साइबर धोखाधड़ी से GDP का 0.7% नुकसान

प्रिलिम्स के लिये: भारतीय साइबर अपराध समन्वय केंद्र (I4C), साइबर धोखाधड़ी, मनी लॉन्ड्रिंग, फिशिंग, मैलवेयर, साइबर बुलिंग, साइबर जासूसी, पेगासस, राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल, राष्ट्रीय साइबर सुरक्षा नीति, भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम (CERT-In), साइबर सुरक्षित भारत पहल, साइबर स्वच्छता केंद्र, राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIIPC), डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023।

मेन्स के लिये: साइबर धोखाधड़ी की आर्थिक लागत, खतरे और आगे की राह।

स्रोत: TH

चर्चा में क्यों?

हाल ही में, केंद्रीय गृह मंत्रालय (MHA) के तहत संचालित भारतीय साइबर अपराध समन्वय केंद्र (I4C) ने साइबर धोखाधड़ी से संबंधित महत्त्वपूर्ण अनुमान लगाए हैं।

भारतीय साइबर अपराध समन्वय केंद्र (I4C) क्या है?

परिचय:

- **साइबर धोखाधड़ी** सहित सभी प्रकार के **साइबर अपराधों** से व्यापक और समन्वित तरीके से निपटने के लिये गृह मंत्रालय द्वारा वर्ष 2020 में I4C लॉन्च किया गया था।

I4C के उद्देश्य:

- देश में **साइबर अपराध** पर अंकुश लगाने के लिये एक **नोडल बिंदु के रूप में कार्य करना।**
- **महिलाओं और बच्चों के** विरुद्ध साइबर अपराध के विरुद्ध **लड़ाई को मज़बूत करना।**
- **साइबर अपराध से संबंधित शिकायतों को आसानी से दर्ज करने** तथा साइबर अपराध की प्रवृत्तियों और पैटर्न की पहचान करने में सुविधा प्रदान करना।
- सक्रिय साइबर अपराध की रोकथाम और पता लगाने हेतु **कानून प्रवर्तन एजेंसियों के लिये** एक प्रारंभिक चेतावनी प्रणाली के रूप में कार्य करना।
- साइबर अपराध को रोकने के विषय में जनता के बीच जागरूकता पैदा 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/केंद्र शासित प्रदेशों 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 कानून के अनुसार कार्रवाई करने के लिये पहुँच बनाई जाएगी।

I4C प्रक्षेपण की मुख्य विशेषताएँ क्या हैं?

- **वित्तीय प्रभाव: वर्ष 2025 में** साइबर धोखाधड़ी के कारण भारतीयों को 1.2 लाख करोड़ रुपए से अधिक का नुकसान होने की आशंका है, जो भारत के सकल घरेलू उत्पाद का 0.7% होगा।

    - जनवरी से **जून 2024 तक** वित्तीय धोखाधड़ी में 11,269 करोड़ रुपए का नुकसान हुआ।
- **साइबर धोखाधड़ी में योगदानकर्त्ता:** I4C द्वारा प्रतिदिन लगभग **4,000 म्यूल बैंक अकाउंट की पहचान की जाती है।**
    - I4C ने पूरे देश में **18 एटीएम हॉटस्पॉट की पहचान की है, जहाँ से धोखाधड़ी से पैसे निकाले गए।**
    - **म्यूल अकाउंट** एक बैंक खाते को संदर्भित करता है जिसका उपयोग **मनी लॉन्ड्रिंग और धोखाधड़ी लेनदेन** जैसी **अवैध गतिविधियों** को सुविधाजनक बनाने के लिये किया जाता है।
- **घोटाले की उत्पत्ति:** सरकार ने साइबर धोखेबाजों के कंबोडिया, म्याँमार और लाओस जैसे दक्षिण पूर्व एशियाई देशों में "स्कैम कम्पाउंड्स" की पहचान की है।
    - अधिकांश घोटाले **चीन या चीन से जुड़ी संस्थाओं से होते हैं।**
- **कार्यप्रणाली:** अंतर्राष्ट्रीय स्कैम कम्पाउंड्स **कॉल सेंटरों से मिलते जुलते हैं और निवेश घोटालों** के केंद्र के रूप में उभरे हैं।
    - धोखेबाज **भारतीय मोबाइल फोन नंबरों** से **अनजान लोगों को कॉल करते हैं तथा लॉटरी और पुरस्कार घोटाले** आदि जैसे विभिन्न तरीकों से लोगों से पैसे ठगते हैं।
- **अवैध गतिविधियाँ:** साइबर घोटालों का उपयोग **आतंकवाद के वित्तपोषण** और **मनी लॉन्ड्रिंग** के लिये किया जा सकता है।
    - उदाहरण के लिये, **मार्च से मई 2024 के दौरान** भारतीय खातों का उपयोग करके **5.5 करोड़ रुपए** मूल्य की क्रिप्टो करेंसी खरीदी गई और भारत के बाहर धनशोधन किया गया।
    - **दुबई, हॉन्गकॉन्ग, बैंकॉक और रूस** के विदेशी एटीएम से म्यूल अकाउंट डेबिट कार्ड का उपयोग कर **नकदी निकासी** की सूचना मिली है।

साइबर धोखाधड़ी क्या है?

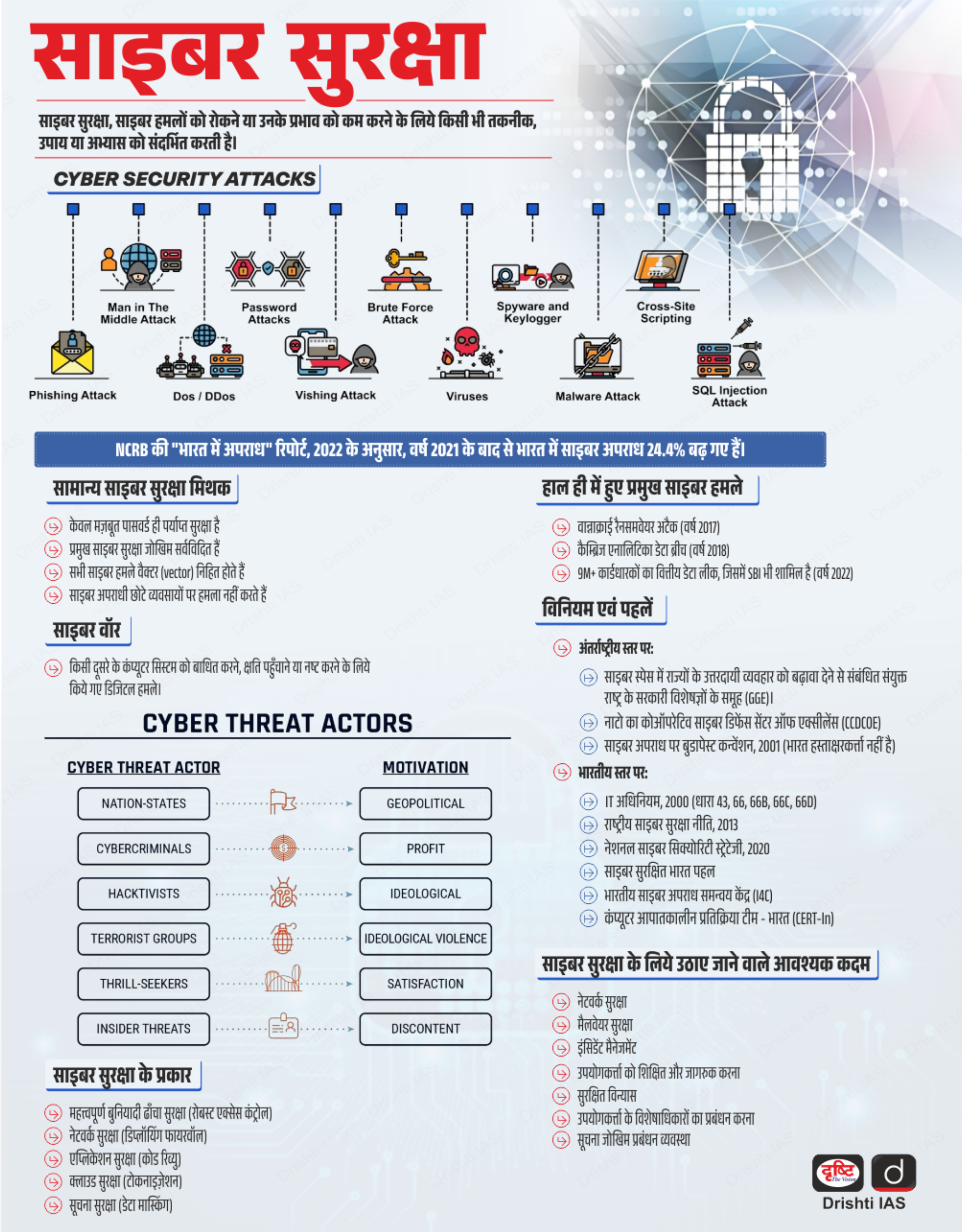
- साइबर धोखाधड़ी एक प्रकार का **साइबर अपराध है** जिसका उद्देश्य किसी संस्था से **धन (या अन्य मूल्यवान संपत्ति) चुराना होता है।**
- इसमें धोखाधड़ी करने के लिये **ऑनलाइन समाधान (इंटरनेट आधारित)** का उपयोग करना शामिल है।

साइबर धोखाधड़ी के प्रकार:

साइबर खतरा	विवरण
फिशिंग	▪ **फिशिंग** में ऐसे ईमेल शामिल होते हैं जो विश्वसनीय स्रोतों से आते प्रतीत होते हैं, जो उपयोगकर्त्ताओं को ऐसे लिंक पर क्लिक करने के लिये प्रेरित करते हैं जो उन्हें नकली वेबसाइटों पर ले जाते हैं और हमलावर संवेदनशील विवरण जैसे क्रेडिट कार्ड नंबर प्राप्त कर लेते हैं।
मैलवेयर	▪ **मैलवेयर का** उपयोग व्यक्तिगत जानकारी चुराने के लिये किया जाता है, जिससे साइबर अपराधी पीड़ित के कंप्यूटर पर नियंत्रण प्राप्त कर लेते हैं।
रैंसमवेयर	▪ **रैनसमवेयर** पीड़ित की फाइलों को एन्क्रिप्ट करता है और डिक्रिप्शन के लिये भुगतान की मांग करता है। उदाहरण के लिये, वर्ष 2016 में **वानाक्राई हमला**
साइबर बुलिंग	▪ **साइबर बुलिंग** में किसी व्यक्ति की सुरक्षा को खतरा पहुँचाना या उसे कुछ भी कहने या करने के लिये मज़बूर करना शामिल है।
साइबर जासूसी	▪ **साइबर जासूसी** वर्गीकृत डेटा, निजी जानकारी या बौद्धिक संपदा तक पहुँच प्राप्त करने के लिये किसी सार्वजनिक या निजी संस्था के नेटवर्क को निशाना बनाती है।
बिज़नेस ईमेल समझौता (BEC)	▪ घोटालेबाज, आपूर्तिकर्त्ताओं, कर्मचारियों या कर कार्यालय के सदस्यों का रूप धारण करने के लिये वैध ईमेल खातों को हैक कर लेते हैं, जिसे व्हाइट-कॉलर अपराध माना जाता है।
डेटिंग हुडविंक्स	▪ हैकर्स डेटिंग वेबसाइटों, चैट रूमों और ऑनलाइन डेटिंग ऐप्स का उपयोग संभावित साझेदारों के रूप में पेश आने तथा व्यक्तिगत डेटा तक पहुँच प्राप्त करने के लिये करते हैं।

- **साइबर धोखाधड़ी के परिणाम:**
    - **व्यक्तियों के लिये:** साइबर अपराधों के कारण क्रेडिट कार्ड पर **अनधिकृत खरीदारी हो सकती है** और वित्तीय खातों तक पहुँच समाप्त हो सकती है। व्यक्तिगत डेटा का उपयोग **पीड़ितों को परेशान करने और ब्लैकमेल करने के लिये** किया जा सकता है, जिससे व्यक्तिगत संकट और बढ़ सकता है।
    - **व्यवसायों के लिये:** जो कंपनियाँ क्लाइंट डेटा की सुरक्षा करने में विफल रहती हैं, उन्हें **भारी जुर्माना और कानूनी दंड** का सामना करना पड़ सकता है। साइबर हमले किसी फर्म के समग्र मूल्य को कम कर सकते हैं, जिसका असर स्टॉक की कीमतों पर पड़ता है।
    - **सरकार के लिये:** साइबर उल्लंघनों का उद्देश्य अक्सर **राष्ट्रीय रक्षा और सुरक्षा संबंधी जानकारी को भ्रष्ट या मुद्रीकृत करना होता है,** जिससे देश की सुरक्षा को गंभीर खतरा उत्पन्न हो सकता है।

//



भारत में साइबर धोखाधड़ी का परदृिश्य क्या है?

- **अवलोकन:** भारत में लगभग **658 मलियिन इंटरनेट उपयोगकर्त्ता** हैं, जो इसे वशि्व की **दूसरी सबसे बड़ी इंटरनेट आबादी बनाता है।**

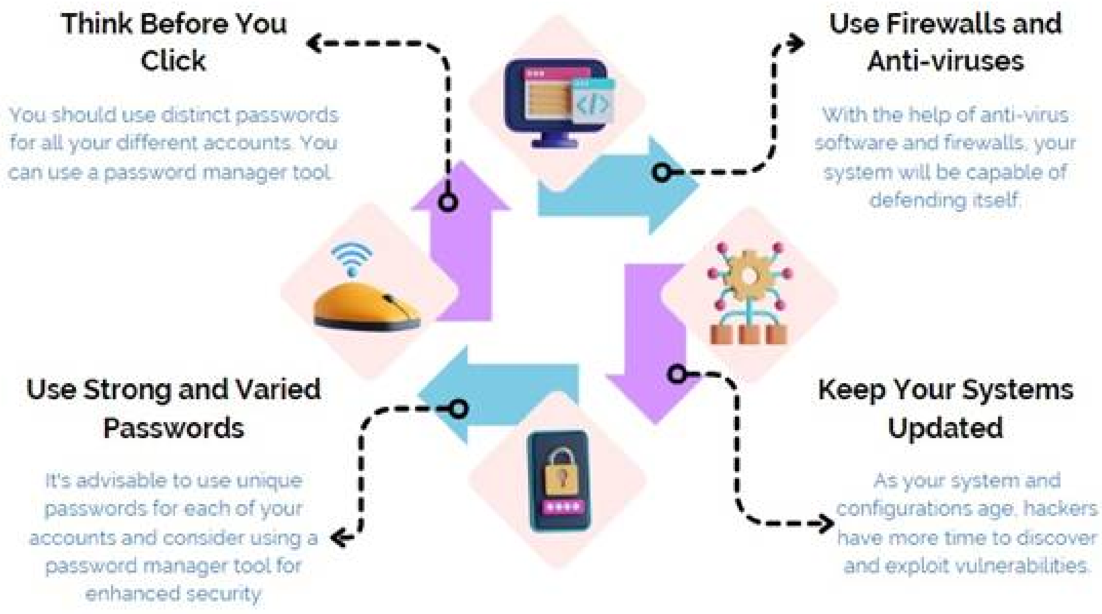
- **साइबर सुरक्षा फर्म Zscaler की "द थ्रेटलैब्ज़ 2024 फिशिंग रिपोर्ट"** के अनुसार, **अमेरिका और ब्रिटेन** के बाद **फिशिंग हमलों के लिये** भारत वैश्विक स्तर पर **तीसरा सबसे बड़ा** देश है।
- **साइबर सुरक्षा के प्रति प्रतिबद्धता:** भारत ने अंतरराष्ट्रीय दूरसंचार संघ (ITU) द्वारा प्रकाशित वैश्विक साइबर सुरक्षा सूचकांक (GCI) 2024 में **टियर 1** का दर्जा हासिल किया है।
  - **100 में से 98.49** के उल्लेखनीय स्कोर के साथ, भारत पूरे विश्व में साइबर सुरक्षा प्रथाओं के प्रति मज़बूत प्रतिबद्धता प्रदर्शित करने वाले **'रोल-मॉडलिंग'** देशों की श्रेणी में शामिल हो गया है।
- **उल्लेखनीय साइबर धोखाधड़ी की घटनाएँ:**
  - **आधार डेटा ब्रीच (2018):** 1.1 बिलियन आधार कार्डधारकों के व्यक्तिगत डेटा से समझौता किया गया, जिसमें **आधार नंबर, स्थायी खाता संख्या (PAN) और बैंक विवरण** जैसी जानकारी शामिल थी।
  - **केनरा बैंक एटीएम अटैक (2018): हैकर्स ने 300 डेबिट कार्ड** पर स्कीमिंग डिवाइस का इस्तेमाल किया और 20 लाख रुपए से अधिक की चोरी की।
  - **पेगासस स्पाइवेयर:** इज़रायल द्वारा निर्मित इस स्पाइवेयर पेगासस का इस्तेमाल उपयोगकर्त्ता की सहमति के बिना डिवाइस से डेटा एकत्र करने के लिये किया गया था, जिससे 300 से अधिक सत्यापित भारतीय फोन नंबर प्रभावित हुए।

भारत में साइबर धोखाधड़ी से संबंधित प्रमुख सरकारी पहल क्या हैं?

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

साइबर धोखाधड़ी से निपटने के लिये क्या किया जा सकता है?

- **साइबर सुरक्षा की सर्वोत्तम पद्धतियों को अपनाना: फायरवॉल** का उपयोग करना जो कंप्यूटरों के लिये रक्षा की पहली पंक्ति के रूप में कार्य करते हैं, अनधिकृत पहुँच को रोकने के लिये नेटवर्क ट्रैफिक की निगरानी और फिल्टरिंग करते हैं।
  - सुरक्षा कमज़ोरियों को दूर करने के लिये सभी सॉफ्टवेयर और हार्डवेयर प्रणालियों को **अद्यतन रखना।**
- **व्यक्तियों के लिये: अवांछित ईमेल, टेक्स्ट और फोन कॉल** से सावधान रहना, विशेषकर उनसे जो उपयोगकर्त्ताओं को सुरक्षा उपायों को दरकिनार करने के लिये मज़बूर करने का प्रयास करते हैं।
  - प्रत्येक खाते के लिये मज़बूत, **अद्वितीय पासवर्ड का उपयोग करना** जिसमें संख्याएँ, अक्षर और विशेष वर्ण सम्मिलित हों।
- **व्यवसायों के लिये: सुरक्षा की** एक अतिरिक्त डिग्री प्रदान करने के लिये, सभी कर्मचारी खातों के लिये टू-फैक्टर ऑथेंटिकेशन सक्षम करना।
  - **वित्तीय रिकॉर्ड,** ग्राहक जानकारी और **बौद्धिक संपदा** सहित संवेदनशील व्यावसायिक डेटा की सुरक्षा के लिये **एन्क्रिप्शन का** उपयोग करना।
- **बैंकों की भूमिका:** बैंकों को **कम शेष वाले या वेतनभोगी खातों** में असामान्य रूप से उच्च मूल्य के लेनदेन पर नजर रखनी चाहिये तथा प्राधिकारियों को सचेत करना चाहिये।
  - सामान्यतः चुराई गई धनराशि को क्रिप्टोकरेंसी में परिवर्तित करने और विदेश में स्थानांतरित करने से पहले अस्थायी रूप से इन खातों में रखा जाता है।
- **सिस्टम अपग्रेड की आवश्यकता:** बैंकों को एक ही IP एड्रेस से एकाधिक खाता लॉगिन का पता लगाने के लिये अपने सिस्टम को अपग्रेड करना चाहिये, विशेषकर यदि IP देश के बाहर हो।
- **कंटेंट क्रिएटर के लिये: बौद्धिक संपदा, कानूनी शुल्क** और विवादों या डेटा उल्लंघनों से होने वाले संभावित वित्तीय नुकसान से सुरक्षा के लिये निर्माता बीमा में निवेश करना।



[illegible]:

प्रश्न: भारत में साइबर धोखाधड़ी के बढ़ते खतरे और अर्थव्यवस्था पर इसके वित्तीय प्रभाव की जाँच कीजिये।

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

[illegible]

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 कंप्यूटर तक उसकी पहुँच 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 जान-बूझकर कंप्यूटर को नुकसान पहुँचाया गया है तो नए कंप्यूटर 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 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)

??????

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

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/cyberfraud-costs-0-7-of-gdp