भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

राज्य सभा

अतारांकित प्रश्न संख्या 3439

जिसका उत्तर 01 अप्रैल, 2022 को दिया जाना है।

11 चैत्र, 1944 (शक)

राष्ट्रीय साइबर सुरक्षा नीति

3439. श्री विशम्भर प्रसाद निषाद:
डा. एल. हनुमंतय्या:
श्री राम नाथ ठाकुर:
श्री जी.सी. चन्द्रशेखर:
चौधरी सुखराम सिंह यादव:
श्रीमती छाया वर्मा:
श्रीमती फूलो देवी नेतम:

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

(क) क्या सरकार हाल ही में राष्ट्रीय सुरक्षा को खतरे में डालने वाले साइबर हमलों को देखते हुए एक नई राष्ट्रीय साइबर सुरक्षा नीति शुरू करने की योजना बना रही है;
(ख) यदि हां, तो तत्संबंधी ब्यौरा क्या है और इसके कार्यान्वयन के लिए प्रस्तावित समय-सीमा क्या है और यदि नहीं तो इसके क्या कारण हैं;
(ग) क्या सरकार ने साइबर हमलों के प्रति नागरिकों की सुभेद्यता को कम करने के लिए कोई कदम उठाए हैं;
(घ) यदि हां, तो तत्संबंधी ब्यौरा क्या है और यदि नहीं, तो इसके क्या कारण हैं;
(ड) क्या सरकार साइबर आतंकवाद पर वैश्विक कानूनी ढांचा विकसित करने के लिए अन्य देशों के साथ समन्वय स्थापित करने की मंशा रखती है; और
(च) यदि हां, तो तत्संबंधी ब्यौरा क्या है और यदि नहीं, तो इसके क्या कारण हैं?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री राजीव चंद्रशेखर)

(क) और (ख): राष्ट्रीय सुरक्षा परिषद सचिवालय (एनएससीएस) ने राष्ट्रीय साइबर सुरक्षा रणनीति 2021 (एनसीएसएस2021) का मसौदा तैयार किया है जो समग्र रूप से राष्ट्रीय साइबर स्पेस की सुरक्षा के मुद्दों को संबोधित करता है।

(ग) और (घ): सरकार यह सुनिश्चित करने के लिए प्रतिबद्ध है कि भारत में इंटरनेट सभी उपयोगकर्ताओं के लिए खुला, सुरक्षित और विश्वसनीय और जवाबदेह हो। सरकार विभिन्न साइबर सुरक्षा खतरों से पूरी तरह अवगत और जागरूक है; और साइबर हमलों के प्रति नागरिकों की संवेदनशीलता को कम करने के लिए निम्नलिखित उपाय किए हैं:

i. सर्ट-इन डिजिटल प्रौद्योगिकियों के सुरक्षित उपयोग को सुनिश्चित करने के लिए नियमित आधार पर नवीनतम साइबर खतरों और प्रति-उपायों के संबंध में अलर्ट और सलाह जारी करता है। सर्ट-इन ने डेटा सुरक्षा और धोखाधड़ी गतिविधियों को कम करने के लिए 68 परामर्श जारी किए हैं।

ii. उपयोगकर्ताओं के लिए उनके डेस्कटॉप, मोबाइल/स्मार्ट फोन को सुरक्षित करने और फ़िशिंग हमलों को रोकने के लिए सुरक्षा युक्तियाँ प्रकाशित की जाती हैं।

iii. सर्ट-इन साइबर स्वच्छता केंद्र (बॉटनेट सफाई और मालवेयर विश्लेषण केंद्र) प्रचालित करता है। केंद्र विद्वेषपूर्णकार्यक्रमों का पता लगाने और उन्हें हटाने के लिए नि:शुल्क उपकरण प्रदान करता है।

iv. सर्ट-इन एक स्वचालित साइबर थ्रेट एक्सचेंज प्लेटफॉर्म का प्रचालन सक्रिय खतरे को कम करने की कार्रवाई के लिए विभिन्न क्षेत्रों के संगठनों के साथ सक्रिय रूप से चेतावनियां एकत्रित करने, विश्लेषण करने और साझा करने के लिए करता है।

v. सरकार ने अनुप्रयोगों/बुनियादी ढांचे को सुरक्षित करने और अनुपालन के लिए मुख्य सूचना सुरक्षा अधिकारियों (सीआईएसओ) की प्रमुख भूमिकाओं और जिम्मेदारियों के संबंध में दिशानिर्देश जारी किए हैं।

vi. सर्ट-इन आईटी अवसंरचना को सुरक्षित करने और साइबर हमलों को कम करने के संबंध में सरकार और महत्वपूर्ण क्षेत्र के संगठनों के नेटवर्क/सिस्टम प्रशासकों और मुख्य सूचना सुरक्षा अधिकारियों (सीआईएसओ) के लिए नियमित प्रशिक्षण कार्यक्रम आयोजित करता है। वर्ष 2020 और 2021 के दौरान क्रमशः 708 और 5169 प्रतिभागियों को शामिल करते हुए कुल 15 और 19 प्रशिक्षण कार्यक्रम आयोजित किए गए।

vii. साइबर खतरों का मुकाबला करने के लिए खतरे के परिदृश्य और सर्वोत्तम प्रथाओं पर जागरूकता पैदा करने के लिए सर्ट-इन द्वारा वरिष्ठ प्रबंधन और मुख्य सूचना सुरक्षा अधिकारियों (सीआईएसओ) के लिए नियमित रूप से टेबल टॉप अभ्यास आयोजित किए जाते हैं। फरवरी, 2022 तक सर्ट-इन द्वारा जागरूकता निर्माण के लिए सरकारी और सार्वजनिक क्षेत्र के संगठनों को शामिल करते हुए 24 ऐसे टेबल टॉप अभ्यास किए गए।

viii. सर्ट-इन ने उद्योग और शिक्षा जगत के सहयोग से देश में नागरिकों के साथ-साथ तकनीकी साइबर समुदाय के लिए विभिन्न कार्यक्रमों और गतिविधियों के आयोजन के माध्यम से अक्टूबर 2021 के दौरान साइबर सुरक्षा जागरूकता माह मनाया। जागरूकता अभियान, वीडियो और पोस्टर प्रकाशित करना और साइबर सुरक्षा प्रश्नोत्तरी सहित गतिविधियों को पूरी तरह से ऑनलाइन प्रशिक्षण प्लेटफॉर्म और सोशल मीडिया चैनलों पर आयोजित किया जाता है।

ix. सर्ट-इन ने 8 फरवरी 2022 को अपने आधिकारिक सोशल मीडिया हैंडल और वेबसाइटों के माध्यम से साइबर सुरक्षा जागरूकता अभियान चलाकर 'सुरक्षित इंटरनेट दिवस' मनाया।

x. इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय (एमईआईटीवाई) सूचना सुरक्षा जागरूकता पैदा करने के लिए कार्यक्रम आयोजित करता है। सूचना सुरक्षा के बारे में बच्चों, माता-पिता और सामान्य उपयोगकर्ताओं के लिए विशिष्ट पुस्तकें, वीडियो और ऑनलाइन सामग्री विकसित की जाती हैं, जिन्हें "www.infosecawareness.in" और "www.csk.gov.in" जैसे पोर्टलों के माध्यम से प्रसारित किया जाता है।

xi. भारतीय रिजर्व बैंक (आरबीआई) ने इलेक्ट्रॉनिक/डिजिटल लेनदेन से संबंधित सुरक्षा और जोखिम कम करने के प्रतिउपायों के संबंध में विभिन्न निर्देश जारी किए हैं जिसमें कार्ड लेनदेन सुरक्षित करना, इंटरनेट बैंकिंग/इलेक्ट्रॉनिक भुगतान, एटीएम लेनदेन, प्रीपेड भुगतान उपकरण (पीपीआई), अनधिकृत इलेक्ट्रॉनिक बैंकिंग लेनदेन पर ग्राहक दायित्व को सीमित करना, अधिकृत गैर-बैंकों द्वारा जारी किए गए पीपीआई में अनधिकृत इलेक्ट्रॉनिक बैंकिंग लेनदेन में ग्राहक देयता को सीमित करना, ईमेल स्पूफिंग हमलों से सुरक्षा आदि के माध्यम से भुगतान सुरक्षित करना शामिल है।

(ड.) और (च): इस मंत्रालय के पास ऐसी कोई सूचना उपलब्ध नहीं है ।

****