भारत में साइबर धोखाधड़ी

प्रलिमि्स के लयि:

डजिटिल अरेस्ट, सूचना प्रौद्योगकिी अधनियिम, 2000, डजिटिल व्यक्तगित डेटा संरक्षण अधनियिम, 2023, भारतीय कंप्यूटर आपातकालीन प्रतकि्रयिा दल, राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIIPC), साइबर स्वच्छता केंद्र, रैनसमवेयर, बुडापेस्ट साइबर अपराध कन्वेंशन, साइबर अपराध

मेन्स के लयि:

भारत में साइबर सुरक्षा के लयि वर्तमान ढाँचा, भारत के डजिटिल परदृिश्य को प्रभावति करने वाले प्रमुख उभरते साइबर खतरे।

स्रोत: IE

चर्चा में क्यों?

भारतीय साइबर अपराध समन्वय केंद्र (I4C), जो गृह मंत्रालय (MHA) के अंतर्गत कार्य करता है, ने भारतीय नागरकिों को लक्षति करने वाले वत्तिीय साइबर धोखाधड़ी के मामलों में तीव्र वृद्धि की रपिोर्ट दी है, जनिका अधकिांश स्रोत दक्षणि-पूर्व एशयिाई देश हैं।

I4C के वशि्लेषण के अनुसार भारत में वत्तिीय साइबर धोखाधड़ी की स्थति क्या है?

- **बढ़ते वत्तिीय नुकसान:** 2025 की पहली छमाही में भारत को साइबर धोखाधड़ी के कारण प्रतमिाह औसतन ₹1,000 करोड़ का नुकसान हुआ, जो कुल ₹7,000 करोड़ तक पहुँच गया।
  - **I4C के अनुसार**, वर्ष 2025 में संभावति वार्षकि नुकसान ₹1.2 लाख करोड़ (₹1.2 ट्रलियिन) से अधकि हो सकता है, जो **भारत की GDP का लगभग 0.7%** है।
- **धोखाधड़ी (स्कैम) की उत्पत्ति और प्रकृति: भारतीय नागरकिों को लक्षति करने वाली 50% से अधकि साइबर धोखाधड़ी दक्षणि-पूर्व एशयिाई देशों जैसे कि कंबोडयिा, म्याँमार, वयितनाम, लाओस और थाईलैंड से संचालति हो रही हैं। ये धोखाधड़ी मुख्यतः उच्च-सुरक्षा परसिरों से संचालति की जाती हैं, जनिका संचालन कथति रूप से चीनी संचालकों द्वारा कयिा जाता है।**
  - प्रमुख धोखाधड़ी के प्रकारों में शामलि हैं: **शेयर बाज़ार/नविेश धोखाधड़ी, डजिटिल अरेस्ट स्कैम, कार्य-आधारति और नविेश-आधारति धोखाधड़ी।**
  - भारतीय खुफयिा एजेंसयिों द्वारा **कंबोडयिा में 45, लाओस में 5, म्याँमार में 1 स्कैम केंद्र** की पहचान की गई।
- **कार्यप्रणाली (Modus Operandi): भारतीय नागरकिों सहति पीड़तिों को फर्जी नौकरी प्रस्तावों के माध्यम से मानव तस्करी का शकिार बनाया जाता है और उन्हें दुबई, चीन, थाईलैंड जैसे देशों के माध्यम से साइबर धोखाधड़ी में लगाया जाता है।**
  - भारत के वभिन्नि राज्यों — **महाराष्ट्र, तमलिनाडु, जम्मू-कश्मीर, उत्तर प्रदेश और दल्लिी** , में सक्रयि भर्ती एजेंट इस प्रक्रयिा का हस्सिा हैं।
- **संरचनात्मक खामयिाँ एवं प्रवर्तन: भारत के साइबर धोखाधड़ी पारस्थितिकिी तंत्र का दुरुपयोग के कारणों में डजिटिल बैंकगि लेनदेन में खामयिाँ, टेलीकॉम सेक्टर में PoS एजेंटों द्वारा फर्जी समि कार्ड जारी करना, आव्रजन में कमज़ोर सत्यापन प्रक्रयिाएँ, आदि शामलि हैं, जसिसे गुमनाम और सीमापार साइबर अपराध संभव हो पाते हैं।**

भारतीय साइबर अपराध समन्वय केंद्र (I4C)

- **परचिय:** I4C की स्थापना गृह मंत्रालय द्वारा **वर्ष 2020** में की गई थी, जसिका उद्देश्य साइबर अपराधों (वशिेष रूप से वत्तिीय धोखाधड़ी) के लयि एक **समन्वति और समग्र प्रतकि्रयिा** प्रदान करना है।
- **मुख्य उद्देश्य:**
  - **राष्ट्रीय नोडल एजेंसी** के रूप में कार्य करना, जो साइबर अपराधों की **नगिरानी, रोकथाम और जाँच में समन्वय** करना, वशिेषकर महलिाओं, बच्चों और महत्त्वपूर्ण अवसंरचना को लक्षति करने वाले अपराधों के मामले में।

- प्रारंभकि चेतावनी प्रणाली वकिसति करना और प्रवृत्तविश्लिेषण, पैटर्न की पहचान तथा डेटा साझा करने की सुवधि प्रदान करना।
- साइबर अपराध की शकियत दर्ज कराने की सुवधि प्रदान करना एवं **साइबर स्वच्छता तथा धोखाधड़ी की रोकथाम** पर जन-जागरूकता बढ़ाना।
- राज्यों/केंद्रशासति प्रदेशों को **साइबर फॉरेंसकि और जाँच में पुलसि, अभयिोजकों और न्यायकि अधकिारयिों** की क्षमता नरि्माण में सहायता देना।

- **राष्ट्रीय साइबर अपराध रपिोर्टगि पोर्टल:** यह एक नागरकि-केंद्रति ऑनलाइन पोर्टल है जो लोगों को साइबर धोखाधड़ी की शकियत दर्ज कराने की सुवधि प्रदान करता है। दर्ज शकियतों को संबंधति कानून प्रवर्तन एजेंसयिों को अग्रेषति कयिा जाता है।

साइबर धोखाधड़ी (Cyber frauds) क्या है?

- **परचिय:** साइबर धोखाधड़ी वे आपराधकि गतविधियिाँ हैं, जो **डजिटिल प्रौद्योगकिी (इंटरनेट)** का उपयोग करके व्यक्तयिों या संस्थानों को वत्तिीय नुकसान पहुँचाने हेतु की जाती हैं।
  - ये साइबर सुरक्षा, डजिटिल प्लेटफॉर्म या मानव व्यवहार की कमज़ोरयिों का फायदा उठाकर **धन, डेटा या पहचान की चोरी** करते हैं।

साइबर धोखाधड़ी के प्रकार:

प्रकार	वविरण
डजिटिल गरिफ्तारी (Digital Arrests)	पुलसि या आयकर अधकिारी बनकर **डराकर धन वसूली** करना।
ऑनलाइन जॉब/कार्य-आधारति धोखाधड़ी	घर बैठे कार्य के फर्जी प्रस्ताव और अग्रमि भुगतान की मांग।
मालवेयर	**कंप्यूटर पर नयिंत्रण** पाने हेतु **व्यक्तगित जानकारी** चुराने वाला सॉफ्टवेयर।
रैनसमवेयर	**फाइलों को एन्क्रप्टि** कर उन्हें खोलने के बदले फरिौती माँगना (जैसे: 2016 का WannaCry हमला)।
फशिगि	भरोसेमंद दखिने वाले ईमेल के ज़रयि उपयोगकर्त्ता को फर्जी लकि पर क्लकि कराकर संवेदनशील जानकारी हासलि करना (जैसे: क्रेडटि कार्ड नंबर)।
साइबर बुलीइंग (Cyberbullying)	कसिी व्यक्तकिो धमकी देना, मानसकि रूप से **परेशान करना या ब्लैकमेल** करना।
साइबर जासूसी (Cyber Spying)	संवेदनशील डेटा, नजिी जानकारी या बौद्धकि संपदा तक पहुँच प्राप्त करने के लयि नेटवर्क को नशिाना बनाना।
बज़िनेस ईमेल समझौता (BEC)	वैध ईमेल हैक कर **सप्लायर, कर्मचारी या टैक्स अधकिारयिों** की पहचान में धोखा देना (वाइट कॉलर अपराध)।
डेटगि हुडवकि्स (Dating Hoodwinks)	डेटगि साइट्स/ऐप्स का उपयोग कर भावनात्मक जुड़ाव के **ज़रयि नजिी जानकारी हासलि** करना।
एटीएम/PoS धोखाधड़ी	कार्ड डटिेल्स की चोरी या अनधकिृत लेनदेन **(स्कमिगि)।**

- **साइबर धोखाधड़ी के परणिाम:**
  - **व्यक्तगित नुकसान:** अनधकिृत वत्तिीय लेनदेन, खाते तक पहुँच खोना और नजिी डेटा का दुरुपयोग कर ब्लैकमेल।
  - **व्यावसायकि जोखमि:** कानूनी दंड, नयिामक जुर्माना और ग्राहक डेटा लीक होने पर ब्रांड की वश्विसनीयता और बाज़ार मूल्य में गरिावट।
  - **राष्ट्रीय सुरक्षा को खतरा:** साइबर उल्लंघनों द्वारा रक्षा और महत्त्वपूर्ण सूचना प्रणालयिों को नशिाना बनाया जाना।
- **उल्लेखनीय साइबर धोखाधड़ी घटनाएँ:**
  - **आधार डेटा लीक (2018):** 1.1 अरब आधार कार्डधारकों की **व्यक्तगित जानकारी लीक, जसिमें आधार संख्या, PAN और बैंक वविरण** शामलि थे।
  - **केनरा बैंक ATM हमला (2018):** हैकरों ने 300 डेबटि कार्ड्स पर स्कमिगि उपकरणों का प्रयोग कर ₹20 लाख से अधकि की चोरी की।
  - **पेगासस स्पाईवेयर मामला:** इज़रायली स्पाईवेयर Pegasus का उपयोग बनिा अनुमतकिे मोबाइल उपकरणों से डेटा चुराने के लयि हुआ, जसिमें 300 से अधकि प्रमाणति भारतीय मोबाइल नंबर प्रभावति हुए।

भारत के डजिटिल परदृिश्य को प्रभावति करने वाले प्रमुख उभरते साइबर खतरे क्या हैं?

पढ़ने के लयि यहाँ क्लकि करें: भारत में उभरते साइबर खतरे

साइबर सुरक्षा से संबंधति प्रमुख पहल क्या हैं?

- **साइबर सुरक्षा पर वैश्विक पहलें:**
  - **बुडापेस्ट कन्वेंशन ऑन साइबरक्राइम:** यह **साइबर अपराध** से निपटने के लिये बना **पहला अंतरराष्ट्रीय संधि-पत्र** है, जो **कानूनी समरूपता (legal harmonization)**, **जाँच में सहयोग (investigative cooperation)** और **क्षमता निर्माण (capacity building)** को बढ़ावा देता है। यह **1 जुलाई, 2004** से लागू हुआ था।
  - भारत **इस संधि का पक्षकार नहीं** है।
- **इंटरनेट गवर्नेंस फोरम (IGF): IGF संयुक्त राष्ट्र (UN)** के अंतर्गत एक **बहु-हितधारक मंच (Multi-Stakeholder Platform)** है, जो इंटरनेट गवर्नेंस और साइबर सुरक्षा से संबंधित सार्वजनिक नीति के मुद्दों पर सरकारों, निजी क्षेत्र, शिक्षाविदों और नागरिक समाज के बीच संवाद को बढ़ावा देता है।
- **ICT सुरक्षा पर UNGA के प्रस्ताव: संयुक्त राष्ट्र महासभा (UNGA)** ने साइबर सुरक्षा से संबंधित मुद्दों के समाधान हेतु **दो प्रमुख मंचों** की स्थापना की है:
  - **ओपन-एंडेड वर्किंग ग्रुप (OEWG):** रूस द्वारा आरंभ किया गया।
    - उद्देश्य: **समावेशी संवाद** और **ICT सुरक्षा में क्षमता निर्माण** को प्रोत्साहित करना।
  - **ग्रुप ऑफ गवर्नमेंटल एक्सपर्ट्स (GGE):** अमेरिका द्वारा आरंभ किया गया।
    - उद्देश्य: **साइबर स्पेस में ज़िम्मेदार राज्य व्यवहार के मानदंड (norms)** और **अंतर्राष्ट्रीय कानूनी ढाँचे** का विकास करना।

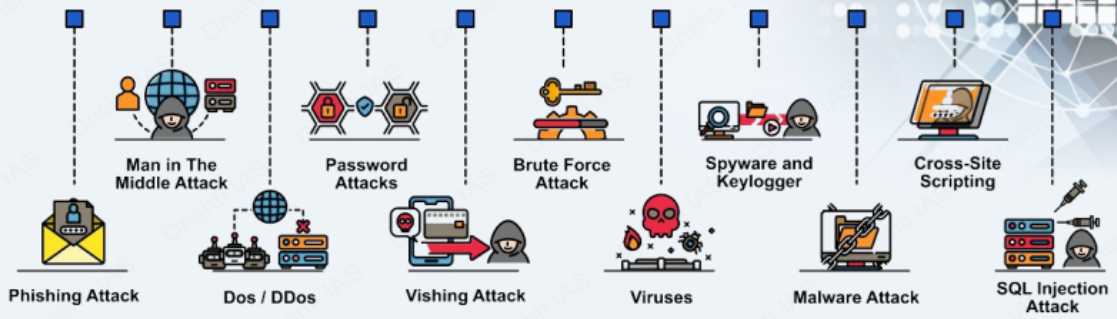
भारत की साइबर सुरक्षा पहल

- **विधायी उपाय:**
  - सूचना प्रौद्योगिकी अधिनियम, 2000 (IT Act)
  - डिजिटल पर्सनल डेटा प्रोटेक्शन एक्ट, 2023
- **संस्थागत ढाँचा:**
  - भारतीय कंप्यूटर इमर्जेंसी रिस्पांस टीम (CERT-In)
  - राष्ट्रीय संवेदनशील सूचना संरचना संरक्षण केंद्र (NCIIPC)
  - भारतीय साइबर अपराध समन्वय केंद्र (I4C)
  - साइबर स्वच्छता केंद्र
  - नागरिक वित्तीय साइबर धोखाधड़ी रिपोर्टिंग एवं प्रबंधन प्रणाली — साइबर धोखाधड़ी मामलों की वास्तविक समय निगरानी, ट्रैकिंग और समाधान सुनिश्चित करने हेतु
    - **केंद्रीय अन्वेषण ब्यूरो (CBI)** — PoS एजेंटों द्वारा धोखाधड़ीपूर्ण समि जारी करने पर FIR दर्ज की गई
- **रणनीतिक पहल:**
  - भारत राष्ट्रीय साइबर सुरक्षा अभ्यास 2024
  - राष्ट्रीय साइबर सुरक्षा नीति, 2013, साइबर स्पेस की सुरक्षा और संवेदनशील सूचना ढाँचे की रक्षा हेतु दृष्टि व रणनीति निर्धारित करती है
- **चक्षु और डिजिटल इंटेलिजेंस प्लेटफॉर्म (DoT द्वारा):**
  - चक्षु: संचार साथी पोर्टल पर उपलब्ध एक उपकरण, जो नागरिकों को **KYC समाप्ति या बैंक खाता अपडेट** जैसे धोखाधड़ी संबंधी फर्जी कॉल/SMS/WhatsApp संदेश रिपोर्ट करने की सुविधा प्रदान करता है
  - डिजिटल इंटेलिजेंस प्लेटफॉर्म (DIP): दूरसंचार संसाधनों के दुरुपयोग की रोकथाम हेतु हितधारकों (टीएसपी, बैंक, कानून प्रवर्तन, आदि) के बीच **वास्तविक समय समन्वय** व **सूचना आदान–प्रदान** सुनिश्चित करता है
- **क्षेत्र-विशिष्ट नियमन:**
  - SEBI द्वारा विनियमित संस्थाओं हेतु साइबर सुरक्षा ढाँचा — प्रतिभूति बाज़ार में साइबर सुरक्षा नीतियों को बाध्यकारी बनाता है
  - दूरसंचार (संवेदनशील दूरसंचार अवसंरचना) नियम, 2024

साइबर सुरक्षा

साइबर सुरक्षा, साइबर हमलों को रोकने या उनके प्रभाव को कम करने के लिये किसी भी तकनीक, उपाय या अभ्यास को संदर्भित करती है।

CYBER SECURITY ATTACKS



NCRB की "भारत में अपराध" रिपोर्ट, 2022 के अनुसार, वर्ष 2021 के बाद से भारत में साइबर अपराध 24.4% बढ़ गए हैं।

सामान्य साइबर सुरक्षा मिथक

- केवल मज़बूत पासवर्ड ही पर्याप्त सुरक्षा है
- प्रमुख साइबर सुरक्षा जोखिम सर्वविदित हैं
- सभी साइबर हमले वैक्टर (vector) निहित होते हैं
- साइबर अपराधी छोटे व्यवसायों पर हमला नहीं करते हैं

साइबर वॉर

- किसी दूसरे के कंप्यूटर सिस्टम को बाधित करने, क्षति पहुँचाने या नष्ट करने के लिये किये गए डिजिटल हमले।

CYBER THREAT ACTORS

CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

साइबर सुरक्षा के प्रकार

- महत्त्वपूर्ण बुनियादी ढाँचा सुरक्षा (रोबस्ट एक्सेस कंट्रोल)
- नेटवर्क सुरक्षा (डिफेंसिव फायरवॉल)
- एप्लिकेशन सुरक्षा (कोड रिव्यू)
- क्लाउड सुरक्षा (टोकनाइज़ेशन)
- सूचना सुरक्षा (डेटा मास्किंग)

हाल ही में हुए प्रमुख साइबर हमले

- वान्नाक्राई रैनसमवेयर अटैक (वर्ष 2017)
- कैम्ब्रिज एनालिटिका डेटा ब्रीच (वर्ष 2018)
- 9M+ कार्डधारकों का वित्तीय डेटा लीक, जिसमें SBI भी शामिल है (वर्ष 2022)

विनियम एवं पहलें

- **अंतर्राष्ट्रीय स्तर पर:**
  - साइबर स्पेस में राज्यों के उत्तरदायी व्यवहार को बढ़ावा देने से संबंधित संयुक्त राष्ट्र के सरकारी विशेषज्ञों के समूह (GGE)।
  - नाटो का कोऑपरेटिव साइबर डिफेंस सेंटर ऑफ एक्सीलेंस (CCDCOE)
  - साइबर अपराध पर बुडापेस्ट कन्वेंशन, 2001 (भारत हस्ताक्षरकर्त्ता नहीं है)
- **भारतीय स्तर पर:**
  - IT अधिनियम, 2000 (धारा 43, 66, 66B, 66C, 66D)
  - राष्ट्रीय साइबर सुरक्षा नीति, 2013
  - नेशनल साइबर सिक्योरिटी स्ट्रेटेजी, 2020
  - साइबर सुरक्षित भारत पहल
  - भारतीय साइबर अपराध समन्वय केंद्र (I4C)
  - कंप्यूटर आपातकालीन प्रतिक्रिया टीम - भारत (CERT-In)

साइबर सुरक्षा के लिये उठाए जाने वाले आवश्यक कदम

- नेटवर्क सुरक्षा
- मैलवेयर सुरक्षा
- इंसिडेंट मैनेजमेंट
- उपयोगकर्त्ता को शिक्षित और जागरुक करना
- सुरक्षित विन्यास
- उपयोगकर्त्ता के विशेषाधिकारों का प्रबंधन करना
- सूचना जोखिम प्रबंधन व्यवस्था

Drishti IAS

भारत में साइबर सुरक्षा ढाँचे को मज़बूत करने हेतु क्या उपाय किये जाने चाहिये?

- **अवसंरचना एवं कृत्रमि बुद्धमित्ता आधारति सुरक्षा: डजिटिल अवसंरचना को मज़बूत कयिा जाना चाहयि**े, जसिमें फायरवॉल, नयिमति सॉफ्टवेयर/हार्डवेयर अपडेट तथा कृत्रमि बुद्धमित्ता (AI) आधारति खतरा पहचान प्रणाली शामलि हो।
    - AI-आधारति उपकरणों को **रैनसमवेयर की पूर्व-भवषि्यवाणी**, **घटनाओं की त्वरति प्रतक्रियिा**, और **फॉरेंसकि वशि्लेषण** में सक्षम बनाया जाना चाहयि।

- **साइबर जागरूकता एवं साक्षरता:** ग्रामीण समुदायों, युवाओं और वरषि्ठ नागरकिों को लक्षति करते हुए **स्थानीय भाषाओं में राष्ट्रव्यापी साइबर साक्षरता कार्यक्रम** शुरू कयि जाएँ।
    - **स्कूलों और वशि्ववद्यिालयों में साइबर सुरक्षा शक्षिा** को शामलि कयिा जाए, ताकि प्रारंभकि स्तर से डजिटिल समुत्थानशीलता वकिसति हो सके। इसके लि**ए सुरक्षति डजिटिल अवसंरचना** और **प्रशक्षिति स्टाफ** की उपलब्धता सुनश्चिति की जाए।
- **संस्थागत सुधार एवं ऑडटि तंत्र: बैंकगि, स्वास्थ्य सेवा और उपयोगति क्षेत्रों** जैसे महत्त्वपूर्ण क्षेत्रों में **अनविार्य साइबर सुरक्षा ऑडटि**, **तनाव परीक्षण (stress tests)** और **कर्मचारी तैयारियों का मूल्यांकन** कयिा जाना चाहयि।
    - **ज़लिा-स्तरीय साइबर सुरक्षा इकाइयाँ** स्थापति की जाएँ जो स्थानीय खतरों से नपिटने और CERT-In के साथ समन्वय कर सकें।
- **कॉर्पोरेट एवं बैंकगि सुरक्षा उपाय: व्यवसायों और बैंकों में दो-चरणीय प्रमाणीकरण (2FA)**, **डेटा एन्क्रप्शिन** और **सतत् नगिरानी प्रणाली** को अनविार्य कयिा जाए।
    - **वत्तिीय संस्थानों** को संदग्धि लेनदेन पर नज़र रखनी चाहयि, वदिशी IP लॉगनि का पता लगाना चाहयि तथा चोरी कयि गए धन को **क्रप्टिोकरेंसी में बदलने** से रोकना चाहयि।

- **व्यक्तगित साइबर स्वच्छता:** नागरकिों को **सुरक्षति डजिटिल व्यवहार** अपनाने के लयि प्रेरति कयिा जाना चाहए, जैसे: संदग्धि संचार (ईमेल, कॉल, SMS आदि) से बचना, मज़बूत एवं अद्वतिीय पासवर्ड का प्रयोग, सुरक्षा चेतावनयिों को नज़रअंदाज़ न करना। इससे व्यक्तगित स्तर पर साइबर धोखाधड़ी की **भेद्यता में कमी** लाई जा सकती है।

दृष्टि मुख्य परीक्षा प्रश्न:

Q. भारत में साइबर सुरक्षा की प्रमुख चुनौतयिाँ क्या हैं? भारत के साइबर सुरक्षा ढाँचे को मज़बूत करने के लयि व्यापक उपाय सुझाएँ?

UPSC सविलि सेवा परीक्षा, वगित वर्ष के प्रश्न (PYQ)

??????????:

प्रश्न.1 भारत में व्यक्तयिों के लयि साइबर बीमा के तहत धन की हानि और अन्य लाभों के भुगतान के अलावा, नम्निलखिति में से कौन से लाभ आम तौर पर कवर कयि जाते हैं? (वर्ष 2020)

1. कसिी के कंप्यूटर तक पहुँच को बाधति करने वाले मैलवेयर के मामले में कंप्यूटर सस्टिम की बहाली की लागत।
2. एक नए कंप्यूटर की लागत अगर ऐसा साबति हो जाता है कि कुछ असामाजकि तत्त्वों ने जानबूझकर इसे नुकसान पहुँचाया है।
3. साइबर जबरन वसूली के मामले में नुकसान को कम करने के लयि एक वशिेष सलाहकार को काम पर रखने की लागत।
4. यदि कोई तीसरा पक्ष मुकदमा दायर करता है तो न्यायालय में बचाव की लागत

नीचे दयि गए कूट का प्रयोग कर सही उत्तर चुनयि:

(A) केवल 1, 2 और 4
(B) केवल 1, 3 और 4
(C) केवल 2 और 3
(D) 1, 2, 3 और 41

उत्तर: (B)

प्रश्न. 2 भारत में नम्निलखिति में से कसिके लयि साइबर सुरक्षा घटनाओं पर रपिोर्ट करना कानूनी रूप से अनविार्य है? (वर्ष 2017)

1. सेवा प्रदाता
2. डेटा केंद्र
3. नगिमति नकिाय

नीचे दयि गए कूट का प्रयोग कर सही उत्तर चुनयि:

(A) केवल 1
(B) केवल 1 और 2
(C) केवल 3
(D) 1, 2 और 3

उत्तर: (D)

??????:

प्रश्न: साइबर सुरक्षा के वभिन्नि घटक क्या हैं? साइबर सुरक्षा में चुनौतियों को ध्यान में रखते हुए जाँच करें कि भारत ने व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति को कसि हद तक सफलतापूर्वक वकिसति कयिा है। (वर्ष 2022)