डिजिटल अरेस्ट स्कैम

[स्रोत: टाइम्स ऑफ इंडिया](#)

चर्चा में क्यों?

गृह मंत्रालय (Ministry of Home Affairs- MHA) ने **'डिजिटल अरेस्ट' घोटालों** में वृद्धि के बारे में चेतावनी जारी की है, जहाँ साइबर अपराधी बिना सोचे-समझे पीड़ितों से पैसे निकालने के लिये सरकारी अधिकारियों का रूप धारण करते हैं।

- भारतीय साइबर अपराध समन्वय केंद्र (Indian Cybercrime Coordination Centre- I4C) , माइक्रोसॉफ्ट के सहयोग से इस संगठित ऑनलाइन आर्थिक अपराध का सक्रिय रूप से मुकाबला कर रहा है।

डिजिटल अरेस्ट स्कैम क्या है?

- **साइबर अपराधी प्रतिरूपण:** घोटालेबाज़ खुद को पुलिस, केंद्रीय अन्वेषण ब्यूरो (Central Bureau Investigation- CBI), नारकोटिक्स विभाग, भारतीय रिज़र्व बैंक (Reserve Bank of India- RBI) या प्रवर्तन निदेशालय (ED) सहित विभिन्न सरकारी एजेंसियों के कर्मियों के रूप में पेश करते हैं।
- **धमकाने की रणनीति:** पीड़ितों को **अवैध गतिविधियों में शामिल होने का आरोप** लगाते हुए कॉल प्राप्त होते हैं, जैसे कि ड्रग्स या नकली पासपोर्ट जैसी प्रतिबंधित वस्तुओं को भेजना या प्राप्त करना।
  - जालसाज़ उस "मामले" को बंद करने के लिये भी पैसे की मांग कर सकते हैं जिसमें किसी प्रियजन को कथित तौर पर आपराधिक गतिविधि या दुर्घटना में फँसाया गया हो।
- **डिजिटल कारावास:** कुछ पीड़ितों को 'डिजिटल गिरफ्तारी' के अधीन किया जाता है, जहाँ उन्हें स्कैमर्स के साथ वीडियो कॉल पर तब तक रहने के लिये मजबूर किया जाता है जब तक कि उनकी मांगें पूरी नहीं हो जातीं।
- **पैसों की मांग:** झूठे कानूनी मामलों को बेनकाब नहीं करने के लिये **सहमत होने के बदले अपराधी पैसे वसूल** रहे हैं।

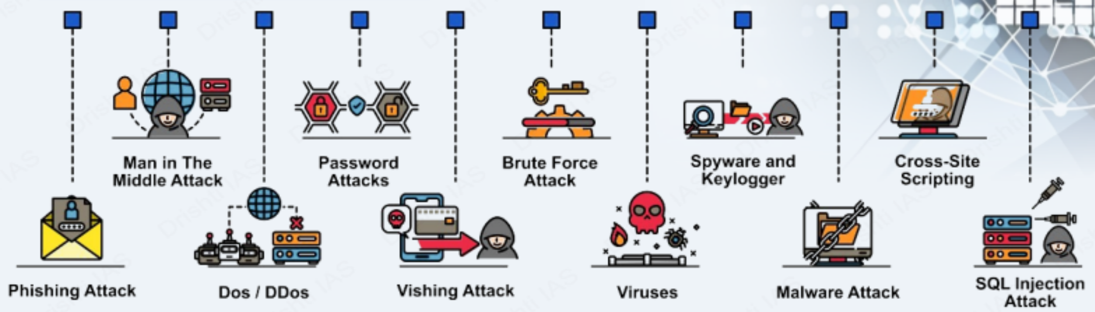
इन घोटालों से निपटने के लिये क्या कदम उठाए जा रहे हैं?

- **धोखाधड़ी वाले खातों को ब्लॉक करना:** I4C ने सरकारी कर्मियों के रूप में प्रस्तुत किये जाने वाले साइबर अपराधियों द्वारा नागरिकों को डराने-धमकाने, ब्लैकमेल करने, ज़बरन वसूली और "डिजिटल गिरफ्तारी" से जुड़े 1,000 से अधिक स्काइप खातों को ब्लॉक कर दिया है।
  - I4C इन धोखेबाजों द्वारा उपयोग किये गए सिमकार्ड, मोबाइल डिवाइस और मूल खातों को ब्लॉक करने की सुविधा भी दे रहा है।
- **क्रॉस-बॉर्डर अपराध सिंडिकेट:** गृह मंत्रालय ने पहचान की है कि ये घोटाले सीमा पार (क्रॉस-बॉर्डर) अपराध सिंडिकेट द्वारा संचालित होते हैं, जो उन्हें एक बड़े, संगठित ऑनलाइन आर्थिक अपराध नेटवर्क का हिस्सा बनाते हैं।
- **सतर्कता और जागरूकता:** I4C ने अपने सोशल मीडिया प्लेटफॉर्म **"साइबर दोस्त"** और अन्य प्लेटफॉर्मों पर इस तरह की धोखाधड़ी के संबंध में सतर्कता को बढ़ाया है।
  - यदि किसी को ऐसी कॉल आती है, तो उन्हें सहायता के लिये तुरंत **साइबर क्राइम हेल्पलाइन नंबर** या वेबसाइट **"नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल"** पर घटना की रिपोर्ट करनी चाहिये।

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

- महत्त्वपूर्ण बुनियादी ढाँचा सुरक्षा (रोबस्ट एक्सेस कंट्रोल)
- नेटवर्क सुरक्षा (डिप्लॉयिंग फायरवॉल)
- एप्लिकेशन सुरक्षा (कोड रिव्यु)
- 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

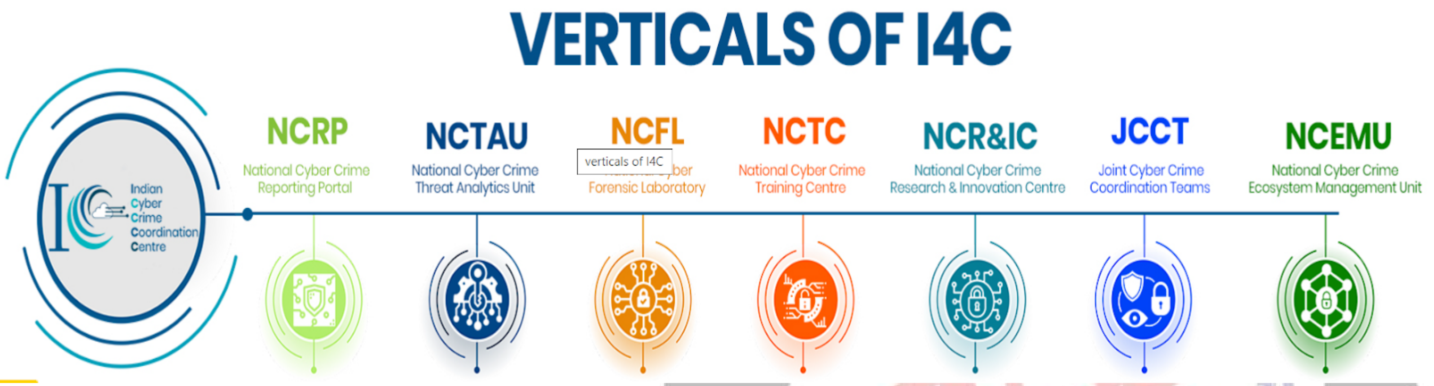
- नेटवर्क सुरक्षा
- मैलवेयर सुरक्षा
- इंसिडेंट मैनेजमेंट
- उपयोगकर्त्ता को शिक्षित और जागरूक करना
- सुरक्षित विन्यास
- उपयोगकर्त्ता के विशेषाधिकारों का प्रबंधन करना
- सूचना जोखिम प्रबंधन व्यवस्था

Drishti IAS

//

भारतीय साइबर अपराध समन्वय केंद्र (I4C):

- इसकी स्थापना गृह मंत्रालय द्वारा नई दिल्ली में साइबर अपराध से समन्वित और व्यापक तरीके से निपटने के लिये **कानून प्रवर्तन एजेंसियों (LEA)** के लिये एक रूपरेखा और पारिस्थितिकी तंत्र प्रदान करने के लिये की गई थी।
    - I4C को देश में साइबर अपराध पर अंकुश लगाने के लिये नोडल बिंदु के रूप में कार्य करने की परिकल्पना की गई है।
- यह **तीव्रता से विकसित हो रही प्रौद्योगिकियों एवं अंतर्राष्ट्रीय सहयोग को बनाए रखने के लिये साइबर कानूनों में संशोधन** का प्रस्ताव करता है।
- गृह मंत्रालय में संबंधित प्राधिकारी के परामर्श से साइबर अपराधों के लिये अन्य देशों के साथ [पारस्परिक कानूनी सहायता संधियों (MLAT)](#) के कार्यान्वयन का समन्वय करना।
    - MLAT दो या दो से अधिक देशों के बीच एक द्विपक्षीय समझौता है जो आपराधिक अथवा सार्वजनिक कानूनों को लागू करने के लिये सूचना और साक्ष्य के आदान-प्रदान की अनुमति देता है।



और पढ़ें: [भारत की साइबर सुरक्षा चुनौती: खतरे और रणनीतियाँ](#)

UPSC सिविल सेवा परीक्षा, विगत वर्ष के प्रश्न

??????????

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

1. यदि कोई किसी मैलवेयर कंप्यूटर तक उसकी पहुँच को 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 एक नए कंप्यूटर की लागत
3. यदि साइबर बलात्-ग्रहण होता है तो इस हानि को न्यूनतम करने के लिये विशेष परामर्शदाता की की सेवाएँ 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 निम्नलिखित में से किसके लिये साइबर सुरक्षा घटनाओं पर रिपोर्ट करना कानूनी रूप से अनिवार्य है? (2017)

1. सेवा प्रदाताओं
2. डेटा केंद्र
3. कॉर्पोरेट निकाय

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)

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/digital-arrest-scams