



साइबर सुरक्षति भारत

हाल ही में [राष्ट्रीय ई-शासन प्रभाग \(National e-Governance Division-NeGD\)](#) ने भारतीय लोक प्रशासन संस्थान (Indian Institute of Public Administration-IIPA), नई दिल्ली में 30वें मुख्य सूचना सुरक्षा अधिकारी (Chief Information Security Officers-CISO) डीप-डाइव प्रशिक्षण कार्यक्रम का आयोजन किया।

साइबर सुरक्षति भारत पहल:

परिचय:

- साइबर सुरक्षति भारत पहल की संकल्पना [साइबर अपराध](#) के बारे में जागरूकता फैलाने और सभी सरकारी विभागों में मुख्य सूचना सुरक्षा अधिकारियों (CISOs) एवं अग्रिम पंक्ति के सूचना प्रौद्योगिकी अधिकारियों की क्षमता निर्माण के मशिन के साथ की गई थी।
- इसे [इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय](#) (Ministry of Electronics and Information Technology-MeitY) द्वारा वर्ष 2018 में लॉन्च किया गया था।
- CISO प्रशिक्षण [सार्वजनिक नजी भागीदारी \(Public Private Partnership-PPP\)](#) मॉडल के तहत सरकार और उद्योग संघ के मध्य इस प्रकार की प्रथम साझेदारी है।

लक्षति प्रतभागी:

- सार्वजनिक क्षेत्र के बैंकों और बीमा कंपनियों, पुलिस एवं सुरक्षा बलों के तकनीकी शाखाओं सहित केंद्र तथा राज्य/केंद्रशासति प्रदेश सरकारों और अधीनस्थ एजेंसियों/सार्वजनिक उपकरणों के अधिकारी:
 - नामति मुख्य सूचना सुरक्षा अधिकारी (CISOs),
 - CTOs और तकनीकी / PMU टीमों के सदस्य, अपने संबंधति संगठन में सूचना प्रौद्योगिकी प्रणाली की सुरक्षा का निरीक्षण करने के लिये जिम्मेदार अधिकारी।
- प्रशिक्षण:
 - NeGD, इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय की एक शाखा, प्रशिक्षण कार्यक्रमों की व्यवस्था में सहायता प्रदान करेगी, जबकि उद्योग संघ, प्रशिक्षण के लिये तकनीकी सहायता प्रदान करेगा।
 - उद्योग के प्रशिक्षण भागीदार माइक्रोसॉफ्ट (Microsoft), आईबीएम (IBM), इंटेल (Intel), पालो (Palo), ऑल्टो नेटवर्क (Alto Networks), ईवाई (E&Y) और Dell-EMC हैं। NIC, CERT-In और CDAC सरकार की ओर से ज्ञान भागीदार हैं।

उद्देश्य:

- इसका उद्देश्य CISOs को साइबर हमलों को व्यापक रूप से और पूरी तरह से समझने के लिये शक्ति और सक्षम करना, सुरक्षा की नवीनतम तकनीकों में आवश्यक प्रभावों के बारे में जानकारी प्राप्त करना एवं व्यक्तिगत संगठनों और नागरिकों को बड़े पैमाने पर एक लचीली ई-बुनियादी ढाँचे के लाभों का अनुवाद करना है।
- साइबर खतरों के उभरते परिदृश्य पर जागरूकता का वसितार करना।
- संबंधति समाधानों की गहन समझ विकसति करना।
- साइबर सुरक्षा से संबंधति लागू ढाँचे, दशानरिदेश और नीतियाँ बनाना।
- सफलता और असफलताओं से सीखने के लिये सर्वोत्तम प्रथाओं को साझा करना।
- अपने संबंधति कार्यात्मक क्षेत्र में साइबर सुरक्षा से संबंधति मुद्दों पर सूचित निर्णय लेने के लिये महत्त्वपूर्ण इनपुट प्रदान करना।

UPSC सविलि सेवा परीक्षा, वगित वर्ष के प्रश्न:

प्रश्न. हाल ही में कभी-कभी समाचारों में आने वाले शब्द 'वानाकराई, पेट्या और इंटरनलब्लू' नमिनलखिति में से कसिसे संबंधति हैं (2018)

- एक्सोप्लैनेट
- क्रिप्टोकॉरेंसी
- साइबर हमले
- लघु उपग्रह

उत्तर: (c)

व्याख्या:

- रैसमवेयर दुरभावनापूर्ण सॉफ्टवेयर (या मैलवेयर) का एक रूप है। एक बार जब यह कंप्यूटर में प्रवेश कर लेता है, तो यह आमतौर पर डेटा तक पहुँच कर उपयोगकर्ताओं को नुकसान पहुँचाता है। भुगतान करने पर डेटा तक पहुँच बहाल करने का वादा करते हुए हमलावर पीड़ति से फरौती की मांग करते है। 'वानाक्राई, पेटया और इंटरनलब्लू' कुछ रैनसम वेयर है, जिन्होंने बटिकॉइन (क्रपिटोकुरेसी) में फरौती के भुगतान की मांग की थी।
- क्रपिटोकुरेसी एक डजिटिल मुद्रा है जिसमें एनक्रपिशन तकनीकों का उपयोग मुद्रा की इकाइयों की पीढ़ी को वनियमति करने और केंद्रीय बैंक से स्वतंत्र रूप से संचालति होने वाले धन के हस्तांतरण को सत्यापति करने के लयि कथिा जाता है। **अतः वकिलप (c) सही है।**

स्रोत: पी.आई.बी.

PDF Referenece URL: <https://www.drishtias.com/hindi/printpdf/cyber-surakshit-bharat-1>

