उभरते साइबर खतरे और उनके नहितिार्थ

यह संपादकीय 29/11/2024 को लाइवमटि में प्रकाशति "Cyber cons go from digital arrests to wedding scams" पर आधारति है। इस लेख में फर्जी शादी के नमिंत्रण घोटालों से लेकर 'डजिटिल अरेस्ट' तक साइबर अपराध की बढ़ती जटलिता को सामने लाया गया है, साथ ही सुदृढ़ डजिटिल जागरूकता और सख्त साइबर सुरक्षा उपायों की तत्काल आवश्यकता पर प्रकाश डाला गया है।

प्रलिमि्स के लयि:

साइबर अपराध, डजिटिल अरेस्ट स्कैम, सूचना प्रौद्योगकिी अधनियिम, 2000, डजिटिल व्यक्तगित डेटा संरक्षण अधनियिम, 2023, भारतीय कंप्यूटर आपातकालीन प्रतक्रियिा दल, राष्ट्रीय क्रटिकिल इंफॉर्मेशन इंफ्रास्ट्रक्चर संरक्षण केंद्र, साइबर स्वच्छता केंद्र, भारत राष्ट्रीय साइबर सुरक्षा अभ्यास 2024, दूरसंचार (महत्त्वपूर्ण दूरसंचार अवसंरचना) नयिम, 2024, रैनसमवेयर अटैक, साइबर अपराध पर बुडापेस्ट कन्वेंशन

मेन्स के लयि:

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

साइबर अपराध के लगातार वकिसति होते परदृिश्य में, धोखेबाज़/घोटालेबाज़ (Fraudsters) डजिटिल कमज़ोरयिों का फायदा उठाने के लयि तेज़ी से अधकि उन्नत तकनीक वकिसति कर रहे हैं, जसिमें 'डजिटिल अरेस्ट' की आवष्कृत अवधारणा से लेकर व्हाट्सएप पर नकली शादी के नमिंत्रण जैसी भ्रामक योजनाएँ शामलि हैं। जैसे-जैसे भारतीय इन उभरते खतरों से जूझ रहे हैं, **आभासी और वास्तवकि दुनयिा की धोखाधड़ी के बीच की सीमाएँ तेज़ी से धूमलि पड़ती** जा रही हैं, जसिसे हमारे **डजिटिल बुनयिादी अवसंरचना में कठनि प्रणालीगत चुनौतयिाँ** सामने आ रही हैं। धोखाधड़ी का प्रसार **व्यापक डजिटिल जागरूकता** और **सख्त साइबर सुरक्षा तंत्र की महत्त्वपूर्ण आवश्यकता** को रेखांकति करता है जसिसे वकिसति हो रही आपराधकि रणनीतयिों का अनुमान लगाकर उन्हें बेअसर कयिा जा सकता है।

भारत में साइबर सुरक्षा के लयि वर्तमान फ्रेमवर्क क्या है?

- **वधिायी उपाय:**
  - सूचना प्रौद्योगकिी अधनियिम, 2000 **(IT अधनियिम):** यह आधारभूत कानून **इलेक्ट्रॉनकि शासन के लयि कानूनी फ्रेमवर्क प्रदान** करता है और **साइबर अपराधों और इलेक्ट्रॉनकि वाणज्यि से नपिटता है।**
    - इसमें **डेटा संरक्षण और साइबर सुरक्षा से संबंधति प्रावधानों को शामलि करने के लयि संशोधन** कयिा गया है।
  - डजिटिल व्यक्तगित डेटा संरक्षण अधनियिम, 2023**: व्यक्तगित डेटा की सुरक्षा के** लयि अधनियिमति, यह अधनियिम व्यक्तगित डेटा के प्रसंस्करण में **व्यक्तयिों के अधकिारों और डेटा फडिुयुशरीज़ के दायत्विों** को रेखांकति करता है।
    - यह वैध प्रसंस्करण, डेटा न्यूनीकरण और जवाबदेही पर ज़ोर देता है।
- **संस्थागत फ्रेमवर्क:**
  - भारतीय कंप्यूटर आपातकालीन प्रतक्रियिा दल **(CERT-In): इलेक्ट्रॉनक्सि और सूचना प्रौद्योगकिी मंत्रालय** के तहत कार्यरत, CERT-In कंप्यूटर सुरक्षा घटनाओं पर प्रतक्रियिा देने वाली राष्ट्रीय नोडल एजेंसी है।
    - यह परामर्श जारी करती है, प्रशक्षिण आयोजति करती है तथा हतिधारकों के बीच समन्वय को सुगम बनाती है।
  - राष्ट्रीय क्रटिकिल इंफॉर्मेशन इंफ्रास्ट्रक्चर संरक्षण केंद्र **(NCIIPC):** NCIIPC बजिली, बैंकगि और दूरसंचार जैसे क्षेत्रों में महत्त्वपूर्ण सूचना अवसंरचना की सुरक्षा पर ध्यान केंद्रति करता है।
    - यह इन परसिंपत्तयिों की सुरक्षा के लयि रणनीतयिाँ और नीतयिाँ वकिसति करता है।
  - भारतीय साइबर अपराध समन्वय केंद्र (I4C)**: गृह मंत्रालय** द्वारा शुरू कयिा गया I4C एक समन्वति उपागम के माध्यम से साइबर अपराध को नयिंत्रति करता है, जसिमें राष्ट्रीय साइबर अपराध रपिोर्टगि पोर्टल और क्षमता नरि्माण पहल शामलि हैं।
  - साइबर स्वच्छता केंद्र**:** फरवरी 2017 में स्थापति, साइबर स्वच्छता केंद्र का उद्देश्य राष्ट्रीय साइबर सुरक्षा नीतकि अनुरूप **बॉटनेट संक्रमण** तथा **मैलवेयर का पता लगाकर और उन्हें कम करके भारत में एक सुरक्षति साइबर पारस्थितिकिी तंत्र स्थापति करना है।**
  - **साइबर सुरक्षति भारत:** इलेक्ट्रॉनक्सि और सूचना प्रौद्योगकिी मंत्रालय (MeitY) की इस पहल की संकल्पना**साइबर अपराध के बारे**

में जागरूकता फैलाने और सभी सरकारी वभिागों में **मुख्य सूचना सुरक्षा अधकिारयिों (CISOs) तथा अग्रमि पंक्त के IT अधकिारयिों की क्षमता नरि्माण** के मशिन के साथ की गई थी।

- **रणनीतकि पहल:**
  - **राष्ट्रीय साइबर सुरक्षा नीत, 2013:** यह नीत साइबरस्पेस को सुरक्षति करने, सुरक्षति कंप्यूटगि वातावरण को बढ़ावा देने और राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना की अनुकूलता बढ़ाने के लयि दृष्टकिोण एवं रणनीतयिों को रेखांकति करती है।
  - **भारत राष्ट्रीय साइबर सुरक्षा अभ्यास 2024:** इस अभ्यास में **साइबर रक्षा और घटना प्रतक्रियिा पर गहन प्रशक्षिण,** IT एवं OT प्रणालयिों पर साइबर हमलों के लाइव-फायर समिुलेशन तथा सरकार व उद्योग के हतिधारकों के लयि सहयोगी मंच शामलि हैं।
- **क्षेत्र-वशिष्टि वनियिम:**
  - **SEBI वनियिमति संस्थाओं के लयि साइबर सुरक्षा और साइबर आघातसह फ्रेमवर्क:** भारतीय प्रतभिूत और वनिमिय बोर्ड द्वारा जारी यह फ्रेमवर्क वनियिमति संस्थाओं को प्रतभिूत बाज़ारों की सुरक्षा के लयि सुदृढ़ साइबर सुरक्षा एवं साइबर आघातसह नीतयिाँ स्थापति करने का अधकिार देता है।
  - **दूरसंचार (महत्त्वपूर्ण दूरसंचार अवसंरचना) नयिम, 2024:** नवंबर 2024 में पेश कयिा गया यह नयिम **महत्त्वपूर्ण दूरसंचार अवसंरचना (CTI) के रूप में चहिनति दूरसंचार संस्थाओं को अपने हार्डवेयर, सॉफ्टवेयर एवं डेटा का नरीक्षण करने** के लयि सरकारी अधकिृत कर्मयिों को अभगिम प्रदान करने का आदेश देता है।

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

- **डजिटिल अरेस्ट घोटाले:** साइबर अपराधयिों ने धोखाधड़ी का एक नया तरीका ईजाद कयिा है, जसिमें वे **कानून प्रवर्तन अधकिारयिों का रूप धारण कर अनजान पीड़तिों में भय** उत्पन्न करते हैं।
  - व्यक्तयिों से संपर्क कर ये धोखेबाज दावा करते हैं कि वे मनगढ़ंत अपराधों के लयि जाँच के दायरे में हैं, तथा फर्जी गरिफ्तारी से बचने के लयि उन्हें भारी जुर्माना भरने के लयि मज़बूर करते हैं।
  - **कानून प्रवर्तन से जुड़े प्राधकिार और पीड़तिों की डजिटिल साक्षरता की कमी** का फायदा उठाकर, ये घोटाले खतरनाक रूप से प्रभावी हो गए हैं।
  - वर्ष 2024 में, भारतीयों ने सामूहकि रूप से इस तरह के **"डजिटिल अटैक" धोखाधड़ी में ₹120.30 करोड़ का नुकसान उठाया।**
- **रैनसमवेयर हमले:** रैनसमवेयर हमले बढ़ गए हैं, ज़ो **महत्त्वपूर्ण बुनयिादी अवसंरचना और वत्तिीय संस्थानों को नशिाना बना रहे हैं,** जसिसे परचिालन संबंधी व्यवधान एवं वत्तिीय नुकसान हो रहा है।
  - **अगस्त 2024** में, **C-Edge टेक्नोलॉजीज़** पर रैनसमवेयर हमले ने लगभग 300 छोटे भारतीय बैंकों की भुगतान प्रणालयिों को बाधति कर दयिा, जसिसे वत्तिीय नेटवर्क में कमज़ोरयिाँ उजागर हुईं।
  - इसके अलावा, दल्लिी में **अखलि भारतीय आयुर्वज्ञिान संस्थान (AIIMS) पर वर्ष 2023** रैनसमवेयर अटैक स्वास्थ्य सेवा के बुनयिादी अवसंरचना की कमज़ोरयिों का उदाहरण है।
- **आपूर्त शृंखला हमले:** साइबर अपराधी बड़े नेटवर्क में घुसपैठ करने के लयि आपूर्त शृंखलाओं की कमज़ोरयिों का तेज़ी से फायदा उठा रहे हैं।
  - उदाहरण के लयि **दसिंबर 2020** में, नेटवर्क प्रबंधन उपकरण प्रदान करने वाली एक अमेरकिी सॉफ्टवेयर कंपनी सोलरवड्सि को नशिाना बनाकर कयि गए एक वैश्वकि साइबर हमले ने **राष्ट्रीय सूचना वज्ञिान केंद्र (NIC), इलेक्ट्रॉनक्सि और सूचना प्रौद्योगकिी मंत्रालय (MeitY),** और **भारत हेवी इलेक्ट्रकिल्स लमिटिेड (BHEL) सहति कई भारतीय संगठनों को प्रभावति कयिा।**
  - भारतीय साइबर अपराध समन्वय केंद्र (I4C) के आँकड़ों के अनुसार वर्ष 2024 के प्रारंभकि नौ महीनों में भारत को साइबर धोखाधड़ी से **11,333 करोड़ रुपए** का नुकसान हुआ।
- **राज्य प्रायोजति साइबर जासूसी:** राष्ट्र-राज्य अभकिर्त्ता साइबर **जासूसी गतविधियिों को तेज़ कर रहे हैं,** संवेदनशील सरकारी और कॉर्पोरेट डेटा को नशिाना बना रहे हैं।
  - **चीन से उत्पन्न एक साइबर हमले को वर्ष 2020 में मुंबई** में बड़े पैमाने पर बजिली कटौती का कारण माना गया, जसिसे शहर के महत्त्वपूर्ण बुनयिादी अवसंरचना की कमज़ोरयिाँ उजागर हुईं।
- **डीपफेक प्रौद्योगकिी का दुरुपयोग:** AI-जनरेटेड **डीपफेक के दुरुपयोग** से गलत सूचना और धोखाधड़ी सहति कई गंभीर खतरे उत्पन्न होते हैं।
  - वर्ष 2024 की एक रपिोर्ट में डीपफेक को भारत में एक आसन्न खतरे के रूप में पहचाना गया है, ज़ो जनता के वश्विास को कम करने और सूचनाओं में हेरफेर करने में सक्षम है।
  - **अभनित्री रश्मकिा मंदाना को** एक डीपफेक फल्मि में दखिाया गया, जो ऑनलाइन वायरल हो गई, जसिसे व्यापक आक्रोश फैल गया।
- **इंटरनेट ऑफ थग्सि (IoT) उपकरणों का शोषण:** **इंटरनेट ऑफ थग्सि (IoT) उपकरणों को** व्यापक रूप से अपनाए जाने से **डजिटिल पारस्थितिकी तंत्र की भेद्यता बहुत** बढ़ गई है, जसिसे साइबर अपराधयिों के लयि नए अवसर उत्पन्न हो गए हैं।
  - इन उपकरणों में प्रायः सुदृढ़ सुरक्षा सुवधिाओं का अभाव होता है तथा इनका उपयोग नेटवर्क में सेंध लगाने या दुर्भावनापूर्ण गतविधियिों को अंजाम देने के लयि आसानी से कयिा जाता है।
  - वर्ष 2024 में, **भारत में IoT-संबंधति साइबर हमलों में 59% की उल्लेखनीय वृद्धि** देखी गई, जो इस उभरते खतरे के पैमाने को रेखांकति करती है।
  - स्मार्ट घरों से लेकर कनेक्टेड औद्योगकि प्रणालयिों तक, असुरक्षति IoT उपकरणों से जुड़े ज़ोखमि बढ़ गए हैं।
- **क्रप्टिोकरेंसी और ब्लॉकचेन-आधारति साइबर धोखाधड़ी:** भारत में क्रप्टिोकरेंसी के उपयोग में तीव्र वृद्धि ने **परष्कृत साइबर धोखाधड़ी तंत्र के लयि बड़े पैमाने पर एक नया, अनयिमति परदृिश्य** तैयार कर दयिा है।
  - **ब्लॉकचेन-आधारति प्लेटफॉर्म तेज़ी से जटलि पोंज़ी स्कीम्स, पंप-एंड-डंप हेरफेर** और **उन्नत मनी लॉन्ड्रगि तकनीकों** का लक्ष्य बन रहे हैं जो नयिामक ग्रे एरयिाज़ का फायदा उठाते हैं।
  - बेंगलुरु स्थति **बटिकॉइन घोटाले** ने एक **हैकर, पुलसि अधकिारयिों और एक साइबर वशिेषज्ञ के बीच साँठ-गाँठ को उजागर कयिा, जसिमें 850 करोड़ रुपए** की क्रप्टिोकरेंसी का अवैध अंतरण, सबूतों से छेड़छाड़ तथा भ्रष्टाचार के आरोप शामलि थे।
- **डार्क वेब-सक्षम साइबर अपराध:** डार्क वेब चुराए गए डेटा और दुर्भावनापूर्ण टूल के अवैध व्यापार का केंद्र बना हुआ है।

- हैकर्स डार्क वेब पर अनुकूलित मैलवेयर और रैनसमवेयर किट बेच रहे हैं, जिससे लेस-स्किल्ड खतरा उत्पन्न करने वाले लोगों के लिये परिष्कृत हमले सुलभ हो रहे हैं।
- हाल ही में हुए एक सुरक्षा उल्लंघन ने **भारत में 750 मिलियन दूरसंचार उपयोगकर्त्ताओं के व्यक्तिगत डेटा** को उजागर कर दिया है, और यह डेटा डार्क वेब पर बेचा जा रहा है।

भारत में साइबर सुरक्षा परिदृश्य को बढ़ाने के लिये क्या उपाय अपनाए जा सकते हैं?

- **राष्ट्रव्यापी साइबर साक्षरता अभियान:** डिजिटल साक्षरता अभियान क्षेत्रीय भाषाओं में चलाए जाने चाहिये, **जिनका लक्ष्य ग्रामीण समुदायों एवं वरिष्ठ नागरिकों जैसी कमज़ोर आबादी को लक्षित करना हो।**
  - ये पहल उपयोगकर्त्ताओं को पहचान सत्यापित करना, धोखाधड़ी को पहचानना और सुरक्षित भुगतान प्रणाली का उपयोग करना सिखा सकती हैं।
  - स्कूलों, कॉलेजों और स्थानीय शासन निकायों के साथ साझेदारी से प्रभाव को बढ़ाया जा सकता है।
- **IoT उपकरणों के लिये अनिवार्य सुरक्षा प्रोटोकॉल: निर्माताओं** को IoT उपकरणों में **सिक्योरिटी-बाय-डिज़ाइन सिद्धांतों को एकीकृत करने के लिये** लागू करने योग्य मानकों को प्रस्तुत किये जाने चाहिये।
  - इसमें फर्मवेयर अपडेट, एन्क्रिप्टेड संचार और टैम्पर-प्रूफ तंत्र शामिल हैं।
  - विनियामक प्राधिकरण से प्रमाणन **यह सुनिश्चित कर सकता है कि केवल सुरक्षित डिवाइस ही बाज़ार तक पहुँचें।** IoT ज़ोखिमों के बारे में सार्वजनिक जागरूकता उपभोक्ता स्तर पर सुरक्षा को और बढ़ाएगी।
- **AI-संचालित खतरा खुफिया और प्रतिक्रिया प्रणाली: नेटवर्क ट्रैफिक का विश्लेषण करने, विसंगतियों की पहचान करने और खतरों का रियल टाइम रेस्पोंड करने** के लिये महत्त्वपूर्ण क्षेत्रों में AI-आधारित उपकरणों को तैनात किया जाना चाहिये।
  - इन प्रौद्योगिकियों में रैनसमवेयर हमलों का पूर्वानुमान लगाने तथा हमलों से पूर्व ही कमज़ोरियों को बेअसर करने की क्षमता है।
  - AI फोरेंसिक जाँच को भी बेहतर बना सकता है, जिससे घटनाओं पर तेज़ी से प्रतिक्रिया मिल सकती है। AI सिस्टम का नियमित परीक्षण सटीकता और विश्वसनीयता सुनिश्चित करता है।
- **CERT-In की क्षमताओं को सुदृढ़ बनाना:** CERT-In के कार्यक्षेत्र का विस्तार किया जाना चाहिये, जिसमें **अंतर्राष्ट्रीय CERT और निजी क्षेत्र के साथ गहन सहयोग शामिल करने के साथ ही** साइबर अपराध पर बुडापेस्ट कन्वेंशन जैसे अंतर्राष्ट्रीय फ्रेमवर्क के साथ प्रयासों को संरेखित किया जाए।
  - **स्थानीय घटनाओं पर तेज़ी से प्रतिक्रिया के लिये क्षेत्रीय CERT हब** शुरू करने की आवश्यकता है। खतरे का पता लगाने और उन्नत फोरेंसिक के लिये CERT-In को अत्याधुनिक उपकरणों से लैस किया जाना चाहिये।
  - संस्थागत आघातसहनीयता में सुधार के लिये सक्रिय रूप से परामर्श और अनुकरण अभ्यास जारी किये जाने चाहिये।
- **राष्ट्रीय डीपफेक डिटेक्शन और रेगुलेशन फ्रेमवर्क:** डीपफेक कंटेंट की रियल टाइम पहचान करने में सक्षम **एथिकल-AI उपकरण** विकसित करने की आवश्यकता है।
  - अद्यतन IT कानूनों के अंतर्गत **हानिकारक डीप फेक मीडिया के निर्माण और प्रसार के लिये दंड का** प्रावधान किया जाना चाहिये।
  - **ऐसे कंटेंट्स को चिह्नित करने और हटाने के लिये सोशल मीडिया प्लेटफॉर्म** के साथ सहयोग करने से इसके प्रसार को कम किया जा सकता है। जन जागरूकता अभियानों से लोगों को हेरफेर किये गए मीडिया को पहचानने के बारे में शिक्षित किया जाना चाहिये।
- **ज़िला स्तरीय साइबर सुरक्षा प्रतिक्रिया इकाइयाँ:** प्रत्येक ज़िले में प्रशिक्षित कर्मियों और फोरेंसिक उपकरणों से सुसज्जित समर्पित साइबर सुरक्षा प्रकोष्ठों की स्थापना की जानी चाहिये।
  - ये इकाइयाँ **'डिजिटल अरेस्ट' धोखाधड़ी जैसे छोटे पैमाने के घोटालों से शीघ्रता से निपट सकती हैं** और बड़े मुद्दों के लिये CERT-In के साथ समन्वय कर सकती हैं।
  - सामुदायिक सहभागिता कार्यक्रम विश्वास का निर्माण कर सकते हैं तथा घटनाओं की समय पर रिपोर्टिंग को प्रोत्साहित कर सकते हैं।
- **आपूर्ति शृंखला साइबर सुरक्षा प्रमाणन:** आपूर्ति शृंखला साझेदारों के लिये प्रमाणन प्रणाली लागू करने की आवश्यकता है, ताकि यह सुनिश्चित किया जा सके कि वे साइबर सुरक्षा की सर्वोत्तम प्रथाओं का पालन करते हैं।
  - इसमें **नियमित ऑडिट, ब्लॉकचेन एकीकरण, सुरक्षित सॉफ्टवेयर विकास प्रथाएँ** और **एन्क्रिप्टेड कम्युनिकेशन चैनल** शामिल हैं।
  - बड़े उद्यमों को विक्रेताओं से इन प्रमाणपत्रों की मांग करनी चाहिये। इससे छोटी इकाइयों के माध्यम से उल्लंघन के ज़ोखिम कम हो जाते हैं।
- **क्रिप्टोकरेंसी विनियमन:** पारदर्शिता और पता लगाने की क्षमता पर ध्यान केंद्रित करते हुए **क्रिप्टोकरेंसी लेनदेन** के लिये स्पष्ट विनियमन स्थापित किये जाने चाहिये।
  - **क्रिप्टो एक्सचेंजों के लिये अनिवार्य KYC** और रियल टाइम मॉनिटरिंग सिस्टम अवैध गतिविधियों को रोक सकती है।
  - विशेष क्रिप्टो फोरेंसिक इकाइयों को धोखाधड़ी का शीघ्रता से समाधान करना चाहिये।
- **अनिवार्य राष्ट्रीय साइबर सुरक्षा ऑडिट:** नियमित, सरकार द्वारा अनिवार्य ऑडिट महत्त्वपूर्ण बुनियादी अवसंरचना प्रणालियों में कमज़ोरियों की पहचान कर उन्हें ठीक कर सकते हैं।
  - **तनाव परीक्षण, प्रवेश परीक्षण और कर्मचारी प्रशिक्षण को** शामिल करने से व्यापक तत्परता सुनिश्चित होती है।
  - स्वास्थ्य सेवा, बैंकिंग और उपयोगिताओं जैसे क्षेत्रों के लिये ये ऑडिट अनिवार्य होने चाहिये। बेहतर सुरक्षा के लिये संसाधन आवंटन को प्राथमिकता देने के लिये परिणामों का उपयोग किया जा सकता है।
- **स्टार्ट-अप्स के लिये साइबर स्वच्छता जागरूकता: स्टार्टअप्स के लिये** सरकार द्वारा समर्थित **साइबर सुरक्षा प्रशिक्षण कार्यक्रम** शुरू किये जाने चाहिये।
  - साइबर सुरक्षा उपकरणों और सेवाओं तक रियायती अभिगम छोटे व्यवसायों को सर्वोत्तम प्रथाओं को अपनाने में सक्षम बना सकती है।
  - **निम्न स्तरीय सुरक्षा स्वच्छता के ज़ोखिमों के बारे में जागरूकता अभियान** स्टार्टअप को सुरक्षा में निवेश को प्राथमिकता देने के लिये प्रेरित कर सकते हैं। क्षेत्र-विशिष्ट मार्गदर्शन प्रासंगिकता सुनिश्चित करता है।
- **सक्रिय डार्क वेब मॉनिटरिंग: ऐसे उपकरणों में निवेश** किये जाने चाहिये जो **चोरी किये गए डेटा, अवैध सामान और मैलवेयर की बिक्री** के लिये

डार्क वेब की सक्रिय रूप से निगिरानी करते हैं।
    - **डार्क वेब गतिविधि से एकत्रित खुफिया जानकारी** से हमलों को रोका जा सकता है तथा कानून प्रवर्तन कार्यों को निर्देशित किया जा सकता है।
    - सार्वजनिक-निजी सहयोग से निगिरानी क्षमताओं का विस्तार किया जा सकता है। समर्पित टास्क फोर्स को अभिनिर्धारित किये गए खतरों पर तुरंत कार्रवाई करनी चाहिये।
- **बहु-कारक प्रमाणीकरण (MFA) प्रवर्तन:** केवल पासवर्ड पर निर्भरता कम करने के लिये महत्त्वपूर्ण प्रणालियों, सरकारी पोर्टलों और वित्तीय प्लेटफॉर्मों पर MFA को अनिवार्य बनाया जाना चाहिये।
    - व्यवसायों को सुरक्षा से समझौता किये बिना उपयोगकर्त्ता अनुभव को बेहतर बनाने के लिये अनुकूली MFA सिस्टम अपनाना चाहिये। इससे अनधिकृत पहुँच के ज़ोखिम कम हो जाते हैं।
- **शिक्षा क्षेत्र के लिये साइबर सुरक्षा:** स्कूलों और विश्वविद्यालयों में साइबर सुरक्षा जागरूकता और बचाव तंत्र शुरू किये जाने चाहिये। इसमें **नियमित बैकअप, सुरक्षित नेटवर्क और खतरों से निपटने के लिये कर्मचारियों को प्रशिक्षण देना शामिल है।**
    - राष्ट्रीय कार्यक्रम छोटे संस्थानों को अपनी सुरक्षा बढ़ाने के लिये संसाधन प्रदान कर सकते हैं। जागरूकता अभियानों में छात्रों को शामिल करने से साइबर सुरक्षा की संस्कृति का निर्माण होता है।
- **डेटा स्थानीयकरण मानदंडों को लागू करना:** यद्यपि **डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023** में डेटा स्थानीयकरण के प्रावधान शामिल हैं, लेकिन इन्हें **केवल कागज़ पर औपचारिकता मात्र** नहीं रहना चाहिये, बल्कि इन्हें अक्षरशः और भावनापूर्वक लागू किया जाना चाहिये।
    - यह अनिवार्य करना कि **महत्त्वपूर्ण एवं संवेदनशील डेटा राष्ट्रीय सीमाओं के भीतर ही संग्रहीत रहे,** नियंत्रण में सुधार कर सकता है और सुरक्षा ज़ोखिम को कम कर सकता है।
    - स्पष्ट अनुपालन रूपरेखा और उल्लंघन के लिये दंड लागू किया जाना चाहिये।

निष्कर्ष:

साइबर अपराध के उभरते परिदृश्य के लिये एक **व्यापक और सक्रिय दृष्टिकोण की आवश्यकता है।** भारत को अपने साइबर सुरक्षा फ्रेमवर्क को सुदृढ़ करने, **डिजिटल साक्षरता को बढ़ावा देने और इन खतरों से प्रभावी ढंग से निपटने के लिये अंतर्राष्ट्रीय सहयोग को बढ़ावा** देने की आवश्यकता है। सख्त सुरक्षा उपायों में निवेश करके, कुशल कार्यबल का निर्माण करके और उभरते खतरों से आगे रहकर, भारत अपने डिजिटल भविष्य की रक्षा कर सकता है तथा अपने नागरिकों को साइबर हमलों के बढ़ते ज़ोखिमों से बचा सकता है।

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

प्रश्न. भारत में डिजिटल प्रौद्योगिकियों पर बढ़ती निर्भरता के साथ, देश को उभरते साइबर खतरों से बढ़ते ज़ोखिम का सामना करना पड़ रहा है। ऐसे उभरते साइबर ज़ोखिमों के विरुद्ध भारत की आघातसहनीयता बढ़ाने के लिये क्या उपाय अपनाए जाने चाहिये?

यूपीएससी सिविल सेवा परीक्षा, पिछले वर्ष के प्रश्न (PYQ)

??????????

प्रश्न. भारत में, किसी व्यक्ति के साइबर बीमा कराने पर, निधि की हानि की भरपाई एवं अन्य लाभों के अतिरिक्त, सामान्यतः निम्नलिखित में से कौन-कौन से लाभ दिये जाते हैं? (2020)

1. यदि कोई मैलवेयर कम्प्यूटर तक उसकी पहुँच बाधित कर देता है, तो कम्प्यूटर प्रणाली को पुनः प्रचालित करने में लगने वाली लागत
2. यदि यह प्रमाणित हो जाता है कि किसी शरारती तत्त्व द्वारा जान-बूझकर कम्प्यूटर को नुकसान पहुँचाया गया है तो नए कम्प्यूटर की लागत
3. यदि साइबर बलात्-ग्रहण होता है तो इस हानि को न्यूनतम करने के लिये विशेषज्ञ परामर्शदाता की सेवाएँ लेने 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 रिपोर्ट करना निम्नलिखित में से किसके/किनके लिये विधितः अधिदेशात्मक है/हैं? (2017)

1. सेवा प्रदाता (सर्विस प्रोवाइडर)
2. डेटा सेंटर
3. कॉर्पोरेट निकाय (बॉडी कॉर्पोरेट)

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 एक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति सफलतापूर्वक वकिसति की है। (2022)