कैशलेस अर्थव्यवस्था (cashless economy) के दौर में साइबर सुरक्षा

कैशलेस अर्थव्यवस्था क्या है?

आर्थिक व्यवस्था का वह स्वरूप जिसमें धन का अधिकांश लेन-देन चेक, क्रेडिटकार्ड, डेबिटकार्ड, नेट बैंकिंग, मोबाइल से भुगतान तथा भिन्न-भिन्न डिजिटल माध्यमों से किया जाता है, कैशलेस अर्थव्यवस्था कहलाती है। इस व्यवस्था में नकदी (कागजी नोट या सिक्के) का चलन कम हो जाता है।

साइबर सुरक्षा क्या है?

साइबर सुरक्षा वे तकनीकी प्रक्रियाएँ हैं, जो किसी कंप्यूटर, इंटरनेट नेटवर्क अथवा अन्य डिजिटल उपकरणों तक किसी अनधिकृत पहुँच को रोकती हैं।

कैशलेस अर्थव्यवस्था की वर्तमान स्थिति

- एक तरफ पेटीएम, फ्रीचार्ज, पेयू, मोबिक्विक जैसे मोबाइल भुगतान माध्यमों के इस्तेमाल में जबरदस्त तेजी आ रही है। वहीं दूसरी तरफ बैंकों के क्रेडिट कार्ड, डेबिट कार्ड और नेट बैंकिंग का प्रयोग बढ़ने से दुकानों, पेट्रोल-पंप व रेस्तराओं में भी कैशलेस व्यवस्था बढ़ी है।
- वहीं अक्तूबर माह में हिताची (Hitachi) नामक कंपनी द्वारा एक्सिस बैंक के एक ATM में प्रबंधन सुरक्षा संबंधी चूक से लाखों उपभोक्ताओं के डेबिट कार्डों का ब्यौरा अपराधी तत्त्वों के हाथों पहुँच गया, जिसे बैंकिंग इतिहास में सबसे बड़ी वित्तीय सुरक्षा सेंध माना जा रहा है।
- वैसे इसका सबसे बड़ा लाभ यह है कि इसमें धन का लेन-देन नकदी आधारित अर्थव्यवस्था की तुलना में काफी हद तक पारदर्शी हो जाता है, जिससे भ्रष्टाचार तथा काले धन पर अंकुश लगता है।

एनक्रिप्टेड डेटा

- डिजिटल माध्यमों के भीतर इंटरनेट पर एक छोर से दूसरे छोर तक यात्रा के दौरान मौजूद डाटा को सुरक्षा प्रदान करने के लिये 40 बिट, 64 बिट या 128 बिट में कूटबद्ध कर प्रेषित किया जाता है। इसमें सर्वाधिक मजबूत 128 बिट एनक्रिप्शन है, जिसे तोड़ने में 10 खरब वर्ष लग जाएंगे।
- इसलिये भारतीय रिज़र्व बैंक के दिशा-निर्देशों के तहत डिजिटल माध्यमों पर ग्राहकों के डेटा को 128 बिट एनक्रिप्शन प्रणालियों के जरिये एनक्रिप्ट की बाध्यता है।

कैशलेस लेन-देन में अपराधा व सावधानियाँ

- कार्ड खो जाने या चुरा लिये जाने, पर तत्काल कस्टमर केयर द्वारा कार्ड ब्लॉक करवा देना चाहिये।
- फिशिंग, कई बार बैंकों के नाम से जाँच के नाम पर ई-मेल, फोन कॉल्स आते हैं। इस पर अपनी गुप्त जानकारी साझा नहीं करनी चाहिये।
- वायरस, स्पाईवेयर, की-लॉगिंग, हमारे कंप्यूटर या वाईफाई नेटवर्किंग में कुछ जासूसी वायरस हमारी गतिविधि पर नजर रख सकते हैं एवं हमारी ऑनलाइन भुगतान की जानकारी को अपने कंट्रोलर तक पहुँचा सकते हैं। इसके लिये कंप्यूटर वायरस सुरक्षा व सिस्टम अपडेट करते रहें।
- स्किमिंग, कई कारोबारी ठिकानों में धोखेबाज कर्मचारी छोटी इलेक्ट्रॉनिक मशीनों द्वारा हमारे क्रेडिट कार्ड की चुंबकीय पट्टी की जानकारी चुरा लेते हैं। इसलिये सावधानीपूर्वक लेन-देन के समय अपने कार्ड पर नजर रखनी चाहिये।
- आइडेंटिटी थेफ़्ट (पहचान की चोरी) कुछ धोखेबाज हमारे नाम पर डाक का पता बदलने का आग्रह बैंक से कर देते हैं। फिर कार्ड खो जाने की शिकायत कर नया कार्ड इश्यू करवा लेते हैं। अतः अपने होम बैंक व बैंक खातों पर नजर रखनी चाहिए।
- बैंक से डेटा चोरी, कई बार बैंक के कंप्यूटर व सर्वर से ही डेटा चोरी हो जाते हैं। इससे बचने के लिये बैंकों को मजबूत सुरक्षा फीचर्स/तंत्र के साथ-साथ अपने बैंक कर्मचारियों की संदेहास्पद गतिविधियों के प्रति भी सतर्क रहना चाहिये।

कुछ सामान्य सावधानियाँ

- वेबसाइट्स पर https:// वाले यूआरएल का प्रयोग करें http:// का नहीं। ऐसे वेबसाइट्स के वेब पते के आगे ताले का चित्र दिखाई देता है।
- ऑनलाइन ट्रांजेक्शन के लिये यदि संभव हो तो वेरीफाई वीजा, मास्टर कार्ड, सिक्योर कोड, नेट सेफ जैसे उपायों को वरीयता दें।
- यदि क्रेडिट कार्ड पर बीमा सुविधा हो तो ले लें, लॉग इन के बाद लॉग आउट अवश्य करें।
- मुफ्त या ट्रायल वर्जन के स्थान पर एक अच्छा एंटी-वायरस, एंटी-स्पाईवेयर, फिशिंग अलर्ट व टोटल सिक्योरिटी का प्रयोग करें।
- दुरुपयोग की स्थिति में तुरंत साइबर क्राइम शाखा, अपने बैंक व अपने बीमाकर्ता को इसकी जानकारी दें।

निष्कर्ष

यह सत्य है कि जितनी सुविधा उतनी दुविधा, किंतु सावधानी में ही तो सुरक्षा है। जब विश्व के अधिकांश देश कैशलेस अर्थव्यवस्था की ओर बढ़ रहे हैं, तो हम उस पुरानी पटरी पर नहीं चल सकते। यदि समस्याएँ हैं; असुरक्षा का डर है तो कुशल तकनीक के प्रयोग का इस्तेमाल कर लोगों में जागरूकता व सतर्कता फैलाकर इसे सफल बनाया भी तो जा सकता है।

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/Cyber-security-in-cashless-economy