भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 410

जिसका उत्तर 24 जुलाई, 2024 को दिया जाना है।

2 श्रावण, 1946 (शक)

साइबर धोखाधड़ी

410. श्री के. सी. वेणुगोपालः

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

(क) क्या सरकार साइबर धोखाधड़ी की बढ़ती घटनाओं के प्रति जागरूक है;

(ख) यदि हां, तो तत्संबंधी ब्यौरा क्या है;

(ग) क्या सरकार ने धोखाधड़ी के जोखिम को कम करने के लिए कोई विशिष्ट पहल की है या नीतियां बनाई हैं;

(घ) क्या साइबर धोखाधड़ी के पीड़ितों के लिए मौजूदा निवारण तंत्र प्रभावी है;

(ङ) यदि हां, तो तत्संबंधी ब्यौरा क्या है;

(च) क्या सरकार ने साइबर धोखाधड़ी से निपटने के लिए कानून प्रवर्तन और निजी क्षेत्र की संस्थाओं के साथ सहयोग स्थापित किया है; और

(छ) यदि हां, तो तत्संबंधी ब्यौरा क्या है?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

(क) से (छ): गृह मंत्रालय के अनुसार, वित्तीय धोखाधड़ियों की तत्काल सूचना देने और धोखेबाजों से निधियों की हेराफेरी को रोकने के लिए नागरिक वित्तीय साइबर धोखाधड़ी रिपोर्टिंग और प्रबंधन प्रणाली शुरू की गई थी। अब तक 7.6 लाख से अधिक शिकायतों में 2,400 करोड़ रुपये से अधिक की वित्तीय राशि धोखाधड़ी से बचाई गई है।

भारत के संविधान की सातवीं अनुसूची के अनुसार 'पुलिस' और 'लोक व्यवस्था' राज्य के विषय हैं। राज्य/संघ राज्य क्षेत्र साइबर धोखाधड़ी सहित अपराधों की रोकथाम करने, उनका पता लगाने, जांच और अभियोजन के लिए अपनी विधि प्रवर्तन एजेंसियों (एलईए) के माध्यम से प्राथमिक रूप से जिम्मेदार हैं। केन्द्र सरकार राज्यों/संघ राज्य क्षेत्रों की क्षमता के निर्माण के लिए विभिन्न स्कीमों के अंतर्गत परामर्शी पत्रों और वित्तीय सहायता के माध्यम से उनकी पहलों में सहायता करती है।

सरकार ने डिजिटल प्रौद्योगिकियों के सुरक्षित उपयोग के लिए और साइबर धोखाधड़ी को रोकने के लिए संगठनों और उपयोगकर्ताओं के बीच जागरूकता बढ़ाने के लिए निम्नलिखित उपाय किए हैं :

1. सरकार ने व्यापक और समन्वित तरीके से साइबर अपराधों से निपटने के लिए एलईए के लिए एक ढांचा और ईको-सिस्टम उपलब्ध कराने के लिए गृह मंत्रालय के तहत भारतीय साइबर अपराध समन्वय केंद्र (14सी) की स्थापना की है। सरकार ने सभी प्रकार के साइबर अपराधों के बारे में सूचना देने के क्रम में जनता को सक्षम बनाने के लिए राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (https://cybercrime.gov.in) शुरू किया है, इस पोर्टल पर घटनाओं की दी गई सूचना पर विशेष ध्यान देने के साथ कानून के प्रावधानों के अनुसार आगे की कार्रवाई के लिए संबंधित राज्य/संघ राज्य क्षेत्र विधि प्रवर्तन एजेंसी को स्वचालित रूप से भेज दिया जाता है।
2. वित्तीय धोखाधड़ी की तत्काल रिपोर्टिंग और धोखेबाजों से धन की हेराफेरी को रोकने के लिए 'नागरिक वित्तीय साइबर धोखाधड़ी रिपोर्टिंग और प्रबंधन प्रणाली' शुरू की गई थी। ऑनलाइन साइबर शिकायतें दर्ज करने में सहायता प्रदान करने के लिए एक टोल-फ्री हेल्पलाइन नंबर '1930' शुरू किया गया है।
3. साइबर अपराधों से व्यापक और समन्वित तरीके से निपटने के लिए तंत्र को सुदृढ़ करने के लिए, केन्द्र सरकार ने साइबर अपराधों के बारे में जागरूकता फैलाने के लिए कदम उठाए हैं; अलर्ट/सलाह जारी करना; कानून प्रवर्तन कर्मियों/अभियोजकों/न्यायिक अधिकारियों की क्षमता निर्माण/प्रशिक्षण; साइबर फॉरेंसिक सुविधाओं आदि में सुधार करना।
4. गृह मंत्रालय ने साइबर अपराध के बारे में जागरूकता फैलाने के लिए अनेक कदम उठाए हैं जिनमें अन्य बातों के साथ-साथ अलर्ट/एडवाइजरी जारी करना, एसएमएस के माध्यम से संदेशों का प्रसार करना, आई4सी सोशल मीडिया अकाउंट अर्थात ट्विटर हैंडल (@Cyberdost), फेसबुक (साइबरदोस्तआई4सी), इंस्टाग्राम (साइबरदोस्तआई4सी), टेलीग्राम (साइबरदोस्तआई4सी), रेडियो अभियान चलाना, बहु-मीडिया में प्रचार के लिए माईगव को शामिल करना, किशोरों/छात्रों के लिए हैंडबुक का प्रकाशन करना, विभिन्न राज्यों/संघ राज्य क्षेत्रों आदि में नीति विभाग के सहयोग से साइबर सुरक्षा और सुरक्षा जागरूकता सप्ताह का आयोजन करना शामिल है। गृह मंत्रालय ने जन जागरूकता पैदा करने के लिए राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (https://cybercrime.gov.in) और टोल-फ्री हेल्पलाइन नंबर 1930 का प्रचार करने के लिए सभी राज्य/संघ राज्य क्षेत्र की सरकारों को सलाह जारी की है।
5. भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट-इन) हाल ही के साइबर खतरों/कमजोरियों के संबंध में चेतावनियां और सलाह जारी करता है तथा कम्प्यूटरों, मोबाइल फोनों, नेटवर्कों और आंकड़ों की सतत् आधार पर सुरक्षा करने के लिए उपाय करता है।
6. सर्ट-इन फिशिंग वेबसाइटों को ट्रैक और अक्षम करने और धोखाधड़ी संबंधी गतिविधियों की जांच को सुविधाजनक बनाने के लिए सेवा प्रदाताओं, नियामकों और कानून प्रवर्तन एजेंसियों (एलईए) के साथ समन्वय का काम करता है।

7. सर्ट-इन ने विभिन्न मंत्रालयों को एक सलाह जारी की है। इस सलाह द्वारा उन सभी संस्थाओं की साइबर सुरक्षा को सुदृढ़ करने के लिए किए जाने वाले उपायों की रूपरेखा दी गई है जो संवेदनशील व्यक्तिगत डेटा या सूचना सहित डिजिटल व्यक्तिगत डेटा या सूचना को प्रोसेस कर रहे हैं।

8. सर्ट-इन द्वारा आरबीआई के माध्यम से देश में प्री-पेड भुगतान लिखत (वॉलेट) जारी करने वाली सभी प्राधिकृत कंपनियों और बैंकों को सर्ट-इन-पैनलबद्ध लेखा परीक्षकों द्वारा विशेष लेखा परीक्षा करने, लेखा परीक्षा रिपोर्ट में चिन्हित गैर-अनुपालनाओं को बंद करने और सुरक्षा सर्वोत्तम प्रथाओं का कार्यान्वयन सुनिश्चित करने की सलाह दी गई है।

9. सर्ट-इन ने सूचना सुरक्षा सर्वोत्तम पद्धतियों के कार्यान्वयन में सहायता करने के साथ-साथ लेखा परीक्षा करने के लिए 176 सुरक्षा लेखा परीक्षा संगठनों को सूचीबद्ध किया है।

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

11. सर्ट-इन सक्रियतापूर्वक इन खतरों को कम करने के लिए सभी क्षेत्रों में संगठनों के साथ अलर्ट एकत्र करने, विश्लेषण करने और साझा करने के लिए एक ऑटोमेटेड साइबर थ्रेट एक्सचेंज प्लेटफॉर्म का संचालन करता है।

12. सर्ट-इन विद्वेषपूर्ण कार्यक्रमों का पता लगाने के लिए साइबर स्वच्छता केंद्र (बोटनेट क्लीनिंग एंड मालवेयर एनालिसिस सेंटर) संचालित करता है और इसे हटाने के लिए मुफ्त उपकरण प्रदान करता है, और नागरिकों और संगठनों के लिए साइबर सुरक्षा युक्तियाँ और सर्वोत्तम प्रविधियां उपलब्ध कराता है।

13. सर्ट-इन ने साइबर हमलों और साइबर आतंकवाद का सामना करने के लिए एक साइबर संकट प्रबंधन योजना तैयार की है जिसका कार्यान्वयन केन्द्र सरकार के सभी मंत्रालयों/विभागों, राज्य सरकारों और उनके संगठनों तथा महत्वपूर्ण क्षेत्रों द्वारा किया जाएगा।

14. साइबर सुरक्षा पोश्चर और सरकार तथा महत्वपूर्ण क्षेत्रों में संगठनों की तैयारी का मूल्यांकन करने के लिए साइबर सिक्योरिटी मॉक ड्रिल आयोजित किए जाते हैं। सर्ट-इन द्वारा अबतक 92 ऐसे मॉक ड्रिल किए गए हैं जिनमें विभिन्न राज्यों/क्षेत्रों के लगभग 1400 संगठनों ने हिस्सा लिया है।

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

16. सर्ट -इन वित्तीय क्षेत्र से सूचित की गई साइबर सुरक्षा घटनाओं का जवाब देने, उन्हें नियंत्रित करने के लिए और कम करने के लिए अपनी सुरक्षा के अंतर्गत कंप्यूटर सुरक्षा घटना प्रतिक्रिया टीम-वित्त क्षेत्र (सीएसआईआरटी-फिन) संचालन के लिए नेतृत्व प्रदान करता है।

17. सर्ट-इन साइबर सुरक्षा के संकेन्द्रित विषयों पर सभी क्षेत्रों में सरकारी, सार्वजनिक और निजी क्षेत्र के संगठनों के अधिकारियों को प्रशिक्षित करने के लिए नियमित रूप से प्रशिक्षण/कार्यशालाएं आयोजित करता है। 2024 के दौरान, जून तक, सीईआरटी-इन ने साइबर सुरक्षा के विभिन्न विशिष्ट विषयों पर 9 प्रशिक्षण आयोजित किए हैं, जिसमें सिस्टम/नेटवर्क प्रशासक और मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) सहित 4,166 प्रतिभागी शामिल हुए हैं।

18. सर्ट-इन, नेशनल इंस्टीट्यूट ऑफ सिक्योरिटीज मार्केट्स और सेंटर फॉर डेवलपमेंट ऑफ एडवांस्ड कंप्यूटिंग (सी-डैक) वित्तीय क्षेत्र में पेशेवरों के लिए 60 घंटे का प्रमाणन साइबर सुरक्षा फाउंडेशन कोर्स आयोजित करते हैं।

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

20. सर्ट-इन नियमित रूप से साइबर हमलों और साइबर धोखाधड़ी के संबंध में जागरूकता और नागरिक सूचना के लिए विभिन्न गतिविधियां आयोजित करता है।

21. 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।

22. इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय सूचना सुरक्षा जागरूकता पैदा करने के लिए कार्यक्रम आयोजित करता है। सूचना सुरक्षा के बारे में पुस्तकें, वीडियो और ऑनलाइन सामग्री सामान्य उपयोगकर्ताओं, बच्चों और माता-पिता के लिए तैयार की जाती हैं, और www.infosecawareness.in और www.csk.gov.in जैसे पोर्टलों के माध्यम से प्रसारित की जाती हैं।

*****