भारत की संदग्धि रजस्टि्री और साइबर सुरक्षा पहल

[स्रोत: इंडयिन एक्सप्रेस]

चर्चा में क्यों?

भारत की **ऑनलाइन** [संदग्धि रजस्टि्री] ने 13 लाख धोखाधड़ी वाले लेनदेन को रोककर लगभग **5,100 करोड़ रुपए** बचाए हैं और यह भारत के साइबर सुरक्षा प्रयासों में एक **केंद्रीय भूमकिा नभिा रहा है**।

संदग्धि रजस्टि्री क्या है?

- **परचिय:** वर्ष 2024 में शुरू की गई संदग्धि रजस्टि्री को **राष्ट्रीय साइबर अपराध रपिोर्टगि पोर्टल (NCRP)** के आधार पर तैयार कयिा गया है और इसे [भारतीय साइबर अपराध समन्वय केंद्र (I4C)] ने वकिसति कयिा है।
  - इसमें लगभग **1.4 मलियिन साइबर अपराधयिों** का डेटा शामलि है, जो वत्तिीय धोखाधड़ी और अन्य साइबर अपराधों से जुड़े हैं तथा यह सभी बैंकों के साथ साझा कयिा गया है।
  - यह डेटा राज्यों, केंद्रशासति प्रदेशों, केंद्रीय जाँच एवं खुफयिा एजेंसयिों के लयि भी उपलब्ध कराया गया है।
- **उद्देश्य:** यह रजस्टि्री बैंकों और वत्तिीय संस्थानों को **ग्राहक की पहचान सत्यापति करने** तथा संदग्धि खातों में वास्तवकि समय में लेनदेन की नगिरानी करने में सहायता करती है।
  - NCRP से प्राप्त डेटा का उपयोग करके यह **धोखाधड़ी जोखमि प्रबंधन** को सुदृढ़ करता है और संभावति साइबर अपराधयिों को चह्निति करता है।
- **संदग्धि रजस्टि्री की आवश्यकता: भारत को साइबर धोखाधड़ी से हर महीने 1,000 करोड़ रुपए से ज़्यादा का नुकसान होता है। 80% से ज़्यादा साइबर अपराध के मामले वत्तिीय धोखाधड़ी से जुड़े होते हैं।**
  - डजिटिल लेनदेन के बढ़ते पैमाने के लयि मज़बूत धोखाधड़ी जोखमि प्रबंधन और वास्तवकि समय नगिरानी की आवश्यकता है।
- **प्रभाव:** दसिंबर 2024 तक लगभग 1,800 करोड़ रुपए मूल्य के 6.1 लाख से अधकि धोखाधड़ी वाले लेनदेन अवरुद्ध कर दयि गए।
  - बैंकों ने 8.67 लाख म्यूल खाते, 7 लाख समि और 1.4 लाख डवािइस फ्रीज कर दयि। वर्ष 2021 से अब तक,**सूचना प्रौद्योगकिी अधनियिम, 2000** के तहत लगभग 3,850 करोड़ रुपए की धोखाधड़ी पकड़ी गई है और संदग्धि ऑनलाइन सामग्री को ब्लॉक कयिा गया है।

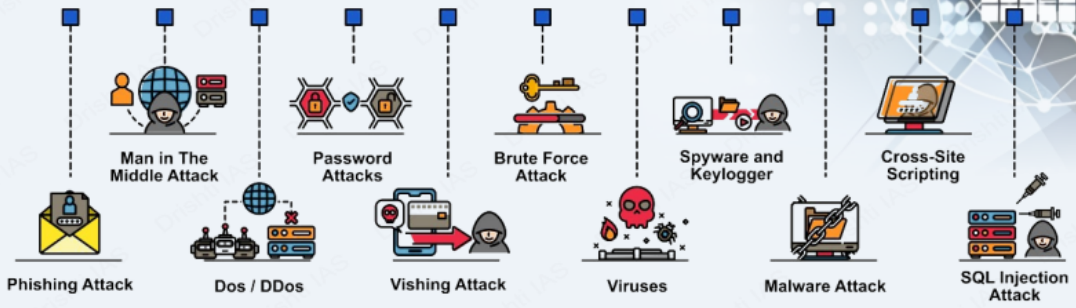
भारत में साइबर अपराध की प्रवृत्तयिाँ

- **बढ़ते साइबर अपराध से नुकसान: NCRP** के अनुसार, भारत में साइबर धोखाधड़ी में भारी बढ़ोतरी हुई है, जसिमें**वर्ष 2021 से 2024 के बीच लगभग 33,165 करोड़ रुपए** का नुकसान हुआ।
- **टयिर 2 और 3 साइबर अपराध हॉटस्पॉट का वकिास:** देवघर, जयपुर, नूह, मथुरा, कोलकाता, सूरत, बेंगलुरु शहरी और कोझकिोड जैसे शहर**साइबर अपराध हॉटस्पॉट** के रूप में पहचाने गए हैं, जसिसे स्पष्ट होता है कि साइबर अपराधी अब छोटे शहरों को भी तेज़ी से नशिाना बना रहे 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 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

- **और पढ़ें:** साइबर धोखाधड़ी

भारत की साइबर सुरक्षा पहल क्या हैं?

- **संवैधानिक संदर्भ:** पुलिस और लोक-व्यवस्था राज्य विषय हैं। राज्य/केंद्रशासित प्रदेश साइबर अपराध सहित अन्य अपराधों को संभालते हैं, जबकि केंद्र मार्गदर्शन, समन्वय और वित्तपोषण प्रदान करता है।
- **नीति तंत्र:**
  - **सूचना प्रौद्योगिकी अधिनियम, 2000:** इसमें **फिशिंग, स्मिशिंग और विशिंग** जैसे साइबर अपराधों को दंड (जुर्माना और कारावास) सहित शामिल किया गया है।
  - **नए आपराधिक कानून:** भारतीय नागरिक सुरक्षा संहिता (BNSS), 2023, भारतीय न्याय संहिता, 2023 और भारतीय साक्ष्य अधिनियम, 2023 आधुनिक साइबर खतरों का समाधान करते हैं।
  - **राष्ट्रीय साइबर सुरक्षा नीति, 2013:** इसका उद्देश्य साइबर स्पेस की रक्षा करना, साइबर सुरक्षा क्षमता का निर्माण करना, कमज़ोरियों को कम करना और राष्ट्रीय डिजिटल सुरक्षा को सशक्त करना है।
- **संस्थागत तंत्र:**
  - **भारतीय साइबर अपराध समन्वय केंद्र (I4C):** गृह मंत्रालय (MHA) के अंतर्गत स्थापित कार्यालय, जिसका उद्देश्य साइबर अपराध के प्रति समन्वित प्रतिक्रिया सुनिश्चित करना है।
    - I4C के अंतर्गत **राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (NCRP)** जनता को सभी प्रकार के साइबर अपराधों की रिपोर्ट करने में सक्षम बनाता है, जिसमें **महिलाओं और बच्चों के विरुद्ध अपराधों पर विशेष ध्यान दिया जाता है।**
    - **I4C** के अंतर्गत **साइबर धोखाधड़ी शमन केंद्र (CFMC)** बैंकों, वित्तीय मध्यस्थों, दूरसंचार सेवा प्रदाताओं, IT मध्यस्थों और कानून प्रवर्तन एजेंसियों (LEA) को वास्तविक समय पर कार्रवाई हेतु एक ही मंच पर लाता है।
    - समन्वय प्लेटफार्म पूरे देश में कानून प्रवर्तन एजेंसियों के बीच साइबर अपराध डेटा, विश्लेषण, मानचित्रण और समन्वय हेतु एक वेब-आधारित पोर्टल है।
    - **हेल्पलाइन 1930** के माध्यम से वित्तीय साइबर धोखाधड़ी की शिकायतों पर तत्काल कार्रवाई हेतु **नागरिक वित्तीय साइबर धोखाधड़ी रिपोर्टिंग एवं प्रबंधन प्रणाली (CFCFRMS) प्लेटफॉर्म**।
  - **CERT-In (भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल):** साइबर सुरक्षा घटनाओं, कमज़ोरियों और समन्वित प्रतिक्रिया से निपटने के लिये IT अधिनियम, 2000 के तहत राष्ट्रीय एजेंसी।
    - **CERT-In राष्ट्रीय साइबर समन्वय केंद्र (NCCC)** का संचालन करता है, जो साइबर खतरों की **स्थिति-जागरूकता** सुनिश्चित करता है। साथ ही यह **साइबर स्वच्छता केंद्र (Cyber Swachhta Kendra)** चलाता है, जो मैलवेयर का पता लगाकर उसे हटाने का कार्य करता है और नागरिकों तथा संगठनों को **निशुल्क उपकरण एवं साइबर सुरक्षा संबंधी मार्गदर्शन** प्रदान करता है।
- **अंतर्राष्ट्रीय सहयोग:** केंद्रीय अन्वेषण ब्यूरो (CBI) इंटरपोल के नेतृत्व वाली साइबर अपराध सहयोग पहल में भाग लेता है।
  - CBI, **G-7 24/7 नेटवर्क** की **नोडल एजेंसी** है, जो साइबर अपराध से संबंधित मामलों में डेटा संरक्षित करने के अनुरोध हेतु एक सुरक्षित माध्यम उपलब्ध कराती है।
- **डिजिटल तंत्र**
  - **'.bank.in' बैंकों के लिये डोमेन:** भारतीय बैंकों के लिये विशेष इंटरनेट डोमेन, जिसका उद्देश्य साइबर धोखाधड़ी को कम करना और डिजिटल विश्वास को सशक्त करना है।
  - **ई-ज़ीरो FIR (e-Zero FIR):** 10 लाख रुपए से अधिक की साइबर वित्तीय अपराध शिकायतों को स्वचालित रूप से प्रथम सूचना रिपोर्ट (FIR) में परिवर्तित करता है।
  - **MuleHunter.AI:** चोरी की गई धनराशि को स्थानांतरित करने के लिये उपयोग किये जाने वाले 'म्यूल अकाउंटों' का पता लगाने के लिये RBI द्वारा विकसित AI उपकरण।
  - **ASTR:** दूरसंचार विभाग (DoT) द्वारा विकसित **टेलीकॉम SIM सब्सक्राइबर सत्यापन के लिये आर्टिफिशियल इंटेलिजेंस और फेस रिकग्निशन से लैस प्रौद्योगिकी संचालित समाधान (ASTR)** का उपयोग एक ही व्यक्ति द्वारा विभिन्न नामों से लिये गए संदिग्ध मोबाइल कनेक्शनों की पहचान करने हेतु किया जाता है।

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

प्रश्न. साइबर अपराध को रोकने और उसका जवाब देने के लिये भारत द्वारा स्थापित संस्थागत तथा डिजिटल तंत्रों पर चर्चा कीजिये।

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

??????????

प्रश्न. भारत में व्यक्तियों के लिये साइबर बीमा के तहत धन की हानि और अन्य लाभों के भुगतान के अलावा, निम्नलिखित में से कौन से लाभ आम तौर पर कवर किये जाते हैं? (2020)

1. किसी के कंप्यूटर तक पहुँच को बाधित करने वाले मैलवेयर के मामले में कंप्यूटर सिस्टम की बहाली की लागत।
2. एक नए कंप्यूटर की लागत अगर ऐसा साबित हो जाता है कि कुछ असामाजिक तत्त्वों ने जानबूझकर इसे नुकसान पहुँचाया है।
3. साइबर जबरन वसूली के मामले में नुकसान को कम करने के लिए एक विशेष 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 4

उत्तर: (b)

प्रश्न. भारत में नम्निलखिति में से कसिके लयि साइबर सुरक्षा घटनाओं पर रपिोर्ट करना कानूनी रूप से अनविार्य है? (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 चुनौतयिों को ध्यान में रखते हुए जाँच करें कि भारत ने व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति को कसि हद तक सफलतापूर्वक वकिसति कयिा है। **(2022)**