भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 644

जिसका उत्तर 06 दिसम्बर, 2023 को दिया जाना है ।

15 अग्रहायण, 1945 (शक)

साइबर हमला

644. श्री मनोज तिवारी:
डॉ. निशिकांत दुबे:
श्री रवनीत सिंह:

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

(क) क्या यह सही है कि साइबर हमले देश की डिजिटल अवसंरचना के लिए आसन्न खतरा हैं;
(ख) यदि हां, तो नागरिकों के डाटा की सुरक्षा सुनिश्चित करने हेतु ऐसे साइबर हमलों को रोकने के लिए सरकार द्वारा किए गए उपायों सहित तत्संबंधी ब्यौरा क्या है;
(ग) क्या सरकार देश की डिजिटल सुरक्षा को सुदृढ़ करने के लिए अन्य देशों और अंतर्राष्ट्रीय विशेषज्ञों के सहयोग से कार्य कर रही है; और
(घ) यदि हां, तो तत्संबंधी ब्यौरा क्या है?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री राजीव चंद्रशेखर)

(क) और (ख) सरकार की नीतियों का उद्देश्य अपने प्रयोक्ताओं के लिए एक खुला, सुरक्षित और विश्वसनीय तथा जवाबदेह इंटरनेट सुनिश्चित करना है। इंटरनेट प्रौद्योगिकी और इंटरनेट को बेहतरी के लिए शक्ति के रूप में देखा जाता था, लेकिन हाल के वर्षों में, उपयोगकर्ता को नुकसान पहुंचाने और आपराधिकता पैदा करने के लिए प्रौद्योगिकी का भी शोषण किया जाता है। भारत में इंटरनेट उपयोगकर्ताओं की संख्या आज 88 करोड़ से बढ़कर वर्ष 2026 तक 120 करोड़ उपयोगकर्ता होने की उम्मीद है।

सरकार विभिन्न साइबर सुरक्षा खतरों और चुनौतियों से पूरी तरह अवगत है और नागरिकों की डेटा सुरक्षा सुनिश्चित करने के लिए साइबर हमलों को रोकने के लिए विभिन्न उपाय किए हैं।

एमईआईटीवाई ने हितधारकों के साथ व्यापक परामर्श के बाद 6 अप्रैल 2023 को सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश और डिजिटल मीडिया आचार संहिता) संशोधन नियमों को अधिसूचित किया। ये नियम डिजिटल नागरिकों के लिए एक खुला, सुरक्षित और विश्वसनीय और जवाबदेह इंटरनेट सुनिश्चित करने के लिए ऑनलाइन गेम के संबंध में ऑनलाइन गेमिंग और सोशल मीडिया मध्यस्थों द्वारा अत्यधिक सम्यक सावधानी बरतने के लिए लागू किए जाते हैं। इसके अलावा, सरकार ने साइबर हमलों को रोकने के लिए निम्नलिखित प्रतिउपाय किए हैं:

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

(ii) एमईआईटीवाई ने साइबर सुरक्षा लेखा परीक्षा के लिए दिशा-निर्देश जारी किए हैं जिसमें सक्षम लेखा परीक्षकों द्वारा आवधिक आधार पर व्यापक और सीमित लेखा परीक्षा दोनों को शामिल किया गया है, जिसमें नियमित रूप से इस तरह की लेखा परीक्षा सुनिश्चित करने के लिए स्पष्ट जिम्मेदारियां हैं, जिसमें सुभेद्यता मूल्यांकन और प्रवेश परीक्षण शामिल हैं।

(iii) भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन) निरंतर आधार पर कंप्यूटरों और नेटवर्कों की सुरक्षा के लिए नवीनतम साइबर खतरों/सुभेद्यताओं और प्रतिउपायों के बारे में अलर्ट और परामर्शी निदेश जारी करता है।

(iv) उपयोगकर्ताओं के लिए अपने डेस्कटॉप और मोबाइल फोन को सुरक्षित करने और फ़िशिंग हमलों को रोकने के लिए सुरक्षा युक्तियाँ प्रकाशित की गई हैं।

(v) सर्ट-इन दुर्भावनापूर्ण कार्यक्रमों का पता लगाने के लिए साइबर स्वच्छता केंद्र (बॉटनेट क्लीनिंग एंड मैलवेयर एनालिसिस सेंटर) संचालित करता है और इसे हटाने के लिए मुफ्त उपकरण प्रदान करता है, और नागरिकों और संगठनों के लिए साइबर सुरक्षा युक्तियां और सर्वोत्तम प्रथाएं भी प्रदान करता है।

(vi) सर्ट-इन विभिन्न क्षेत्रों के संगठनों के साथ सक्रिय खतरे को कम करने की कार्रवाइयों के लिए सक्रिय रूप से एकत्रित करने, विश्लेषण करने और साझा करने के लिए एक स्वचालित साइबर-खतरा विनिमय मंच संचालित करता है।

(vii) सर्ट-इन ने मौजूदा और संभावित साइबर सुरक्षा खतरों के बारे में स्थितिजन्य जागरूकता पैदा करने के लिए राष्ट्रीय साइबर समन्वय केंद्र की स्थापना की है।

(viii) सर्ट-इन ने केंद्र सरकार के सभी मंत्रालयों और विभागों, राज्य सरकारों और उनके संगठनों और महत्वपूर्ण क्षेत्रों द्वारा कार्यान्वयन के लिए साइबर हमलों और साइबर आतंकवाद का मुकाबला करने के लिए एक साइबर संकट प्रबंधन योजना तैयार की है।

(ix) साइबर सुरक्षा मॉक ड्रिल साइबर सुरक्षा की स्थिति और सरकार और महत्वपूर्ण क्षेत्रों में संगठनों की तैयारी का आकलन करने में सक्षम बनाने के लिए आयोजित किए जाते हैं। सर्ट-इन द्वारा अब तक ऐसे 86 अभ्यास आयोजित किए गए हैं, जिनमें विभिन्न राज्यों और क्षेत्रों के 1159 संगठनों ने भाग लिया है।

(x) सर्ट-इन ने सूचना सुरक्षा सर्वोत्तम प्रथाओं के कार्यान्वयन का समर्थन और लेखा परीक्षा करने के लिए 177 सुरक्षा लेखा परीक्षा संगठनों को सूचीबद्ध किया है।

(xi) सर्ट-इन नियमित रूप से सूचना प्रसारित करता है और अपने आधिकारिक सोशल मीडिया हैंडल और वेबसाइटों के माध्यम से साइबर सुरक्षा और संरक्षा पर सुरक्षा युक्तियां साझा करता है। सर्ट-इन ने दिनांक 7.02.2023 को सुरक्षित इंटरनेट दिवस और अक्टूबर 2023 में साइबर सुरक्षा जागरूकता माह के दौरान सोशल मीडिया प्लेटफार्मों और वेबसाइटों पर पोस्टर और वीडियो का उपयोग करके सुरक्षा युक्तियों को पोस्ट करके नागरिकों के लिए विभिन्न कार्यक्रमों और गतिविधियों का आयोजन किया। सर्ट-इन ने सेंटर फॉर डेवलपमेंट ऑफ एडवांस्ड कंप्यूटिंग के साथ मिलकर

नागरिकों के लिए एक ऑनलाइन जागरूकता अभियान चलाया, जिसमें सामान्य ऑनलाइन सुरक्षा, सोशल मीडिया जोखिम और सुरक्षा, मोबाइल से संबंधित धोखाधड़ी और सुरक्षा, सुरक्षित डिजिटल भुगतान प्रथाओं आदि जैसे विषयों को शामिल किया गया।

(xii) सर्ट-इन और भारतीय रिजर्व बैंक (आरबीआई) संयुक्त रूप से डिजिटल इंडिया प्लेटफॉर्म के माध्यम से 'वित्तीय धोखाधड़ी से सावधान रहें और जागरूक रहें' विषय पर साइबर सुरक्षा जागरूकता अभियान चलाते हैं।

(xiii) सर्ट-इन सूचना प्रौद्योगिकी 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 2021 और 2022 के दौरान 11,486 प्रतिभागियों को शामिल करते हुए कुल 42 प्रशिक्षण कार्यक्रम आयोजित किए गए हैं। वर्ष 2023 में, अक्टूबर तक, सरकारी, महत्वपूर्ण क्षेत्रों, सार्वजनिक और निजी क्षेत्र के कुल 7007 अधिकारियों को साइबर सुरक्षा के क्षेत्र में 21 प्रशिक्षण कार्यक्रमों में प्रशिक्षित किया गया है।

(xiv) राष्ट्रीय सूचना विज्ञान केंद्र (एनआईसी) विभिन्न ई-गवर्नेंस समाधानों के लिए केंद्र सरकार, राज्य सरकारों और जिला प्रशासन के उपयोगकर्ता मंत्रालयों, विभागों और एजेंसियों को आईटी सहायता प्रदान करता है और इसके हिस्से के रूप में, नागरिकों के डेटा वाले विभिन्न सरकारी डेटाबेस को बनाए रखने में मदद करता है। एनआईसी उद्योग मानकों और पद्धतियों के अनुरूप सूचना सुरक्षा नीतियों और प्रथाओं का पालन करता है, जिसका उद्देश्य साइबर हमलों को रोकना और डेटा की सुरक्षा करना है।

(xv) दूरसंचार विभाग साइबर हमलों और भारतीय दूरसंचार नेटवर्क के लिए खतरों की निगरानी करता है और उनका पता लगाता है, जिसमें विदेशों से शुरू किए गए खतरे भी शामिल हैं, और आवश्यक कार्रवाई के लिए हितधारकों को समय पर अलर्ट प्रदान करता है।

(xvi) महत्वपूर्ण सूचना अवसंरचना की सुरक्षा और ऐसे बुनियादी ढांचे से संबंधित साइबर घटनाओं पर प्रतिक्रिया देने के लिए राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र की स्थापना की गई है। केंद्र लगभग वास्तविक समय में खतरा आसूचना और स्थितिजन्य जागरूकता प्रदान करता है, जिसके आधार पर ऐसे बुनियादी ढांचे से संबंधित संस्थाओं को नियमित अलर्ट और अनुरूप परामर्शी निदेश भेजे जाते है।

(xvii) गृह मंत्रालय के तहत भारतीय साइबर अपराध समन्वय केंद्र (I4सी) को साइबर अपराध से निपटने हेतु नोडल बिंदु के रूप में नामित किया गया है। नागरिकों को अपनी भाषा में ऑनलाइन शिकायत दर्ज करने में सहायता प्राप्त करने के लिए एक टोल-फ्री नंबर 1930 चालू है। साइबर अपराध पर जागरूकता फैलाने के लिए, मंत्रालय ने कई कदम उठाए हैं, जिनमें ट्विटर हैंडल @cyberDost और रेडियो अभियानों के माध्यम से साइबर अपराध पर संदेशों का प्रसार शामिल है।

(xviii) भारतीय रिजर्व बैंक ने इलेक्ट्रॉनिक/डिजिटल लेन-देन से संबंधित सुरक्षा और जोखिम न्यूनीकरण उपायों के संबंध में विभिन्न अनुदेश जारी किए हैं। इनमें कार्ड लेनदेन को सुरक्षित करना, इंटरनेट बैंकिंग / इलेक्ट्रॉनिक भुगतान, एटीएम लेनदेन के माध्यम से भुगतान सुरक्षित करना, प्री-पेड भुगतान उपकरण (पीपीआई), अनधिकृत इलेक्ट्रॉनिक बैंकिंग लेनदेन (अधिकृत गैर-बैंकों द्वारा जारी पीपीआई सहित) पर ग्राहक देयता को सीमित करना, ईमेल स्पूफिंग हमलों से सुरक्षा करना आदि शामिल हैं।

(ग) और (घ) साइबर स्पेस सीमारहित है और इसलिए अन्य देशों के साथ सहयोग और भागीदारी अपेक्षित है। सरकार भारत की साइबर सुरक्षा स्थिति को सुदृढ़ करने और सभी डिजिटल नागरिकों की सुरक्षा सुनिश्चित करने के लिए अन्य देशों की सरकारों, निजी कंपनियों और स्टार्ट-अप सहित भागीदारों के साथ काम करने के लिए प्रतिबद्ध है। साइबर सुरक्षा के मुद्दों से प्रभावी ढंग से निपटने के लिए हितधारकों के साथ सहयोग को सुदृढ़ करने के लिए निम्नलिखित कार्रवाई की गई है:

(i) सर्ट-इन ने साइबर सुरक्षा के क्षेत्र में सहयोग के लिए अपनी विदेशी समकक्ष एजेंसियों के साथ समझौता ज्ञापन (एमओयू) के रूप में सहयोग व्यवस्था की है। वर्तमान में बांग्लादेश, ब्राजील, मिस्र, एस्टोनिया, जापान, मालदीव, नाइजीरिया, रूसी संघ, यूनाइटेड किंगडम, उजबेकिस्तान और वियतनाम के साथ इस तरह के समझौता ज्ञापन (एमओयू) पर हस्ताक्षर किए गए हैं।

(ii) सर्ट-इन अंतर्राष्ट्रीय सर्ट, विदेशी संगठनों और सेवा प्रदाताओं के साथ-साथ कानून प्रवर्तन एजेंसियों के साथ घटना प्रतिक्रिया उपायों का सहयोग, कार्य और समन्वय भी करता है।

(iii) सर्ट-इन एशिया पैसिफिक कंप्यूटर इमरजेंसी रिस्पांस टीमों का एक परिचालन सदस्य है, जो एशिया-प्रशांत क्षेत्र में इंटरनेट सुरक्षा के लिए एक क्षेत्रीय मंच है।

(iv) सर्ट-इन साइबर सुरक्षा दलों के लिए एक वैश्विक मंच, फोरम ऑफ इंसिडेंट रिस्पांस एंड सिक्योरिटी टीम्स (एफ़आईआरएसटी) का सदस्य है।

(v) सर्ट-इन कंप्यूटर सुरक्षा घटना प्रतिक्रिया दलों/ विश्वसनीय परिचयकर्ता के लिए टास्क फोर्स का एक मान्यता प्राप्त सदस्य है। यह अन्य पक्षों को संकेत देता है कि सर्ट-इन परिपक्वता और कार्यक्षमता के एक निश्चित स्तर तक पहुंच गया है, जो सर्ट समुदाय के भीतर विश्वास बढ़ाने के लिए अत्यधिक महत्वपूर्ण है।

****