भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 3075

जिसका उत्तर 19 मार्च, 2025 को दिया जाना है

28 फाल्गुन, 1946 (शक)

राष्ट्रीय साइबर सुरक्षा रणनीति

3075. श्री गुरजीत सिंह औजला:

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

(क) क्या सरकार साइबर खतरों से प्रभावी ढंग से निपटने और डिजिटल बुनियादी ढांचे की सुरक्षा के लिए एक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति तैयार करने और उसे लागू करने के लिए ठोस कदम उठा रही है;

(ख) यदि हां, तो इसका ब्यौरा क्या है और इसके प्रमुख फोकस क्षेत्र क्या हैं और यदि ऐसी कोई रणनीति नहीं है, तो इसका उद्देश्य किस तरह से बढ़ती साइबर धोखाधड़ी और डेटा सुरक्षा चिंताओं को दूर करना है;

(ग) बढ़ती साइबर धोखाधड़ी से निपटने के लिए भारत के साइबर सुरक्षा ढांचे को मजबूत करने और साइबर रक्षा तंत्र को बढ़ाने के लिए सरकार द्वारा क्या उपाय किए गए हैं;

(घ) वित्तीय साइबर अपराधों, ओटीपी धोखाधड़ी और ऑनलाइन घोटालों पर अंकुश लगाने के लिए सरकार द्वारा क्या कदम उठाए गए हैं; और

(ङ) क्या सरकार यह मानती है कि हमारे नागरिकों की बढ़ती डिजिटल निर्भरता को देखते हुए नागरिकों की सुरक्षा के लिए एक सक्रिय और मजबूत साइबर सुरक्षा नीति की तत्काल आवश्यकता है और यदि हां, तो इसका ब्यौरा क्या है और इस संबंध में क्या कार्रवाई की गई है?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

(क), (ख) और (ङ): सरकार की नीतियों का उद्देश्य अपने उपयोगकर्ताओं के लिए एक खुला, सुरक्षित और विश्वसनीय और जवाबदेह इंटरनेट सुनिश्चित करना है। सरकार ने देश में साइबर सुरक्षा चुनौतियों का सामना करने के लिए कई कानूनी, तकनीकी और प्रशासनिक नीतिगत उपाय किए हैं। सरकार ने देश में साइबर सुरक्षा मामलों से निपटने के लिए एक राष्ट्रव्यापी एकीकृत और समन्वित प्रणाली को भी संस्थागत रूप दिया है, जिसमें अन्य बातों के साथ-साथ निम्नलिखित भी शामिल हैं:

i. विभिन्न एजेंसियों के बीच समन्वय सुनिश्चित करने के लिए राष्ट्रीय सुरक्षा परिषद सचिवालय (एनएससीएस) के अंतर्गत राष्ट्रीय साइबर सुरक्षा समन्वयक (एनसीएससी) की स्थापना की गई है।

ii. सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70ख के प्रावधानों के अंतर्गत भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट-इन) को साइबर सुरक्षा घटनाओं पर प्रतिक्रिया करने के लिए राष्ट्रीय एजेंसी के रूप में नामित किया गया है।

iii. सर्ट-इन द्वारा कार्यान्वित राष्ट्रीय साइबर समन्वय केंद्र (एनसीसीसी) देश में साइबर स्पेस को स्कैन करने और साइबर सुरक्षा खतरों का पता लगाने के लिए नियंत्रण कक्ष के रूप में कार्य करता है। एनसीसीसी साइबर सुरक्षा खतरों को कम करने के लिए कार्रवाई करने हेतु साइबरस्पेस से मेटाडेटा साझा करके विभिन्न एजेंसियों के बीच समन्वय की सुविधा प्रदान 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 बोटनेट क्लीनिंग और मैलवेयर विश्लेषण केंद्र है और दुर्भावनापूर्ण कार्यक्रमों का पता लगाने में मदद करता है और इसे हटाने के लिए मुफ्त उपकरण प्रदान करता है, और नागरिकों और संगठनों के लिए साइबर सुरक्षा युक्तियाँ और सर्वोत्तम अभ्यास भी प्रदान करता है।

v. गृह मंत्रालय (एमएचए) ने समन्वित और प्रभावी तरीके से साइबर अपराधों से निपटने के लिए भारतीय साइबर अपराध समन्वय केंद्र (आई 4सी) बनाया है।

vi. सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000 की धारा 70क के प्रावधानों के अंतर्गत सरकार ने देश में महत्वपूर्ण सूचना मूलसंरचना के संरक्षण के लिए राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र (एनसीआईआईपीसी) की स्थापना की है।

सुरक्षित और लचीला साइबर स्पेस सुनिश्चित करने के लिए, प्राथमिक फोकस राष्ट्रीय साइबरस्पेस को सुरक्षित करने, लोगों, प्रक्रियाओं और क्षमताओं से युक्त मौजूदा संरचनाओं को मजबूत करने और देश में डिजिटल पर्यावरण की रक्षा के लिए उनके इष्टतम उपयोग हेतु संसाधनों का तालमेल करने के तीन स्तंभों पर है।

(ग) और (घ) : सरकार ने वित्तीय साइबर अपराधों पर अंकुश लगाने सहित भारत के साइबर सुरक्षा ढांचे को सुदृढ़ करने और साइबर धोखाधड़ी को रोकने के लिए निम्नलिखित उपाय किए हैं, जिनमें अन्य बातों के साथ-साथ निम्नलिखित भी शामिल हैं:

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

ii. सर्ट-इन ने जून 2023 में सरकारी संस्थाओं के लिये सूचना सुरक्षा पद्धतियों पर दिशानिर्देश जारी किए, जिसमें डेटा सुरक्षा, नेटवर्क सुरक्षा, पहचान और पहुँच प्रबंधन, एप्लिकेशन सुरक्षा, तृतीय-पक्षकार आउटसोर्सिंग, सख्त प्रक्रियाएँ, सुरक्षा निगरानी, घटना प्रबंधन और सुरक्षा लेखा परीक्षा जैसे डोमेन शामिल हैं।

iii. सर्ट-इन ने सितंबर 2023 में सुरक्षित एप्लिकेशन डिज़ाइन, विकास और कार्यान्वयन और संचालन के लिए दिशानिर्देश जारी किए। सर्ट-इन ने अक्टूबर 2024 में संस्थाओं, विशेष रूप से सार्वजनिक क्षेत्र, सरकारी क्षेत्र, आवश्यक सेवाओं, सॉफ्टवेयर निर्यात और सॉफ्टवेयर सेवा उद्योग में शामिल संगठनों के लिए सॉफ्टवेयर बिल ऑफ मैटेरियल्स (एसबीओएम) दिशानिर्देश भी जारी किए हैं ताकि संगठनों को यह जानने में मदद मिल सके कि उनके सॉफ़्टवेयर या संपत्ति में कौन से घटक हैं, जिससे सुभेद्यताओं की पहचान करना और उन्हें ठीक करना आसान हो जाता है।

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

v. सर्ट-इन नवीनतम साइबर खतरों/सुभेद्यताओं के संबंध में चेतावनियां और परामर्शी निदेश जारी करता है तथा कम्प्यूटरों, मोबाइल फोनों, नेटवर्कों और आंकड़ों की सतत आधार पर सुरक्षा करने के लिए प्रतिउपाय करता है।

vi. सर्ट-इन फिशिंग वेबसाइटों को ट्रैक और अक्षम करने और धोखाधड़ी गतिविधियों की जांच को सुविधाजनक बनाने के लिए सेवा प्रदाताओं, नियामकों और कानून प्रवर्तन एजेंसियों (एलईए) के साथ समन्वय हेतु कार्य करता है।

vii. कंप्यूटर सुरक्षा घटना प्रतिक्रिया दल-वित्त क्षेत्र (सीएसआईआरटी-फिन) की स्थापना सर्ट-इन के व्यापक क्षेत्र और मार्गदर्शन के तहत वित्तीय क्षेत्र से रिपोर्ट की गई साइबर सुरक्षा घटनाओं पर प्रतिक्रिया देने और उन्हें नियंत्रित करने और कम करने के लिए की गई है।

viii. एनसीआईआईपीसी साइबर हमलों और साइबर आतंकवाद से निवारक उपाय करने के लिए महत्वपूर्ण सूचना अवसंरचना (सीआईआई)/संरक्षित प्रणाली (पीएस) वाले संगठनों को खतरे की आसूचना, स्थितिजन्य जागरूकता, चेतावनियां और परामर्शी निदेश और सुभेद्धताओं पर जानकारी प्रदान करता है।

ix. सर्ट -इन एक स्वचालित साइबर थ्रेट इंटेलिजेंस एक्सचेंज प्लेटफॉर्म संचालित करता है जो सक्रिय रूप से सभी क्षेत्रों में संगठनों के साथ चेतावनियां एकत्रित करने, विश्लेषण करने और साझा करने के लिए उनके द्वारा सक्रिय खतरे को कम करने हेतु है।

x. सर्ट-इन ने सूचना सुरक्षा सर्वोत्तम पद्धतियों के कार्यान्वयन का समर्थन और लेखा परीक्षा करने हेतु 200 सुरक्षा लेखा परीक्षा संगठनों को सूचीबद्ध किया है।

xi. साइबर सुरक्षा मॉक ड्रिल नियमित रूप से आयोजित की जाती है ताकि साइबर सुरक्षा की स्थिति और संगठनों की तैयारी का मूल्यांकन किया जा सके और सरकार और महत्वपूर्ण क्षेत्रों में लचीलापन बढ़ाया जा सके। सर्ट -इन द्वारा अब तक 109 ऐसे अभ्यास आयोजित किए गए हैं जिनमें विभिन्न राज्यों और क्षेत्रों के 1438 संगठनों ने भाग लिया।

xii. सर्ट-इन सूचना प्रौद्योगिकी अवसंरचना की सुरक्षा और साइबर हमलों को कम करने के संबंध में नेटवर्क और प्रणाली प्रशासकों तथा सरकारी और महत्वपूर्ण क्षेत्र के संगठनों के मुख्य सूचना सुरक्षा अधिकारियों के लिए नियमित प्रशिक्षण कार्यक्रम आयोजित करता है। वर्ष 2024 में 23 प्रशिक्षण कार्यक्रमों में कुल 12,014 अधिकारियों को प्रशिक्षित किया गया है।

xiii. सर्ट-इन साइबर हमलों और साइबर धोखाधड़ी के संबंध में जागरूकता और नागरिकों को संवेदनशील बनाने के लिए नियमित रूप से विभिन्न गतिविधियां चला रहा है।

xiv. राष्ट्रीय सूचना विज्ञान केन्द्र (एनआईसी) सुभेद्धताओं को समाप्त करने और वैश्विक सुरक्षा मानकों तथा हार्डवेयर के सुभेद्यता मूल्यांकन का अनुपालन सुनिश्चित करने के लिए सर्ट-इन-पैनलबद्ध एजेंसियों के माध्यम से सरकारी वेबसाइटों और अनुप्रयोगों की आवधिक सुरक्षा लेखापरीक्षा अधिदेशित करता है जिन पर ऐसे अनुप्रयोग होस्ट किए जाते हैं।

xv. एनआईसी विभिन्न ई-शासन समाधानों के लिए केंद्र 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।

xvi. एनआईसी ने सरकारी नेटवर्क से संबद्ध सुरक्षा मुद्दों की पहचान करने के लिए खतरा आसूचना प्लेटफार्म सहित उन्नत सुरक्षा तंत्र संस्थापित किए हैं।

xvii. इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय सूचना सुरक्षा जागरूकता पैदा करने के लिए कार्यक्रम आयोजित करता है। डीपफेक सहित साइबर स्वच्छता और 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 ने व्यापक और समन्वित तरीके से साइबर अपराधों से निपटने के लिए एलईए के लिए एक ढांचा और इकोसिस्टम प्रदान करने के लिए एक संलग्न कार्यालय के रूप में भारतीय साइबर अपराध समन्वय केंद्र (आई4सी) की स्थापना की है। एमएचए ने सभी प्रकार के साइबर अपराधों की रिपोर्ट करने के लिए जनता को सक्षम करने हेतु राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (https://cybercrime.gov.in) भी लॉन्च किया है। इस पोर्टल पर रिपोर्ट की गई साइबर अपराध की घटनाओं को कानून के प्रावधानों के अनुसार आगे की कार्रवाई के लिए संबंधित राज्य/केंद्र शासित प्रदेश कानून प्रवर्तन एजेंसी को स्वचालित रूप से भेज दिया जाता है। वित्तीय धोखाधड़ी की तत्काल रिपोर्टिंग और धोखेबाजों द्वारा निधि की हेराफेरी को रोकने के लिए 'नागरिक वित्तीय साइबर धोखाधड़ी रिपोर्टिंग और प्रबंधन प्रणाली' शुरू की गई है।

xix. आई4सी में साइबर फ्रॉड मिटिगेशन सेंटर (सीएफएमसी) की स्थापना की गई है, जहां प्रमुख बैंकों, वित्तीय मध्यस्थों, भुगतान एग्रीगेटर्स, दूरसंचार सेवा प्रदाताओं, आईटी मध्यस्थों के प्रतिनिधि और राज्यों/केंद्र शासित प्रदेशों की कानून प्रवर्तन एजेंसी के

प्रतिनिधि साइबर अपराध से निपटने के लिए तत्काल कार्रवाई और निर्बाध सहयोग के लिए मिलकर काम कर रहे हैं। वित्तीय संस्थानों को एक साथ लाकर, सीएफएमसी का उद्देश्य विभिन्न वित्तीय क्षेत्रों में धोखाधड़ी संबंधी निधि के प्रसार को रोककर साइबर वित्तीय धोखाधड़ी का पता लगाना, रोकना और शमन करना है।

xx. गृह मंत्रालय ने जन जागरूकता पैदा करने के लिए राष्ट्रीय साइबर अपराध रिपोटग पोर्टल (https://cybercrime.gov.in) और टोल-फ्री हेल्पलाइन नंबर 1930 का प्रचार करने के लिए सभी राज्य/केंद्र शासित प्रदेश सरकारों को परामर्शी निदेश जारी किए है।

xxi. दूरसंचार विभाग ने दूरसंचार क्षेत्र के भीतर एक सुरक्षा घटना के लिए प्रतिक्रिया के प्रदर्शन, समन्वय और समर्थन के लिए दिनांक 03.08.2022 को दूरसंचार साइबर सुरक्षा घटना प्रतिक्रिया (टी-सीएसआईआरटी), क्षेत्रीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सीईआरटी) के लिए रूपरेखा जारी की। इसकी समीक्षा की गई है और दिनांक 31.01.2023 को जारी किया गया है।

xxii. भारतीय रिज़र्व बैंक (आरबीआई) ने विनियमित संस्थाओं अर्थात (i) वाणिज्यिक बैंकों (क्षेत्रीय ग्रामीण बैंकों सहित) और अखिल भारतीय वित्तीय संस्थाओं के लिए धोखाधड़ी जोखिम प्रबंधन; (ii) सहकारी बैंक (शहरी सहकारी बैंक/राज्य सहकारी बैंक/केन्द्रीय सहकारी बैंक); और (iii) गैर-बैंकिंग वित्त कंपनियों (आवास वित्त कंपनियों सहित) को दिनांक 15.07.2024 को प्रारंभिक चेतावनी संकेतों (ईडब्ल्यूएस) पर ढांचे को मजबूत करने के लिए, अन्य बातों के साथ-साथ, गैर-केवाईसी अनुपालन और निधि निहित खातों आदि में लेनदेन/असामान्य गतिविधियों की निगरानी करने के लिए, अनधिकृत/धोखाधड़ी लेनदेन को रोकने हेतु मास्टर निर्देश जारी किए हैं।

xxiii. भारतीय रिजर्व बैंक ने आरबीआई कहता है के माध्यम से जनता में जागरूकता पैदा करने के लिए डिजिटल भुगतान लेन-देन के दौरान और विज्ञापन (प्रमुख व्यक्तियों के माध्यम से) आदि के माध्यम से किए जाने वाले विभिन्न प्रकार की धोखाधड़ियों, तौर-तरीकों और प्रतिउपायों जैसे पहलुओं पर जागरूकता सामग्री/उपयोगी सूचना जारी की है।

xxiv. भारतीय रिजर्व बैंक ने जनता को शिक्षित करने के लिए सार्वजनिक क्षेत्र में वित्तीय धोखाधड़ियों की कार्य-प्रणाली पर पुस्तिका बी(अ)वेयर जारी की है।

*****