भारत सरकार
पृथ्वी विज्ञान मंत्रालय
लोक सभा
अतारांकित प्रश्न संख्या 5174
बुधवार, 2 अप्रैल, 2025 को उत्तर दिए जाने के लिए

आईएनसीओआईएस में साइबर धोखाधड़ी

†**5174. श्री ससिकांत सेंथिल:**

क्या **पृथ्वी विज्ञान** मंत्री यह बताने की कृपा करेंगे कि:

(क) क्या हाल ही में विशेषकर भारतीय राष्ट्रीय महासागर सूचना सेवा केन्द्र (आईएनसीओआईएस) में साइबर धोखाधड़ी की घटनाएं हुई हैं और यदि हां, तो इन धोखाधड़ी की गतिविधियों के कारण हुए वित्तीय नुकसानों सहित तत्संबंधी ब्यौरा क्या है;

(ख) सरकार द्वारा साइबर धोखाधड़ी की और घटनाओं को रोकने तथा संवेदनशील वित्तीय आंकड़ों की सुरक्षा के लिए अपनी एजेंसियों के भीतर, विशेषकर आईएनसीओआईएस में साइबर सुरक्षा उपायों को सुदृढ़ करने के लिए क्या कदम उठाए गए हैं;

(ग) क्या सरकार ने आईएनसीओआईएस और अन्य संबंधित संस्थाओं की वर्तमान साइबर सुरक्षा अवसंरचना में व्याप्त कमजोरियों का आकलन करने के लिए कोई आंतरिक लेखापरीक्षा या समीक्षा की है और यदि हां, तो तत्संबंधी ब्यौरा क्या है; और

(घ) वित्तीय लेन-देन की सुरक्षा बढ़ाने और सार्वजनिक निधियों को साइबर खतरों से बचाने के लिए सरकार द्वारा साइबर सुरक्षा विशेषज्ञों अथवा एजेंसियों के साथ किए गए सहयोगात्मक प्रयासों का ब्यौरा क्या है और ऐसी धोखाधड़ी की पहचान करने और उसे रोकने के लिए कर्मचारियों को प्रशिक्षित करने के लिए क्या विशिष्ट कार्रवाई की जा रही है?

उत्तर
विज्ञान एवं प्रौद्योगिकी तथा पृथ्वी विज्ञान राज्य मंत्री (स्वतंत्र प्रभार)
(डॉ. जितेंद्र सिंह)

(क) जी हां। भारतीय राष्ट्रीय महासागर सूचना सेवा केन्द्र (INCOIS), हैदराबाद में साइबर धोखाधड़ी की दो घटनाएं हुई हैं। दिनांक 29 जून 2024 और 15 जुलाई 2024 को मैन-इन-द-मिडल (MITM) हमला हुआ, जिससे क्रमशः 44,946 यूरो और 1,98,943.65 अमेरिकी डॉलर का वित्तीय नुकसान हुआ।

तथापि, सभी हितधारकों के साथ लगातार फॉलो-अप करने के बाद 1,98,943.65 अमेरिकी डॉलर पूरी तरह से पुन: प्राप्त कर लिए गए और 07 अक्टूबर 2024 को INCOIS के पास वापस जमा करवा दिए गए। 44,946 यूरो वाली घटना वाले मामले में, साइबर अपराध पुलिस, भारतीय बैंकर्स और विदेशी बैंकर्स के साथ-साथ पुर्तगाल में भारतीय दूतावास के साथ समन्वय करके निधियों को पुन: प्राप्त करने के प्रयास शुरू किए गए थे।

(ख) INCOIS में साइबर सुरक्षा सिस्टम को सुदृढ़ बनाने के लिए किए गए उपाय निम्नानुसार हैं:

- INCOIS ईमेल/सिस्टम का एक्सेस सुरक्षित करने हेतु अधिकृत कर्मियों के लिए वर्चुअल प्राइवेट नेटवर्क (वीपीएन) का उपयोग किया जाना।
- टू फैक्टर ऑथेंटिकेशन (2FA), जटिल पासवर्ड, नियमित रूप से पासवर्ड बदलने आदि के माध्यम से ईमेल/सिस्टम एक्सेस को सुदृढ़ बनाना।

- स्पैम को फिल्टर करना।
- साइबर धोखाधड़ी की रोकथाम के लिए साइबर सुरक्षा पहलुओं के बारे में कर्मचारियों को जानकारी प्रदान करना।
- ईमेल सेवाओं को NIC में माइग्रेट करना।

(ग) जी हां। INCOIS ने साइबर सुरक्षा अवसंरचना की आंतरिक समीक्षा की और उपर्युक्त उपायों को कार्यान्वित किया।

(घ) वित्तीय लेनदेनों की सुरक्षा बढ़ाने के लिए, INCOIS ने

- विदेशीऑर्डरों के लिए यूसेंस लेटर्स ऑफ क्रेडिट (ULC) जारी करने की व्यवस्था स्थापित की है।
- इंडियन कंप्यूटर इमरजेंसी रिस्पॉन्स टीम (CERT-In), इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय की पैनलबद्ध एजेंसियों के साथ समन्वय से साइबर सुरक्षा पहलुओं के बारे में कर्मचारियों के लिए प्रशिक्षण आयोजित किया है।

इसके अतिरिक्त, सरकार ने भारत की साइबर सुरक्षा अवसंरचना को सुदृढ़ बनाने और वित्तीय साइबर अपराधों पर अंकुश लगाने सहित साइबर धोखाधड़ी की रोकथाम के लिए निम्नलिखित उपाय किए हैं, जिनमें अन्य बातों के साथ-साथ शामिल हैं:

i. गृह मंत्रालय ने साइबर अपराधों से व्यापक और समन्वित तरीके से निपटने हेतु LEAs के लिए एक रूपरेखा और पारिस्थितिकी तंत्र प्रदान करने हेतु एक संबद्ध कार्यालय के रूप में भारतीय साइबर अपराध समन्वय केंद्र (I4C) की स्थापना की है।

ii. I4C में साइबर धोखाधड़ी शमन केंद्र (CFMC) की स्थापना की गई है, जहां प्रमुख बैंकों, वित्तीय मध्यस्थों, भुगतान एग्रीगेटर्स, दूरसंचार सेवा प्रदाताओं, आईटी मध्यस्थों और राज्यों/संघ राज्य क्षेत्रों की कानून प्रवर्तन एजेंसियों के प्रतिनिधि साइबर अपराध से निपटने हेतु तत्काल कार्रवाई और निर्बाध सहयोग के लिए मिलकर काम कर रहे हैं। CFMC का लक्ष्य वित्तीय संस्थानों को एक साथ लाकर विभिन्न वित्तीय क्षेत्रों में धोखाधड़ी वाली निधियों के प्रसार को रोककर साइबर वित्तीय धोखाधड़ी का पता लगाना, रोकना और उसे कम करना है।

iii. भारतीय रिजर्व बैंक (आरबीआई) ने दिनांक 15.07.2024 को धोखाधड़ी जोखिम प्रबंधन के बारे में विनियमित संस्थाओं अर्थात् (i) वाणिज्यिक बैंकों (क्षेत्रीय ग्रामीण बैंक सहित) और अखिल भारतीय वित्तीय संस्थानों; (ii) सहकारी बैंकों (नगरीय सहकारी बैंकों/राज्य सहकारी बैंकों/केन्द्रीय सहकारी बैंकों); और (iii) गैर-बैंकिंग वित्त कंपनियों (हाउसिंग फाइनेंस कंपनियों सहित) के लिए प्रमुख निर्देश (मास्टर डायरेक्टिव्स) जारी किए हैं, जिसका उद्देश्य, अन्य बातों के साथ-साथ प्रारंभिक चेतावनी संकेतों (EWS) संबंधी रूपरेखा को सुदृढ़ बनाना है, और KYC का अनुपालन न करने वाले खातों और मनी म्यूल खातों आदि में लेनदेन/असामान्य गतिविधियों की निगरानी करना है ताकि अनाधिकृत/धोखाधड़ी वाले लेनदेन को रोका जा सके।

iv. भारतीय रिजर्व बैंक (RBI) ने "आरबीआई कहता है" के माध्यम से विभिन्न प्रकार की धोखाधड़ी, धोखाधड़ी के तौर-तरीकोंऔर डिजिटल भुगतान लेनदेन के दौरान अपनाए जाने वाले सुरक्षा उपायों जैसे पहलुओं के बारे में जागरूकता सामग्री/उपयोगी जानकारी जारी की है और जनता के बीच जागरूकता सृजित करने के लिए विज्ञापन (विख्यात महानुभावों के माध्यम से) भी जारी किए हैं। RBI ने जनता को शिक्षित करने के लिए सार्वजनिक स्तर पर वित्तीय धोखाधड़ी के तौर-तरीकों के बारे में “BE (A)WARE" बुकलेट भी जारी की है।

v. विभिन्न एजेंसियों के बीच समन्वय सुनिश्चित करने के लिए राष्ट्रीय सुरक्षा परिषद सचिवालय (NSCS) के अंतर्गत राष्ट्रीय साइबर सुरक्षा समन्वयक (NCSC)।

vi. CERT-In द्वारा कार्यान्वित राष्ट्रीय साइबर समन्वय केंद्र (NCCC) देश में साइबरस्पेस को स्कैन करने और साइबर सुरक्षा खतरों का पता लगाने के लिए नियंत्रण कक्ष के रूप में कार्य करता है। राष्ट्रीय साइबर समन्वय केंद्र (NCCC) 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।

vii. साइबर स्वच्छता केंद्र (CSK) CERT-In द्वारा प्रदान की जाने वाली एक नागरिक-केंद्रित सेवा है, जो स्वच्छ भारत के दृष्टिकोण का साइबर स्पेस तक विस्तार करती है। साइबर स्वच्छता केंद्र, बॉटनेट सफाई और मैलवेयर विश्लेषण केंद्र है, तथा दुर्भावनापूर्ण प्रोग्रामों का पता लगाने में मदद करता है और उन्हें हटाने के लिए फ्री टूल्स प्रदान करता है। यह नागरिकों और संगठनों के लिए साइबर सुरक्षा सुझाव और सर्वोत्तम अभ्यास भी प्रदान करता है।

viii. CERT-In ने अप्रैल 2022 में सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70ख की उपधारा (6) के तहत सुरक्षित एवं विश्वसनीय इंटरनेट के लिए सूचना सुरक्षा परिपाटियों, प्रक्रिया, रोकथाम, प्रतिक्रिया और साइबर घटनाओं की रिपोर्टिंग से संबंधित साइबर सुरक्षा निर्देश जारी किए।

ix. CERT-In ने जून 2023 में सरकारी संस्थाओं के लिए सूचना सुरक्षा परिपाटियों संबंधी दिशानिर्देश जारी किए, जिसमें डेटा सुरक्षा, नेटवर्क सुरक्षा, पहचान और पहुंच प्रबंधन, एप्लिकेशन सुरक्षा, तृतीय-पक्ष आउटसोर्सिंग, सख्त प्रक्रियाएं, सुरक्षा निगरानी, घटना प्रबंधन और सुरक्षा ऑडिटिंग जैसे विषय शामिल हैं।

x. CERT-In ने नवंबर 2023 में विभिन्न मंत्रालयों को एक परामर्शिका जारी की है, जिसमें संवेदनशील व्यक्तिगत डेटा या सूचना सहित डिजिटल व्यक्तिगत डेटा या सूचना को प्रोसेस करने वाली सभी संस्थाओं द्वारा साइबर सुरक्षा को मजबूत करने के लिए किए जाने वाले उपायों की रूपरेखा बताई गई है। CERT-In कंप्यूटर, मोबाइल फोन, नेटवर्क और डेटा की सुरक्षा के लिए नवीनतम साइबर खतरों/संवेदनशीलताओं और इन्हें रोकने के उपायों के संबंध में निरंतर अलर्ट और परामर्शिका जारी करता है।

xi. NIC ने सरकारी नेटवर्क से जुड़े सुरक्षा मुद्दों की पहचान करने के लिए थ्रेट इंटेलिजेंस प्लेटफॉर्म सहित उन्नत सुरक्षा उपकरण तैनात किए हैं।

*****