

उभरते साइबर खतरे और उनके नहितार्थ

यह संपादकीय 29/11/2024 को लाइवमटि में प्रकाशित [“Cyber cons go from digital arrests to wedding scams”](#) पर आधारित है। इस लेख में फर्जी शादी के नमित्करण घोटालों से लेकर 'डजिटल अरेस्ट' तक साइबर अपराध की बढ़ती जटिलता को सामने लाया गया है, साथ ही सुदृढ़ डजिटल जागरूकता और सख्त साइबर सुरक्षा उपायों की तत्काल आवश्यकता पर प्रकाश डाला गया है।

प्रलमिस के लिये:

[साइबर अपराध](#), [डजिटल अरेस्ट स्कैम](#), [सूचना प्रौद्योगिकी अधिनियम, 2000](#), [डजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023](#), [भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल](#), [राष्ट्रीय करटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर संरक्षण केंद्र](#), [साइबर स्वच्छता केंद्र](#), [भारत राष्ट्रीय साइबर सुरक्षा अभ्यास 2024](#), [दूरसंचार \(महत्त्वपूर्ण दूरसंचार अवसंरचना\) नियम, 2024](#), [रैनसमवेयर अटैक](#), [साइबर अपराध पर बुडापेस्ट कन्वेंशन](#)

मेन्स के लिये:

भारत में साइबर सुरक्षा के लिये वर्तमान फ्रेमवर्क, भारत के डजिटल परिदृश्य को प्रभावित करने वाले प्रमुख उभरते साइबर खतरे।

साइबर अपराध के लगातार वकिसति होते परदृश्य में, धोखेबाज़/घोटालेबाज़ (Fraudsters) डजिटल कमज़ोरियों का फायदा उठाने के लिये तेज़ी से अधिक उन्नत तकनीक वकिसति कर रहे हैं, जसिमें '[डजिटल अरेस्ट](#)' की आवषिकृत अवधारणा से लेकर व्हाट्सएप पर नकली शादी के नमित्करण जैसी भ्रामक योजनाएँ शामिल हैं। जैसे-जैसे भारतीय इन उभरते खतरों से जूझ रहे हैं, आभासी और वास्तविक दुनिया की धोखाधड़ी के बीच की सीमाएँ तेज़ी से धूमिल पड़ती जा रही हैं, जसिसे हमारे डजिटल बुनियादी अवसंरचना में कठिन प्रणालीगत चुनौतियाँ सामने आ रही हैं। धोखाधड़ी का प्रसार व्यापक डजिटल जागरूकता और सख्त साइबर सुरक्षा तंत्र की महत्त्वपूर्ण आवश्यकता को रेखांकित करता है जसिसे वकिसति हो रही अपराधिक रणनीतियों का अनुमान लगाकर उन्हें बेअसर किया जा सकता है।

भारत में साइबर सुरक्षा के लिये वर्तमान फ्रेमवर्क क्या है?

■ वधायी उपाय:

- [सूचना प्रौद्योगिकी अधिनियम, 2000](#) (IT अधिनियम): यह आधारभूत कानून इलेक्ट्रॉनिक शासन के लिये कानूनी फ्रेमवर्क प्रदान करता है और साइबर अपराधों और इलेक्ट्रॉनिक वाणजिय से नपिटता है।
 - इसमें डेटा संरक्षण और साइबर सुरक्षा से संबंधित प्रावधानों को शामिल करने के लिये संशोधन किया गया है।
- [डजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023](#): व्यक्तिगत डेटा की सुरक्षा के लिये अधिनियमिति, यह अधिनियम व्यक्तिगत डेटा के प्रसंस्करण में व्यक्तियों के अधिकारों और डेटा फडियुशरीज़ के दायित्वों को रेखांकित करता है।
 - यह वैध प्रसंस्करण, डेटा न्यूनीकरण और जवाबदेही पर ज़ोर देता है।

■ संस्थागत फ्रेमवर्क:

- [भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल \(CERT-In\)](#): इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय के तहत कार्यरत, CERT-In कंप्यूटर सुरक्षा घटनाओं पर प्रतिक्रिया देने वाली राष्ट्रीय नोडल एजेंसी है।
 - यह परामर्श जारी करती है, प्रशिक्षण आयोजित करती है तथा हतिधारकों के बीच समन्वय को सुगम बनाती है।
- [राष्ट्रीय करटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर संरक्षण केंद्र \(NCIIPC\)](#): NCIIPC बजिली, बैंकगि और दूरसंचार जैसे क्षेत्रों में महत्त्वपूर्ण सूचना अवसंरचना की सुरक्षा पर ध्यान केंद्रित करता है।
 - यह इन परसिपत्तियों की सुरक्षा के लिये रणनीतियाँ और नीतियाँ वकिसति करता है।
- [भारतीय साइबर अपराध समन्वय केंद्र \(I4C\)](#): गृह मंत्रालय द्वारा शुरू किया गया I4C एक समन्वयित उपागम के माध्यम से साइबर अपराध को नयित्त्रति करता है, जसिमें राष्ट्रीय साइबर अपराध रपिर्टगि पोर्टल और क्षमता नरिमाण पहल शामिल हैं।
- [साइबर स्वच्छता केंद्र](#): फरवरी 2017 में स्थापित, साइबर स्वच्छता केंद्र का उद्देश्य राष्ट्रीय साइबर सुरक्षा नीति के अनुरूप बॉटनेट संक्रमण तथा मैलवेयर का पता लगाकर और उन्हें कम करके भारत में एक सुरक्षित साइबर पारसिथितिकी तंत्र स्थापित करना है।
- [साइबर सुरक्षति भारत](#): इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MeitY) की इस पहल की संकल्पना साइबर अपराध के बारे

में जागरूकता फैलाने और सभी सरकारी विभागों में मुख्य सूचना सुरक्षा अधिकारियों (CISOs) तथा अग्रिम पंक्तिके IT अधिकारियों की क्षमता निर्माण के मशिन के साथ की गई थी।

■ रणनीतिक पहल:

- **राष्ट्रीय साइबर सुरक्षा नीति, 2013**: यह नीति साइबरस्पेस को सुरक्षित करने, सुरक्षित कंप्यूटिंग वातावरण को बढ़ावा देने और राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना की अनुकूलता बढ़ाने के लिये दृष्टिकोण एवं रणनीतियों को रेखांकित करती है।
- **भारत राष्ट्रीय साइबर सुरक्षा अभ्यास 2024**: इस अभ्यास में साइबर रक्षा और घटना प्रतिक्रिया पर गहन प्रशिक्षण, IT एवं OT प्रणालियों पर साइबर हमलों के लाइव-फायर समुलेशन तथा सरकार व उद्योग के हतिधारकों के लिये सहयोगी मंच शामिल हैं।

■ क्षेत्र-वशिष्ट विनियम:

- **SEBI विनियमिता संस्थाओं के लिये साइबर सुरक्षा और साइबर आघातसह फ्रेमवर्क**: भारतीय प्रतभूति और विनियम बोर्ड द्वारा जारी यह फ्रेमवर्क विनियमिता संस्थाओं को प्रतभूति बाजारों की सुरक्षा के लिये सुदृढ़ साइबर सुरक्षा एवं साइबर आघातसह नीतियों स्थापित करने का अधिकार देता है।
- **दूरसंचार (महत्त्वपूर्ण दूरसंचार अवसंरचना) नियम, 2024**: नवंबर 2024 में पेश किया गया यह नियम महत्त्वपूर्ण दूरसंचार अवसंरचना (CTI) के रूप में चिह्नित दूरसंचार संस्थाओं को अपने हार्डवेयर, सॉफ्टवेयर एवं डेटा का निरीक्षण करने के लिये सरकारी अधिकृत कर्मियों को अभिगम प्रदान करने का आदेश देता है।

भारत के डिजिटल परदृश्य को प्रभावित करने वाले प्रमुख उभरते साइबर खतरे क्या हैं?

- **डिजिटल अरेस्ट घोटाले**: साइबर अपराधियों ने धोखाधड़ी का एक नया तरीका ईजाद किया है, जिसमें वेकानून प्रवर्तन अधिकारियों का रूप धारण कर अनजान पीड़ितों में भय उत्पन्न करते हैं।
 - व्यक्तियों से संपर्क कर ये धोखेबाज दावा करते हैं कि वे मनगढ़ंत अपराधों के लिये जाँच के दायरे में हैं, तथा फर्जी गरिफ्तारी से बचने के लिये उन्हें भारी जुर्माना भरने के लिये मजबूर करते हैं।
 - कानून प्रवर्तन से जुड़े प्राधिकार और पीड़ितों की डिजिटल साक्षरता की कमी का फायदा उठाकर, ये घोटाले खतरनाक रूप से प्रभावी हो गए हैं।
 - वर्ष 2024 में, भारतीयों ने सामूहिक रूप से इस तरह के “डिजिटल अटैक” धोखाधड़ी में ₹120.30 करोड़ का नुकसान उठाया।
- **रैनसमवेयर हमले**: रैनसमवेयर हमले बढ़ गए हैं, जो महत्त्वपूर्ण बुनियादी अवसंरचना और वित्तीय संस्थानों को नशाना बना रहे हैं, जिससे पर्याप्त संबंधी व्यवधान एवं वित्तीय नुकसान हो रहा है।
 - अगस्त 2024 में, C-Edge टेक्नोलॉजीज़ पर रैनसमवेयर हमले ने लगभग 300 छोटे भारतीय बैंकों की भुगतान प्रणालियों को बाधित कर दिया, जिससे वित्तीय नेटवर्क में कमजोरियों उजागर हुईं।
 - इसके अलावा, दिल्ली में अखिल भारतीय आयुर्विज्ञान संस्थान (AIIMS) पर वर्ष 2023 रैनसमवेयर अटैक स्वास्थ्य सेवा के बुनियादी अवसंरचना की कमजोरियों का उदाहरण है।
- **आपूर्ति शृंखला हमले**: साइबर अपराधी बड़े नेटवर्क में घुसपैठ करने के लिये आपूर्ति शृंखलाओं की कमजोरियों का तेज़ी से फायदा उठा रहे हैं।
 - उदाहरण के लिये दिसंबर 2020 में, नेटवर्क प्रबंधन उपकरण प्रदान करने वाली एक अमेरिकी सॉफ्टवेयर कंपनी सोलरवडिस को नशाना बनाकर किये गए एक वैश्विक साइबर हमले ने राष्ट्रीय सूचना विज्ञान केंद्र (NIC), इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MeitY), और भारत हेवी इलेक्ट्रिकल्स लिमिटेड (BHEL) सहित कई भारतीय संगठनों को प्रभावित किया।
 - भारतीय साइबर अपराध समन्वय केंद्र (I4C) के आँकड़ों के अनुसार वर्ष 2024 के प्रारंभिक नौ महीनों में भारत को साइबर धोखाधड़ी से 11,333 करोड़ रुपए का नुकसान हुआ।
- **राज्य प्रायोजित साइबर जासूसी**: राष्ट्र-राज्य अभिक्रिया साइबर जासूसी गतिविधियों को तेज़ कर रहे हैं, संवेदनशील सरकारी और कॉर्पोरेट डेटा को नशाना बना रहे हैं।
 - चीन से उत्पन्न एक साइबर हमले को वर्ष 2020 में मुंबई में बड़े पैमाने पर बजिली कटौती का कारण माना गया, जिससे शहर के महत्त्वपूर्ण बुनियादी अवसंरचना की कमजोरियों उजागर हुईं।
- **डीपफेक प्रौद्योगिकी का दुरुपयोग**: AI-जनरेटेड डीपफेक के दुरुपयोग से गलत सूचना और धोखाधड़ी सहित कई गंभीर खतरे उत्पन्न होते हैं।
 - वर्ष 2024 की एक रिपोर्ट में डीपफेक को भारत में एक आसन्न खतरे के रूप में पहचाना गया है, जो जनता के विश्वास को कम करने और सूचनाओं में हेरफेर करने में सक्षम है।
 - अभिनेत्री रश्मिका मंदाना को एक डीपफेक फ्लिम में दिखाया गया, जो ऑनलाइन वायरल हो गई, जिससे व्यापक आक्रोश फैल गया।
- **इंटरनेट ऑफ थिंग्स (IoT) उपकरणों का शोषण**: इंटरनेट ऑफ थिंग्स (IoT) उपकरणों को व्यापक रूप से अपनाए जाने से डिजिटल पारस्थितिकी तंत्र की भेद्यता बहुत बढ़ गई है, जिससे साइबर अपराधियों के लिये नए अवसर उत्पन्न हो गए हैं।
 - इन उपकरणों में प्रायः सुदृढ़ सुरक्षा सुविधाओं का अभाव होता है तथा इनका उपयोग नेटवर्क में सेंध लगाने या दुर्भावनापूर्ण गतिविधियों को अंजाम देने के लिये आसानी से किया जाता है।
 - वर्ष 2024 में, भारत में IoT-संबंधित साइबर हमलों में 59% की उल्लेखनीय वृद्धि देखी गई, जो इस उभरते खतरे के पैमाने को रेखांकित करती है।
 - स्मार्ट घरों से लेकर कनेक्टेड औद्योगिक प्रणालियों तक, असुरक्षित IoT उपकरणों से जुड़े जोखिम बढ़ गए हैं।
- **क्रिप्टोकॉरेंसी और ब्लॉकचेन-आधारित साइबर धोखाधड़ी**: भारत में क्रिप्टोकॉरेंसी के उपयोग में तीव्र वृद्धि ने परिष्कृत साइबर धोखाधड़ी तंत्र के लिये बड़े पैमाने पर एक नया, अनियमित परदृश्य तैयार कर दिया है।
 - ब्लॉकचेन-आधारित प्लेटफॉर्म तेज़ी से जटिल पॉज़ी स्कीम्स, पंप-एंड-ड्रॉप हेरफेर और उन्नत मनी लॉन्ड्रिंग तकनीकों का लक्ष्य बन रहे हैं जो नियामक गैर-एरियाज़ का फायदा उठाते हैं।
 - बेंगलुरु स्थित बटिकॉइन घोटाले ने एक हैकर, पुलिस अधिकारियों और एक साइबर विशेषज्ञ के बीच साँट-गाँट को उजागर किया, जिसमें 850 करोड़ रुपए की क्रिप्टोकॉरेंसी का अवैध अंतरण, सबूतों से छेड़छाड़ तथा भ्रष्टाचार के आरोप शामिल 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 कटि बेच रहे हैं, जिससे लेस-स्कलिड खतरा उत्पन्न करने वाले लोगों के लिये परषिकृत हमले सुलभ हो रहे हैं।
- हाल ही में हुए एक सुरक्षा उल्लंघन ने भारत में 750 मिलियन दूरसंचार उपयोगकर्ताओं के व्यक्तिगत डेटा को उजागर कर दिया है, और यह डेटा डार्क वेब पर बेचा जा रहा है।

भारत में साइबर सुरक्षा परदृश्य 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 वरषिड नागरिकों जैसी कमजोर आबादी को लक्षित करना हो।
 - ये पहल उपयोगकर्ताओं 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 सक्रियरटी-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।
 - वनियामक प्राधिकरण से प्रमाणन यह सुनिश्चित कर सकता है कि केवल सुरक्षित डिवाइस ही बाज़ार तक पहुँचें। IoT ज़ोखमिों के बारे में सार्वजनिक जागरूकता उपभोक्ता स्तर पर सुरक्षा को और बढ़ाएगी।
- **AI-संचालित खतरा खुफिया और प्रतिक्रिया प्रणाली:** नेटवर्क ट्रैफिक का विश्लेषण करने, वसिगतियों की पहचान करने और खतरों का रयिल टाइम रैस्पॉड 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 कमजोरियों 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 नयिमति परीक्षण सटीकता और वशि्वसनीयता सुनिश्चित करता है।
- **CERT-In की क्षमताओं को सुदृढ़ बनाना:** CERT-In के कार्यक्षेत्र का वसितार किया जाना चाहिये, जिसमें अंतरराष्ट्रीय CERT और नज्जि क्षेत्र के साथ गहन सहयोग शामिल करने के साथ ही साइबर अपराध पर बुडापेसट कन्वेंशन जैसे अंतरराष्ट्रीय 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 रयिल टाइम पहचान करने में सक्रिय एथिकल-AI उपकरण वकिसति 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 चहिनति 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 शक्ति किये 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 वशिवास 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 नयिमति ऑडिट, ब्लाकचेन एकीकरण, सुरक्षित साफ्टवेयर विकास प्रथाएँ और एन्क्रिप्टेड कम्युनिकेशन चैनल शामिल हैं।
 - बड़े उद्यमों को वकिरेताओं से इन प्रमाणपत्रों की मांग करनी चाहिये। इससे छोटी इकाइयों के माध्यम से उल्लंघन के ज़ोखमि कम हो जाते हैं।
- **क्रेडिटोकरेंसी वनियमन:** पारदर्शिता और पता लगाने की क्षमता पर ध्यान केंद्रित करते हुए क्रेडिटोकरेंसी लेनदेन के लिये स्पष्ट वनियमन स्थापित किये जाने चाहिये।
 - क्रेडिटो एक्सचेंजों के लिये अनिवार्य KYC और रयिल टाइम मॉनिटरिंग सिस्टम अवैध गतिविधियों को रोक सकती है।
 - वशिष क्रेडिटो फोरेंसिक इकाइयों को धोखाधड़ी का शीघ्रता से समाधान करना चाहिये।
- **अनिवार्य राष्ट्रीय साइबर सुरक्षा ऑडिट:** नयिमति, सरकार द्वारा अनिवार्य ऑडिट महत्त्वपूर्ण बुनयादी अवसंरचना प्रणालियों में कमजोरियों 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-अप के लिये साइबर स्वच्छता जागरूकता:** स्टार्टअप के लिये सरकार द्वारा समर्थित साइबर सुरक्षा प्रशिक्षण कार्यक्रम शुरू किये जाने चाहिये।
 - साइबर सुरक्षा उपकरणों और सेवाओं तक रयायती अभिगम छोटे व्यवसायों को सर्वोत्तम प्रथाओं को अपनाने में सक्रिय बना सकती है।
 - नमिन स्तरीय सुरक्षा स्वच्छता के ज़ोखमिों के बारे में जागरूकता अभियान स्टार्टअप को सुरक्षा में नविश को प्राथमिकता देने के लिये प्रेरित कर सकते हैं। क्षेत्र-वशिषिट मार्गदर्शन प्रासंगिकता सुनिश्चित करता है।
- **सक्रिय डार्क वेब मॉनिटरिंग:** ऐसे उपकरणों में नविश किये जाने चाहिये जो चोरी किये गए डेटा, अवैध सामान और मैलवेयर की बकिरी के लिये

डार्क वेब की सक्रिय रूप से नगिरानी करते हैं।

- **डार्क वेब गतिविधि से एकत्रित खुफिया जानकारी** से हमलों को रोका जा सकता है तथा कानून प्रवर्तन कार्यों को नरिदेशित किया जा सकता है।
- सार्वजनिक-नज्जी सहयोग से नगिरानी क्षमताओं का वसितार किया जा सकता है। समरपति टास्क फोर्स को अभनिरिधारित किये गए खतरों पर तुरंत कार्रवाई करनी चाहिये।

- **बहु-कारक प्रमाणीकरण (MFA) प्रवर्तन:** केवल पासवर्ड पर नरिभरता कम करने के लिये महत्त्वपूर्ण प्रणालियों, सरकारी पोर्टलों और वित्तीय प्लेटफॉर्मों पर MFA को अनविर्य बनाया जाना चाहिये।
 - व्यवसायों को सुरक्षा से समझौता किये बिना उपयोगकर्ता अनुभव को बेहतर बनाने के लिये अनुकूली MFA ससि्टम अपनाना चाहिये। इससे अनधिकृत पहुँच के ज़ोखमि कम हो जाते हैं।
- **शिक्षा कषेत्र के लिये साइबर सुरक्षा:** स्कूलों और वशिवदियालयों में साइबर सुरक्षा जागरूकता और बचाव तंत्र शुरू किये जाने चाहिये। इसमें नयिमति बैकअप, सुरक्षित नेटवर्क और खतरों से नपिटने 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 संस्कृतिका नरिमाण होता है।
- **डेटा स्थानीयकरण मानदंडों को लागू करना:** यद्यपि डिजिटल व्यक्तगित डेटा संरक्षण अधनियम, 2023 में डेटा स्थानीयकरण के प्रावधान शामिल हैं, लेकिन इन्हें केवल कागज़ पर औपचारिकता मात्र नहीं रहना चाहिये, बल्कि इन्हें अक्षरशः और भावनापूर्वक लागू किये जाने चाहिये।
 - यह अनविर्य करना कि महत्त्वपूर्ण एवं संवेदनशील डेटा राष्ट्रीय सीमाओं के भीतर ही संग्रहीत रहे, नयितरण में सुधार कर सकता है और सुरक्षा ज़ोखमि को कम कर सकता है।
 - स्पष्ट अनुपालन रूपरेखा और उल्लंघन के लिये दंड लागू किये जाने चाहिये।

नरिष्कर्ष:

साइबर अपराध के उभरते परदृश्य 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 नपिटने के लिये अंतरराष्ट्रीय सहयोग को बढ़ावा देने की आवश्यकता है। सख्त सुरक्षा उपायों में नविश करके, कुशल कारयबल का नरिमाण करके और उभरते खतरों से आगे रहकर, भारत अपने डिजिटल भवषिय की रक्षा कर सकता है तथा अपने नागरिकों को साइबर हमलों के बढ़ते ज़ोखमि से बचा सकता है।

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

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

यूपीएससी सविलि सेवा परीक्षा, पछिले वर्ष के प्रश्न (PYQ)

????????????

प्रश्न. भारत में, कसिी व्यक्त के साइबर बीमा कराने पर, नधिकी हानिकी भरपाई एवं अन्य लाभों के अतरिकित, सामान्यतः नमिनलखिति में से कौन-कौन से लाभ दरे जाते हैं ? (2020)

1. यदि कोई मैलवेयर कम्प्यूटर तक उसकी पहुँच बाधति कर देता है, तो कम्प्यूटर प्रणाली को पुनः प्रचालति करने में लगने वाली लागत
2. यदि यह प्रमाणति हो जाता है कि कसिी 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 हानिको न्यूनतम करने के लिये वशिषज्ज 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 दये 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 रपिर्त करना नमिनलखिति में से कसिके/कनिके लिये वधिति: अधदिशात्मक है/है? (2017)

1. सेवा प्रदाता (सर्वसि प्रोवाइडर)
2. डेटा सेंटर
3. कॉर्पोरेट नकाय (बॉडी कॉर्पोरेट)

नीचे दिये गए कूट का प्रयोग कर सही उत्तर चुनिये:

- (a) केवल 1
- (b) केवल 1 और 2
- (c) केवल 3
- (d) 1, 2 और 3

उत्तर: (d)

?????

प्रश्न. साइबर सुरक्षा के विभिन्न तत्त्व क्या हैं? साइबर सुरक्षा की चुनौतियों को ध्यान में रखते हुए समीक्षा कीजिये कि भारत ने कसि हद तक एक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति सफलतापूर्वक विकसित की है। (2022)

PDF Reference URL: <https://www.drishtias.com/hindi/printpdf/emerging-cyber-threats-and-their-implications>

