स्टैंडिंग कमिटी की रिपोर्ट का सारांश

डिजिटल भुगतान और डेटा प्रोटेक्शन के लिए ऑनलाइन सुरक्षा उपाय

- संचार और सूचना प्रौद्योगिकी संबंधी स्टैंडिंग कमिटी (चेयर: श्री प्रतापराव जाधव) ने 8 फरवरी, 2024 को 'डिजिटल भुगतान और डेटा प्रोटेक्शन के लिए ऑनलाइन सुरक्षा उपाय' पर अपनी रिपोर्ट प्रस्तुत की। कमिटी के मुख्य निष्कर्षों और सुझावों में निम्नलिखित शामिल हैं:

- **ऑनलाइन वित्तीय धोखाधड़ी में बढ़ोतरी**: कमिटी ने कहा कि साइबर अपराध के मामलों की संख्या और गंवाई गई धनराशि में काफी बढ़ोतरी हुई है। साइबर अपराध की शिकायतों की संख्या 2022 में 9.7 लाख से बढ़कर 2023 में 11.5 लाख हो गई। वित्तीय धोखाधड़ी कुल शिकायतों का लगभग 60% है। जनवरी और अक्टूबर 2023 के बीच 5,574 करोड़ रुपए की वित्तीय धोखाधड़ी दर्ज की गई, जो 2022 (पूरे वर्ष में 2,296 करोड़ रुपए) की तुलना में काफी अधिक है। वित्तीय धोखाधड़ी के प्रकारों में ग्राहक सेवा नंबर धोखाधड़ी, केवाईसी-आधारित धोखाधड़ी और आधार एनेबल पेमेंट सिस्टम (एईपीएस) आधारित धोखाधड़ी शामिल हैं।

- कमिटी ने कहा कि साइबर अपराध को रोकने के लिए एक बहुआयामी दृष्टिकोण की आवश्यकता है, जिसमें सभी संबंधित मंत्रालय शामिल हों। उसने गृह मंत्रालय को सुझाव दिया कि वह एक नोडल एजेंसी का गठन करे जिसमें सभी संबंधित एजेंसियों के प्रतिनिधि शामिल हों।

- **एईपीएस आधारित अपराध**: एईपीएस ग्राहकों को बायोमेट्रिक प्रमाणीकरण का उपयोग करके अपने आधार-लिंक्ड खातों से लेनदेन करने की सुविधा प्रदान करता है। कमिटी ने कहा कि एईपीएस का उपयोग करके होने वाली धोखाधड़ी बढ़ रही हैं। गृह मंत्रालय ने बताया था कि आधार का उपयोग करके बायोमेट्रिक प्रमाणीकरण को गलत साबित करने के लिए डमी या रबर उंगलियों का उपयोग किया जा रहा था।

- **धन की वसूली**: कमिटी ने कहा कि वसूल की गई और ग्राहकों को लौटाई गई धनराशि की मात्रा बहुत कम थी (2021 और 2022 के बीच 10.4%)। यह भी कहा गया कि शिकायत दर्ज करने का तरीका जटिल था और शिकायत को हल करने में बहुत अधिक समय लगता था। उसने सुझाव दिया कि पीड़ितों को फ्रीज की गई धनराशि वापस करने की प्रक्रिया को गृह मंत्रालय सुव्यवस्थित करे।

- **क्षेत्र आधारित अपराध**: गृह मंत्रालय ने कहा कि अधिकांश साइबर धोखाधड़ी दो जगहों से हुई: राजस्थान, उत्तर प्रदेश, हरियाणा में मेवात क्षेत्र और बिहार और झारखंड में जामताड़ा। कमिटी ने कहा कि इन क्षेत्रों में बड़ी संख्या में माइक्रो-एटीएम मौजूद हैं, जिससे पैसे की हेराफेरी होती है। इस प्रकार कमिटी ने सुझाव दिया कि इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय (एमईआईटीवाई) को क्षेत्र-विशिष्ट रणनीतियां तैयार करनी चाहिए।

- **सख्त दंडात्मक उपायों की जरूरत**: साइबर अपराध के मामलों में सजा की दर बहुत कम है (2021 में 0.89%)। कमिटी ने कहा कि साइबर अपराधों को रोकने में दंडात्मक उपाय बहुत प्रभावी नहीं रहे हैं। उसने आगे कहा कि साइबर अपराध के क्षेत्र में सख्त दंडात्मक उपायों के साथ वैधानिक और नियामक सुधारों की आवश्यकता है।

- **फिनटेक प्लेटफॉर्म्स का रेगुलेशन**: भारतीय बाजार पर हावी फिनटेक एप्लिकेशंस विदेशी संस्थाओं के स्वामित्व में हैं। कमिटी ने कहा कि कुछ फिनटेक ऐप्स और प्लेटफॉर्म्स का इस्तेमाल मनी लॉन्ड्रिंग के लिए किया जा रहा है। इसलिए उसने सुझाव दिया कि स्वदेशी फिनटेक ऐप्स और प्लेटफार्म्स के प्रचार पर अधिक ध्यान दिया जाना चाहिए। उसने यह भी कहा कि स्वदेशी प्लेटफार्म्स का रेगुलेशन अधिक व्यावहारिक होगा क्योंकि विदेशी संस्थाओं के विभिन्न क्षेत्राधिकार होते हैं।

- कमिटी ने यह भी कहा कि आम घोटालों और उनकी रोकथाम की रणनीति के बारे में जागरूकता पैदा करने के लिए फिनटेक ऐप्स/प्लेटफॉर्म का उपयोग किया जाना चाहिए। कमिटी ने एमईआईटीवाई को जागरूकता पैदा करने के लिए बैंकों/फिनटेक प्लेटफार्म्स और ऐप्स के लिए विस्तृत दिशानिर्देश लाने का सुझाव दिया। ये

प्रतिनव दमानी
pratinav@prsindia.org

29 फरवरी, 2024

अभियान किसी क्षेत्र की स्थानीय भाषा में भी चलाए जा सकते हैं।

- **विशिष्ट कर्मचारियों की कमी**: कमिटी ने कहा कि सीईआरटी-इन और सीएसआईआरटी-फिन जैसी विशेष एजेंसियों में कई रिक्तियां मौजूद हैं। सीईआरटी-इन में, 142 स्वीकृत पदों में से 26 खाली (27%) थे।
- आयोग ने सुझाव दिया कि साइबर सुरक्षा प्रोफेशनल्स की बढ़ती मांग को पूरा करने के लिए केंद्रीय निगरानी एजेंसियों और राज्य कानून प्रवर्तन एजेंसियों के कर्मचारियों को प्रशिक्षित किया जाना चाहिए।
- **सरकारी वेबसाइट्स पर साइबर हमले**: एमईआईटीवाई के अनुसार, हर साल सरकारी वेबसाइट्स पर विभिन्न हमलों की कोशिश की जाती है। 2022 में ऐसी 50 घटनाएं हुईं। सरकार के कुछ विभाग/शाखाएं पुराने सॉफ़्टवेयर का उपयोग करती थीं। कमिटी ने मंत्रालय द्वारा जारी साइबर सुरक्षा संबंधी दिशानिर्देशों का पालन करने की आवश्यकता पर जोर दिया। उसने मंत्रालय को साइबर खतरों से निपटने के संबंध में सरकारी इंफ्रास्ट्रक्चर को अपग्रेड करने का भी सुझाव दिया।