साइबर बीमा पॉलिसी

चर्चा में क्यों?

हाल ही में भारतीय बीमा विनियामक और विकास प्राधिकरण (**Insurance Regulatory and Development Authority of India**- IRDAI) द्वारा गठित एक समिति ने साइबर बीमा पॉलिसी लाने की सिफारिश की है।

- साइबर बीमा पॉलिसी, साइबर जोखिम के हस्तांतरण के लिये एक तंत्र है।
  साइबर जोखिम को आमतौर पर सूचना प्रणाली के उल्लंघन या उस पर हुए हमले के रूप में परिभाषित किया जाता है।
- यह पॉलिसी नीतिधारकों को साइबर अपराधों से बचाने में मदद करेगी।

प्रमुख बिंदु:

पृष्ठभूमि:

- अक्तूबर 2020 में IRDAI ने **पी उमेश** की अध्यक्षता में साइबर देयता बीमा के लिये एक समिति का गठन किया था।
- कोविड-19 महामारी के दौरान साइबर हमले और हाई-प्रोफ़ाइल डेटा उल्लंघन की घटनाओं में वृद्धि हुई।

प्रमुख आँकड़े:

- समिति की रिपोर्ट के अनुसार, वर्तमान में **भारत में इंटरनेट उपयोगकर्त्ताओं की संख्या 700 मिलियन** आँकी गई है।
- वर्ष 2019 में भारत को विश्व में **दूसरे सबसे बड़े** (चीन के बाद) ऑनलाइन बाज़ार के रूप में स्थान दिया गया।
- शहरी और ग्रामीण दोनों क्षेत्रों में इंटरनेट उपयोगकर्त्ताओं की संख्या बढ़ने का अनुमान है। इंटरनेट उपयोगकर्त्ताओं की संख्या तेज़ी से बढ़ने की वजह से ऑनलाइन बैंकिंग उपयोगकर्त्ताओं की संख्या में भी वृद्धि होगी।
- **व्यक्तिगत साइबर बीमा पॉलिसी की विशेषताएँ (कवर):**
  फंड्स की चोरी, आइडेंटिटी थेफ्ट कवर, सोशल मीडिया कवर, साइबर स्टॉकिंग, मालवेयर कवर, फिशिंग कवर, डेटा ब्रीच और प्राइवेसी ब्रीच कवर आदि इसकी विशेषताएँ हैं।

- **अनुशंसाएँ: वर्तमान में उपलब्ध साइबर बीमा पॉलिसियाँ लोगों की आवश्यकताओं को यथोचित पूरा करती हैं। हालाँकि उत्पाद सुविधाओं और प्रक्रियाओं में कुछ ऐसे क्षेत्र हैं जिनमें सुधार की आवश्यकता है।**
- **उच्च दावों पर पुलिस प्राथमिकी (First Information Report-FIR):**
    - बीमा कंपनियों को 5,000 रुपए तक के दावों के लिये पुलिस प्राथमिकी (FIR) पर ज़ोर नहीं देना चाहिये।
        दावों का आकलन करने के लिये FIR एक महत्त्वपूर्ण आवश्यकता है।
    - **स्पष्टता:**
        ब्रिकिंग से संबंधित प्रक्रियाएँ और उनकी लागत को कम करने के लिये उचित कवरेज की आवश्यकता है।
            ब्रिकिंग (Bricking) एक साइबर घटना के परिणामस्वरूप हार्डवेयर के उपयोग या कार्यक्षमता में गिरावट को संदर्भित करती है।
    - **साइबर बीमा पॉलिसी का मानकीकरण :**
        साइबर जोखिम व्यापक होने के साथ-साथ लगातार विस्तारित हो रहे हैं। मानकीकरण एक अच्छा विचार है, परंतु यह सभी उभरते जोखिमों से निपटने में सक्षम नहीं हो सकता है तथा यह नवाचार को भी सीमित कर सकता है।

साइबर सुरक्षा:

साइबर सुरक्षा के संबंध में:

- साइबर हमला किसी कंप्यूटर और कंप्यूटर नेटवर्क के अनधिकृत उपयोग तथा उसे उजागर करने, बदलने, अक्षम करने, नष्ट करने, चोरी करने या उस तक अनधिकृत पहुँच प्राप्त करने का प्रयास है।
- साइबर हमला किसी भी प्रकार की ऐसी आक्रामक युक्ति है जो कंप्यूटर सूचना प्रणाली, इन्फ्रास्ट्रक्चर, कंप्यूटर नेटवर्क या व्यक्तिगत कंप्यूटर उपकरणों को लक्षित करती है।

आवश्यकता:

नैसकॉम की **डेटा सिक्योरिटी काउंसिल ऑफ इंडिया** (DSCI) की **रिपोर्ट 2019** के अनुसार, **विश्व में** भारत ऐसा दूसरा देश है जहाँ वर्ष 2016 और वर्ष 2018 के बीच **सबसे ज़्यादा साइबर हमले** हुए।

साइबर हमलों के तरीके:

- **फिशिंग या स्पूफिंग हमले:**
    स्पूफिंग में हमलावर अपनी असल पहचान को छिपाकर खुद को एक विश्वसनीय स्रोत के रूप में प्रस्तुत करते हैं अर्थात् वह वैध उपयोगकर्त्ता की पहचान का उपयोग करने की कोशिश करता है। फिशिंग वह प्रक्रिया है जिसमें कोई व्यक्ति उपयोगकर्त्ता की संवेदनशील जानकारी जैसे- बैंक खाता विवरण आदि को चुराता है।

- **मैलवेयर या स्पाइवेयर:**
    स्पाइवेयर एक प्रकार का मैलवेयर है जो डिज़िटल डिवाइस जैसे- कंप्यूटर, मोबाइल, टेबलेट आदि से गुप्त एवं निजी जानकारियाँ चुराता है। यह जीमेल अकाउंट, बैंक डिटेल्स, सोशल मीडिया से लेकर टेक्स्ट मैसेज जैसी गतिविधियों पर नज़र रखता है एवं वहाँ से डेटा चोरी कर अपने ऑपरेटर तक पहुँचाता है।
- **सिम स्वैप (SIM Swap):**
    इसमें मूल सिम का एक क्लोन बनाकर मूल सिम को अमान्य कर दिया जाता है और डुप्लिकेट सिम का उपयोग उपयोगकर्त्ता के ऑनलाइन बैंक खाते से धनराशि स्थानांतरित करने के लिये किया जा सकता है।
- **क्रेडेंशियल स्टफिंग (उपकरणों से समझौता करना और डेटा चुराना):**
    क्रेडेंशियल स्टफिंग एक प्रकार का साइबर हमला है, जिसमें चोरी किये गए अकाउंट क्रेडेंशियल्स में आमतौर पर उपयोगकर्त्ता का नाम और/या ईमेल शामिल होता है और संबंधित पासवर्ड का उपयोग वेब एप्लीकेशन के खिलाफ निर्देशित बड़े पैमाने पर स्वचालित लॉगिन अनुरोधों के माध्यम से उपयोगकर्त्ता के अकाउंट तक अनधिकृत पहुँच प्राप्त करने के लिये किया जाता है।
- ऑनलाइन भुगतान या लेन-देन आदि के दौरान साईबर हमले होते हैं।

साइबर हमले से निपटने हेतु सरकार की पहलें:

- **साइबर सुरक्षित भारत पहल:**
    इसकी शुरुआत वर्ष 2018 में मुख्य सरकारी सुरक्षा अधिकारियों (CISOs) और सरकारी विभागों में फ्रंटलाइन आईटी कर्मचारियों के सुरक्षा उपायों के लिये साइबर क्राइम तथा निर्माण क्षमता के बारे में जागरूकता फैलाने के उद्देश्य से की गई थी।
- **राष्ट्रीय साइबर सुरक्षा समन्वय केंद्र (NCCC):**
    इसका कार्य वास्तविक समय में साइबर खतरों का पता लगाने के लिये देश में इंटरनेट ट्रैफिक और कम्युनिकेशन मेटाडेटा (जो प्रत्येक कम्युनिकेशन में शामिल जानकारी के छोटे-छोटे भाग होते हैं) को स्कैन करना है।
- **साइबर स्वच्छता केंद्र:**
    इसकी शुरुआत वर्ष 2017 में इंटरनेट उपयोगकर्त्ताओं के लिये वायरस और मैलवेयर को डिलीट कर उनके कंप्यूटर तथा उपकरणों को साफ करने के उद्देश्य से की गई थी।
- **सूचना सुरक्षा शिक्षा और जागरूकता परियोजना (ISEA):**
    यह परियोजना सूचना सुरक्षा के क्षेत्र में जागरूकता बढ़ाने और अनुसंधान, शिक्षा एवं प्रशिक्षण प्रदान करने से संबंधित है।
- **राष्ट्रीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम** (CERT-In) सभी साइबर सुरक्षा प्रयासों, आपातकालीन प्रतिक्रियाओं और संकट प्रबंधन के समन्वय के लिये नोडल एजेंसी के रूप में कार्य करती है।
- सरकार ने अति-संवेदनशील सूचनाओं के संरक्षण के लिये **'राष्ट्रीय अतिसंवेदनशील सूचना अवसंरचना संरक्षण केंद्र** (National Critical Information Infrastructure Protection Centre-NCIIPC) का गठन किया।
    NCIIPC को भारत के महत्त्वपूर्ण सूचना बुनियादी ढाँचे को सुरक्षित करने के लिये सूचना प्रौद्योगिकी अधिनियम, 2000 के तहत स्थापित किया गया था।

- **सूचना प्रौद्योगिकी अधिनियम, 2000:**
    यह अधिनियम कंप्यूटर, कंप्यूटर सिस्टम, कंप्यूटर नेटवर्क और इलेक्ट्रॉनिक प्रारूप में डेटा और सूचना के उपयोग को नियंत्रित करता है।

अंतर्राष्ट्रीय तंत्र:

- अंतर्राष्ट्रीय दूरसंचार संघ (ITU): यह संयुक्त राष्ट्र की एक विशेष एजेंसी है जो दूरसंचार और साइबर सुरक्षा मुद्दों के मानकीकरण तथा विकास में अग्रणी भूमिका निभाती है।
- साइबर अपराध पर बुडापेस्ट सम्मेलन: बुडापेस्ट कन्वेंशन साइबर क्राइम पर एक कन्वेंशन है, जिसे साइबर अपराध पर बुडापेस्ट कन्वेंशन या बुडापेस्ट कन्वेंशन के नाम से जाना जाता है।
    - यह अपनी तरह की पहली ऐसी अंतर्राष्ट्रीय संधि है जिसके अंतर्गत राष्ट्रीय कानूनों को सुव्यवस्थित कर जाँच-पड़ताल की तकनीकों में सुधार करने तथा इस संबंध में विश्व के अन्य देशों के बीच सहयोग बढ़ाने हेतु इंटरनेट और कंप्यूटर अपराधों पर रोक लगाने की मांग की गई है।
    - यह 1 जुलाई, 2004 को लागू हुआ। भारत इस सम्मेलन का हस्ताक्षरकर्त्ता नहीं है।
- **इंटरनेट गवर्नेंस फोरम (IGF): यह इंटरनेट गवर्नेंस डिबेट पर सभी हितधारकों यानी सरकार, निजी क्षेत्र और नागरिक समाज को एक साथ लाता है।**

स्रोत: इंडियन एक्सप्रेस