कैप्चा

[स्रोत: द हिंदू](#)

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) एक चैलेंज-रिस्पॉन्स परीक्षण है जिसका उपयोग मानव उपयोगकर्त्ताओं से Bots को अलग करने के क्रम में ऑनलाइन सुरक्षा बढ़ाने और उपयोगकर्त्ता डेटा की सुरक्षा के लिये किया जाता है।

- **बॉट्स (Bots)** स्वचालित सॉफ्टवेयर प्रोग्राम हैं जो **रिपीटेटिव ऑनलाइन** कार्य करने पर केंद्रित हैं।

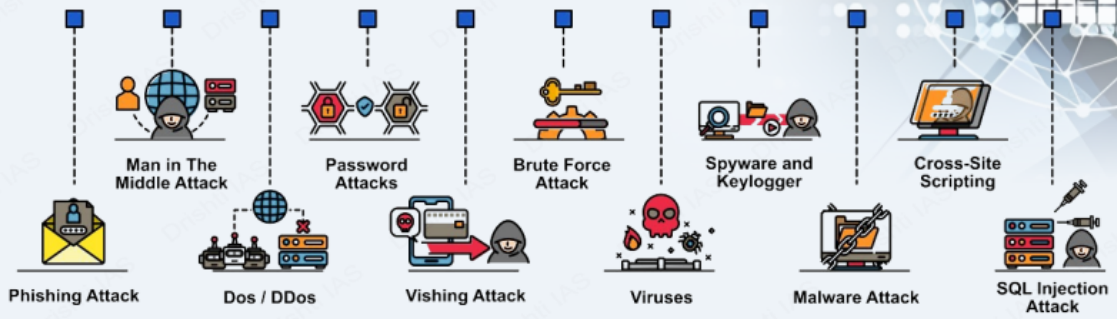
कैप्चा:

- **उत्पत्ति:** इसे **लुइस वॉन आहन** द्वारा 2000 के दशक की शुरुआत में बॉट्स को ब्लॉक करने के लिये विकसित किया गया, CAPTCHA **विकृत टेक्स्ट (वर्ष 2003)** से शुरू हुआ और यह **स्कैन्ड बुक वर्ल्डस का उपयोग करके reCAPTCHA (वर्ष 2009)** में विकसित हुआ और बाद में **Google द्वारा व्यवहार विश्लेषण का उपयोग करके अदृश्य reCAPTCHA (वर्ष 2014)** में विकसित हुआ। इसका **आधुनिक संस्करण इमेज पहचान, चेकबॉक्स और इंटरैक्शन ट्रैकिंग** के उपयोग पर केंद्रित है।
- **लाभ:** इससे **बॉट्स को ब्लॉक करने, फर्जी अकाउंट, स्पैम** और डेटा चोरी को रोकने के साथ यह सुनिश्चित होता है कि केवल मानव उपयोगकर्त्ता ही डिजिटल प्लेटफॉर्म का उपयोग कर सकें।
- **अनुप्रयोग: CAPTCHA का उपयोग लॉगिन, पंजीकरण, लेन-देन, खाता पुनर्प्राप्ति और सर्वेक्षणों में बॉट्स को ब्लॉक करने तथा उपयोगकर्त्ताओं को सत्यापित करने के लिये किया जाता है। reCAPTCHA बुक डिजिटिलीकरण में भी सहायक है।**
- **हानियाँ:** इससे **डिसेबल्ड उपयोगकर्त्ताओं के लिये पहुँच में बाधा** उत्पन्न होने के साथ **मोबाइल उपयोगकर्त्ताओं** के लिये यह बोझिल हो सकता है। इसे उन्नत बॉट्स द्वारा दरकिनार किये जाने से उपयोगकर्त्ता अनुभव प्रभावित हो सकता है।
- **अन्य साइबर सुरक्षा उपाय:** अन्य उपायों में **टू फैक्टर ऑथेंटिकेशन (2FA),** डिवाइस कोड के माध्यम से दूसरा सत्यापन स्तर, फिंगरप्रिंट या चेहरे की पहचान का उपयोग करके **बायोमेट्रिक सत्यापन, बॉट्स को ट्रैप करने के लिये हनीपॉट्स** और **व्यवहारिक बायोमेट्रिक्स** (जिसमें मनुष्यों को बॉट्स से अलग करने हेतु टाइपिंग या स्वाइप पैटर्न को ट्रैक किया जाता है) शामिल 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

- महत्त्वपूर्ण बुनियादी ढाँचा सुरक्षा (रोबस्ट एक्सेस कंट्रोल)
- नेटवर्क सुरक्षा (डिफेंसिव 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: [उभरते साइबर खतरे और उनके निहितार्थ]