस एप के अंतर्गत ग्राहक को यूपीआई (Universal Payment Interface - UPI) के माध्यम से सीधे अपने बैंक खाते से ऑनलाइन पैसे भेजने एवं प्राप्त करने के साथ-साथ कुछ अन्य बुनियादी लेन-देन की सुविधा भी प्रदान की गई है।
- इस संबंध में सबसे महत्वपूर्ण बात यह है कि इस प्रकार की किसी भी एप के अंतर्गत ग्राहक की बैंक खाते से संबंधित सूचनाएँ रखने संबंधी कोई दावा नहीं किया जाता है बल्कि किसी भी लेन-देन के समय ग्राहक के खाते को सीधे उसके लेन-देन से संबद्ध कर दिया जाता है जो कि बैंक खाते की सुरक्षा के संबंध में एक गंभीर चिंता का विषय है।
- डिजिटल लेन-देन के सन्दर्भ में मोबाइल पर्स (Mobile wallets) एप का भी काफी प्रयोग किया जाता है। मोबाइल पर्स वस्तुतः वास्तविक पर्स न होकर डिजिटल पर्स होते हैं, जिनका प्रयोग डिजिटल भुगतान के लिये किया जाता है।
- मोबाइल पर्स में ग्राहक सीधे अपने बैंक खाते से धन का संचरण करता है। वर्तमान में बहुत सी मोबाइल पर्स एपों का प्रयोग किया जा रहा है उदाहरण के तौर पर, एसबीआई बडी (SBI Buddy), चिल्लर (Chillr), पेटीएम (Paytm), ऑक्सीजन (Oxygen), मोबिक्रिक (MobiKwik) इत्यादि।
- मोबाइल पर्स के विषय में सबसे महत्वपूर्ण बात यह है कि इस प्रकार के पर्स का प्रयोग केवल तभी किया जा सकता है जब विक्रेता एवं ग्राहक दोनों के द्वारा एक ही प्रकार के वॉलेट का प्रयोग किया जा रहा हो अन्यथा इस प्रकार के पर्स का प्रयोग संभव नहीं हो पाता है।
- ध्यातव्य है कि उक्त मोबाइल एपों में मुद्रा के लेन-देन एवं उपयोग हेतु 2 जी, 3 जी अथवा वाईफाई जैसी सुरक्षित संचार

(Secure Communication) तकनीकों का प्रयोग किया जाता है।

- जबकि भीम एप के अंतर्गत बैंकों के मध्य मुद्रा के लेन-देन के संबंध में विश्वसनीय यूपीआई नेटवर्क का प्रयोग किया जाता है।
- गौरतलब है कि वर्तमान में एनपीसीआई के तहत पंजीकृत तकरीबन 47 बैंकों द्वारा मुद्रा के सुरक्षित लेन-देन हेतु यूपीआई नेटवर्क का प्रयोग किया जा रहा है।
- इसके अतिरिक्त डिजिटल भुगतान के रूप को सरलीकृत करने हेतु अपेक्षाकृत न्यूनतम प्रौद्योगिकी का इस्तेमाल किया गया है। ध्यातव्य है कि इन सभी डिजिटल लेन-देनों में यूएसएसडी आधारित भुगतान प्रणाली का प्रयोग किया जाता है।
- एनपीसीआई द्वारा विकसित इस भुगतान प्रणाली के अंतर्गत उपभोक्ताओं को उनके बैंक खातों का वायरलेस टेलीफोन नेटवर्क (Wireless Telephone Network) के माध्यम से उपयोग करने की भी सुविधा प्रदान की गई है। इसका अर्थ यह हुआ कि अब मोबाइल बैंकिंग के लिये स्मार्ट फ़ोन की आवश्यकता नहीं है।
- ध्यातव्य है कि ये सभी लेन-देन न केवल बहुभाषी हैं बल्कि देश के विकास के सन्दर्भ में भी अत्यंत लाभकारी हैं।

भुगतान संबंधी चुनौतियाँ

वर्तमान में मौजूद भुगतान प्रणालियों के सटीक क्रियान्वयन एवं सुरक्षा के संबंध में बहुत सी चुनौतियाँ मुहँ बाए खड़ी है, इनमें से कुछ इस प्रकार हैं-

समझौता अनुप्रयोग संबंधी चुनौतियाँ (Compromised applications)

- गौरतलब है कि डिजिटल भुगतान के संबंध में सबसे बड़ी चुनौती अथवा परेशानी ग्राहक के मोबाइल फ़ोन में अन्य अनुप्रयोगों (Applications) की उपस्थिति होना है।
- यदि ग्राहक के पास कोई अन्य वैकल्पिक की-बोर्ड अनुप्रयोग (Alternative keyboard application) उपलब्ध है तो सुरक्षा संबंधी चुनौतियाँ और अधिक बढ़ जाती हैं। क्योंकि कई बार मोबाइल एप को डाउनलोड करते समय मोबाइल में संगृहित सूचनाओं के प्रयोग की अनुमति देना आवश्यक होता है। ऐसी स्थिति में बैंकिंग सूचनाओं को सुरक्षित रख पाना एक चुनौतीपूर्ण कार्य होता है।

कुछ विशेष सेवाओं के प्रयोग को मनाही

- गौरतलब है कि भुगतान प्रणाली के सभी रूपों के साथ संबद्ध जोखिमों को एक पूरे नेटवर्क व्यवस्था के रूप में समझे जाने की आवश्यकता है।
- प्रायः यह देखा जाता है कि मोबाइल फ़ोन में मौजूद एप्लीकेशनों के कारण निरंतर उत्पन्न होने वाले अवरोधों से अक्सर नेटवर्क अथवा उपकरण जाम हो जाते हैं अर्थात् उनका मार्ग अवरुद्ध हो जाता है। जिसके कारण वस्तुतः डिजिटल लेन-देन के संबंध में बहुत सी परेशानियों का सामना करना पड़ता है।

अन्य चुनौतियाँ

- ऐसी स्थिति में हैकरों के लिये दूरसंचार नेटवर्क के साथ-साथ भुगतान मोबाइल पर्स तथा बैंकिंग नेटवर्क तक पहुँच बनाना बहुत आसान हो जाता है।
- मोबाइल फ़ोन में संगृहित सूचनाओं से अधिक मोबाइल फ़ोन पर होने वाली बातचीत के माध्यम से महत्वपूर्ण सूचनाओं की चोरी करना अधिक आसान कार्य होता है। इस प्रकार की चुनौतियों को गूढ़ चुनौतियों के रूप में वर्णित किया जाता है।
- ध्यातव्य है कि किसी बैंकिंग व्यवस्था अथवा एनपीसीआई के सर्वर को हैक करने के स्थान पर किसी व्यक्ति के मोबाइल फ़ोन को हैक करना अधिक लाभदायक होता है क्योंकि बैंक सर्वर के माध्यम से हैकर किसी ग्राहक की मात्र निजी

सूचनाओं को ही उजागर कर सकता है।

- परंतु यदि मोबाइल फ़ोन के जीसीएम नेटवर्क (इसे वस्तुतः A5/1 एन्क्रिप्शन कमजोरियों के रूप में जाना जाता है) को हैक किया जाता है तो इसके माध्यम से ग्राहक की निजी जानकारियों के साथ-साथ उसकी बातचीत, उसके संदेशों के साथ-साथ उसके यूएसएसडी आधारित लेन-देन संबंधी सूचनाओं की भी जानकारी प्राप्त की जा सकती है।
- हालाँकि जैसा की हम सभी जानते हैं कि डिजिटल भुगतान के विषय में सुविधा के साथ-साथ सुरक्षा को सुनिश्चित रख पाना एक अत्यंत ही जोखिमपूर्ण कार्य है। अतः ऐसी किसी भी स्थिति का सामना करने के लिये ग्राहक एवं सरकार को कुछ अत्यंत महत्वपूर्ण कदम उठाने की आवश्यकता है ताकि भविष्य में ऐसी किसी भी समस्या का सहजता से सामना किया जा सके।
- वस्तुतः मोबाइल भुगतान प्रणाली के संबंध में सबसे बड़ी चुनौती उपभोक्ता के स्तर पर आती है। अतः इस समस्या का सामना करने के लिये आवश्यक है कि ग्राहक द्वारा अपने मोबाइल फ़ोन को अनाधिकृत उपयोगों (Unauthorised Access) से अधिक से अधिक सुरक्षित बनाया जाना चाहिये।
- इसके लिये आवश्यक है कि प्रत्येक उपभोक्ता के मोबाइल फोन में पिनकोड आधारित एक लॉक व्यवस्था होनी चाहिये। इस दिशा में बायोमीट्रिक्स (Biometrics) आधारित सुरक्षा व्यवस्था अधिक प्रभावी होती है।
- डिजिटल भुगतान एवं बैंकिंग आधारित एप्लीकेशनों को अधिक से अधिक सुरक्षित बनाए रखने हेतु आवश्यक है कि इनकी सुरक्षा व्यवस्था पिनकोड आधारित ही होनी चाहिये।

निष्कर्ष

उल्लेखनीय है कि भारत को कॅशलेस अर्थव्यवस्था के रूप में तब्दील करने हेतु भारत सरकार द्वारा कई महत्वपूर्ण कदम उठाए गए हैं। सरकार द्वारा इस सम्पूर्ण व्यवस्था को सुरक्षित बनाए रखने हेतु लोगों को डिजिटल भुगतान करते समय बरती जाने वाली सावधानियों के विषय में भी सचेत करने की दिशा में कई महत्वपूर्ण पहलें आरंभ करने की आवश्यकता है। इसके लिये आवश्यक है कि एक मज़बूत प्रशिक्षण कार्यक्रम का संचालन किया जाए ताकि डिजिटल लेन-देन को और अधिक सुरक्षित बनाया जा सके। अंततः इस दिशा में एक ऐसे विशेष तंत्र को विकसित किये जाने की आवश्यकता है जिसके माध्यम से सूचनाओं की चोरी रोकने, डिजिटल लेन-देन के मार्ग में आने वाले अवरोधों को कम करने तथा जनता को और अधिक सचेत करने पर बल दिया जाना चाहिये।