भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 2986

जिसका उत्तर 06 अगस्त, 2025 को दिया जाना है ।

15 श्रावण, 1947 (शक)

साइबर जागरूकता शिविर

2986. डॉ. सी. एन. मंजूनाथः

क्या इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्री यह बताने की कृपा करेंगे कि:

(क) क्या सरकार बेंगलुरु ग्रामीण संसदीय निर्वाचन क्षेत्र सहित ग्रामीण इंटरनेट उपयोगकर्ताओं को प्रभावित करने वाली ऑनलाइन धोखाधड़ी, फ़िशिंग हमलों और वित्तीय घोटालों को रोकने के लिए कोई सहायता प्रदान कर रही है औ यदि हाँ, तो तत्संबंधी ब्यौरा क्या है;

(ख) क्या राज्य पुलिस या जिला प्रशासन के साथ साझेदारी में कोई साइबर जागरूकता शिविर या शिकायत निवान प्रशिक्षण आयोजित किया गया है और यदि हाँ, तो तत्संबंधी व्यौरा क्या है; और

(ग) क्या सरकार का क्षेत्रीय भाषाओं में साइबर स्वच्छता पर एक स्थानीय जन जागरूकता अभियान शुरू करने का विचार है?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

(क) से **(ग):** सरकार ने सभी उपयोगकर्ताओं के लिए एक मुक्त, सुरक्षित, विश्वसनीय और जवाबदेह इंटरनेट सेवा सुनिश्चित करने के उद्देश्य से, साइबर धोखाधड़ी की रोकथाम और साइबर सुरक्षा जागरूकता को बढ़ावा देने के लिए कई पहल शुरू की हैं। सरकार साइबर खतरों और चुनौतियों के प्रति सजग और सतर्क है। सरकार ने निम्नलिखित प्रमुख पहल की हैं:

- इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय (एमईआईटीवाई) सूचना सुरक्षा के क्षेत्र में मानव संसाधन तैयार करने और आम जनता में साइबर स्वच्छता/साइबर सुरक्षा के विभिन्न पहलुओं पर सामान्य जागरूकता पैदा करने के लिए 'सूचना सुरक्षा शिक्षा एवं जागरूकता (आईएसईए)' परियोजना का कार्यान्वयन कर रहा है। जागरूकता घटक के अंतर्गत, बेंगलुरु ग्रामीण निर्वाचन क्षेत्र में 24 जागरूकता कार्यशालाएं आयोजित की गई हैं, जिनमें 1,644 प्रतिभागियों ने भाग लिया। इन जागरूकता कार्यशालाओं और www.staysafeonline.in तथा www.csk.gov.in जैसे पोर्टलों के माध्यम से साइबर स्वच्छता एवं साइबर सुरक्षा के विभिन्न पहलुओं पर हैंडबुक, लघु वीडियो, पोस्टर, ब्रोशर, बच्चों के लिए कार्टून कहानियां, परामर्श आदि के रूप में बहुभाषी जागरूकता सामग्री का प्रसार किया जा रहा है।
- इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय (एमईआईटीवाई) प्रत्येक वर्ष अक्तूबर माह के दौरान साइबर सुरक्षा जागरूकता माह (एनसीएसएएम), प्रत्येक वर्ष फरवरी माह के दूसरे मंगलवार को सुरक्षित इंटरनेट दिवस, प्रत्येक वर्ष 1 से 15 फरवरी तक स्वच्छता पखवाड़ा और प्रत्येक माह के पहले बुधवार को साइबर जागरूकता दिवस (सीजेडी) के रूप में नागरिकों के साथ-साथ भारत में तकनीकी साइबर समुदाय के लिए विभिन्न कार्यक्रमों और गतिविधियों का आयोजन किया जाता है।
- सर्ट-इन नवीनतम साइबर खतरों/कमजोरियों के बारे में चेतावनी और सलाह जारी करता है, जिसमें सोशल इंजीनियरिंग, फिशिंग और विशिंग अभियान शामिल हैं, तथा कंप्यूटर, मोबाइल फोन, नेटवर्क और डेटा की सुरक्षा के लिए निरंतर उपाय भी करता है।
- सर्ट-इन उपयोगकर्ताओं के लिए उनके डेस्कटॉप और मोबाइल फोन को सुरक्षित रखने तथा फ़िशिंग हमलों को रोकने के लिए सुरक्षा सुझाव प्रकाशित करता है।
- सर्ट-इन फ़िशिंग वेबसाइटों को ट्रैक करने और उन्हें निष्क्रिय करने तथा धोखाधड़ी गतिविधियों की जांच को सुविधाजनक बनाने के लिए सेवा प्रदाताओं, नियामकों और कानून प्रवर्तन एजेंसियों (एलईए) के समन्वय से कार्य कर रहा है।
- साइबर स्वच्छता केंद्र (सीएसके) सर्ट-इन द्वारा प्रदान की जाने वाली एक नागरिक-केंद्रित सेवा है, जो स्वच्छ भारत के दृष्टिकोण को साइबर स्पेस तक विस्तारित करता है। साइबर स्वच्छता केंद्र एक बॉटनेट क्लीनिंग और मैलवेयर विश्लेषण केंद्र है जो दुर्भावनापूर्ण प्रोग्रामों का पता लगाने में मदद करता है और

उन्हें हटाने के लिए निःशुल्क उपकरण प्रदान करता है। साथ ही नागरिकों और संगठनों के लिए साइबर सुरक्षा सुझाव और सर्वोत्तम परिपाटी भी प्रदान करता है।

- सर्ट-इन ने उपयोगकर्ताओं को साइबर सुरक्षा की सर्वोत्तम परिपाटियों और फ़िशिंग तथा साइबर धोखाधड़ी अभियानों के विरुद्ध उठाए जा सकने वाले उपायों के बारे में शिक्षित करने के लिए जागरूकता कार्यक्रम आयोजित किए हैं।
- सर्ट-इन नियमित रूप से अपनी आधिकारिक वेबसाइटों और सोशल मीडिया हैंडल जैसे फेसबुक, ट्विटर, इंस्टाग्राम, यूट्यूब और लिंक्डइन के माध्यम से सुरक्षा संबंधी सुझाव, जागरूकता पोस्टर, इन्फोग्राफिक्स, पुस्तिकाएं और वीडियो साझा कर रहा है, ताकि इंटरनेट उपयोगकर्ताओं को साइबर सुरक्षा हमलों और धोखाधड़ी तथा रोकथाम के उपायों के बारे में जागरूक किया जा सके।
- गृह मंत्रालय (एमएचए) ने देश में सभी प्रकार के साइबर अपराधों से समन्वित और व्यापक तरीके से निपटने के लिए एक संबद्ध कार्यालय के रूप में 'भारतीय साइबर अपराध समन्वय केंद्र' (आई4सी) की स्थापना की है।
- साइबर अपराध के बारे में जागरूकता प्रसारित करने के लिए, गृह मंत्रालय ने कई कदम उठाए हैं, जिनमें अन्य बातों के साथ-साथ; एसएमएस, आई4सी सोशल मीडिया अकाउंट अर्थात् एक्स (पूर्व में ट्विटर) (@साइबरदोस्त), फेसबुक (साइबरदोस्तआई4सी), इंस्टाग्राम (साइबरदोस्तआई4सी), टेलीग्राम (साइबरदोस्ती4सी), एसएमएस अभियान, टीवी अभियान, रेडियो अभियान, स्कूल अभियान, सिनेमा हॉल में विज्ञापन, सेलिब्रिटी समर्थन, आईपीएल अभियान, कुंभ मेला 2025 के दौरान अभियान, मन की बात, कॉलर ट्यून, कई माध्यमों में प्रचार के लिए माईगव को समनुदेशित करना, राज्यों/संघ राज्य-क्षेत्रों के सहयोग से साइबर सुरक्षा और सुरक्षा जागरूकता सप्ताह का आयोजन, किशोरों/छात्रों के लिए हैंडबुक का प्रकाशन, डिजिटल गिरफ्तारी घोटाले पर समाचार पत्र विज्ञापन, डिजिटल गिरफ्तारी और साइबर अपराधियों के अन्य तौर-तरीकों पर दिल्ली महानगरों में घोषणा, डिजिटल गिरफ्तारी पर विशेष पोस्ट बनाने के लिए सोशल मीडिया प्रभावितों का उपयोग, रेलवे स्टेशनों और हवाई अड्डों पर डिजिटल डिस्प्ले आदि शामिल हैं।
- I4C ने दूरसंचार विभाग (डीओटी) के साथ मिलकर साइबर अपराध के बारे में जागरूकता बढ़ाने और साइबर अपराध हेल्पलाइन नंबर 1930 और एनसीआरपी पोर्टल को बढ़ावा देने के लिए 19.12.2024 से कॉलर ट्यून अभियान शुरू किया है।
- दूरसंचार विभाग (डीओटी) ने अपने एआई और फेशियल रिकॉग्निशन आधारित दूरसंचार सिम ग्राहक सत्यापन समाधान (एएसटीआर) टूल के माध्यम से उन मोबाइल कनेक्शनों का पता लगाया, जो जाली दस्तावेजों के माध्यम से प्राप्त किए गए थे।
- दूरसंचार विभाग ने हितधारकों के बीच दूरसंचार संसाधनों के दुरुपयोग से संबंधित जानकारी साझा करने के लिए एक ऑनलाइन सुरक्षित डिजिटल इंटेलिजेंस प्लेटफ़ॉर्म (डीआईपी) विकसित किया है। दूरसंचार विभाग और दूरसंचार सेवा प्रदाताओं (टीएसपी) ने भारतीय मोबाइल नंबरों वाले आने वाले अंतर्राष्ट्रीय नकली कॉलों की पहचान करने और उन्हें ब्लॉक करने के लिए सेंट्रलाइज्ड इंटरनेशनल आउटरोमर रजिस्टर (सीआईओआर) नामक एक प्रणाली विकसित की है।
- दूरसंचार विभाग ने मानव संसाधन कौशल के उन्नत क्षमता निर्माण और एआई एवं बिग डेटा एनालिटिक्स टूल्स के विकास के माध्यम से दूरसंचार संसाधनों के दुरुपयोग को रोकने के लिए ईकोसिस्टम विकसित किया है, जिसमें एएसटीआर, सीआईओआर और डीआईपी शामिल हैं। इसके अलावा, संचार साथी, एक नागरिक केंद्रित पहल शुरू की गई है, जो वेब पोर्टल और मोबाइल ऐप के माध्यम से सुलभ है और नागरिकों को संदिग्ध धोखाधड़ी संचार की रिपोर्ट करने, उनके नाम पर मोबाइल कनेक्शन जानने, खोए/चोरी हुए मोबाइल हैंडसेट की रिपोर्ट करने आदि की सुविधा प्रदान करती है। इसके अलावा, वित्तीय धोखाधड़ी जोखिम संकेतक (एफआरआई) विकसित किया गया है, जो एक जोखिम-आधारित मेट्रिक है, जो मोबाइल नंबर को वित्तीय धोखाधड़ी के मध्यम, उच्च या बहुत उच्च जोखिम से संबद्ध के रूप में वर्गीकृत करता है। एफआरआई हितधारकों-विशेषकर बैंकों, गैर-बैंकिंग वित्तीय कंपनियों (एनबीएफसी), और एकीकृत भुगतान इंटरफेस (यूपीआई) सेवा प्रदाताओं को प्रवर्तन को प्राथमिकता देने और मोबाइल नंबर के उच्च जोखिम होने की स्थिति में अतिरिक्त ग्राहक सुरक्षा उपाय करने के लिए सशक्त बनाता है।
- आरबीआई और बैंक लघु एसएमएस, रेडियो अभियान, 'साइबर अपराध' की रोकथाम पर प्रचार आदि के माध्यम से जागरूकता अभियान भी चला रहे हैं। आरबीआई ने मनी म्यूल की पहचान के लिए कृत्रिम बुद्धिमता (एआई) आधारित टूल 'म्यूल हंटर' लॉन्च किया है और बैंकों और वित्तीय संस्थानों को इसके उपयोग के बारे में सलाह दी है।
- इसके अतिरिक्त, एनपीसीआई सभी बैंकों को एआई/एमएल आधारित मॉडलों का उपयोग करके अलर्ट जारी करने और लेनदेन को अस्वीकार करने के लिए धोखाधड़ी निगरानी समाधान प्रदान करता है।

*****