भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 1458

जिसका उत्तर 31 जुलाई, 2024 को दिया जाना है।

9 श्रावण, 1946 (शक)

व्यक्तिगत डेटा माइनिंग और फिशिंग

1458. श्री मनीष जायसवालः

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

(क) क्या सरकार को असामाजिक तत्वों द्वारा व्यक्तिगत आंकड़ों की 'माइनिंग' और 'फिशिंग' गतिविधियों की बढ़ती घटनाओं की जानकारी है;

(ख) यदि हां, तो सरकार द्वारा झारखंड सहित देश में इन गतिविधियों को रोकने और नागरिकों के व्यक्तिगत आंकड़ों की सुरक्षा करने के लिए क्या उपाय किए गए हैं;

(ग) उक्त गतिविधियों के शिकार होने से बचने के लिए, 'डेटा माइनिंग' और 'फिशिंग' के जोखिमों के बारे में जन जागरूकता बढ़ाने के लिए क्या कदम उठाए गए हैं;

(घ) क्या झारखंड में हाल में 'डेटा माइनिंग' और 'फिशिंग' के मामले रिपोर्ट किए गए हैं;

(ङ) यदि हां, तो तत्संबंधी ब्यौरा क्या है और दोषियों के विरुद्ध क्या कार्रवाई की गई है; और

(च) सरकार द्वारा देश भर में साइबर सुरक्षा उपायों को बढ़ाने और व्यक्तिगत 'डेटा माइनिंग' और 'फिशिंग' गतिविधियों को रोकने के लिए क्या भावी योजनाएं प्रस्तावित की गई हैं?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

(क) से (च): सरकार की नीतियों का उद्देश्य सभी उपयोगकर्ताओं के लिए खुला, सुरक्षित, विश्वसनीय और जवाबदेह इंटरनेट सुनिश्चित करना है। सरकार ने झारखंड सहित पूरे देश में खतरों से बचाव और नागरिकों के व्यक्तिगत डेटा की सुरक्षा के लिए कई उपाय किए हैं। इन उपायों में शामिल ये हैं:

i. गृह मंत्रालय ने बच्चों के खिलाफ साइबर अपराध सहित सभी प्रकार के साइबर अपराधों से समन्वित और व्यापक तरीके से निपटने के लिए भारतीय साइबर अपराध समन्वय केंद्र (I4सी) की स्थापना की है। नागरिकों को अपनी भाषा में ऑनलाइन शिकायत दर्ज करने में सहायता प्रदान करने के लिए एक टोल-फ्री नंबर 1930 चालू किया गया है। गृह मंत्रालय ने साइबर अपराध के बारे में जागरूकता फैलाने के लिए कई कदम उठाए हैं, जिसमें ट्विटर हैंडल @CyberDost और रेडियो अभियानों के माध्यम से साइबर अपराध पर संदेशों का प्रसार शामिल है।

ii. भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम (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 के साथ समन्वय करती है।

iii. सर्ट-इन कंप्यूटर, मोबाइल फोन, नेटवर्क और डेटा की सुरक्षा के लिए नवीनतम साइबर खतरों/कमजोरियों और प्रतिउपायों के संबंध में निरंतर अलर्ट और सलाह जारी करता है।

iv. सर्ट-इन ने विभिन्न मंत्रालयों को एक परामर्श जारी किया है, 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 उठाए जाने वाले उपायों की रूपरेखा बताई गई है।

v. सर्ट-इन ने भारतीय रिजर्व बैंक के माध्यम से देश में प्रीपेड भुगतान उपकरण (वॉलेट) जारी करने वाली सभी अधिकृत संस्थाओं और बैंकों को सलाह दी है कि वे सर्ट-इन के पैनल में शामिल लेखा परीक्षकों द्वारा विशेष ऑडिट कराएं, ऑडिट रिपोर्ट में पहचाने गए गैर-अनुपालन को बंद करें और सुरक्षा संबंधी सर्वोत्तम पद्धतियों का कार्यान्वयन सुनिश्चित करें।

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

vii. सर्ट-इन एक स्वचालित साइबर आपदा विनिमय प्लैटफ़ार्म संचालित करता है, जो सक्रिय रूप से विभिन्न क्षेत्रों के संगठनों के साथ अलर्ट एकत्रित करने, उनका विश्लेषण करने और साझा करने के लिए कार्य करता है ताकि वे सक्रिय रूप से खतरा कम करने संबंधी कार्रवाई कर सकें।

viii. सोशल मीडिया खातों की हैकिंग का पता चलने पर सर्ट-इन प्रभावित संस्थाओं और सेवा प्रदाताओं के साथ घटना प्रतिक्रिया उपायों का समन्वय करता है।

ix. सर्ट-इन फ़िशिंग वेबसाइटों को ट्रैक करने और डिसएबल करने तथा धोखाधड़ी गतिविधियों की जांच को सुविधाजनक बनाने के लिए सेवा प्रदाताओं के साथ समन्वय करता है।

x. सर्ट-इन ने सूचना सुरक्षा की सर्वोत्तम पद्धतियों के कार्यान्वयन का सहयोग देने और लेखापरीक्षा करने के लिए 176 सुरक्षा लेखापरीक्षा संगठनों को सूचीबद्ध किया है।

xi. सर्ट-इन विद्वेषपूर्ण कार्यक्रम का पता लगाने के लिए साइबर स्वच्छता केंद्र (बॉटनेट क्लीनिंग और मॉलवेयर विश्लेषण केंद्र) संचालित करता है और उन्हें हटाने के लिए निःशुल्क उपकरण प्रदान करता है, साथ ही नागरिकों और संगठनों के लिए साइबर सुरक्षा टिप्स और सर्वोत्तम अभ्यास भी उपलब्ध कराता है।

xii. सर्ट-इन वित्तीय क्षेत्र से रिपोर्ट की गई साइबर सुरक्षा घटनाओं पर प्रतिक्रिया देने, उन्हें रोकने और कम करने के लिए इसके तहत कंप्यूटर सुरक्षा घटना प्रतिक्रिया टीम-वित्त क्षेत्र (सीएसआईआरटी-फिन) के संचालन के लिए नेतृत्व प्रदान करता है।

xiii. सर्ट-इन नियमित रूप से साइबर हमलों और साइबर धोखाधड़ी के संबंध में साइबर सुरक्षा क्षमताओं के विकास, कौशल निर्माण, जागरूकता और नागरिक संवेदनशीलता के लिए विभिन्न गतिविधियाँ करता है। सरकार, सार्वजनिक और निजी क्षेत्र के संगठनों के भीतर सुरक्षा जागरूकता पैदा करने के लिए सर्ट-इन नियमित रूप से साइबर सुरक्षा के केंद्रित विषयों पर सभी क्षेत्रों में सरकारी, सार्वजनिक और निजी क्षेत्र के संगठनों के अधिकारियों को प्रशिक्षित करने के लिए प्रशिक्षण / कार्यशालाएँ आयोजित करता है ।

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

xv. इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय सूचना सुरक्षा जागरूकता पैदा करने के लिए कार्यक्रम आयोजित करता है। सूचना सुरक्षा के बारे में किताबें, वीडियो और ऑनलाइन सामग्री आम उपयोगकर्ताओं, बच्चों और अभिभावकों के लिए तैयार की जाती हैं और www.infosecawareness.in और www.csk.gon.in जैसे पोर्टलों के माध्यम से प्रसारित की जाती हैं ।

****