डिजिटिल अरेस्ट

प्रलिम्सि के लयि:

डिजिटिल अरेस्ट, CBI, प्रवर्तन निदेशालय, नारकोटिक्स ब्यूरो, भारतीय साइबर अपराध समन्वय केंद्र, CBDC, क्रिप्टोकरेंसी, राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल, वर्चुअल प्राइवेट नेटवर्क, पोंजी या पिरामिड योजनाएँ, राष्ट्रीय साइबर अपराध हेल्पलाइन, आधार

मेन्स के लयि:

साइबर धोखाधड़ी की आर्थिक लागत, संबंधित जोखिम एवं आगे की राह।

स्रोत: द हिंदू

चर्चा में क्यों?

डिजिटिल अरेस्ट साइबर स्कैम का सबसे नवीन रूप है जिससे **वर्ष 2024 में 92,000** से अधिक भारतीय प्रभावित हुए हैं, जिसमें कर या कानूनी बकाया को हल करने की आड़ में ऑनलाइन अंतरण के माध्यम से धन निकाला जाता है।

डिजिटिल अरेस्ट के बारे में मुख्य तथ्य क्या हैं?

- डिजिटिल अरेस्ट घोटाले में साइबर अपराधी **विधि प्रवर्तन अधिकारियों या सरकारी एजेंसियों** जैसे राज्य पुलिस, CBI, **ED** और **नारकोटिक्स ब्यूरो** की नकली पहचान बनाकर आम **लोगों** से ठगी करते हैं।
  - घोटालेबाज लोग **बिना किसी संदेह के लोगों को फोन करके** दावा करते हैं कि उनके खिलाफ मामला दर्ज किया गया है तथा अपने आरोपों को विश्वसनीय बनाने के लिये वे **फेक पुलिस थाने** का भी इस्तेमाल करते हैं।
- **साइबर अपराधी फोन या ईमेल के माध्यम** से पीड़ितों से संपर्क करते हैं। ये शुरुआत ऑडियो कॉल से करते हैं और फिर हवाई अड्डों, पुलिस स्टेशनों या न्यायालयों जैसे स्थानों से **वीडियो कॉल** करते हैं।
  - ये वैध दिखने के लिये अपने सोशल मीडिया अकाउंट पर **पुलिस अधिकारियों, वकीलों और न्यायाधीशों** की तस्वीरों को डिस्प्ले पिक्चर के रूप में इस्तेमाल करते हैं।
  - ये ईमेल या मैसेजिंग ऐप के माध्यम से **फेक गिरफ्तारी वारंट, कानूनी नोटिस या आधिकारिक दिखने वाले दस्तावेज़** भी भेज सकते हैं।
- **पीड़ितों को फँसाना:** साइबर अपराधी आमतौर पर पीड़ितों पर गंभीर अपराधों जैसे धन शोधन, मादक पदार्थों की तस्करी **या साइबर अपराध** का आरोप लगाते हैं।
  - वे अपने आरोपों को विश्वसनीय बनाने के लिये नकली **साक्ष्य बना** सकते हैं।
- **लोगों की भेद्यता:**
  - **भय और घबराहट**: गिरफ्तारी की धमकी या भय से पीड़ित **बिना सोचे-समझे ऐसे लोगों की बात सही** मान लेते हैं।
  - **जानकारी का अभाव**: विधि प्रवर्तन प्रक्रियाओं से अनभिज्ञता के कारण पीड़ितों के लिये वैध दावों और धोखाधड़ी के बीच अंतर करना कठिन हो जाता है।
  - **सामाजिक कलंक: सामाजिक कलंक** एवं परिवार पर पड़ने वाले प्रभाव के डर से पीड़ित ठगी का शिकार होते हैं।
  - **तकनीक का प्रयोग:** विश्वसनीय दिखने के लिये **इसमें AI आवाज़ों, पेशेवर लोगों और नकली वीडियो कॉल** का उपयोग किया जाता है।
  - **तकनीकी संवेदनशीलता**: **तकनीकी की कम जानकारी रखने वाले** या तनावग्रस्त व्यक्ति आसानी से धोखाधड़ी का शिकार हो जाते हैं।

भारत में 'साइबर स्कैम' की स्थिति क्या है?

- **अवलोकन:** भारतीय साइबर अपराध समन्वय केंद्र (I4C) के अनुसार, भारत में साइबर स्कैम/साइबर धोखाधड़ी की **आवृत्ति और वित्तीय प्रभाव** दोनों में उल्लेखनीय वृद्धि हुई है।
  - यह चिंताजनक प्रवृत्ति भारत के डिजिटिल पारिस्थितिकी तंत्र में **लगातार बढ़ते खतरे का संकेत देती है।**
- **शिकायतें और नुकसान**: पिछले कुछ वर्षों में शिकायतों की संख्या में उल्लेखनीय वृद्धि हुई है, **वर्ष 2021 में 1,35,242, वर्ष 2022 में 5,14,741**

और वर्ष 2023 में 11,31,221 शिकायतें दर्ज की गई हैं।
    - **वर्ष 2021 से सितंबर, 2024** के बीच **साइबर स्कैम** से **कुल मौद्रिक नुकसान 27,914 करोड़ रुपए तक पहुँच गया है।**
- **प्रमुख स्कैम:**
    - **स्टॉक ट्रेडिंग स्कैम: 2,28,094** शिकायतों से **4,636 करोड़ रुपए की** हानि के साथ यह नुकसान का सबसे महत्त्वपूर्ण स्रोत है।
        - स्कैम करने वाले इसका उपयोग इक्विटी, विदेशी मुद्रा या क्रिप्टोकरेंसी का व्यापार करते समय अतार्किक लाभ का वादा करने के लिये करते हैं, लेकिन पीड़ित अंततः धोखे का शिकार हो जाते हैं।
    - **पोंजी स्कीम स्कैम**: **1,00,360** शिकायतों के कारण **3,216 करोड़ रुपए** का नुकसान हुआ है।
    - **"डिजिटल अरेस्ट" धोखाधड़ी**: **63,481** शिकायतों से **1,616 करोड़ रुपए** का नुकसान हुआ है।
- **धन के धोखाधड़ी की नई रणनीति:** साइबर अपराधियों ने धन के धोखाधड़ी के लिये अपनी रणनीतियाँ अपना ली हैं।
    - **निकासी के तरीके**: चोरी किये गए पैसे अक्सर विभिन्न चैनलों के माध्यम से निकाले जाते हैं, जिनमें **चेक, CBDC, फिनटेक क्रिप्टोकरेंसी, ATM, मर्चेंट पेमेंट** और **ई-वॉलेट शामिल हैं।**
    - **मुले अकाउंट (Mule Accounts)**: I4C ने लगभग **4.5 लाख मुले अकाउंट** की पहचान की है और उन्हें फ्रीज कर दिया है, जिनका उपयोग मुख्य रूप से साइबर अपराध से धन शोधन के लिये किया जाता था।

भारतीय साइबर अपराध समन्वय केंद्र (I4C):

- **परिचय: I4C को गृह मंत्रालय** द्वारा वर्ष 2020 में '**साइबर स्कैम** सहित सभी प्रकार के **साइबर अपराधों** से व्यापक और समन्वित तरीके से निपटने के लिये लॉन्च किया गया था।
- **I4C के उद्देश्य:**
    - देश में **साइबर अपराध** पर अंकुश लगाने के लिये एक **नोडल निकाय के रूप में कार्य करना।**
    - **महिलाओं और बच्चों के** विरुद्ध साइबर अपराध के विरुद्ध **लड़ाई को मजबूत करना।**
    - **साइबर अपराध से संबंधित शिकायतों को आसानी से दर्ज करने** और साइबर अपराध की प्रवृत्तियों और पैटर्न की पहचान करने में सुविधा प्रदान करना।
    - सक्रिय साइबर अपराध की रोकथाम और पता लगाने के लिये **कानून प्रवर्तन एजेंसियों के लिये** एक प्रारंभिक चेतावनी प्रणाली के रूप में कार्य करना।
    - साइबर अपराध को रोकने के बारे में जनता में **जागरूकता उत्पन्न करना।**
    - साइबर फोरेंसिक, जाँच, साइबर स्वच्छता, साइबर अपराध विज्ञान आदि के क्षेत्र में **पुलिस अधिकारियों, सरकारी अभियोजकों और न्यायिक अधिकारियों की क्षमता निर्माण** में राज्यों/संघ राज्य क्षेत्रों की सहायता करना।
- **राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल:**
    - I4C के तहत, राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल एक **नागरिक-केंद्रित पहल है जो नागरिकों को साइबर धोखाधड़ी की ऑनलाइन रिपोर्ट करने** में सक्षम बनाएगी और सभी शिकायतों तक संबंधित कानून प्रवर्तन एजेंसियों द्वारा विधि के अनुसार कार्रवाई करने के लिये पहुँच सुनिश्चित की जाएगी।

साइबर स्कैम के निपटान हेतु क्या चुनौतियाँ हैं?

- **गोपनीयता: साइबर अपराधी अपनी पहचान और स्थान को छिपाने के लिये वर्चुअल प्राइवेट नेटवर्क (VPNA)** और **एन्क्रिप्टेड मैसेजिंग** ऐप जैसे उपकरणों का उपयोग करते हैं, जिससे उन्हें पता लगाने और गिरफ्तार करने के प्रयास जटिल हो जाते हैं।
- **अंतर्राष्ट्रीय दायरा**: साइबर स्कैम अक्सर **कई देशों तक फैले होते हैं,** जिससे स्थानीय कानून प्रवर्तन एजेंसियों के लिये कार्रवाई करना मुश्किल हो जाता है।
- स्कैम का एक बड़ा हिस्सा **दक्षिण पूर्व एशिया और चीन से आता है।**
- **तेज़ी से विकसित हो रही रणनीतियाँ**: फिशिंग घोटाले ईमेल के माध्यम से अधिक परिष्कृत तरीकों से किये जाते हैं, जिनमें **सोशल इंजीनियरिंग, टेक्स्ट मैसेज और वॉयस कॉल शामिल हैं,** जिससे धोखाधड़ी का पता लगाना कठिन हो गया है।
- **उन्नत मैलवेयर :** साइबर स्कैम उन्नत मैलवेयर का उपयोग करते हैं जो डेटा चोरी करने या अनधिकृत पहुँच प्राप्त करने के लिये **एंटीवायरस प्रोग्राम और फायरवॉल को बायपास** कर सकते हैं।
- **विनियामक विखंडन :** विभिन्न देशों के अलग-अलग नियम हैं, जिससे साइबर अपराध से निपटने के लिये सुसंगत अंतर्राष्ट्रीय रणनीति बनाना कठिन हो जाता है।
    - इसके अलावा, देशों के पास **डेटा साझा किये बिना** उभरते साइबर स्कैम के रुझान और रणनीति की पहचान करने के लिये **व्यापक खतरा खुफिया जानकारी का अभाव है।**
- **बढ़ता डिजिटल बाज़ार : ई-कॉमर्स और डिजिटल भुगतान प्रणालियों** के विकास के कारण **फेक ऑनलाइन स्टोर, कार्ड स्कीमिंग और धोखाधड़ी भुगतान योजनाओं** जैसे स्कैम में वृद्धि हुई है।

साइबर स्कैम के प्रकार

- **फिशिंग स्कैम :** धोखेबाज़, विश्वसनीय संगठनों की नकल करते हुए **नकली ईमेल या संदेश भेजते हैं,** ताकि पीड़ितों से **पासवर्ड या वित्तीय विवरण** जैसी संवेदनशील जानकारी साझा करवा सकें।
- **लॉटरी और पुरस्कार स्कैम :** पीड़ितों को सूचना मिलती है कि उन्होंने एक **महत्त्वपूर्ण पुरस्कार** जीता है और उसे प्राप्त करने के लिये उनसे **प्रोसेसिंग शुल्क या कर का भुगतान** करने के लिये कहा जाता है।
- **भावनात्मक हेरफेर स्कैम : डेटिंग ऐप्स** पर स्कैमर पीड़ितों के साथ संबंध बनाते हैं और बाद में आपात स्थिति के लिये पैसे मांगते हैं,

अक्सर **क्रिप्टोकरेंसी** में भुगतान की मांग करते हैं।

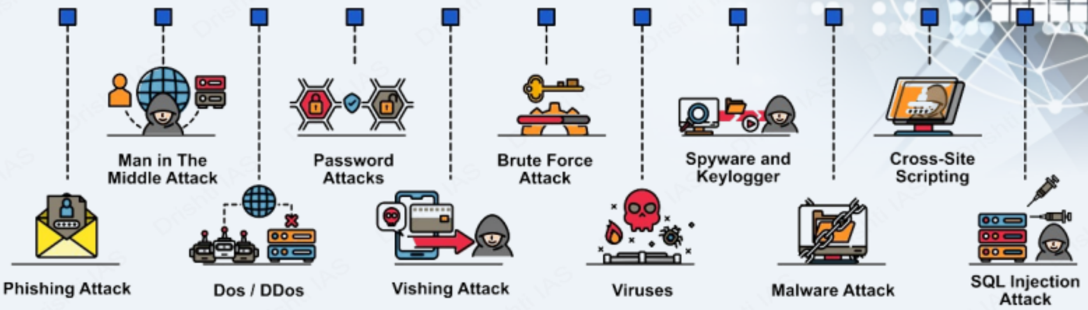
- **जॉब स्कैम :** स्कैमर जॉब चाहने वालों, विशेष रूप से नए स्नातकों को **व्यक्तिगत जानकारी या पैसा** देने के लिये भर्ती प्लेटफार्मों या सोशल मीडिया पर **फेक जॉब लिस्टिंग** पोस्ट करते हैं।
- **निवेश स्कैम :** ये स्कैम **पोंजी या पिरामिड योजनाओं** के माध्यम से उच्च, अवास्तविक रिटर्न का वादा करके **पीड़ित की त्वरित धन कमाने की इच्छा** को आकर्षित करते हैं।
- **कैश-ऑन-डिलीवरी (CoD) स्कैम :** स्कैमर **नकली ऑनलाइन स्टोर** बनाते हैं जो CoD ऑर्डर स्वीकार करते हैं। जब उत्पाद डिलीवर किया जाता है, तो यह या तो **नकली होता है या विज्ञापित के अनुसार नहीं होता है।**
- **फेक चैरिटी अपील स्कैम :** स्कैमर **आपदा राहत या स्वास्थ्य पहल** जैसे अनुपयुक्त कारणों के लिये **फेक वेबसाइट या सोशल मीडिया पेज** बनाते हैं, तथा **तात्कालिकता और सहानुभूति** पैदा करने के लिये भावनात्मक कहानियों या छवियों का उपयोग करते हैं।
- **गलत तरीके से धन-हस्तांतरण स्कैम :** स्कैमर पीड़ितों से संपर्क कर दावा करते हैं कि उनके खाते में **गलती से धन भेज दिया गया है,** तथा **कानूनी परेशानी** से बचने के लिये धन वापस करने के लिये उन पर दबाव डालने के लिये फेक लेनदेन रसीदों का उपयोग करते हैं।
- **क्रेडिट कार्ड स्कैम** : स्कैमर **कम ब्याज दरों पर ऋण** की पेशकश करते हैं और उसे तुरंत मंज़ूरी दे देते हैं। पीड़ित द्वारा ऋण सुरक्षित करने के लिये **अग्रिम शुल्क का भुगतान करने** के बाद, स्कैमर गायब हो जाते हैं।

//

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

- महत्वपूर्ण बुनियादी ढाँचा सुरक्षा (रोबस्ट एक्सेस कंट्रोल)
- नेटवर्क सुरक्षा (डिप्लॉयिंग फायरवॉल)
- एप्लिकेशन सुरक्षा (कोड रिव्यु)
- 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 हस्ताक्षरकर्ता नहीं है)
- **भारतीय स्तर पर:**
  - IT अधिनियम, 2000 (धारा 43, 66, 66B, 66C, 66D)
  - राष्ट्रीय साइबर सुरक्षा नीति, 2013
  - नेशनल साइबर सिक्योरिटी स्ट्रेटजी, 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 स्कैम से संबंधित प्रमुख सरकारी पहल क्या हैं?

- राष्ट्रीय साइबर सुरक्षा नीति
- कंप्यूटर आपातकालीन प्रतिक्रिया टीम - भारत (CERT-In)
- साइबर सुरक्षित भारत पहल
- साइबर स्वच्छता केंद्र
- राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIIPC)
- डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023
- साइबर अपराध समन्वय केंद्र
- नागरिक वित्तीय साइबर धोखाधड़ी रिपोर्टिंग और प्रबंधन प्रणाली

आगे की राह

- **डिजिटल सुरक्षा: भारत के प्रधानमंत्री ने** डिजिटल अरेस्ट से बचाव के लिये एक सरल **तीन-चरणीय सुरक्षा प्रोटोकॉल की रूपरेखा प्रस्तुत की।**
  - **विराम:** शांत रहें एवं त्वरित **व्यक्तिगत जानकारी देने से बचें।**
  - **विचार करना:** ध्यान रखें कि **विधिक एजेंसियाँ** कॉल के माध्यम से ऐसी पूछताछ नहीं करती हैं या कॉल के माध्यम से भुगतान की मांग नहीं करती हैं।
  - **कार्रवाई करना:** राष्ट्रीय साइबर अपराध हेल्पलाइन **(1930) या** राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल पर घटनाओं की रिपोर्ट करना, परिवार के सदस्यों को सूचित करना एवं साक्ष्य दर्ज करना।
- **साइबर सुरक्षा के सर्वोत्तम अभ्यास: फायरवॉल का** उपयोग करना, जो कंप्यूटरों के लिये **सुरक्षा की प्रथम पंक्ति के रूप में कार्य करते हैं,** अनधिकृत पहुँच को रोकने के लिये नेटवर्क ट्रैफिक की निगरानी और फिल्टर करते हैं।
  - सुरक्षा संबंधित कमियों को दूर करने के लिये सभी सॉफ्टवेयर और हार्डवेयर प्रणालियों को **अद्यतन रखना।**
- **उन्नत सुरक्षा: सुरक्षा की एक अतिरिक्त स्तर जोड़ने के लिये टू-फैक्टर प्रमाणीकरण** लागू करना। वित्तीय रिकॉर्ड सहित संवेदनशील डेटा की सुरक्षा के लिये एन्क्रिप्शन का उपयोग करना।
- **सतर्कता में वृद्धि: बैंकों को कम शेष वाले या वेतनभोगी खातों में उच्च मूल्य के लेनदेन की** निगरानी करनी चाहिये तथा प्राधिकारियों को सचेत करना चाहिये, क्योंकि **चोरी का पैसा** अक्सर इन खातों में स्थानांतरित कर दिया जाता है **तथा उसके बाद उसे क्रिप्टोकरेंसी में परिवर्तित कर विदेश भेज दिया जाता है।**
- **जागरूकता:** कोई भी व्यक्तिगत जानकारी (जैसे आधार **या** पैन कार्ड विवरण) एवं पैसा न देना।
  - हमेशा आधिकारिक चैनलों के माध्यम से **कॉल करने वाले की पहचान स्वतंत्र रूप से सत्यापित करना।**
  - **सामान्य धोखाधड़ी की रणनीति** के बारे में जानें और ऐसी घटनाओं को रोकने के लिये इस जानकारी को अपने परिवार और दोस्तों के साथ साझा करना।
- **अंतर्राष्ट्रीय सहयोग : समान कानून बनाने, खुफिया जानकारी साझा करने और प्रतिक्रियाओं में समन्वय स्थापित करने** के लिये राष्ट्रों के बीच सहयोग से सीमा पार साइबर अपराध से निपटने में सहायता मिल सकती है।

??????? ?????? ????????? ???????:

प्रश्न: साइबर स्कैम के विभिन्न प्रकार क्या हैं? साइबर स्कैम से निपटने में क्या चुनौतियाँ विद्यमान हैं?

UPSC सिविल सेवा परीक्षा, विगत वर्ष के प्रश्न (PYQ)

??????????

प्रश्न. भारत में, किसी व्यक्ति के साइबर बीमा कराने पर, निधि की हानि की भरपाई एवं अन्य लाभों के अतिरिक्त

निम्नलिखित में से कौन-कौन से लाभ दिये जाते हैं? (2020)

1. यदि कोई किसी मैलवेयर कंप्यूटर तक उसकी पहुँच को बाधित कर देता है तो कंप्यूटर प्रणाली को पुनः प्रचालित करने में लगने वाली लागत
2. यदि यह प्रमाणित हो जाता है कि किसी शरारती तत्त्व द्वारा जानबूझ कर कंप्यूटर को नुकसान पहुँचाया गया है तो एक नए कंप्यूटर की लागत
3. यदि साइबर बलात्-ग्रहण होता है तो इस हानि को न्यूनतम करने के लिये विशेष परामर्शदाता की की सेवाएँ पर लगने वाली लागत
4. यदि कोई तीसरा पक्ष मुकदमा दायर करता है तो न्यायालय में बचाव करने में लगने वाली लागत

नीचे दिये गए कूट का प्रयोग कर सही उत्तर चुनिये:

(a) केवल 1,2 और 4
(b) केवल 1, 3 और 4

(c) केवल 2 और 3
(d) 1, 2, 3 और 4

उत्तर: (b)

प्रश्न. भारत में साइबर सुरक्षा घटनाओं पर रपिोर्ट करना नम्निलखिति में से कसिके/कनिके लयि वधितिः अधदिशात्मक है? (2017)

1. सेवा प्रदाता
2. डेटा सेंटर
3. कॉर्पोरेट 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 तत्त्व क्या हैं? साइबर सुरक्षा की चुनौतयिों को ध्यान में रखते हुए समीक्षा कीजयि कि भारत ने कसि हद तक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति सिफलतापूर्वक वकिसति की है। (2022)

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/rising-digital-arrests