भारत सरकार
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
लोक सभा
अतारांकित प्रश्न संख्या2624
जिसका उत्तर 11 दिसंबर, 2024 को दिया जाना है ।
20 अग्रहायण, 1946 (शक)

साइबर खतरों के बारे में जागरूकता

2624.श्री राम प्रसाद चौधरी:

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

(क) क्या सरकार को इस बात की जानकारी है कि अविश्वासनीय घोटालों को अंजाम देने के लिए साइबर अपराधी तेजी से होते जा रहे हैं और वे डीपफेक प्रौद्योगिकी, कृत्रिम आसूचना (एआई) और सोशल इंजीनियरिंग/वेबसाइटों का लाभ उठा रहे हैं; और

(ख) यदि हां, तो सरकार द्वारा साइबर खतरों के बारे में जागरूकता बढ़ाने, सुरक्षित ऑनलाइन व्यवहार को बढ़ावा देने और संगठनों को उभरते डिजिटल जोखिमों से निपटने के लिए आवश्यक उपकरणों से लैस करने के लिए क्या कदम उठाए गए हैं/उठाए जा रहे हैं?

उत्तर
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

(क) और **(ख):** सरकार की नीतियों का उद्देश्य अपने उपयोगकर्ताओं के लिए एक खुला, सुरक्षित, विश्वसनीय और जवाबदेह इंटरनेट सुनिश्चित करना है। सरकार उभरती प्रौद्योगिकियों के कारण होने वाले विभिन्न साइबर सुरक्षा खतरों के बारे में पूरी तरह से जागरूक और सजग है। देश की साइबर सुरक्षा स्थिति को मजबूत करने के लिए, सरकार ने साइबर खतरों के बारे में जागरूकता बढ़ाने और सुरक्षित ऑनलाइन व्यवहार को बढ़ावा देने के लिए कई प्रमुख पहल की हैं, जिनमें अन्य बातों के साथ-साथ निम्नलिखित भी शामिल हैं:

i. भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन) को सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70ख के प्रावधानों के तहत साइबर सुरक्षा घटनाओं पर प्रतिक्रिया देने के लिए राष्ट्रीय एजेंसी के रूप में नामित किया गया है।

ii. सर्ट-इन द्वारा कार्यान्वित राष्ट्रीय साइबर समन्वय केंद्र (एनसीसीसी) देश में साइबरस्पेस को स्कैन करने और साइबर सुरक्षा खतरों का पता लगाने के लिए नियंत्रण कक्ष के रूप में कार्य करता है। एनसीसीसी साइबर सुरक्षा खतरों का शमन करने के लिए कार्रवाई करने के लिए साइबरस्पेस से मेटाडेटा साझा करके विभिन्न एजेंसियों के बीच समन्वय की सुविधा प्रदान करता है।

iii. 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 साथ समन्वय से कार्य करता है।

iv. 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 करती है। साइबर स्वच्छता केंद्र बॉटनेट क्लीनिंग और मैलवेयर विश्लेषण केंद्र है और दुर्भावनापूर्ण कार्यक्रमों का पता लगाने में मदद करता है और उन्हें हटाने के लिए निःशुल्क उपकरण प्रदान करता है, और नागरिकों और संगठनों के लिए साइबर सुरक्षा युक्तियाँ और सर्वोत्तम अभ्यास भी प्रदान करता है।

v. भारतीय रिजर्व बैंक के माध्यम से सर्ट-इन ने देश में प्रीपेड भुगतान उपकरण (वॉलेट) जारी करने वाली सभी अधिकृत संस्थाओं और बैंकों को सर्ट-इन के पैनलबद्ध लेखा परीक्षकों द्वारा विशेष लेखा परीक्षा कराने, लेखा परीक्षा रिपोर्ट में पहचाने गए गैर-अनुपालनों को बंद करने और सुरक्षा संबंधी सर्वोत्तम प्रथाओं का कार्यान्वयन सुनिश्चित करने की सलाह दी है।

vi. सर्ट-इन ने सूचना सुरक्षा सर्वोत्तम प्रथाओं के कार्यान्वयन का समर्थन और लेखापरीक्षा करने के लिए 155 सुरक्षा लेखापरीक्षा संगठनों को सूचीबद्ध किया है।

vii. साइबर सुरक्षा स्थिति और संगठनों की तैयारियों का आकलन करने तथा सरकारी और महत्वपूर्ण क्षेत्रों में लचीलापन बढ़ाने के लिए साइबर सुरक्षा मॉक ड्रिल नियमित रूप से आयोजित की जाती हैं।

viii. सर्ट-इन, सूचना प्रौद्योगिकी अवसंरचना की सुरक्षा और साइबर हमलों को कम करने के संबंध में सरकारी, सार्वजनिक और निजी क्षेत्र के संगठनों के नेटवर्क और सिस्टम प्रशासकों और सीआईएसओ के लिए नियमित प्रशिक्षण कार्यक्रम आयोजित करता है।

ix. कंप्यूटर सुरक्षा घटना प्रतिक्रिया दल-वित्त क्षेत्र (सीएसआईआरटी-फिन) की स्थापना सर्ट-इन के तत्वावधान और मार्गदर्शन में वित्तीय क्षेत्र से रिपोर्ट की गई साइबर सुरक्षा घटनाओं पर प्रतिक्रिया देने, उन्हें रोकने और कम करने के लिए की गई है।

x. सर्ट-इन एक स्वचालित साइबर खतरा आसूचना आदान-प्रदान मंच संचालित करता है, जो सक्रिय रूप से विभिन्न क्षेत्रों के संगठनों के साथ चेतावनियाँ एकत्रित करने, उनका विश्लेषण करने और साझा करने के लिए कार्य करता है, ताकि वे सक्रिय रूप से खतरा न्यूनीकरण कार्रवाई कर सकें।

xi. सर्ट-इन ने अप्रैल 2022 में सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70ख की उपधारा (6) के तहत सुरक्षित एवं विश्वसनीय इंटरनेट के लिए सूचना सुरक्षा पद्धतियाँ, प्रक्रिया, रोकथाम, साइबर घटनाओं की रिपोर्टिंग और प्रतिक्रिया से संबंधित साइबर सुरक्षा निर्देश जारी किए।

xii. सर्ट-इन आर्टिफिशियल इंटेलिजेंस का उपयोग करके सोशल इंजीनियरिंग, फ़िशिंग और विशिंग अभियानों सहित नवीनतम साइबर खतरों/सुभेद्धताओं के बारे में चेतावनियाँ और परामर्शी निदेश जारी करता है और कंप्यूटर, नेटवर्क और डेटा की सुरक्षा के लिए निरंतर आधार पर प्रतिउपाय करता है। इस संदर्भ में, आर्टिफिशियल इंटेलिजेंस (एआई) आधारित अनुप्रयोगों से उत्पन्न होने वाले प्रतिकूल खतरों का शमन करने के लिए किए जाने वाले सुरक्षा उपायों पर एक परामर्शी निदेश मई 2023 में प्रकाशित किया गया था।

xiii. सर्ट-इन ने जून 2023 में सरकारी संस्थाओं के लिए सूचना सुरक्षा प्रथाओं पर दिशानिर्देश जारी किए, जिसमें डेटा सुरक्षा, नेटवर्क सुरक्षा, पहचान और अभिगम प्रबंधन, एप्लिकेशन सुरक्षा, तृतीय-पक्ष आउटसोर्सिंग, सख्त प्रक्रियाएं, सुरक्षा निगरानी, घटना प्रबंधन और सुरक्षा ऑडिटिंग जैसे डोमेन शामिल हैं।

xiv. सर्ट-इन ने नवंबर 2023 में विभिन्न मंत्रालयों को एक परामर्शी निदेश जारी किया, जिसमें संवेदनशील व्यक्तिगत डेटा या सूचना सहित डिजिटल व्यक्तिगत डेटा या सूचना का प्रसंस्करण करने वाली सभी संस्थाओं द्वारा साइबर सुरक्षा को मजबूत करने के लिए किए जाने वाले प्रतिउपायों की रूपरेखा बताई गई।

xv. सर्ट-इन ने नवंबर 2024 में डीपफेक खतरों और डीपफेक से सुरक्षित रहने के लिए अपनाए जाने वाले प्रतिउपायों पर एक परामर्शी निदेश प्रकाशित किया है।

xvi. राष्ट्रीय सूचना विज्ञान केन्द्र (एनआईसी) विभिन्न ई-गवर्नेंस समाधानों के लिए केन्द्र सरकार, राज्य सरकारों और जिला प्रशासकों के मंत्रालयों, विभागों और एजेंसियों को सूचना प्रौद्योगिकी (आईटी) सहायता प्रदान करता है और साइबर हमलों को रोकने और डेटा की सुरक्षा के उद्देश्य से उद्योग मानकों और प्रथाओं के अनुरूप सूचना सुरक्षा नीतियों और प्रथाओं का पालन करता है।

xvii. इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय सूचना सुरक्षा जागरूकता पैदा करने के लिए कार्यक्रम आयोजित करता है। साइबर स्वच्छता और डीपफेक सहित साइबर सुरक्षा के विभिन्न पहलुओं पर हैंडबुक, लघु वीडियो, पोस्टर, ब्रोशर, बच्चों के लिए कार्टून कहानियां, परामर्शी निदेश आदि के रूप में जागरूकता सामग्री www.staysafeonline.in, www.infosecawareness.in और www.csk.gov.in जैसे पोर्टलों के माध्यम से प्रसारित की जाती है ।

xviii. गृह मंत्रालय (एमएचए) ने सभी प्रकार के साइबर अपराधों से निपटने के लिए भारतीय साइबर अपराध समन्वय केंद्र (आई4सी) की स्थापना की है। एमएचए ने सभी प्रकार के साइबर अपराधों की रिपोर्ट करने में जनता को सक्षम बनाने के लिए राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल

(https://cybercrime.gov.in) लॉन्च किया है। नागरिकों को अपनी भाषा में ऑनलाइन शिकायत दर्ज करने में सहायता प्राप्त करने के लिए एक टोल-फ्री नंबर 1930 चालू किया गया है।

****