भारत सरकार
गृह मंत्रालय
राज्य सभा
अतारांकित प्रश्न संख्या 228
दिनांक 27 नवम्बर, 2024/ 06 अग्रहायण, 1946 (शक) को उत्तर के लिए

'डिजिटल अरेस्ट' संबंधी धोखाधड़ी के मामले

228 डा. सुधांशु त्रिवेदीः

क्या गृह मंत्री यह बताने की कृपा करेंगे किः

(क) देश में 'डिजिटल अरेस्ट' संबंधी धोखाधड़ी के मामलों में हो रही चिंताजनक वृद्धि से निपटने के लिए क्या उपाय किए जा रहे हैं;
(ख) क्या मंत्रालय इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय के समन्वय से अपने आप को सरकारी और विधि प्रवर्तन अधिकारी बताने वाले फ़र्जी व्यक्तियों की पहचान करने और उन्हे गिरफ्तार करने के लिए कड़ी कार्रवाई करेगा;
(ग) मंत्रालय उन सभी सिम से किस प्रकार निपटने का विचार रखता है जिनका पता नहीं लगाया जा सकता और जिनके कारण धोखेबाज पीड़ितों को धोखा दे पाते हैं क्योकि ऐसे सिम का तत्काल पता लगाए जाने का जोखिम बहुत कम होता है; और
(घ) विभिन्न सोशल मीडिया पोर्टलों के माध्यम से संभावित धोखाधड़ी के बारे में उपयोगकर्ताओं को शिक्षित और सचेत करने के लिए क्या नई पहलें की गई हैं और किन-किन फर्जी कानून प्रवर्तन हैंडलों को निष्क्रिय कर दिया गया है?

उत्तर

गृह मंत्रालय में राज्य मंत्री
(श्री बंडी संजय कुमार)

(क) से (घ) : भारत के संविधान की सातवीं अनुसूची के अनुसार, 'पुलिस' और 'लोक व्यवस्था' राज्य के विषय हैं। राज्य/संघ राज्य क्षेत्र अपनी विधि प्रवर्तन एजेंसियों के माध्यम से साइबर अपराध और डिजिटल अरेस्ट घोटालों समेत अपराधों की रोकथाम करने, उनका पता लगाने, जाँच करने और अभियोजन चलाने के

लिए प्राथमिक रूप से जिम्मेदार हैं। केंद्र सरकार, राज्यों / संघ राज्य क्षेत्रों की विधि प्रवर्तन एजेंसियों (एलईए) के क्षमता संवर्धन के लिए उनके द्वारा किए जा रहे प्रयासों में एडवाइजरी और विभिन्न स्कीमों के अंतर्गत वित्तीय सहायता के माध्यम से सहायता प्रदान करती है।

केंद्र सरकार ने डिजिटल अरेस्ट समेत साइबर अपराधों से व्यापक और समन्वित ढंग से निपटने हेतु तंत्र को सुदृढ़ बनाने के लिए उपाय किए हैं, जिनमें अन्य बातों के साथ-साथ निम्नलिखित शामिल हैं:

i. गृह मंत्रालय ने देश में सभी प्रकार के साइबर अपराधों से समन्वित और व्यापक ढंग से निपटने के लिए एक संबद्ध कार्यालय के रूप में 'भारतीय साइबर अपराध समन्वय केंद्र' (आई4सी) स्थापित किया है।

ii. केंद्र सरकार और दूरसंचार सेवा प्रदाताओं (टीएसपी) ने एक ऐसी प्रणाली तैयार की है, जिसके तहत ऐसी फर्जी अंतर्राष्ट्रीय कॉलों की पहचान की जा सकेगी और उन्हें ब्लॉक किया जा सकेगा, जिनमें भारतीय मोबाइल नंबर प्रदर्शित होता है और जो भारत से आती हुई प्रतीत होती हैं। फर्जी डिजिटल गिरफ्तारियों, फेडेक्स घोटालों, सरकारी और पुलिस अधिकारी के रूप में छद्मवेश धारण करने आदि के हाल के मामलों में साइबर-अपराधियों द्वारा इस तरह की अंतर्राष्ट्रीय फर्जी कॉल की गई हैं। दूरसंचार सेवा प्रदाताओं को ऐसी आने वाली अंतर्राष्ट्रीय फर्जी कॉलों को ब्लॉक करने के निर्देश जारी किए गए हैं।

iii. आई4सी में एक अत्याधुनिक साइबर धोखाधड़ी शमन केंद्र (सीएफएमसी) स्थापित किया गया है, जहां प्रमुख बैंकों, वित्तीय मध्यस्थों, भुगतान एग्रीगेटर्स, दूरसंचार सेवा प्रदाताओं, आईटी मध्यस्थों और राज्यों/संघ राज्य क्षेत्रों की विधि प्रवर्तन एजेंसियों के प्रतिनिधि साइबर अपराध से निपटने के लिए तत्काल कार्रवाई और निर्बाध सहयोग के लिए साथ मिलकर काम कर रहे हैं।

iv. दिनांक 15.11.2024 तक पुलिस अधिकारियों द्वारा रिपोर्ट किए गए 6.69 लाख से अधिक सिम कार्ड और 1,32,000 आईएमईआईएस को भारत सरकार ने ब्लॉक कर दिया है।

v. समन्वय प्लेटफॉर्म (संयुक्त प्रबंधन सूचना प्रणाली) अप्रैल 2022 से कार्यरत है, जो साइबर अपराध संबंधी डेटा के आदान-प्रदान और विश्लेषण के लिए प्रबंधन सूचना प्रणाली (एमआईएस) प्लेटफॉर्म, डेटा भंडार और एलईए के लिए समन्वय मंच के रूप में कार्य करेगा। यह विभिन्न राज्यों/संघ राज्य क्षेत्रों में साइबर अपराध की शिकायतों में शामिल अपराधों और अपराधियों के अंतर्राज्यीय संबंधों

पर आधारित विश्लेषण प्रदान करता है। मॉड्यूल 'प्रतिबिंब' अपराधियों और अपराध संबंधी अवसंरचना के स्थानों को मानचित्र पर प्रदर्शित करता है, ताकि क्षेत्राधिकारियों को इसकी जानकारी मिल सके। यह मॉड्यूल विधि प्रवर्तन एजेंसियों द्वारा आई4सी और अन्य एसएमई (SMEs) से तकनीकी-कानूनी सहायता मांगने तथा प्राप्त करने की सुविधा भी प्रदान करता है।

vi. बैंकों/वित्तीय संस्थानों के सहयोग से आई4सी द्वारा दिनांक 10.09.2024 को साइबर अपराधियों की पहचान की एक संदिग्ध रजिस्ट्री शुरू की गई है।

vii. केंद्र सरकार ने https://cybercrime.gov.in पर 'रिपोर्ट एंड चेक सस्पेक्ट' नामक एक नई सुविधा शुरू की है। यह सुविधा नागरिकों को 'संदिग्ध खोज' के माध्यम से साइबर अपराधियों के पहचान संबंधी आई4सी के भंडार में खोजने के लिए एक खोज विकल्प प्रदान करती है।

viii. आई4सी डिजिटल गिरफ्तारी के लिए इस्तेमाल की गई फर्जी आईडी की सक्रिय रूप से पहचान कर उसे ब्लॉक करता है।

ix. केंद्र सरकार ने राज्य/संघ राज्य क्षेत्र पुलिस, एनसीबी, सीबीआई, आरबीआई और अन्य विधि प्रवर्तन एजेंसियों का छद्म भेष धारण करने वाले साइबर अपराधियों द्वारा 'ब्लैकमेल' और 'डिजिटल गिरफ्तारी' की घटनाओं के खिलाफ अलर्ट पर एक प्रेस विज्ञप्ति प्रकाशित की है।

x. राज्यों/संघ राज्य क्षेत्रों की विधि प्रवर्तन एजेंसियों के बीच समन्वय संबंधी कार्यढांचे को सुदृढ़ करने के लिए राज्यों/संघ राज्य क्षेत्रों को साथ लेकर साइबर अपराध संक्रेंद्रित स्थलों (हॉटस्पॉट)/ बहु-क्षेत्राधिकार संबंधी मुद्दों वाले क्षेत्रों के आधार पर, पूरे देश को कवर करते हुए मेवात, जामताड़ा, अहमदाबाद, हैदराबाद, चंडीगढ़, विशाखापत्तनम, और गुवाहाटी के लिए सात संयुक्त साइबर समन्वय टीमों (जेसीसीटी) का गठन किया गया है। जेसीसीटी के लिए सात कार्यशालाएं हैदराबाद, अहमदाबाद, गुवाहाटी, विशाखापत्तनम, लखनऊ, रांची और चंडीगढ़ में आयोजित की गईं।

xi. महिलाओं और बच्चों के प्रति साइबर अपराधों पर विशेष बल देते हुए, सभी प्रकार के साइबर अपराधों से संबंधित घटनाओं की सूचना देने में जनता को समर्थ बनाने हेतु आई4सी के भाग के रूप में 'राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल' (https://cybercrime.gov.in) शुरू किया गया है। इस पोर्टल पर सूचित की गई साइबर अपराध की घटनाओं, उन्हें एफआईआर में बदलने और उन पर आगे कार्रवाई से जुड़े कार्य राज्य/संघ राज्य क्षेत्र की संबंधित विधि प्रवर्तन एजेंसियों द्वारा कानून के प्रावधानों के अनुसार किए जाते हैं।

राज्य सभा अता.प्र.स. 228 दिनांक 27.11.2024

xii. वित्तीय धोखाधड़ियों की तत्काल सूचना देने और धोखाधड़ी करने वालों के द्वारा निधियों की चोरी को रोकने के लिए वर्ष 2021 में आई4सी के तहत 'नागरिक वित्तीय साइबर धोखाधड़ी रिपोर्टिंग और प्रबंधन प्रणाली' शुरू की गई है। अब तक 9.94 लाख से अधिक शिकायतों में 3431 करोड़ रुपये से अधिक की राशि को बचाया गया है। साइबर शिकायतों को ऑनलाइन दर्ज करने में सहायता प्राप्त करने के लिए एक टोल-फ्री हेल्पलाइन नम्बर '1930' शुरू किया गया है।

xiii. आई4सी ने भारत सरकार के विभिन्न मंत्रालयों/विभागों के 7,330 अधिकारियों को साइबर स्वच्छता प्रशिक्षण प्रदान किया है।

xiv. आई4सी ने 40,151 से अधिक एनसीसी कैडेटों को साइबर स्वच्छता प्रशिक्षण प्रदान किया है।

xv. केंद्र सरकार ने साइबर अपराध के बारे में जागरूकता बढ़ाने के लिए कई कदम उठाए हैं, जिनमें अन्य बातों के साथ-साथ एसएमएस, आई4सी सोशल मीडिया अकाउंट जैसे कि एक्स (पूर्व में ट्विटर) (@CyberDost), फेसबुक (CyberDostI4C), इंस्टाग्राम (cyberDostI4C), टेलीग्राम (cyberdosti4c), रेडियो कैंपेन के माध्यम से संदेश प्रसारित करना, कई माध्यमों से प्रचार हेतु माईगव का उपयोग करना, राज्यों/संघ राज्य क्षेत्रों के सहयोग से साइबर सुरक्षा एवं संरक्षा जागरूकता सप्ताह का आयोजन करना, किशोरों/ छात्रों के लिए हैंडबुक का प्रकाशन करना, डिजिटल गिरफ्तारी घोटाले पर अखबार में विज्ञापन, डिजिटल गिरफ्तारी और साइबर अपराधियों की अन्य कार्यप्रणालियों पर दिल्ली मेट्रो में उदघोषणा, डिजिटल गिरफ्तारी पर विशेष पोस्ट बनाने के लिए सोशल मीडिया प्रभावकारी व्यक्तियों (Influencers) का उपयोग, रेलवे स्टेशनों और हवाई अड्डों पर डिजिटल प्रदर्शन (Displays) आदि शामिल हैं।

*****