सुरक्षित डिजिटल कनेक्टिविटी हेतु सुधार

प्रिलिम्स के लिये:

सुरक्षित डिजिटल कनेक्टिविटी हेतु सुधार, डिजिटल पारिस्थितिकी तंत्र, नो योर कस्टमर, प्वाइंट ऑफ सेल, विश्व दूरसंचार दिवस

मेन्स के लिये:

सुरक्षित डिजिटल कनेक्टिविटी हेतु सुधार

चर्चा में क्यों?

हाल ही में **स्वच्छ और सुरक्षित** डिजिटल पारिस्थितिकी तंत्र को बढ़ावा देने के लिये मोबाइल उपयोगकर्ता सुरक्षा हेतु दो सुधार पेश किये गए हैं।

- ये दोनों सुधार **KYC (अपने ग्राहक को जानें/नो योर कस्टमर)** और **प्वाइंट ऑफ सेल पंजीकरण** से संबंधित हैं। ये सुधार नागरिक-केंद्रित पोर्टल **संचार साथी** (साइबर अपराध एवं वित्तीय धोखाधड़ी के खतरे के खिलाफ भारत को सशक्त बनाने हेतु शुरू की गई पहल) के लॉन्च के साथ शुरू किये गए पहले के सुधारों की दिशा में अगला पड़ाव है।

किये गए सुधार:

- **KYC सुधार:** ये सुधार दूरसंचार सेवाओं के ग्राहकों को संभावित धोखाधड़ी से बचाने और डिजिटल पारिस्थितिकी तंत्र में जनता के विश्वास में वृद्धि करने में प्रमुख भूमिका निभाते हैं।
  - **आधार संख्या की QR कोड स्कैनिंग:** KYC प्रक्रिया के दौरान प्राप्त डेटा के दुरुपयोग को रोकने के लिये मुद्रित आधार के QR कोड को स्कैन करके जनसांख्यिकीय जानकारी एकत्र की जाती है।
  - **बंद मोबाइल नंबर के तत्काल पुन: उपयोग पर रोक:** मोबाइल नंबर बंद किये जाने की अवधि से 90 दिनों तक यह नंबर नए ग्राहकों को आवंटित नहीं किया जाएगा, इससे किसी भी नंबर के तत्काल पुन: उपयोग को रोका जा सकेगा।
  - **सिम रिप्लेसमेंट/बदलने के लिये KYC की अनिवार्यता:** सब्सक्राइबर्स को अपना सिम कार्ड बदलते समय KYC पूरा करना अनिवार्य होगा।
  - **बायोमेट्रिक प्रमाणीकरण:** अँगूठे के निशान और आईरिस-आधारित प्रमाणीकरण के अलावा आधार E-KYC में चेहरे-आधारित बायोमेट्रिक प्रमाणीकरण की अनुमति है।
  - **व्यावसायिक कनेक्शन:** कंपनियाँ, संगठन, ट्रस्ट और सोसायटी जैसी संस्थाएँ आदि सभी अंतिम उपयोगकर्ता KYC पूरा करने के बाद ही मोबाइल कनेक्शन प्राप्त कर सकते हैं। सफल KYC और इकाई के भौतिक सत्यापन के बाद ही सिम को चालू/सक्रिय (Activation) किया जाता है।
- **प्वाइंट-ऑफ-सेल (POS) पंजीकरण सुधार: इस सुधार का उद्देश्य फ्रेंचाइज़ी, एजेंटों और वितरकों (PoS) को अनिवार्य रूप से पंजीकृत करके वितरण नेटवर्क की सत्यनिष्ठा सुनिश्चित करना है।**
  - इस प्रक्रिया में PoS और लाइसेंसधारियों के बीच **मज़बूत सत्यापन एवं लिखित समझौते** शामिल हैं। **अवैध गतिविधियों** में लिप्त किसी भी PoS की सेवा **को समाप्त कर तीन वर्ष के लिये ब्लैकलिस्ट में शामिल कर दिया जाएगा।**

संचार साथी पोर्टल:

- **परिचय:**
  - **दूरसंचार विभाग (Department of Telecommunications- DoT)** के तहत **सेंटर फॉर डेवलपमेंट ऑफ टेलीमैटिक्स (Centre for Development of Telematics- C-DOT)** द्वारा विकसित संचार साथी पोर्टल, भारत के दूरसंचार क्षेत्र में एक क्रांतिकारी कदम है।
  - इसे विश्व दूरसंचार दिवस **[World Telecommunication Day (17 मई, 2023)]** पर लॉन्च किया गया था।
- **उद्देश्य:**

- संचार साथी पोर्टल का प्राथमिक उद्देश्य दूरसंचार उद्योग में प्रचलित विभिन्न धोखाधड़ी की गतिविधियों, जैसे **आइडेंटिटी थेफ्ट, जाली KYC और बैंकिंग फ्रॉड** को संबोधित करना है।
    - उन्नत प्रौद्योगिकियों और रूपरेखाओं का लाभ उठाकर, इस पोर्टल का लक्ष्य उपयोगकर्ताओं को एक सुरक्षित तथा भरोसेमंद दूरसंचार का अनुभव प्रदान करना है।

- **सुधार:**
    - **CEIR (केंद्रीय उपकरण पहचान रजिस्टर):**
        - **इसे चोरी या खोए हुए मोबाइल फोन को ब्लॉक करने** के लिये लागू किया गया।
        - उपयोगकर्ता चोरी हुए उपकरणों के सत्यापन और उन्हें ब्लॉक करने के लिये पुलिस शिकायत की एक प्रति के साथ **IMEI नंबर** जमा कर सकते हैं।
        - दूरसंचार सेवा प्रदाताओं को कानून प्रवर्तन एजेंसियों के साथ एकीकृत किया गया।
        - यह **चोरी हुए उपकरणों के भारतीय नेटवर्क में प्रयोग को रोकता** है तथा आवश्यकता पड़ने पर कानून प्रवर्तन एजेंसियों के माध्यम से पता लगाने की अनुमति देता है।
    - **अपने मोबाइल कनेक्शन को जानें:**
        - यह उपयोगकर्ताओं को उनके नाम पर **पंजीकृत मोबाइल कनेक्शन की जाँच करने** की अनुमति देता है।
        - अनधिकृत या **कपटपूर्ण कनेक्शनों की पहचान करने में सक्षम** बनाता है।
        - उपयोगकर्ता धोखाधड़ी या अनधिकृत कनेक्शन की रिपोर्ट किये जाने की स्थिति में उक्त कनेक्शन को **पुन: सत्यापित या बंद** किया जा सकता है।
    - **ASTR (आर्टिफिशियल इंटेलिजेंस और फेशियल रिकग्निशन पावर्ड सॉल्यूशन फॉर टेलीकॉम सिम सब्सक्राइबर वेरिफिकेशन):**
        - इसे **कपटपूर्ण या ज़ाली दस्तावेज़ों का उपयोग करके कनेक्शन प्राप्त करने वाले ग्राहकों की पहचान करने** के लिये विकसित किया गया।
        - यह **चेहरे की पहचान और डेटा विश्लेषण** तकनीकों का उपयोग करता है।
        - **कागज़ आधारित KYC दस्तावेज़ों के माध्यम से प्राप्त कनेक्शनों** का विश्लेषण करता है।
- **प्रभाव:**
    - इसके तहत 40 लाख से अधिक फर्जी कनेक्शनों की पहचान की गई, साथ ही पोर्टल का उपयोग करके 36 लाख से अधिक कनेक्शन समाप्त कर दिये गए।
    - यह उपयोगकर्ताओं को एक सुरक्षित और भरोसेमंद दूरसंचार का अनुभव प्रदान करता है।
    - यह पहचान की चोरी, जाली KYC, मोबाइल उपकरण की चोरी और बैंकिंग धोखाधड़ी से सुरक्षा करता है।

निष्कर्ष:

- व्यापक सुधारों की शुरुआत कर और **'संचार साथी' पोर्टल तथा ASTR** जैसे तकनीकी उपकरणों का उपयोग करके विभाग ने धोखाधड़ी की गतिविधियों की प्रभावी ढंग से पहचान की है एवं उनके खिलाफ कार्रवाई की है।
- यह दृष्टिकोण सभी नागरिकों को एक सुरक्षित और विश्वसनीय संचार वातावरण प्रदान करने के सरकार के मिशन के अनुरूप है।

स्रोत: पी.आई.बी.

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/reforms-for-secure-digital-connectivity