साइबर सिक्योरिटी 6

साइबर अपराध

कम्प्यूटर तथा इंटरनेट के माध्यम से किया गया गैर-कानूनी कार्य या अपराध, **साइबर क्राइम** कहलाता है। इसे **नेट क्राइम (Net Crime)** भी कहा जाता है। साइबर क्राइम के कुछ उदाहरण हैं-

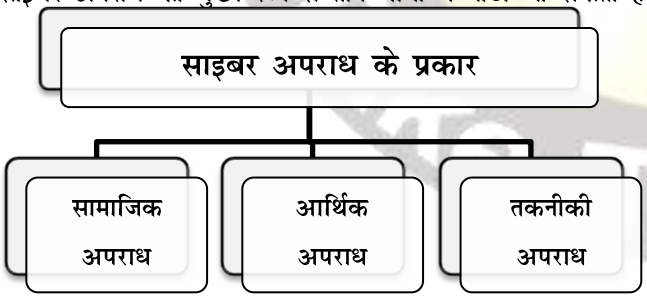
- नेटवर्क का अनाधिकृत तौर पर प्रयोग।
- व्यक्तिगत (Private) तथा गुप्त (Confidential) सूचना प्राप्त करना।
- वायरस द्वारा कम्प्यूटर तथा डाटा को नुकसान पहुंचाना।
- गैर-कानूनी तथा असामाजिक तथ्यों तथा चित्रों को प्रदर्शित करना।
- आर्थिक अपराध (Financial Fraud) करना आदि।
- **साइबर अपराध** संविधान की सातवीं अनुसूची के अनुसार **राज्य सूची के अंतर्गत** आता है तथा **साइबर कानून अवशिष्ट शक्तियों के अंतर्गत** आते हैं अर्थात् संसद अकेले इन विषयों पर कानून बना सकती है।
- आर्थिक सहयोग और विकास संगठन **(Organisation for Economic Co-Operation and Development-OECD)** के अनुसार साइबर अपराधों की श्रेणी में गैर-कानूनी, अनैतिक और अनाधिकृत प्रकृति के ऐसे कार्यों को शामिल किया जाता है, जिनके माध्यम से पूर्व अनुमति के बगैर आँकड़ों का प्रसारण किया जाता है।
- **साइबर स्पेस (Cyber Space)** शब्द सबसे पहले अमेरिकन कनेडियन लेखक **विलियम गिब्सन ने 1984** में अपनी पुस्तक **न्यूरोमेंसर** में प्रयोग किया।

साइबर हमले के निम्न रूप हो सकते हैं-

- इंटरप्शन (व्यवधान)
- मॉडीफिकेशन (संशोधन)
- इंटरसेप्शन (अवरोधन)
- फैब्रीकेशन (संरचना)

साइबर अपराध के प्रकार

साइबर अपराध को मुख्य रूप से तीन भागों में बांटा जा सकता है-



1. *सामाजिक अपराध*

- **साइबर वारफेयर (Cyber Warfare)**-किसी राष्ट्र द्वारा दूसरे राष्ट्र के कम्प्यूटर नेटवर्क में घुसकर गुप्त व संवेदनशील डाटा को चुराना, नष्ट करना या नेटवर्क संचार को बाधित करना, **साइबर वारफेयर** कहलाता है। संचार क्रांति में इसे वायु, समुद्र, जमीन तथा अंतरिक्ष के बाद **'युद्ध का पांचवा क्षेत्र' (Fifth Domain of Warfare)** भी कहा जाता है।
- **साइबर पोर्नोग्राफी (Cyber Pornography)**- इसके तहत् अश्लील सामग्रियों का प्रसारण, जैसे- अश्लील चित्र भेजना, अश्लील साहित्य लिखना तथा डाउनलोड करना आदि शामिल हैं।
- **साइबर बुलिंग (Cyber Bullying)**- इंटरनेट सेवा और वेब पेज जैसी मोबाइल तकनीकों का उपयोग करके एसएमएस, टेक्स्ट मैसेजिंग द्वारा दूसरे व्यक्ति को हानि पहुँचाना **साइबर बुलिंग** है।
- **फ्लैम**- इंटरनेट पर किसी व्यक्ति के लिए लिखे हुए अपशब्द **फ्लैम** कहलाते हैं।
- **आइडेंटिटी थेफ्ट**- अपराधियों द्वारा छद्म रूप धारण कर यूजर की व्यक्तिगत पहचान जैसे User ID, पासवर्ड तथा अन्य गोपनीय जानकारी चुराना **आइडेंटिटी थेफ्ट** कहलाता है।
- **Eavesdropping**- इसमें अटैकर, भेजे जाने वाले संदेशों की निगरानी रखता है।
- **छद्मवेश (Masquerading)**- इसमें अटैकर, वेलिड (Valid) यूजर होने का नाटक करता है और अवैध रूप से विशेष अधिकार प्राप्त कर, साइबर अपराध करता है।
- **साइबर ग्रूमिंग (Cyber Grooming)**- जब कोई बड़ा व्यक्ति, छोटे एवं इंटरनेट या सोशल नेटवर्किंग साइट पर नये आये लोगों को अपने जाल में फंसाता है, तो यह **साइबर ग्रूमिंग** है
- **ईगोसर्फर (Egosurfer)**- एक ऐसा व्यक्ति जो इंटरनेट पर किसी भी व्यक्ति विशेष के संबंध स्वयं से या किसी और से जोड़ने के लिए जानकारी एकत्रित करता है, **ईगोसर्फर** कहलाता है।
- **डिजिटल अरेस्ट (Digital Arrest)**- यह ब्लैकमेल करने का एडवांस तरीका है, जिसमें साइबर ठग नकली पुलिस अधिकारी बनकर, अंजान नंबर से कॉल या वॉट्सएप करके लोगों को धमकाते हैं और अपना शिकार बनाते हैं। इसमें ठग डिजिटल रूप से घर में ही बंधक बनाकर लोगों से पैसे ट्रांसफर करवाते रहते हैं।

2. *आर्थिक अपराध*

- **सलामी हमला (Salami Attack)**-जब साइबर अपराधी द्वारा बैंकों के खाता धारकों (Account Holders) के खाते से धन निकासी (प्रायः बहुत ही मामूली रकम) के उद्देश्य से **बैंक की कम्प्यूटर प्रणाली में एक अवांछित प्रोग्राम** को डाला जाता है, तो यह **सलामी हमला** है। इसमें खाता धारकों के खाते से **कुछ रकम** उक्त अपराधी के खाते में हस्तांतरित हो जाती है।
- **साइबर स्टॉकिंग (Cyber Stalking)**- साइबर अपराधी इंटरनेट उपयोगकर्त्ताओं से चैटिंग के दौरान तथा किसी अन्य इंटरनेट माध्यम द्वारा उनके नाम, पता, फोन नंबर तथा अन्य जानकारियाँ हासिल कर उन्हें ब्लैकमेल करते हैं तब यह **साइबर स्टॉकिंग** है।
- **पाइरेसी**- मूल उत्पाद की नकल उतारकर या उसकी प्रतिलिपि को कालाबाजारी के माध्यम से बाजार में बेचना **पाइरेसी** है।

❖ **स्पूफिंग (Spoofing)**- 'स्पूफ' का अर्थ होता है- झूठी तरकीब या छलावा। इसमें अधिकृत स्रोत से उत्पन्न दिखने वाला ईमेल भेजा जाता है, जो वास्तव में साइबर अपराधी द्वारा भेजा जाता है तथा यह एक फिशिंग हमले के रूप में डाटा चुराने, कम्प्यूटर को मालवेयर से संक्रमित करने या पैसे मांगने के लिए डिजाइन किया जाता है।

सीधे परीक्षा स .....

प्र. एक ई-मेल जो एक स्रोत से उत्पन्न दिखता है, जो कि वास्तव में दूसरे से भेजा गया है।

(a) फिशिंग (b) स्पूफिंग
(c) स्पैमिंग (d) स्नीफिंग

उत्तर- (b) **(MPPSC -2021)**

❖ **विशिंग (Vishing)**- इसमें फोन कॉल के माध्यम से जाल-साज ग्राहक आईडी, नेटवर्किंग पासवर्ड, ATM Pin, OTP, कार्ड की समाप्ति तिथि आदि गोपनीय जानकारी प्राप्त करने की कोशिश करते हैं।

❖ **साइबर स्क्वॉटिंग (Cyber Squatting)**- जब किसी अन्य के ट्रेडमार्क का, लाभ के इरादे से पंजीकरण, तस्करी या डोमेन नाम का उपयोग किया जाता है तो यह **साइबर स्क्वॉटिंग** है।

❖ **क्रिप्टोजैकिंग (Cryptojacking)**- इसमें कम्प्यूटिंग संसाधनों का अनाधिकृत रूप से क्रिप्टो करेंसी को माइन करने के लिए उपयोग किया जाता है।

❖ **स्कीमिंग (Skimming)**- साइबर अपराधियों द्वारा कार्डधारकों की व्यक्तिगत भुगतान जानकारी चुराने या प्राप्त करने की रणनीति **स्कीमिंग** है तथा जिस उपकरण या कोड से यह किया जाता है वह **स्कीमर** कहलाता है।

3. *तकनीकी अपराध*

❖ **स्पैम (Spame)**- अनेक व्यक्तियों को अवांछित तथा अवैध रूप से भेजा गया ई-मेल **स्पैम** कहलाता है। स्पैम सामान्यत: कम्प्यूटर, नेटवर्क तथा डाटा को किसी तरह का नुकसान नहीं पहुंचाते।

- वास्तव में स्पैम एक छोटा प्रोग्राम है जो मुख्यत: **विज्ञापन** होता है तथा इसे हजारों की संख्या में इंटरनेट पर भेजा जाता है।
- **स्पैम फिल्टर, एंटीस्पैम साफ्टवेयर, बोगोफिल्टर, D-spam, स्पैम एसैसिन** का प्रयोग कर इससे बचा जा सकता है।

सीधे परीक्षा से .....

प्र. निम्नलिखित में से कौन एंटी-स्पैम सॉफ्टवेयर नहीं है?

(a) बोगोफिल्टर (b) डीएसपीएएम
(c) एमएलकपैम (d) स्पैमएसैसिन

उत्तर- (c) **(MPPSC GEO-2023)**

❖ **कुकीज (Cookies)**- कुकीज वह साफ्टवेयर है, जिसके द्वारा कोई वेबसाइट कुछ सूचनाएं उपयोगकर्त्ता की जानकारी के बिना कम्प्यूटर पर स्टोर करती है। जब उपयोगकर्ता उस वेबसाइट पर पुन: जाता है, तो सर्वर, कुकीज के माध्यम से उसकी प्राथमिकताओं को प्रस्तुत करता है अर्थात् इसमें **सूचनाओं की एक स्ट्रिंग** होती है, जो आपके **कम्प्यूटर की हार्ड डिस्क पर ब्राउजिंग जानकारी संग्रहित** करती है।

- कुकीज का प्रयोग उपयोगकर्ता की **रुचि के अनुरूप** वेबसाइट पर **विज्ञापन भेजने** के लिए किया जाता है।
- कुकीज वेबसाइटों का विवरण रखकर उपयोगकर्ता की **गोपनीयता** को **खत्म** करते हैं।

सीधे परीक्षा से .....

प्र. एक टेक्स्ट फाईल जिसमें सूचनाओं की एक स्ट्रिंग होती है जो आपके कम्प्यूटर की हार्डडिस्क पर ब्राउजिंग जानकारी संग्रहित करती है, कहलाती है।

(a) कुकी (b) यू.आर. एल.
(c) डी.एन.एस. (d) प्लन-इन

उत्तर- (a) **(MPPSC AP-2023)**

❖ **डाटा डिडलिंग (Data Diddling)**- यह एक ऐसी गतिविधि है, जिसके माध्यम से पहले तो डाटा को कम्प्यूटर पर प्रोसेस होने से पूर्व ही परिवर्तित या हेर-फेर कर दिया जाता है तत्पश्चात् कम्प्यूटर प्रोसेस होने के बाद डाटा को वास्तविक रूप में परिवर्तित कर दिया जाता है।

❖ **क्लिक जैकिंग (Click Jacking)-** क्लिक + हाइजैकिंग अर्थात् क्लिकजैकिंग में HTML Elements को अदृश्य करके हैकर अपना मेलीसियस कोड इसमें डालता है और जब यूजर पेज पर क्लिक करता है, तो वह बिना जाने हैकर के जाल में फँस जाता है। क्लिकजैकिंग शब्द का उपयोग पहली बार **ग्रॉसमैन तथा रोवर हेन्सन** द्वारा **2008** में किया गया था।

❖ **फिशिंग (Phishing)**- इंटरनेट पर उपयोगकर्त्ताओं के यूजर नेम, पासवर्ड तथा अन्य व्यक्तिगत सूचनाओं को प्राप्त करने का प्रयास करना **फिशिंग** कहलाता है। इसमें अपराधकर्त्ता कानूनी दिखने वाले **फोन कॉल, ई-मेल** तथा **SMS** भेजता है या **सॉफ्टवेयर इंस्टॉल** करने के लिए कहता। ताकि पढ़ने वाले से व्यक्तिगत तथा वित्तीय संवेदन शील सूचना को प्राप्त किया जा सके। इसमें जानकारी हासिल करने के लिए उपयोगकर्ता **छल/दिखावा** करता है।

सीधे परीक्षा से .....

प्र. ------हमला भ्रामक ईमेल या टेक्स्ट संदेशों के रूप में आता है जो आपसे सॉफ्टवेयर इंस्टॉल करने या व्यक्तिगत जानकारी प्रकट करने के लिए कह सकता है।

(a) स्पैमिंग (b) वायरस साइनिंग
(c) फिशिंग (d) स्कैनिंग

उत्तर- (c) **(MPPSC Pre-2024)**

सीधे परीक्षा से .....

प्र. हैकिंग, फिशिंग ईमेल भेजना, रेनसमवेयर किसके उदाहरण हैं?

(a) ऑनलाइन बैंकिंग सेवाएँ
(b) ऑनलाइन व्यापार गतिविधियाँ
(c) साइबर क्राइम गतिविधियाँ
(d) सरकार की ऑनलाइन सेवाएँ

उत्तर- (c) **(MPPSC AP-2022)**

सीधे परीक्षा से .....

प्र. निम्नलिखित में से कौन-सा साइबर हमले का एक प्रकार है जिसमें उपयोगकर्त्ता को संवेदनशील सूचना को ज़ाहिर करने के लिए छल करना शामिल है?

(a) फिशिंग हमला (b) SQL इंजेक्शन हमला
(c) DOSहमला (d) उपर्युक्त में से कोई नहीं

उत्तर- (a) **(MPPSC Pre-2023)**

सीधे परीक्षा से .....

प्र. ''फिशिंग'' का प्रयास निम्नलिखित में से किसके द्वारा किया जाता है?

(a) ई-मेल (b) एस.एम.एस.
(c) फोन कॉल (d) उपर्युक्त सभी

उत्तर- (d) **(MPPSC D.S.P– 2021)**

❖ **फार्मिंग (Pharming)**- इस प्रकार के साइबर हमलों में एक वेबसाइट के ट्रैफिक को दूसरी फर्जी वेबसाइट पर पुनर्निर्देशित किया जाता है।

❖ **स्मिशिंग (Smishing)**- यह एक प्रकार का साइबर सुरक्षा हमला है, जो **टेक्स्ट मैसेज के माध्यम** से किया जाता है जिसमें दुर्भावनापूर्ण वेवसाइट से सामग्री डाउनलोड करने के लिए कहा जाता है इसे **SMS फिशिंग** भी कहते हैं।

❖ **साइबर हाईजैकिंग या कम्प्यूटर हाईजैकिंग (Cyber Hijacking / Computer Hijacking)**- यह एक प्रकार का नेटवर्क सिक्योरिटी अटैक है, जिसमें अटैकर कम्प्यूटर सिस्टम के सॉफ्टवेयर या प्रोग्राम पर अधिकार स्थापित कर लेता है।

- **Zero-day Exploit/Vulnerability**- जब किसी सिस्टम में कमी की घोषणा उजागर हो जाती है, तो अटैकर **पैच प्रबंधन** से **पहल** इस **कमजोरी का फायदा** उठाने की कोशिश करते हैं, यही **Zero-day Exploit/ Vulnerability** है।
- **SQL इंजेक्सन अटैक**- इस अटैक में जब एक दुर्भावनापूर्ण कोड को एक कमजोर वेबसाइट खोज बॉक्स में इंजेक्ट किया जाता है तो सर्वर महत्वपूर्ण जानकारी प्रकट करता है। इसके परिणामस्वरूप हमलावर डेटाबेस बदलकर **प्रशासनिक अधिकार** भी हासिल कर सकते हैं।
- **Watering Hole Attack**- इस तरह के हमले में हमलावर उन वेबसाइटों को निशाना बनाकर मालवेयर से संक्रमित करता है, जिन्हें लक्षित समूह द्वारा अक्सर इस्तेमाल किया जाता है।
- **स्नूपिंग/स्निफिंग (Snoofing/Sniffing)**- नेटवर्क ट्रेफिक को **गुप्त रूप से पकड़ने (जासूसी)** और उसका **विश्लेषण** करने की प्रक्रिया **स्नूपिंग/स्नफिंग** है। इसमें हमलावर आमतौर पर असुरक्षित या खुले नेटवर्क संचार और अनएन्क्रिप्टेड डाटा तक अनाधिकृत पहुँच द्वारा निगरानी रखते हैं।

.....सीधे परीक्षा से

प्र. नेटवर्क ट्रॉफिक को गुप्त रूप से पकड़ने और उसका विश्लेषण करने की प्रक्रिया को कहा जाता है।

(a) स्पूफिंग (b) इव्ज ड्रॉपिंग
(c) स्नूपिंग (d) डिनायल ऑफ सर्विस

उत्तर- (c) **(MPPSC AP-2023)**

.....सीधे परीक्षा से

प्र. निम्नलिखित में से क्या साइबर क्राइम का उदाहरण नहीं है?

(a) डिनायल ऑफ सर्विस (b) फिशिंग
(c) स्पैमिंग (d) क्रिप्टोग्राफी

उत्तर- (d) **(A.D.P.O. – 2021)**

- **क्रैकिंग**- किसी की इजाजत के बिना निजी जानकारी या डाटा चुराना **क्रैकिंग** है। क्रैकर इस डाटा का दुर्पयोग करते हैं। इन्हें **ब्लैक हैट हैकर** भी कहा जाता है।

.....सीधे परीक्षा से

प्र. निम्न में से कौन-सा एक साइबर अपराध नहीं है?

(a) साइबर आतंकवाद (b) इंटरप्रेटर
(c) डेटा चोरी (d) जालसाजी

उत्तर- (b) **(MPPSC SFS-2019)**

महत्त्वपूर्ण शब्दावली

- **बग**-किसी प्रोग्राम या सिस्टम में रह जाने वाली गलती को **बग (छिद्र)** कहा जाता है।
- **डिबग**-किसी प्रोग्राम में गलतियाँ पकड़ने की क्रिया को **डिबग** कहा जाता है।
- **फ्लैमर**- यह वो व्यक्ति है जो किसी फोरम या इंटरनेट मैसेज बोर्ड पर निम्न स्तरीय या बेइज्जती से भरी हुई टिप्पणी लिखता है।
- **ग्रीफर**- ऑनलाइन गेम का एक खिलाड़ी जो दूसरे खिलाड़ियों को परेशान करता है **ग्रीफर** कहलाता है।
- **माइनिंग**- यह संवेदनशील डाटा और लेन-देन की सुरक्षा के लिए उपयोग किया जाने वाला घटक है।
- **नूब (Noob)**- एक **नया या अप्रशिक्षित व्यक्ति**, जिसने हाल ही में ज्वाइन किया है तथा जो वेबसाइट के नियमों को नहीं जानता, **नूब** कहलाता है।
- **फिशिंग ट्रिप**- अपनी गलत पहचान बताकर किसी गोपनीय सूचना को प्राप्त करना **फिशिंग ट्रिप** है।
- **ट्रॉल (Troll)**- वह व्यक्ति जो फोरम पर या चैटिंग के दौरान किसी की कॉपी, मिमिक्री करके अथवा किसी अन्य कार्य से बदनामी करता है **ट्रॉल** कहलाता है।

परीक्षा उपयोगी महत्वपूर्ण साइबर हमले

- **मैन-इन-द-मिडिल (MITM) Attack** – इसमें **साइबर हमला** करने वाला **व्यक्ति** खुद को **उपयोगकर्ता और एप्लिकेशन के बीच** में रखता है, ताकि उनके संचार और डेटा एक्सचेंजों को बाधित कर दुर्भावनापूर्ण उद्देश्यों की प्राप्ति कर सके। जैसे- अनाधिकृत खरीददारी करना या हैंकिंग करना।
  - यह **डिफी-हेलमैन एल्गोरिद्म** तथा **RSA एल्गोरिद्म** में पाया जाता है।
- **Replay हमला**- अन्य नाम- रिपीट अटैक या प्लेबैक अटैक।
  - यह नेटवर्क हमले का एक रूप है जिसमें वध डेटा ट्रांसमिशन दुर्भावनापूर्ण या धोखाधड़ी से दोहराया या विलंबित होता है।
  - यह या तो प्रवर्तक द्वारा या एक प्रतिद्वंद्वी द्वारा किया जाता है, जो डेटा को रोकता है और इसे फिर से प्रसारित करता है।
  - यह हमला **मैन-इन-द मिडिल हमले का एक निम्न संस्करण** है।
- **क्रॉस साइट स्क्रिप्टिंग (Cross Site Scripting)**- यह अटैक हमलावरों को एक वेबसाइट में मैलिशियस कोड इंजेक्ट करने की अनुमति देते हैं, जिसे बाद में साइट पर आने वाले यूजर्स द्वारा निष्पादित किया जाता है।
- **Whaling (व्हेलिंग) हमला**-यह एक तरह का **फिशिंग हमला** है। जिसे **CEO धोखाधड़ी** भी कहते हैं। इसमें कंपनियों से संवदेनशील जानकारी प्राप्त करने के लिए प्रमुख वित्तीय अधिकारियों या मुख्य कार्यकारी अधिकारियों को लक्षित किया जाता है।

.....सीधे परीक्षा से

प्र. मैन-इन-द-मिडिल अटैक, निम्नलिखित में से किस एल्गोरिद्म में पाया जाता है?

(a) RSA एल्गोरिदम
(b) डिफी-हेलमैन एल्गोरिद्म
(c) (a) और (b) दोनों
(d) न तो (a) और न ही (b)

उत्तर- (a,b,c)

(MPPSC ITI Assitant Principal-2023)

हैकिंग

- अनाधिकृत रूप से नेटवर्क में घुसकर डाटा या सॉफ्टवेयर से छेड़छाड़ करने की प्रक्रिया **हैकिंग (Hacking)** कहलाती है।
- हैकिंग के कारण अधिकृत उपयोगकर्त्ता नेटवर्क तथा संसाधनों का सही उपयोग नहीं कर पाता। इसे **Denial of Service (DoS)** कहते हैं।
- हैकिंग को साइबर तकनीकी के क्षेत्र में चिंता एवं अपराध के विषय के रूप में **1970 के दशक में संकलित** किया गया।
- **DEFCON** को **हैकर का पहला सम्मेलन** माना जाता है, जो कि **1993 में, लास-वेगास नेवदा (USA)** में हुआ।
- **Wifi Hacking** के लिए **एयर क्रैकिंग** का उपयोग किया जाता है, जोकि एक **Wifi Security ऑडिट टूल** है।

हैकर

- **हैकर**- हैकर वह व्यक्ति होता है, जो साफ्टवेयर तथा नेटवर्क में विद्यमान सुरक्षा **खामियों का पता लगाकर** उनका उपयोग नेटवर्क में घुसने तथा **डाटा या संग्रहित जानकारी की चोरी अनाधिकृत प्रयोग** करने के लिए करता है।
- आरम्भ में हैकर फोन कॉल का उपयोग करते थे, जिसे **फ्रीक्रिंग** कहते हैं।

.....सीधे परीक्षा से

प्र. किसी कम्प्यूटर में संग्रहित जानकारी को अनाधिकृत तरीके से चोरी करने वाले व्यक्ति को कहा जाता है।

(a) हैकर (b) वायरस
(c) प्रोसेसर (d) एडिटर

उत्तर- (a) **(MPPSC SFS-2019)**

हैकर के प्रकार

व्हाइट हैट हैकर (White Hat Hacker)

- इस श्रेणी में आने वाले हैकर **अच्छे काम** करते हैं, यानी इन्हें **लोगों की सुरक्षा के लिये नियुक्त** किया जाता है। इन्हें सरकार के द्वारा या किसी भी संस्था के द्वारा रखा जाता है।
- इनका **प्रयोग नेटवर्क की कमजोरियों का पता लगाने** में किया जाता है।
- इन्हें सरकार या किसी संस्था के द्वारा रखा जाता है।
- इन्हें **एथिकल हैकर** भी कहते हैं।

ब्लैक हैट हैकर (Black Hat Hacker)

- इन्हें **क्रैकर्स** भी कहा जाता है।
- यह कम्प्यूटर तथा नेटवर्क की सुरक्षा पद्धति में **सेंध लगाकर** या **अनाधिकृत साफ्टवेयर** द्वारा पासवर्ड प्राप्त कर, **अवैध कार्य** करते हैं।
- क्रैकर **अपराध या आर्थिक लाभ के लिए गैर-कानूनी कार्य** करते हैं।

ग्रे हैट हैकर (Gray Hat Hacker)

- इस श्रेणी के हैकर **ब्लैक और व्हाइट का सम्मिश्रण** होते हैं।
- यह कुछ समय के लिये अच्छा काम और कभी-कभी गैर-कानूनी काम भी करते हैं।

ग्रीन हैट हैकर (Green Hat Hacker)

- जो अभी हैकिंग सीख रहे हैं, इन्हें **प्री हैकर** भी कहा जाता है।

रेड हैट हैकर (Red Hat Hacker)

- ये **White Hat Hacker के समान** कार्य करते हैं, लेकिन इनका कार्य करने का **तरीका आक्रामक** होता है।

ब्लू हैट हैकर (Blue Hat Hacker)

- सॉफ्टवेयर को उपयोग करने से पहले उसकी **कमियों को उजागर कर सही करने वाले ब्लू हैट हैकर (Blue Hat Hacker)** कहलाते हैं।
- यह किसी भी **संस्था के लिए काय नहीं** करते हैं।

स्क्रिप्ट किडीज (Script Kidies)

- ऐसे हैकर होते हैं, जिन्हें **कम्प्यूटर का ज्यादा ज्ञान नहीं** होता है, लेकिन दूसरे कुशल हैकर्स के बनाये टूल का उपयोग करके हैकिंग करते हैं।

हैक्टिविस्ट (Hacktivist)

- यह सामाजिक, धार्मिक और राजनीतिक आदि संदेश भेजने के लिए हैकिंग का उपयोग करते हैं।
- यह वेबसाइटों को हाईजैक करके उन पर संदेश छोड़ने का काम करते हैं।

Elite Hacker

- वैसे हैकर जो **हैकिंग में सबसे ज्यादा कुशल** होते हैं।

फ्रीकर/फ्रेकर (Phreaker)

- यह **टेलीफोन सिस्टम में हेर-फेर** या **हैकिंग** करके लोगों का शोषण करते हैं।
- यह अनाधिकृत कॉल करके धोखाधड़ी या हैकिंग करते हैं।

Malicious Insider or Whistleblower

- यह हैकर किसी संगठन के व्यक्ति होते हैं, जो पैसा, व्यक्तिगत दुश्मनों के लिए संगठन की गोपनीय जानकारी दूसरे लोगों के साथ साझा करते हैं।

ब्लूबगिंग (हैकिंग)

- इसमें हैकर अनाधिकृत पहुंच के लिए ब्लूटूथ खामियों का फायदा उठाकर **सक्षम ब्लूटूथ डिवाइसों को लक्षित** करता है।
- इसमें हैकर उपयोगकर्ता की जानकारी के बिना उसके सिस्टम में कॉल, संदेश या डेटा तक पहुंचकर उसकी गतिविधियों पर नजर रखता है।

DoS (Denial of Service Attack)

- एक एसा हमला जो **Network/Internet** के माध्यम से **मशीनों को अथवा नेटवर्क को बंद करने के लिए** किया जाता है जिसके कारण नेटवर्क access होने में समर्थ नहीं (Inaccessible) होता है ऐसे हमले को **डिनायल ऑफ सर्विस अटैक** कहा जाता है।
- इसके कारण वेब उपयोगकर्ता को, खाताधारक को तथा कर्मचारियों को सेवाओं से वंचित रहना पड़ता है और उन्हें जानकारी प्राप्त नहीं हो पाती।
- इसमें कोई हैकर किसी अनाधिकृत उपयोगकर्ता को अवैध अनुरोधों के साथ किसी सेवा, उपकरण या किसी संसाधन तक पहुंचने से सीमित करता है।
- इस प्रकार के हमलों में **ज्यादातर बड़े संगठन** जैसे- **बैंक, मास मीडिया, सरकार, व्यापारिक संगठन** जो सर्वर (Server) के माध्यम से एक दूसरे से जुड़े होते हैं तथा इनका पूरा कामकाज ऑनलाइन ही इंटरनेट के माध्यम से चलता है, को **निशाना** बनाया जाता है।
- इस प्रकार के हमले में किसी प्रकार की संपत्ति की हानि नहीं होती, **केवल सूचनाओं (Information) की हानि** होती है।

.....सीधे परीक्षा से

प्र. जब कोई हैकर किसी अनाधिकृत उपयोगकर्ता को अवैध अनुरोधों के साथ किसी सेवा, उपकरण या किसी संस्थान तक पहुंचने से सीमित करता है, तो इस परिदृश्य को-----कहा जाता है।

(a) DoS (b) चोरी छुपे सुनना
(c) स्नूपिंग (d) फिशिंग

उत्तर- (a) **(MPPSC SM-2023)**

DoS अटैक के प्रकार

यह तीन प्रकार के होते हैं-

1. एप्लीकेशन लेयर फ्लड अटैक (Application Layer flood Attack)

- इस प्रकार के Dos हमले में **Hacker IP Address को Request** से इतना **भर देता** है कि वह क्रैश होकर **नेटवर्क** को इतना **Slow** कर देता है कि, सूचनाएँ (Information) उपयोगकर्ता तक नहीं पहुँच पाती हैं।

2. डिस्ट्रिब्यूटिड डिनायल ऑफ सर्विस अटैक (डी-डॉस) (Distributed Denial of Service Attack-DDoS)-

- यह हमला भी DoS Attack की तरह ही है लेकिन इसमें एक **Distributed नेटवर्क** होता है **जिसमें कई सारे Hacker** एक साथ हमला करके नेटवर्क में स्थित सभी मशीनों अथवा संगठनों को नियंत्रित कर लेते हैं जिससे Legal User अपना कार्य करने में सक्षम नहीं रहता।

- इसमें एक प्रकार के **आउटसोर्सिंग नेटवर्क (Outsourcing Newtork)** का उपयोग किया जाता है।

3. अनइंटेंडिड डिनायल ऑफ सर्विस अटैक्स (Unintended Denial of Service Attacks)

- यह एक प्रकार का **अनापेक्षित नेटवर्क** है तथा इस प्रकार के हमले **नेटवर्क को नुकसान नहीं** पहुंचाते हैं।
- यह कई सारे उपयोगकर्ताओं को अपने साथ जोड़ने का अवसर प्रदान करता है जिससे वेबसाइट पर उपयोगकर्ताओं का अत्यधिक **ट्रैफिक बढ़ जाने से सर्वर डाउन होकर बहुत ही Slow** काम करता है।

मालवेयर

- यह एक **द्वेषपूर्ण (Malicious) सॉफ्टवेयर (वायरस)** है जो कम्प्यूटर सिस्टम में घुसकर प्रोग्राम से छेड़छाड़ करता है। इसे **असुरक्षित प्लग इन** भी कहा जाता है। सभी **वायरस, वोर्म, ट्रोजन हॉर्स, स्पाइवेयर** आदि मालवेयर के उदाहरण हैं।
- हमलावर द्वारा संक्रमित विज्ञापनों को अपलोड कर हमला करने को **मालवेयर टाईजीन** कहा जाता है।

प्रमुख मालवेयर प्रोग्राम

- **वायरस**- यह **द्वेषपूर्ण या दुर्भावनापूर्ण (Malicious) सॉफ्टवेयर** है, जो कम्प्यूटर में डाटा को मिटाने, उसे खराब करने या उसमें परिवर्तन करने का कार्य कर सकता है। **उदाहरण**- क्रीपन, ब्रेन, जेरूसलम, कॉन्फिगर आदि।
- **वोर्म**- यह एक प्रकार का **द्वेषपूर्ण (Malicious) सॉफ्टवेयर (वायरस)** है, जो किसी **प्रोग्राम से जुड़े बिना नेटवर्क की सुरक्षा खामियों का उपयोग कर फैलता** है। यह डाटा या फाइल में किसी प्रकार का परिवर्तन नहीं करता। यह अपनी **कॉपी खुद बनाकर तेजी से फैलता** है जिससे कम्प्यूटर की मेमोरी भरती है और गति धीमी हो जाती है तथा मेमोरी क्रैश भी हो सकती है। उदाहरण- **ऑटोस्टार्ट 9805, DM सेटअप, IRC वार्म जेनेटिक, मोरिस, बेगल, आई लव आदि।**

✍ .....सीधे परीक्षा से

प्र. निम्न में से किसे दुर्भावनापूर्ण (मैलीशियस) सॉफ्टवेयर के रूप में जाना जाता है?
1. वर्म **2. वायरस**
उपरोक्त प्रश्न का सही उत्तर चुनिए-
(a) केवल 1 सत्य हैं। (b) केवल 2 सत्य है।
(c) दोनों असत्य है। (d) दोनों सत्य हैं।
उत्तर- (d) **(MPPSC SFS-2019)**

- **ट्रोजन हॉर्स**- यह एक प्रकार का वायरस है जो **इंटरनेट के माध्यम से कम्प्यूटर में प्रवेश** करता है तथा स्वयं को एक **उपयोगी सॉफ्टवेयर** जैसे-गेम **यूटीलिटी प्रोग्राम** आदि की तरह प्रस्तुत करके अटैच कर लेता है। ट्रोजन हॉर्स **अपनी कॉपी स्वयं नहीं बनाता। उदाहरण- बैंक ऑरीफाइस ट्रॉजन, नेटबस ट्रॉजन, नेटबस 160 डब्ल्यू.95 ट्राजन,** नेटबस 170 डब्ल्यू 95 ट्रॉजन, **डीप थ्रोट ट्रॉजन, Beast, Sub 7.Zeus, Zero Access Rootkit** आदि।
  - यह एक प्रकार का **नॉन-शेल्फ रेपलिकेटिंग मालवेयर** है, जिसे **Hide मालवेयर** भी कहा जाता है।
- **रूटकिट (RootKit)- यह एक प्रकार का मालवेयर** है, जो कम्प्यूटर सॉफ्टवेयरों का संग्रह है तथा आमतौर पर गलत उद्देश्यों को पूरा करने के लिए बनाया जाता है। तथा यह कम्प्यूटर सिस्टम में **एडमिनिस्ट्रेटिव स्तर पर नियंत्रण** करता है। इसे **जेलब्रेकिंग मालवेयर** भी कहते हैं।
  - यह साइबर अपराधियों के लक्षित डिवाइस तक पहुँच आर नियंत्रण हेतु डिजाइन किया गया है।
  - यह **सॉफ्टवेयर** व **ऑपरेटिंग सिस्टम** के साथ-साथ **हार्डवेयर और फर्मवेयर को भी संक्रमित** कर सकते हैं।

रूटकिट के प्रकार
1. हार्डवेयर या फर्मवेयर रूटकिट
2. बूटलोडर रूटकिट
3. एप्लीकेशन रूटकिट
4. कारनेल, मोड रूटकिट

- **स्पाइवेयर**-यह एक **द्वेषपूर्ण सॉफ्टवेयर (वायरस)** है। इसका **उद्देश्य कम्प्यूटर उपयोगकर्त्ता के विरूद्ध जासूसी करना** होता है। यह कम्प्यूटर की **पृष्ठभूमि में चलता** है और उपयोगकर्ता की **ब्राउजिंग जानकारी चुराता** है साथ ही यह कर्मचारियों की गतिविधियाँ जैसे- ई-मेल का पासवर्ड, सर्च की गई वेबसाइट का **डाटा इकट्ठा करता** है।
- **उदाहरण- की-लॉगर,** Cool Web Search, Zango, Zlob Trojan, **पेगासस** आदि।
- **क्राइम वेयर**- यह एक **दोषयुक्त सॉफ्टवेयर (वायरस)** है, जो इंटरनेट पर क्राइम करने के लिए तैयार किया गया है। तथा यह **आइडेन्टिटी थेप्ट** और **फ्रॉड** के लिए इस्तेमाल होते हैं।
- **स्केअर वेयर**- यह कम्प्यूटर **मालवेयर प्रोग्राम** है जो **अधिकृत सॉफ्टवेयर तथा फ्री एंटीवायरस की तरह** दिखता है जिसे डाइनलोड करते ही यह इंटरनेट से जुड़े कम्प्यूटर को प्रभावित करता है।
- **रेंसमवेयर**- यह कम्प्यूटर में घुसकर **एक तरह से ताला** है और उसे खोलने के बदले में **पैसे या फिरौती की मांग** की जाती है। पैसा मिलने पर यह ताला खोल दिया जाता
- उदाहरण- **क्रिप्टोलॉकर, वन्नाक्राई, पेट्या, इटर्नब्लू पद, रेवेटॉन, बैड रैबिट, लॉकी, गोल्डन आई** आदि।
- **पैगासस** - यह **इजरायली साइबर सुरक्षा कम्पनी** द्वारा विकसित किया गया है, जो उपयोगकर्त्ता के मोबाइल और कम्प्यूटर से गोपनीय एवं व्यक्तिगत जानकारियों को नुकसान पहुँचाता है। **इसमें लिंक या मिस्ड वीडियो कॉल से ही सॉफ्टवेयर,** मोबाइल या कम्प्यूटर में **इंस्टॉल** हो जाता है।

✍ .....सीधे परीक्षा से

प्र. पेगासस एक उदाहरण है-
(a) मोबाइल ऑपरेटिंग सिस्टम का
(b) ब्रूट फोर्स अटैक का
(c) स्पाईवेयर का
(d) डिनायल ऑफ सर्विस अटैक का
उत्तर- (c) **(A.D.P.O. – 2021)**

- **स्टक्सनेट**- यह एक **माइक्रोसॉफ्ट विण्डोज कम्प्यूटर वोर्म** है जिसकी **खोज 2010** में हुई। यह औद्योगिक सॉफ्टवेयर एवं संयंत्रों को प्रभावित करता है। इस वोर्म में **अति विशिष्ट मालवेयर (Malware) शामिल** होते हैं जो केवल **सीमेन्स सुपरवायजरी कण्ट्रोल एण्ड डाटा एक्वेजिशन (SCADA)** को प्रभावित करते हैं।
- **स्ट्रैंडहाग**- यह एक **एंड्रॉएड ऑपरेटिंग सिस्टम का मालवेयर** है, जिसके जरिये हैकर्स यूजर्स द्वारा इस्तेमाल किये जा रहे ऐप्स का पासवर्ड और दूसरी संवेदनशील जानकारी चुरा सकते हैं। इसके बारे में पता नार्वे की एक कंपनी ने लगाया।
- **लॉजिक बम (Logic Bomb)**-यह **मालवेयर में अन्तर्विष्ट कोड** है, जिसको किसी प्रोग्राम में जान-बूझकर डाला जाता है, जो किसी सिस्टम में पूर्व निर्धारित स्थिति होने पर सक्रिय हो जाता है।
- **Time Bomb**- ऐसे वायरस जो समय बीतने पर या किसी खास तारीख को चलते हैं **Time Bomb** कहलाते हैं।
- **एडवेयर (Adware)**- ऐसे सॉफ्टवेयर प्रोग्राम जो कम्प्यूटर सिस्टम में **अनचाहे विज्ञापन दिखात** हैं, **एडवेयर** कहलाते हैं। यह **ऑनलाइन होने पर पॉप-अप** के रूप में दिखाई देते हैं।
- **जोक प्रोग्राम्स (Joke Programms)**- यह अपेक्षाकृत **हानिरहित प्रोग्राम** होते हैं, जो **फाइलों को संक्रमित नहीं** करते। यह अक्सर उपयोगकर्ताओं को **परेशान करने या मजाक उड़ाने** के लिए डिजाइन किए जाते हैं। **उदाहरण के लिए** तेज आवाज में ऑडियो फाइल्स को चला देना या कोई वीडियो पॉपअप कर देना।

- **डायलर्स**- यह एक **दुर्भावनापूर्ण प्रोग्राम** होता है, जो कम्प्यूटर पर इंस्टॉल किया जाता है तथा यह **डायलिंग सुविधाओं** का उपयोग करके अन्य नंबरों पर कॉल करने की कोशिश करता है। यह **फोन बिल को बढ़ा सकता है** तथा **वैध फोन को डिस्कनेक्ट** कर सकता है।
- **की-लॉगर**- यह **सॉफ्टवेयर तथा हार्डवेयर का बना स्पाईवेयर का एक प्रकार** है, जो उपयोगकर्ता की सूचना के बिना कम्प्यूटर में चलाया जाता है। यह कम्प्यूटर में दबाए गए **बटनों (Keys) का रिकॉर्ड** रखता है या **लॉग बनाता है** तथा इस रिकॉर्ड का उपयोग बाद में किसी गुप्त सूचना कोड या पासवर्ड की अनाधिकृत जानकारी प्राप्त करने के लिए करता है।
- यह वचअल कीबोर्ड के माध्यम से दर्ज की गई जानकारी को रिकॉर्ड करने में सक्षम नहीं होते हैं।

.....सीधे परीक्षा से

प्र. कीलॉगर्स होते हैं-

(a) हार्डवेयर (b) सॉफ्टवेयर
(c) (a) तथा (b) दोनों (d) न तो (a) और नही (b)

उत्तर- (c) **(MPPSC GEO-2023)**

.....सीधे परीक्षा से

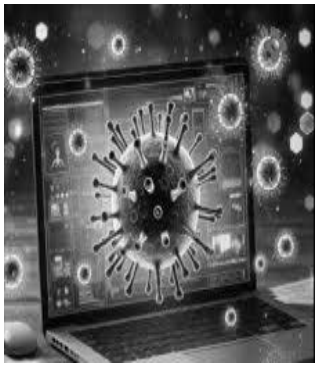
प्र. कीलॉगर----------।

(a) एक ऑन स्क्रीन कीबोर्ड है, जो निश्चित क्वेरी कुंजी लेआउट का उपयोग करता है।
(b) यादृच्छिक कुंजी लेआउट के साथ ऑनलाइन वर्चुअल कीबोर्ड है।
(c) दैनिक कीबोर्ड उपयोग का लॉग बनाता है।
(d) अवांछित ऑनलाइन विज्ञापन प्रदर्शित करता है।

उत्तर- (c) **(MPPSC SM-2023)**

- **पैकेट स्निफिंग (Packet sniffing)**- इंटरनेट पर डाटा को पैकेट में बांटकर भेजा जाता है। डाटा पैकट्स को अपने गंतव्य तक पहुंचने से पहले ही उसकी पहचानकर उसे रिकॉर्ड कर लेना **पैकेट स्निफिंग** कहलाता है।
- **बोटनेट्स**- यह इंटरनेट से जुड़े **कई डिवाइसों का एक नेटवर्क** होता है, **जो हैकस द्वारा कंट्रोल** किया जाता है। इसका उपयोग आईडी पासवर्ड चुराने, कम्प्यूटर को कंट्रोल करने तथा डिस्ट्रीब्यूटेड डेनियल सर्विस अटैक (DDoS) के लिए किया जाता है।
- **बेकडोर (Backdoor)**- यह एक **मालवेयर प्रोग्राम** है, जो कम्प्यूटर सिस्टम में अनाधिकृत कार्य करता है तथा इसका **उपयोग विभिन्न प्रकार के मालवेयर इंस्टॉल करने के लिए** किया जाता है।
- **फाइललैस मालवेयर**- यह **मालवेयर अटैक** चोरी छुपे होता है तथा इस अटैक के बारे में यूजर को कोई जानकारी नहीं होती है। इसे **एंटीवायरस के द्वारा नहीं पकड़ा जा सकता।**
- **इमोटेट (Emotet)**- यह **सबसे महंगे और विनाशकारी मालवेयर में से एक** है, जो मुख्य रूप से अन्य बैंकिंग ट्रोजन के डाउनलोडर या ड्रोपर के रूप में कार्य करता है। इसे **उन्नत, मॉड्यूलर बैंकिंग ट्रोजन (An Advanced, Moduler Banking Trojen)** कहा जाता है।
- **ग्रेवेयर**- यह **एक प्रोग्राम** है जो किसी प्रोग्राम अनुप्रयोगों को अवांछित एवं अनैच्छिक तरीकों से वर्गीकृत करता है। यह **मालवेयर की तुलना में कम हानिकारक** होता है। ग्रेवेयर के अंतर्गत निम्न शामिल हैं-
  - स्पाईवेयर (Spyware)
  - एडवेयर (Adware)
  - डायलर्स (Dialers)
  - जोक प्रोग्राम्स (Joke Programms)

कम्प्यूटर वायरस



- वायरस शब्द का सर्वप्रथम प्रयोग **फ्रेड कोहेन** ने किया था।
- पूर्ण नाम- **वाइटल इन्फॉर्मेशन रिसोसस अण्डर सीज (Vital Information Resources Under Siege- VIRUS)** है।
- यह **द्वेषपूर्ण या दुर्भावनापूर्ण (Malicious) सॉफ्टवेयर** है, जो कम्प्यूटर में डाटा को मिटाने, उसे खराब करने या उसमें परिवर्तन करने का कार्य कर सकता है। यह हार्ड डिस्क में प्रवेश कर डिस्क की क्षमता को कम कर सकत। है **कम्प्यूटर की गति को धीमा/रोक** सकता है।
- यह **मालवेयर का एक प्रकार** है अर्थात् सभी वायरस मालवेयर होते हैं, लेकिन सभी मालवेयर वायरस नहीं होते हैं।
- किसी प्रोग्राम से जुड़ा वायरस तब तक सक्रिय नहीं होता जब तक उस प्रोग्राम को चलाया न जाए।
- जब वायरस सक्रिय होता है तो वह **कम्प्यूटर मेमोरी में स्वयं को स्थापित** कर लेता है तथा मेमोरी के खाली स्थान में फैलने लगता है। कम्प्यूटर वायरस में स्वयं की पुनरावृत्ति के लिए **स्पॉन** का प्रयोग किया जाता है।
- कम्प्यूटर वायरस मुख्यत: **इंटरनेट** (ई-मेल, गेम या इंटरनेट फाइल) या **मेमोरी उपकरण** जैसे- फ्लॉपी डिस्क, सीडी, डीवीडी, पेन ड्राइव आदि के **सहारे कम्प्यूटर में प्रवेश** करता है।
- कम्प्यूटर वायरस **मानव निर्मित** होता है तथा यह कम्प्यूटर के **हार्डवेयर को प्रभावित नहीं** करता।
- कम्प्यूटर वायरस का वैध फेज- **डोर्मेंट, प्रोपेगेशन, ट्रिगरिंग, एक्सक्यूटिंग** है।
- प्रथम कम्प्यूटर वायरस **क्रीपर** (1971) था, जो नेटवर्क पर फैलने वाला प्रथम वायरस भी था।

.....सीधे परीक्षा से

प्र. इनमें से किसने शब्द 'कम्प्यूटर वाइरस' को गढ़ा था?

(a) फ्रेड कोहेन (b) डेविड ए.हफमैन
(c) जिम ग्रे (d) ब्रेनडन इच

उत्तर- (a) **(MPPSC SFS-2020)**

.....सीधे परीक्षा से

प्र. कम्प्यूटर वायरस है।

(a) प्राकृतिक रूप से उत्पन्न (b) मशीन द्वारा निर्मित
(c) मानव निर्मित (d) उपरोक्त सभी

उत्तर- (c) **(MPPSC GE-2023)**

वायरस का कम्प्यूटर पर प्रभाव

- कम्प्यूटर **स्वत: री-बूट** हो जाता है।
- वेब ब्राउसर असामान्य या **गलत होम पेज खोल** देता है।
- कम्प्यूटर की **गति को धीमा** कर देता है।
- कम्प्यूटर **बार-बार हैंग** हो जाता है।
- कम्प्यूटर **मेमोरी की सही स्थिति तथा साइज नहीं** बताता है।
- कुछ प्रोग्राम कम्प्यूटर पर चल नहीं पाते हैं।

कम्प्यूटर वायरस के प्रकार

- **डायरेक्ट एक्शन वायरस** - यह वायरस किसी **फाइल में होता** है और जब उस फाइल का उपयोग किया जाता है तब यह वायरस स्वयं को क्रियान्वित कर देता है। **उदाहरण**- Vienna Virus

- **ओवर राइट वायरस**- यह संक्रमित फाइलों में रखे हुए डेटा व सूचना को डिलीट कर देता है। **उदाहरण**- Way, Trivial, 88-D
- **बूट सेक्टर वायरस**- यह कम्प्यूटर के **बूट्स-अप होने पर फैलता है** क्योंकि यह वायरस **हार्डडिस्क या फ्लॉपी डिस्क के** मास्टर बूट रिकॉर्ड के **बूट सेक्टर** में होता है। सबसे पहला बूट सेक्टर पीसी वायरस **'ब्रेन' (1986)** था। **उदाहरण**- **Antiexe,** विन.सी.एच, माइकेल एंजिलो, स्टोन्ड एंजेलिना, स्टोन्ड नो INTA बेलकॉम्ब, डाईहार्ड 4000 ए आदि।
- **मैक्रो वायरस**- ये केवल उन्हीं एप्लीकेशनों तथा प्रोग्रामों को संक्रमित करता है जिनमें **.doc, .xls, .pps इत्यादि मैक्रोस** होते हैं। **उदाहरण**- Melissa.A आदि।
- **फाइल वायरस/पैरासिटिक वायरस**- वह वायरस जो **एक्जीक्यूटेबल (EXE.) फाइलों के साथ संलग्न होकर उसे संक्रमित या इन्फेक्टेड कर देता है** और इन्फेक्टेड EXE. फाइल अन्य EXE. फाइलों पर हमला कर उन्हें भी संक्रमित कर देते हैं।
- **पॉलीमॉर्फिक वायरस**- यह जब भी किसी सिस्टम को संक्रमित करता है तो अपने आप को **प्रत्येक बार एनकोड या एन्क्रिप्ट** करता है। इस प्रकार **वायरस की ज्यादा से ज्यादा कॉपी** तैयार हो जाती हैं। **उदाहरण**- Elkern, Tuareg, डेड-2039, पेरेटी बूट बी, डब्ल्यू एम/वाज्जू.ए.रिपर, ऑटोस्टार्ट 9805 आदि।
- **फाइल सिस्टम वायरस**- यह किसी भी फाइल के **डायरेक्टरी पथ को बदलकर मैमोरी प्रबंधन में गड़बड़** कर देता है। इसे **क्लस्टर वायरस या डायरेक्टरी वायरस** भी कहते हैं। उदाहरण- Dir-2 वायरस आदि।
- **फैट वायरस**- यह फाइलों की **लोकेशन** व **अप्रयोगित मैमोरी** स्थान के बारे में सभी प्रकार की जानकारियों को संग्रहित करने के लिए प्रयोग होता है। **उदाहरण**-लिंक वायरस आदि।
- **वेब स्क्रिप्टिंग वायरस**- कई वेबसाइटों में रोचक सूची को डालने के लिए **कठिन कोड का इस्तेमाल** होता है। यह वायरस इन्हीं कोड्स को **संक्रमित** करता है। **उदाहरण**- J.S. Fort night आदि।
- **रेजिडेंट वायरस**- यह अपने आप को **सिस्टम की मैमोरी में स्थिर** कर लेता है और खोले जाने वाली सभी फाइलों को प्रभावित करता है। **उदाहरण**- Randex, Meve आदि।
- **मल्टीपार्टाइट वायरस**- यह वायरस **कई तरीकों** से फैलता है। जैसे- ऑपरेटिंग सिस्टम इंस्टॉल करने पर। **उदाहरण**- फ्लिप, टेक्यूला, जन्की एम.पी. 1027 ए, एंटी ई एक्स.ई.ए., एम्पायर मंकी बी आदि।
- **नेटवर्क वायरस**- इस प्रकार का वायरस **लेन (LAN)** और **इंटरनेट** के माध्यम से फैलता है। उदाहरण- SQL Slammer, Nimda
- **ब्राउजर हाइजैकर वायरस**- यह वायरस **वेब ब्राउजर को संक्रमित** करता है, जिससे हम विभिन्न फर्जी वेबसाइटों पर पहुंचते हैं। **उदाहरण**- Sweet Page, Ask Tookbar
- **प्रोग्राम वायरस**- यह प्रोग्राम फाइल जैसे **.EXE , .BIN, .COM आदि एक्सटेंशन** के साथ एक्सीक्यूटेबल प्रोग्राम फाइल को संक्रमित करते हैं। यह वायरस **अपनी कॉपी बनाकर फाइलों को संक्रमित कर मेमोरी में एक्टिव** हो जाता है। **उदाहरण**- Sunday, Cascade आदि।
- **स्पेसकिलर वायरस**-यह एक **दुर्लभ प्रकार का वायरस** है, जो फाइलों के खाली स्थान को वायरस से भर देता है। इसे **कैविटी वायरस** के नाम से जाना जाता है।

प्रमुख वायरस

नाम	विशेष
क्रीपर (1971)	प्रथम कम्प्यूटर वायरस जो नेटवर्क पर फैलने वाला भी प्रथम वायरस था।
ब्रेन (1986)	**पहला बूटसेक्टर वायरस,** पाकिस्तान में निर्मित
Elk Cloner (1982)	पर्सनल कम्प्यूटर में फैलने वाला प्रथम वायरस
हैप्पी बर्थडे जोशी (1990)	**भारत** में फैलने वाला प्रथम कम्प्यूटर वायरस
आई लव यू (2000)	**सबसे बड़ा** कम्प्यूटर वायरस
माइकल एंजिलो (1991)	**अन्य नाम**- 6 मार्च वायरस
वंदे मातरम् (2021)	**भारत में निर्मित वायरस**
जेरूसलम (1987)	**केवल शुक्रवार को सक्रिय** वायरस था।
कोलम्बस (1989)	**अन्य नाम- डेटा क्राइम** तथा **13 अक्टूबर** तथा हार्डडिस्क को नुकसान पहुंचाता था।
विएना वायरस (1987)	पहली बार **IBM प्लैटफार्म पर प्रभावी**
लीप (Leap) (2006)	इसने एप्पल के **मैकबुक को प्रभावित** किया।
कॉन्फिकर वायरस (2008)	**सोशल नेटवर्किंग साइट से प्रसारित** वायरस
वनहॉफ	यह हार्डडिस्क को अपना शिकार बनाता है।
मंकी	मुख्य बूट रिकॉर्ड पर घात लगाने वाला **बेहद खतरनाक** एवं तजी से फैलने वाला वायरस था।
बोजा	**विंडोज 95** जैसे विश्व प्रसिद्ध सिस्टम के खिलाफ यह **पहला व एकमात्र वायरस** था जिसे ब्रिटिश अनुसंधानकर्त्ताओं द्वारा खोजा गया। यह वायरस **विंडोज 3.1 को प्रभावित करने में सक्षम था।**

- **अन्य कम्प्यूटर वायरस हं**-साइपर रॉयट, विनवर्ड न्यूक्लियर, माइकेलेंग्लो, **ब्रेन**, बैच फाइल वायरस, फिलीप, स्वदेश, चूंग-मूंग, देशी, ब्लडी, **जेरूसलम, जोशी,** हांगकांग, **कोडरेड,** सैसर, **कॉन्फिकर** आदि।
- **प्रमुख फाइल वायरस**-हंड्रेड ईयर्स, डब्ल्यू 97 एम.क्लास.एस., **फ्राइडे थर्टीन्थ**, डब्ल्यू 95 मराबर्ग बी।

एंटीवायरस (Antivirus)

- ऐसे **सॉफ्टवेयर** जिनका प्रयोग कम्प्यूटर को **वायरस, स्पाइवेयर, वॉर्म्स, ट्रॉजन से बचाने के लिए** होता है।
- इसमें वे प्रोग्राम भी सम्मिलित होते हैं जिनका कार्य वायरस या अन्य मालवेयर को ढूँढकर खत्म करना होता है।
- यह एक प्रकार का **यूटिलिटी सॉफ्टवेयर** होता है।
- यह इस्तेमाल से पूर्व किसी सॉफ्टवेयर, ई-मेल या इंटरनेट फाइल की जांच करता है तथा **वायरस पाये जाने पर उन्हें नष्ट** करता है।
- एंटी वायरस को **समय-समय पर अपडेट** करते रहना चाहिए। एंटी वायरस सॉफ्टवेयर किसी भी प्रोग्राम या फाइल को चालू किए जाने से पहले उसकी जांच करता है, अत: वह **कंप्यूटर की गति को कम भी करता है।**
- **विश्व का पहला एंटीवायरस 'रोपर' था, जो 1970 के दशक में अमेरिका द्वारा बनाया तथा लॉन्च किया गया था।**
- **ग्रेगरी बेनफोर्ड** ने सर्वप्रथम अपनी पुस्तक **द स्केरेड मैन** में वायरस शब्द को लिखा।
- **कुछ प्रचलित एंटीवायरस**- Symantec, **Norton, McAFee, Avira,** Lavasoft **Ad-Aware**, Net Protector, eScan, Malwarebytes, **BitDefender, PANDA, Quick** heal, **Kaspersky**, **AVG, AVAST,** K-7, G Data, **Bullguard,** F Secure, Trend Micro आदि।

.....सीधे परीक्षा से

प्र. सॉफ्टवेयर जो कंप्यूटर की वायरस से सुरक्षा के लिये कम्प्यूटर पर स्थापित किए जाते हैं।
(a) बैकअप (b) कीलॉगर
(c) एंटीवायरस (d) कंपाइलर
उत्तर- (c) **(MPPSC SFS-2019)**

.....सीधे परीक्षा से

प्र. निम्न में से कौन-सा एंटी-वायरस सॉफ्टवेयर है?
(a) मंकी (b) नार्टन
(c) एडवेयर (d) ट्रोजन हॉर्स
उत्तर- (b) **(MPPSC D.S.E– 2021)**

- **स्मार्टडॉग**-यह एक प्रकार का **सॉफ्टवेयर** है, जिसका **उपयोग कम्प्यूटर वायरस को समाप्त करने के लिए** किया जाता है।
- **पलाडियम**- वह प्रणाली जिसे **माइक्रोसॉफ्ट कंपनी** ने **कम्प्यूटर सुरक्षा** को चुस्त-दुरुस्त करने के लिए **विकसित** किया है, जिससे आँकड़ों की सुरक्षा और बौद्धिक संपदा चिंताओं को दूर किया जा सकेगा।

साइबर सुरक्षा

विभिन्न प्रकार के साइबर हमलों से बचाव एवं सुरक्षा हेतु किये गये प्रयासों को साइबर सुरक्षा के अंतर्गत रखा जाता है। सुरक्षा हेतु निम्नलिखित चार तरीके इस्तेमाल किए जाते हैं-

- **सिस्टम एक्सेस कण्ट्रोल**- यह एक ऐसी प्रणाली है जो **किसी कम्प्यूटर में डेटा का उपयोग या उसमें कुछ परिवर्तन करने को अनुमति प्रदान करती है।** आमतौर पर एक उपयोगकर्ता किसी कम्प्यूटर में लॉग इन (log-in) करता है, जिसके पश्चात् एक्सेस कण्ट्रोल तय करता है कि उस उपयोगकर्ता के लिए (उपयोगकर्ता आई डी के आधार पर) कौन-सा डेटा पहुँच में होना चाहिए और कौन-सा नहीं।
- **डेटा एक्सेस कण्ट्रोल- कौन-सा डेटा, कौन नियन्त्रित कर सकता** है? इस बात की निगरानी इस कण्ट्रोल के तहत की जाती है। सिस्टम किसी भी व्यक्ति विशेष, फाइलों तथा अन्य किसी भी ऑब्जेक्ट्स की सुरक्षा के स्तरों पर आधारित होकर ही एक्सेस नियमों को बनाता है।

- **सिस्टम तथा सिक्योरिटी प्रशासन**- इसके अन्तर्गत **ऑफलाइन प्रक्रिया का निष्पादन** होता है। जिससे कोई भी सिस्टम या तो सुरक्षित बनाया जाता है या फिर उसकी सुरक्षा को तोड़ा जाता है।
- **सिस्टम डिजाइन**- यह कम्प्यूटर के **हार्डवेयर तथा सॉफ्टवेयर की बुनियादी सुरक्षा की विशेषताओ से लाभ** लेती हैं।

साइबर सुरक्षा की विशेषताएँ तथा दायरा

- **आंतरिक खतरों से प्रतिरक्षा**- सुरक्षा अलर्ट का वास्तविक समय विश्लेषण प्रदान करता है।
- **घुसपैठ का पता लगाने वाली प्रणाली**- दुर्भावनापूर्ण गतिविधियों की पहचान करने के लिए नेटवर्क ट्रेफिक पर नजर रखता है।
- **अनुपालन**- पहचान सत्यापित करने के लिए पासवर्ड बायोमैट्रिक डेटा और उपयोगकर्ता पहचान के अन्य रूपों का उपयोग करता है।
- **डेटा हानि रोकथाम**- संवेदनशील डेटा को सुरक्षित नेटवर्क छोड़ने से रोकता है। जिससे डाटा हानि नहीं होती है।
- **घटना प्रतिक्रिया (Accident Response)**- सुरक्षा भंग या हमले की प्रतिक्रिया की योजना और प्रबंधन करता है। जिससे नुकसान तथा रिकवरी का समय कम होगा।
- **कूटलेखन**- अनाधिकृत एक्सेस को रोकने के लिए संवेदनशील डेटा को कोडित भाषा में परिवर्तित करता है।
- **भेद्यता की कमी (Vulnarability Reduction)**- इसे दूर करने के लिए सिस्टम अपडेट, पैच प्रबंधन आदि किया जा सकता है।
- **नेटवर्क सेगमेंटेशन**- हमले की सतहों को सीमित करने और प्रदर्शन में सुधार करने के लिए नेटवर्क को अलग-अलग हिस्सों में विभाजित करता है।
- **डाटा की पुनर्प्राप्ति (Recovery of Data)**- साइबर हमले से बचाव के लिए डाटा का बैकअप रखना तथा अनाधिकृत पहुंच से उसे दूर रखना चाहिए, ताकि हमला होने पर भी डाटा की पुनर्प्राप्ति हो सके।
- **खतरे की रोकथाम**- इसमें डाटा को एन्क्रिप्ट करके, एंटीवायरस का प्रयोग करके तथा सॉफ्टवेयर तथा ऑपरेटिंग सिस्टम को अपडेट आदि उपाय अपनाकर सुरक्षा की जा सकती है।

.....सीधे परीक्षा से

प्र. सायबर सिक्यूरिटी का दायरा है।
(a) वनरेबिलिटी रिडक्शन (b) इन्सीडेंट रिस्पांस
(c) रिकवरी पॉलिसी (d) उपरोक्त सभी
उत्तर- (d) **(MPPSC AE-2020)**

.....सीधे परीक्षा से

प्र. साइबर सुरक्षा की विशेषता/विशेषताएँ है/हैं:
(a) अनुपालन
(b) आन्तरिक खतरों से प्रतिरक्षा
(c) खतरे की रोकथाम
(d) उपर्युक्त सभी
उत्तर- (d) **(MPPSC Pre-2022)**

साइबर सिक्योरिटी के घटक

- **गोपनीयता (Confidentiality)-** किसी भी जानकारी/डेटा के अन्य **अवैध व्यक्ति द्वारा एक्सेस न होने की घटना** को सुनिश्चित करना, इसके अंतर्गत आता है।
- **नॉन-रेपुडिएशन (Non-Repudiation)-** मैसेज को भेजने वाला ऑरिजिनल व्यक्ति कहीं अपने मैसेज को स्वयं का होने से न इन्कार कर दे। इस प्रकार की सुनिश्चितता को **गैर-प्रत्याख्यान (नॉन-रेपुडिएशन)** कहते हैं। इससे धोखाधड़ी से बचाव तथा साइबर सुरक्षा सुनिश्चित होती है।
- **प्रमाणीकरण (Authentication)-** यह कम्प्यूटर सिस्टम को इस्तेमाल करने वाले **व्यक्ति के वैध अथवा अवैध होने को सुनिश्चित** करता है।

ऑथेंटिकेशन प्रोटोकॉल (Authentication Protocol)

- यह एक प्रकार का **कम्प्यूटर संचार प्रोटोकॉल या क्रिप्टोग्राफिक प्रोटोकॉल** है जिसे विशेष रूप से दो संस्थाओं के बीच प्रमाणिक डेटा के हस्तांतरण के लिए डिजाइन किया गया है।
- यह कम्प्यूटर नेटवर्क के भीतर **सुरक्षित संचार के लिए** आवश्यक एवं महत्वपूर्ण परत है।
- **प्रकार**-
  1. **PPP**-Point to Point Protocol
  2. **PAP**-Password Authentication Protocol
  3. **CHAP**-Challenge Handshake Authentication Protocol
  4. **EAP** – Extensible Authentication Protocol
  5. **RADIUS**-Remote Authentication Dial- in use service
  6. **DIAMETER**-RADIUS प्रोटोकॉल का उन्नत वर्जन।
- **वायरलेस सुरक्षा प्रोटोकॉल**-
  1. **WEP (Wired Equivalent Privacy)**
  2. **WPA (Wife Protected Access)**
  3. **WPA 2**
  4. **WPA 3**
- **WPA 3-सबसे उच्च कोटि का Wifi सुरक्षा प्रोटोकॉल** है, जो वर्तमान में उपस्थित लगभग सभी प्रकार के Wifi सिक्योरिटी थ्रेट से बचाता है।

- **प्राधिकरण (Authorization)-** यह किसी **उपयोगकर्ता** को किसी डिजिटल या भौतिक संसाधन जैसे कि वेबसाइट एप्लीकेशन डेटाबेस या दस्तावेज तक पहुँचने की **अनुमति देने की प्रक्रिया** है।
- **एक्सेस कंट्रोल (Access Control)-** जिस उपयोगकर्ता को जिन संसाधनों का प्रयोग करने की अनुमति प्राप्त हो वह केवल उन्हीं संसाधनों को इस्तेमाल करे। इस बात की सुनिश्चितता को **एक्सेस कंट्रोल** कहा जाता है।
- **उपलब्धता (Availability)-** सभी सिस्टमों के कार्य करने की प्रणाली का सही होना व किसी भी वैध उपयोगकर्ता को सेवाएँ देने से मना नहीं करना को, **उपलब्धता** के नाम से जाना जाता है।
- **यूजर आइडेंटीफिकेशन (User Identification)-** कम्प्यूर तथा नेटवर्क पर **अधिकृत उपयोगकर्ता की पहचान करना यूजर आइडेंटीफिकेशन** कहलाता है। जबकि इस पहचान को सत्यापित करने की प्रक्रिया **ऑथेंटिकेशन (Authentication)** कहलाती है। उपयोगकर्ता की पहचान स्थापित करने तथा उसे सत्यापित करने की सर्वाधिक प्रचलित विधि **यूजर नेम** तथा **पासवर्ड** है।

.....सीधे परीक्षा से

प्र. सायबर सिक्यूरिटी मेंटेन करने हेतु---इन्फार्मेशन ऐस्योरेन्स फन्डामेंटल टूल्स का उपयोग किया जाता है।

(a) ऑथेन्टीकेशन (b) ऑथराइजेशन
(c) नान-रेप्यूडेशन (d) उपर्युक्त सभी

उत्तर- (d) **(MPPSC SFS-2022)**

साइबर अपराध से बचने के तकनीकी उपाय या कम्प्यूटर सुरक्षा के उपाय

प्रॉक्सी सर्वर (Proxy Server)

- यह स्थानीय नेटवर्क से जुड़ा हुआ एक ऐसा सर्वर होता है, जो मुख्य सर्वर तथा उपयोगकर्त्ता के बीच **फिल्टर का काय** करता है तथा अनाधिकृत उपयोगकर्त्ताओं से नेटवर्क को सुरक्षा प्रदान करता है। इसे **एप्लिकेशन-लेवल-गेटवे** भी कहा जाता है। प्रॉक्सी सर्वर का प्रयोग निम्न उद्देश्यों से किया जाता है-
  - अवांछित वेब पेज या वेब साइट को प्रतिबंधित करना।
  - मालवेयर तथा वायरस पर नियंत्रण रखना।
  - मुख्य सर्वर की गोपनीयता बनाए रखना।
  - डाटा ट्रांसफर की गति को बढ़ाना।
  - वर्गीकृत डाटा को सुरक्षित रखना, आदि।
- यह यूजर तथा इंटरनेट के बीच **मध्यस्थ का काम** करता है।
- यह **सॉफ्टवेयर या हार्डवेयर या दोनों हो** सकता है।

एप्लीकेशन गेटवे (Application Gateway)

- यह कुछ विशिष्ट एप्लीकेशनों पर सुरक्षा कार्यविधि को लागू करता है। इन विशिष्ट एप्लीकेशनों में **फाइल ट्रांसफर प्रोटोकॉल** तथा **टेलनेट सेवाएँ** इत्यादि सम्मिलित हैं।

कूटलेखन (Cryptography)

- सूचना या डाटा को इंटरनेट पर भेजने से पहले उसे गुप्त कोड में परिवर्तित करना तथा प्राप्तकर्ता द्वारा उसे प्रयोग से पहले पुनः सामान्य सूचना में परिवर्तित करना **क्रिप्टोग्राफी** कहलाता है।
- क्रिप्टोग्राफी से डाटा स्थानांतरण के दौरान **डाटा चोरी होने या लीक होने की संभावना नहीं** रहती।

एन्क्रिप्शन (Encryption)

- एन्क्रिप्शन एक ऐसी प्रक्रिया है जिसके द्वारा **Plain Text संदेश को कोडेड संदेश (साइफर टैक्स्ट) में परिवर्तित** किया जाता है। जिससे डाटा या सूचना की सुरक्षा सुनिश्चित होती है। **उदाहरण के लिए-** जब हैलो जैसे सामान्य शब्द को कोड/एन्क्रिप्ट कर दिया जाता है तो वह "43+64 = BM" जैसे कूट शब्द में परिवर्तित हो जाता है।
- एन्क्रिप्शन, डेटा को **मैन-इन-द-मिडिल हमलों (Man-in-the-Middle Attacks)** जैसी दुर्भावनापूर्ण गतिविधियों से **बचाने** में भी मदद करता है।

एन्क्रिप्शन के प्रकार

- एन्क्रिप्शन को **तीन प्रकारों** में विभाजित किया जाता है।

सिमेट्रिक (सममित) एन्क्रिप्शन

- यह **क्रिप्टोग्राफी में निर्देशों का एक सेट** है। जो डेटा को एन्क्रिप्ट और डिक्रिप्ट करने के लिए **एक कुंजी का उपयोग** करता है। इसे **निजी कुंजी क्रिप्टोग्राफी** या **गुप्त कुंजी एल्गोरिद्म** भी कहा जाता है। **उदाहरण**- ब्लोफिश, टूफिश
  - **ब्लोफिश (Blowfish)**- यह **सार्वजनिक डोमेन** है जिसका उपयोग ई-कॉमर्स प्लेटफॉर्म, सुरक्षित भुगतान और पासवर्ड प्रबंधन में किया जाता है। यह सममित उपकरण संदेशों को **64 बिट ब्लॉक** में बांट कर उन्हें व्यक्तिगत रूप से एन्क्रिप्ट करता है।
  - **टूफिश (Twofish)**- यह **लाइसेंस फ्री सममित एन्क्रिप्शन** है, जो ब्लो फिश की कमी को पूरा करता है। यह **128 बिट डेटा ब्लॉक** को डिस्क्रिप्ट करता है और प्रत्येक डेटा को 16 राउंड में एन्क्रिप्ट करता है

असममित एन्क्रिप्शन

- इसे **सार्वजनिक कुंजी क्रिप्टोग्राफी** भी कहा जाता है। इस पद्धति के अंतर्गत एन्क्रिप्शन हेतु दो कुंजियों (सार्वजनिक, निजी) का प्रयोग किया जाता है।

हैशिंग एन्क्रिप्शन/हैश फंक्शंस

- यह एक प्रकार का **एक तरफा एन्क्रिप्शन एल्गोरिद्म** है, जो डेटा को एक निश्चित लंबाई वाले कोड में बदल देता है। इसका उपयोग केवल **डाटा को सत्यापित** करने के लिए किया जाता है।

कुछ विशेष एन्क्रिप्शन एल्गोरिथम

1. **AES (Advanced Encryption Standard)**- यह एक आधुनिक एल्गोरिथम है। जिसका प्रयोग राज्य सरकार तथा अन्य बड़े संगठनों द्वारा किया जाता है। इस एल्गोद्रिम में 128, 192 तथा 256 बिट तक की कुंजियों का उपयोग किया जाता है।
2. **Triple DES (Data Encryption Standard)** यह मूल डेटा एन्क्रिप्शन DES का आधुनिक स्वरूप है जो जो हैकर्स के हमलों को रोकने हेतु बनाया गया था। यह एक सममित एन्क्रिप्शन है। मुख्यतः यूनिक पासवर्ड तथा एटीएम पिन को एन्क्रिप्ट करने के लिए इनका उपयोग किया जाता है।
3. **RSA (Rivest Shamir Adleman)**- यह एक सार्वजनिक कुंजी एन्क्रिप्शन है इसका प्रयोग ज्यादातर Sensitive डेटा को सुरक्षित नेटवर्क (जैसे- Internet) में सुरक्षित Transmission करने के लिए किया जाता है। यह एक असममित एन्क्रिप्शन का प्रकार है।
4. **डाटा एन्क्रिप्शन**- यह एन्क्रिप्शन की वह प्रक्रिया है जिसमें किसी डाटा या जानकारी को एन्क्रिप्शन प्रक्रिया द्वारा कूट शब्द में परिवर्तित करके सुरक्षित किया जाता है ताकि कोई भी **अनाधिकृत व्यक्ति उस डाटा को एक्सेस न कर सके।**
5. **एण्ड-टू-एण्ड एन्क्रिप्शन**- यह एक ऐसी प्रक्रिया है जिसमें डाटा को एन्क्रिप्ट करके (कूट शब्द में परिवर्तित करके) भेजने वाले द्वारा प्राप्तकर्त्ता को भेजा जाता है। जिससे उस डाटा **को सिर्फ भेजने वाला और प्राप्त करने वाला ही देख और पढ़ पाता है।**

एन्क्रिप्शन के अनुप्रयोग

- वायरलेस नेटवर्क सुरक्षा में WEP तथा WPA एन्क्रिप्शन का उपयोग किया जाता है।
- एन्क्रिप्शन तकनीक का प्रयोग Adobe Acrobat और Intuit Turbo Tax जैसे सामान्य प्रोग्रामों में भी किया जाता है।
- कई वेबसाइट और अन्य ऑनलाइन सर्विसेज SSL उपयोग करके डेटा ट्रांसमिशन को एन्क्रिप्ट करती है जैसे- कोई भी वेबसाइट HTTP प्रोटोकॉल के बिना चालू नहीं को जा सकती।

.....सीधे परीक्षा से

प्र. डेटा/सूचना की सुरक्षा सुनिश्चित करने के लिए हमें डेटा को क्या करने की आवश्यकता होती है?

(a) एन्क्रिप्ट **(b) डिलिट**
(c) एक्सटेंड **(d) अपडेट**

उत्तर- (a) **(MPPSC GE-2023)**

डिक्रिप्शन (Decryption)

- यह **इन्क्रिप्शन प्रक्रिया का रिवर्स** होता है अर्थात् इसमें साइफर टैक्स्ट (कोडेड संदेश), को प्लेन टैक्स्ट में परिवर्तित किया जाता है।

एण्टीवायरस सॉफ्टवेयर (Antivirus Software)

- ये उस प्रकार के **सॉफ्टवेयर** होते हैं, जिनका प्रयोग कम्प्यूटर को वायरस स्पाईवेयर, वॉर्म्स, ट्रोजन इत्यादि से बचाना होता है। **उदाहरण**- Avast, Avg, Norton, McAFee आदि।

डिजिटल सिग्नेचर (Digital Signature)

- डिजिटल हस्ताक्षर एक **इलेक्ट्रॉनिक हस्ताक्षर** है, जिनका उपयोग कर किसी डिजिटल संदेश/दस्तावेज को भेजने वाले की पहचान की जाती है और यह सुनिश्चित किया जाता है कि संदेश अथवा दस्तावेज में **किसी प्रकार की छेड़छाड़ या जालसाजी नहीं** की गई है।
- **सूचना प्रौद्योगिकी अधिनियम-2000** की **धारा 2(1) (p)** में **डिजिटल हस्ताक्षर को परिभाषित** किया गया है। अधिनियम की **धारा-3** में डिजिटल हस्ताक्षर के निर्माण एवं सत्यापन संबंधी सम्पूर्ण प्रक्रिया वर्णित की गई है।
- भारत में **सूचना प्रौद्योगिकी अधिनियम-2000** एवं **संशोधित, 2008** के तहत डिजिटल हस्ताक्षर को **वैधानिक मान्यता** प्रदान की गई है।
- डिजिटल हस्ताक्षर के मुख्यतः **चार प्रकार** हैं, जिनकी **वैधता अवधि एक या दो वर्ष** होती है। ये प्रकार Class '0' (Zero) Certificate, Class '1' (One) Certificate, Class '2' (Two) Certificate, Class '3' (Three) Certificate।
- आई.टी. अधिनियम, 2000 की **धारा-24** के तहत् **प्रमाणकर्ता प्राधिकारी (CA)** को डिजिटल हस्ताक्षर प्रमाण-पत्र जारी करने का लाइसेंस दिया गया है।
- डिजिटल हस्ताक्षर हेतु अधिकृत अथॉरिटीज **Safescrypt, NIC, IDRBT, TCS, MtnlTrustline , GNFC** आदि हैं।

.....सीधे परीक्षा से

प्र. आई.टी. अधिनियम, 2000 की किस धारा के तहत प्रमाणकर्ता प्राधिकारी (CA) को डिजिटल हस्ताक्षर प्रमाण-पत्र जारी करने का लाइसेंस दिया गया है?

(a) धारा-65 (b) धारा-24
(c) धारा-43 (d) धारा-42

उत्तर- (b) **(MPPSC A.V.S.E. – 2021)**

.....सीधे परीक्षा से

प्र. डिजिटल हस्ताक्षर को वैधानिक स्वीकृति किस एक्ट के द्वारा दी गई है?

(a) इण्डियन एविडेंस एक्ट
(b) इन्फॉर्मेशन टेक्नोलॉजी एक्ट
(c) रिजर्व बैंक ऑफ इण्डिया एक्ट
(d) बैंकर्स बुक्स एविडेंस एक्ट

उत्तर- (b) **(A.D.P.O. – 2021)**

फायरवाल (Firewall)

- यह एक डिवाइस है जिसमें **हार्डवेयर एवं सॉफ्टवेयर** दोनों होते हैं। यह किसी कम्प्यूटर, डाटा या स्थानीय नेटवर्क को अनाधिकृत उपयोगकर्ता से सुरक्षा प्रदान करता है। सामान्य शब्दों में 'यह एक ऐसा सॉफ्टवेयर प्रोग्राम है जो कि **इंटरनेट से आने वाले डाटा को फिल्टर** करता है।
- इसे **निजी नेटवर्क** में या निजी नेटवर्क से अनाधिकृत अधिगम को रोकने के लिए डिजाइन किया गया है।
- यह कम्प्यूटर को नेटवर्क के खतरों जैसे-**वायरस, वोर्म, हैकर आदि से सुरक्षा** प्रदान करता है।
- फायरवाल, इनकमिंग डाटा की **जांच यूजरनेट तथा पासवर्ड के जरिए** करता है, अधिकृत उपयोगकर्त्ता को ही नेटवर्क का प्रयोग करने देता है तथा इंटरनेट पर लेन (LAN) की गोपनीयता बनाए रखता है। इसे **कम्प्यूटर** का **सेफ्टी वाल्व** भी कहते हैं।

.....सीधे परीक्षा से

प्र. ------एक ऐसा साफ्टवेयर प्रोग्राम है जो कि इन्टरनेट से आने वाले डाटा को फिल्टर करता है।

(a) एंटीवायरस (b) कूकीज
(c) मालवेयर (d) फायरवाल

उत्तर- (d) **(MPPSC AE-2020)**

.....सीधे परीक्षा से

प्र. साइबर सुरक्षा में एक फायरवॉल का क्या उद्देश्य है?

(a) एक नेटवर्क को अबाधित पहुँच की अनुमति देना।
(b) एक नेटवर्क की अनाधिकृत पहुँच को अवरुद्ध करना।
(c) एक नेटवर्क के डाटा का बैकअप तैयार करना।
(d) उपर्युक्त में से कोई नहीं

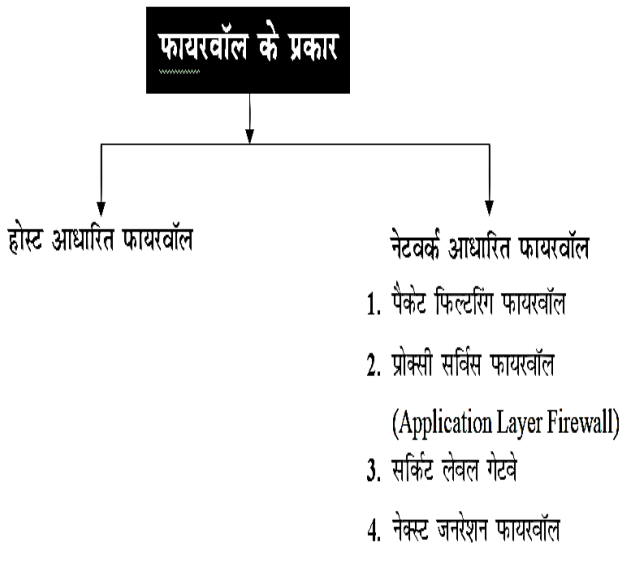
उत्तर- (b) **(MPPSC Pre-2023)**

फायरवॉल के प्राथमिक अवयव

प्रमुख रूप से 4 होते हैं-

1. **नेटवर्क पॉलिसी**- दो प्रकार की होती है-
   (i) सर्विस एक्सेस पॉलिसी
   (ii) फायरवॉल डिजाइन पॉलिसी
2. एडवांस ऑथेंटिकेशन (Advance Authentication)
3. पैकेट फिल्टरिंग (Packet Filtering)
4. एप्लीकेशन गेटवे (Application Gateway)

फायरवॉल के प्रकार



1. **पैकेट फिल्टरिंग फायरवॉल (Packet Filtering Firewall)**-यह आने जाने वाले डाटा के प्रवाह को नियंत्रित करता है तथा डाटा पैकेट के सोर्स के आधार पर डाटा को रोकने एवं अनुमति देने का कार्य करता है।
2. **प्रोक्सी सर्विस फायरवॉल (Proxy Service Firewall)**-यह पैकेट **फायरवॉल एवं सर्किट लेवल गेटवे से मिलकर बना** होता है।
3. **सर्किट लेवल गेटवे (Circuit Level Gateway)**- यह TCP हेडसेक तथा अन्य नेटवर्क प्रोटोकॉल द्वारा आरम्भ किये जाने वाले संदेशों को जो नेटवर्क में प्रवाहित होते हैं, की देखरेख करता है।
4. **नेक्स्ट जनरेशन फायरवॉल (Next Generation Firewall)**-यह सुरक्षा की उत्तम तकनीक जैसे- **Sandbox तकनीकी, Threat रोकथाम तकनीक** का उपयोग करती है।

पासवर्ड (Password)

- किसी कम्प्यूटर तथा नेटवर्क को सुरक्षा प्रदान करने के लिए पासवर्ड का प्रयोग किया जाता है। यह एक प्रकार के **गोपनीय शब्द या कैरेक्टर्स की एक स्ट्रिंग** है जिसे **उपयोगकर्ता को प्रमाणित** करने के लिए प्रयोग किया जाता है। यह सामान्यतः 2 प्रकार के होते हैं-
  1. **कमजोर पासवर्ड (Weak password)**- इन्हें **आसानी से याद** किया जा सकता है, जैसे- नाम, जन्म दिवस, फोन नम्बर आदि।
  2. **मजबूत पासवर्ड (Strong Passoword)**- ये **एल्फाबेट्स तथा संकेतों का कॉम्बीनेशन** है जिसे तोड़ पाना बेहद मुश्किल होता है। जैसे- 23@Deep#$

बायोमैट्रिक (Biometric)

- किसी **व्यक्ति की पहचान सुनिश्चित** करने के लिए **बायोलॉजिकल डाटा** जैसे- फिंगरप्रिंट, रेटिना, चेहरे की आकृति आदि का उपयोग करके पहचान स्थापित करने की तकनीक **बायोमैट्रिक** कहलाती है।

डिजिटल सर्टिफिकेट (Digital Certificate)

- यह सिक्योरिटी उद्देश्यों के लिए **इलेक्ट्रॉनिक संदेशों में प्रयुक्त होने वाली कॉपी** है। डिजिटल सर्टिफिकेट, किसे प्रेषित किया गया था व इसे किसने प्रेषित किया था इत्यादि जानकारी इसमें सम्मिलित होती हैं।

SSL (Secure Sockets Layer) Certificate

संवेदनशील जानकारियों (जैसे क्रेडिट कार्ड नम्बर, उपयोगकर्ता के नाम, पासवर्ड और ईमेल आदि) को हैकर्स और Online चोरी या छेड़छाड किए जाने की जोखिम को कम करने के लिए लाखों लोगों द्वारा इसका उपयोग किया जाता है। अर्थात् **SSL Certificate दो इच्छित पक्षों के बीच एक निजी और सुरक्षित ऑनलाइन वार्तालाप / सूचना के आदान प्रदान की अनुमति** देता है।

इंटरनेट पर **सभी वेबसाइटों को HTTPS में कन्वर्ट करने के लिए SSL Certificate की आवश्यकता** होती है। खास तौर पर, सभी ऐसी वेबसाइटों के लिए यह बेहद ही आवश्यक होता है, जो कि उपयोगकर्ताओं की जानकारी को एकत्रित करते हैं, जैसे लॉगिन का विवरण, भुगतान की जानकारी, क्रेडिट कार्ड की गुप्त जानकारी आदि।

प्रकार

इसके मुख्यतः छः प्रकार हैं-

1. Single Domain SSl Certificates
2. Multi-Domain SSL Certificates (MDC)
3. Wildcard SSL Certificates
4. Domain Validation SSL Certificates
5. Organization Validation SSL Certificates
6. Extended Validation SSL Certificates.

.....सीधे परीक्षा से

प्र. इंटरनेट पर डेटा के आदान-प्रदान को सुरक्षित रखने के लिए प्रयुक्त तकनीक एस.एस.एल. का पूरा नाम है-

(a) सेफ सॉकेट लेयर (b) सॉकेट सिक्युरिटी लेयर
(c) सिक्योर सॉकेट्स लेयर
(d) सिक्योर सेफ लेयर

उत्तर- (c) **(A.D.P.O. – 2021)**

.....सीधे परीक्षा से

प्र. HTTPS आधारित वेबसाइटों में आवश्यकता होती है-

(a) कोड साइनिंग सर्टिफिकेट
(b) क्लाइंट सर्टिफिकेट
(c) एस.एस.एल. डिजिटल सर्टिफिकेट
(d) मालवेयर

उत्तर- (c) **(A.D.P.O. – 2021)**

TLS (Transport Layer Security)

यह एक **डेटा एन्क्रिप्शन प्रोटोकॉल** होता है, जो **इंटरनेट पर होने वाले संचार को सुरक्षा प्रदान करने के लिए डिजाइन** किया गया है। TLS इंटरनेट पर अनुप्रयोगों और उनके उपयोगकर्ता के बीच होने वाले संचारों की गोपनीयता और डेटा Integrity को सुनिश्चित करता है। Transport Layer Security (TLS), **SSL का ही अपग्रेड वर्जन** है।

कैप्चा (CAPTCHA)

- इसका **उपयोग वेबसाइट को स्पैमर से बचाने के लिए** किया जाता है। कैप्चा कम्प्यूटर तथा मानव को अलग बताने के लिए पूरी तरह से स्वचालित प्रोग्राम है।
- इसका पूरा नाम **Completely Automated Public Turing Test to Tell Computers and Humans Apart** होता है।

पैचस (Patches)

- यह सॉफ्टवेयर का एक ऐसा भाग होता है जिसे उस **सॉफ्टवेयर में सुधार हेतु बनाया** जाता है।
- यह पैच सॉफ्टवेयर **मुख्य सॉफ्टवेयर के साथ ही काय** करते हैं।

VPN (Virtual Private Network)

- यह एक प्रकार का टूल है जिसकी मदद से **इंटरनेट कनेक्शन को सिक्योर** कर सकते हैं और **अपनी प्राइवेसी को प्रोटेक्ट** कर सकते हैं।
- यह यूजर को इंटरनेट के उपयोग के दौरान **Identity** और **लोकेशन को गोपनीय रखने में मदद** करता है।
- VPN सॉफ्टवेयर उपयोगकर्ता को **एक नया आईपी एड्रेस** देता है। जिससे ऑरीजनल आईपी एड्रेस को छुपा लिया जाता है।

- **क्रोजर**- यह एक ऐसा सॉफ्टवेयर है, जो बच्चों की मानसिकता पर बुरा प्रभाव डालने वाले इंटरनेट पर मौजूद कार्यक्रमों को रोकने में मदद करेगा।
- **कम्प्यूटर फोरेंसिक**- अपराधियों द्वारा कम्प्यूटर से डिलीट/डैमेज की गई फाइलों को पुनः प्राप्त करना, **कम्प्यूटर फोरेंसिक** कहलाता है।
- **ECC (एलिप्टिक कर्व क्रिप्टोग्राफी)**- यह एक आधुनिक और व्यापक रूप से उपयोग की जाने वाली **क्रिप्टोग्राफी तकनीक** है जो विभिन्न कम्प्यूटर सुरक्षा अनुप्रयोगों के लिये सुरक्षा तथा दक्षता प्रदान करती है।
- **हैंड-सेक**- सूचनाओं की वह श्रृंखला जो दो या दो से अधिक कम्प्यूटर नेटवर्क में सूचनाओं के आदान-प्रदान हेतु प्रयुक्त होती है। यह कम्प्यूटर नेटवर्क में सूचनाओं के गमन को सुरक्षित व सुनिश्चित करता है इसे **Flow Control** के नाम से भी जाना जाता है।
- **साइबर चैक**- यह **सी-डैक पुणे द्वारा विकसित साइबर फोरेंसिक टूल किट** है, जो लॉ इन्फॉर्समेंट एजेंसियों द्वारा साक्ष्य फाइलों को देखने तथा विश्लेषित करने के लिए उपयोग में लाया जाता है।
- **हनी पोट्स**- यह एक ऐसा फर्जी सिस्टम वैध लक्ष्य जसा प्रतीत होता है, जो साइबर सुरक्षा रणनीति में हमलावरों (घुसपैठियों) को पकड़ने के इरादे से लुभाने (आकर्षित) तथा उनके व्यवहार का अध्ययन करने के लिए उपयोग किया जाता है।
- **की-ट्रेसर (Key Tracer)**-यह एक **कुंजी प्रबंधन प्रणाली** है जो संगठनों को **कुंजियों को ट्रैक करने, प्रबंधित करने** तथा **सुरक्षित करने में** मदद करती है। यह भौतिक कुंजियों को स्मार्ट कुंजियों में बदलने के लिए **RFID तकनीक** का उपयोग करता है। यह एन्क्रिप्टेड जानकारी की सुरक्षा के साथ-साथ डिजिटल परिसम्पतियों की भी साइबर खतरों से रक्षा करती है।

.....सीधे परीक्षा से

प्र. सुरक्षा के लिए उपयोग किये जाने वाले शब्द हनी-पोट्स का क्या मतलब है?

(a) यह घुसपैठिये के लिए वेबसाइट द्वारा प्रदान की जाने वाली सेवाओं तक सीधी पहुँच है।
(b) यह घुसपठिये के लिए वेबसाइट द्वारा प्रदान की जाने वाली सेवाओं तक अप्रत्यक्ष पहुँच है।
(c) इसका उपयोग घुसपैठिये को पकड़ने के इरादे से घुसपैठिये को आकर्षित करने के लिए किया जाता है।
(d) इसका उपयोग घुसपैठिये को प्रतियोगी की वेबसाइट पर डायवर्ट करने के लिए किया जाता है।

उत्तर- (c) **(MPPSC CSIT-2021)**

ब्लॉकचैन प्रौद्योगिकी

- यह **डाटा ब्लॉकों की एक श्रृंखला** होती है, जो एक सुरक्षित एवं आसानी से सुलभ नेटवर्क पर लेन-देन का एक **विकेन्द्रीकृत (डाटाबेस)** तैयार करती है।
- लेन-देन के इस साझा रिकॉर्ड को नेटवर्क पर स्थित कोई भी व्यक्ति देख सकता है।
- यह **डिजिटल मुद्रा का सबसे लोकप्रिय अनुप्रयोग** है।
- **बिटकॉइन** इस पद्धति पर आधारित एक महत्वपूर्ण नेटवर्क है।
- इस प्रौद्योगिकी में हैकिंग और साइबर अपराध की सम्भावनाएँ कम हो जाती हैं।
- ब्लॉकचैन तकनीक तीन अलग-अलग तकनीकों **इंटरनेट, पर्सनल कुंजी (की) की क्रिटोग्राफी** तथा **प्रोटोकॉल पर नियंत्रण,** का समायोजन है।
- भारत में **तेलंगाना** और **आंध्रप्रदेश** में **पायलट परियोजना** के रूप में ब्लॉकचैन तकनीक आरम्भ की गई है।

✍ .....सीधे परीक्षा से

प्र. डिज़िटल मुद्रा का सबसे लोकप्रिय अनुप्रयोग है-

(a) रोबोटिक्स (b) मशीन लर्निंग
(c) आर्टिफिशियल इंटेलीजेन्स (d) ब्लॉकचैन

उत्तर- (d) **(MPPSC A.M.O– 2021)**

✍ .....सीधे परीक्षा से

प्र. एक विकेन्द्रीकृत डिजिटल बहीखाता तकनीक जो कई कम्प्यूटरों पर लेन-देन को सुरक्षित रूप से रिकार्ड करती है और मुख्य रूप से बिटकॉइन जैसी क्रिप्टोकरेंसी में उपयोग की जाती है, कहलाती है।

(a) आर्टिफिशियल इंटेलिजेन्स (b) क्लाउड कम्प्यूटिंग
(c) ब्लॉक चन (d) इंटरनेट ऑफ थिंग्स

उत्तर- (c) **(MPPSC AP-2024)**

भारत में साइबर सुरक्षा के लिए किए गये उपाय

सूचना प्रौद्योगिकी अधिनियम,2000

- यह अधिनियम कम्प्यूटर प्रणालियों, कम्प्यूटर नेटवर्कों एवं उनके डेटा के प्रयोग को नियंत्रित करता है, यह अधिनियम इलेक्ट्रॉनिक प्रमाणीकरण, डिजिटल हस्ताक्षर का साझा समन्वयित रूप है।
- वर्ष **2008 में इस अधिनियम में संशोधन** किया गया जिसके अंतर्गत साइबर सुरक्षा के लिए वैधानिक फ्रेमवर्क तैयार हुआ है।
- इस अधिनियम की धारा **43, 43(A) 66, 66B, 66C, 66D, 66E, 66F, 67, 67,, 67(A), 70, 72, 72(A), और 74** हैकिंग और साइबर अपराधों से संबंधित हैं।
- इसी के तहत् **CERT-in का गठन** किया गया है।

कम्प्यूटर इमरजेंसी रिस्पांस टीम (Computer Emergency Responses Team- CERT-in)

- **गठन**- साइबर सुरक्षा के लिए उत्तरदायी राष्ट्रीय एजेंसी के रूप में कार्य करने के लिए **आई.टी.संशोधन अधिनियम, 2000 के अंतर्गत** अधिदेशित।
- यह एजेंसी हैकिंग, फिशिंग तथा अन्य साइबर सुरक्षा खतरों से निपटान हेतु अधिकृत है।
- **उद्देश्य**- भारतीय समुदाय के लिए कम्प्यूटर सुरक्षा से संबंधित साइबर हमले को विफल करना।

✍ .....सीधे परीक्षा से

प्र निम्नलिखित में से कौन-सी भारतीय नोडल एजेंसी हैकिंग, फिशिंग और अन्य साइबर सुरक्षा खतरों से निपटने के लिए अधिकृत है?

(a) भारतीय कम्प्यूटर आपातकालीन प्रतिक्रिया टीम
(b) प्रगत संगणन विकास केंद्र
(c) सेंटर फॉर डेवलपमेंट ऑफ टेलीमेटिक्स
(d) राष्ट्रीय सूचना विज्ञान केन्द्र

उत्तर- (a) **(MPPSC SFS-2019)**

CERT-fn

- इसका गठन **वित्तीय स्थिरता तथा विकास परिषद्** की एक उप समिति की अनुशंसाओं के आधार पर **वित्तीय क्षेत्र से संबंधित खतरों से निपटने के लिए** एक विशेषज्ञ एजेंसी के रूप में किया गया है।

राष्ट्रीय साइबर सुरक्षा नीति 2013

इसके मुख्य प्रावधानों में निम्नलिखित सम्मिलित हैं-

- देश की महत्वपूर्ण अवसंरचनाओं की रक्षा हतु चौबीस घंटे सातों दिन के लिए **राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र (NCIIPC)** की स्थापना।
- साइबर सुरक्षा चुनौतियों से निपटने के लिए एक गतिशील **विधिक फ्रेमवर्क** का विकास।
- इसके तहत् साइबर सुरक्षा के मुद्दों हेतु **CERT-in को नोडल एजेंसी** बनाया गया है तथा विभिन्न स्तरों पर समन्वय हेतु **स्थानीय स्तर पर सीईआरटी (CERT) निकायों का गठन** किया जाना है।

राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (National Critical Information Infrastructure Protection Centre- NCIIPC)

- इसकी स्थापना साइबर सुरक्षा संबंधी खतरों से निपटने हेतु की गई है।
- यह **राष्ट्रीय तकनीकी अनुसंधान संगठन (NTRO)** के अधीन कार्य करेगा।

सीसीटीएनएस (CCTNS- Crime and Criminal Tracking Network and Systems)

- **प्रारंभ**- 2009
- **उद्देश्य**- सभी स्तरों पर अपराधियों के अन्वेषण तथा उनकी रोकथाम हेतु तकनीकी प्रयोग के साथ-साथ साइबर अपराधों को रोकने हेतु पुलिस को सशक्त बनाना।
- यह राष्ट्रीय **ई-गवर्नेंस योजना के तहत मिशन मोड प्रोजेक्ट** है।

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल

- **शुरुआत**- 30 अगस्त, 2019
- **स्थापना**- ग्रह मंत्रालय के अंतर्गत।
- यह पोर्टल नागरिकों विशेषकर महिलाओं, बच्चों को ऑनलाइन साइबर अपराध जैसे-स्टॉकिंग एवं साइबर बुलिंग के खिलाफ शिकायत करने में सक्षम बनाता है।
- इसमें **कोई भी व्यक्ति स्वयं सेवक** के रूप में कार्य करके साइबर अपराध निवारण में सहयोग कर सकता है।

भारतीय साइबर अपराध समन्वय केंद्र (I-4C) (Indian Cyber Crime Co-Ordination Center)

- **स्थापना/केन्द्र**- अक्टूबर, 2018 (दिल्ली)
- **उद्देश्य**- साइबर खतरों, बाल अश्लीलता और ऑनलाइन स्टॉकिंग (पीछा करना) जैसे इंटरनेट अपराधों से निपटना।
- यह **अंतर एजेंसी समन्वय** के लिए साइबर और सूचना सुरक्षा विभाग (गृह मंत्रालय के अधीन) के अंतर्गत स्थापित है।
- वर्तमान में **15 राज्यों और केन्द्र शासित प्रदेशों में क्षेत्रीय साइबर अपराध समन्वय केन्द्र स्थापित करने की योजना** है। इस योजना को सम्पूर्ण भारत में 7 प्रमुख घटकों के साथ लागू किया गया-
  - नेशनल साइबर क्राइम थ्रेट एनालिटिक्स यूनिट।
  - नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल।
  - प्लेटफार्म फॉर जॉइंट साइबर क्राइम इन्वेस्टिगेशन टीम।
  - नेशनल साइबर क्राइम फॉरेंसिक लेबोरेटरी ईकोसिस्टम।
  - नेशनल साइबर क्राइम ट्रेनिंग सेंटर।
  - साइबर क्राइम इकोसिस्टम मैनेजमेंट यूनिट।
  - नेशनल साइबर रिसर्च एंड इनोवेशन सेंटर।

साइबर सुरक्षित भारत पहल

- **प्रारंभ**- 19 जनवरी, 2018
- **उद्देश्य**- साइबर सुरक्षा को सुदृढ़ बनाने हेतु लोगों को जागरुक करना।
- भारत में यह अपनो तरह की **पहली सार्वजनिक-निजी साझेदारी** है।
- इस कार्यक्रम के तीन स्तंभ हैं- **जागरूकता, शिक्षा एवं सामथ्य**।

12वां भारतीय सुरक्षा सम्मेलन

- **आयोजन**- 28 अगस्त 2019 को नई दिल्ली में।
- **विषय**- 'नई राष्ट्रीय सुरक्षा रणनीति की ओर'।
- इसमें **डिजिटल इंडिया मुहिम के क्रियान्वयन** तथा इस मुहिम के अंतर्गत **साइबर स्वच्छता केन्द्र** बनाने पर सहमति प्रदान की गयी।

अन्य प्रयास

- **राष्ट्रीय साइबर समन्वय केन्द्र (NCCC)**- यह भारत सरकार की एक ई-निगरानी एवं ऑपरेशनल साइबर सुरक्षा परियोजना है।
- **केरल सरकार** द्वारा **साइबर सुरक्षा** तथा **हैकिंग हेतु cOcOn** नामक **वार्षिक सम्मेलन** किया जा रहा है।
- सरकार ने साइबर सुरक्षा से संबंधित फ्रेमवर्क का अनुमोदन किया है और इसके लिए **राष्ट्रीय सुरक्षा परिषद् सचिवालय** को **नोडल एजेंसी** बनाया गया है।

.....सीधे परीक्षा से

प्र. NCCC भारत सरकार की एक ई-निगरानी एवं ऑपरेशनल साइबर सुरक्षा परियोजना है। यहाँ NCCC का तात्पर्य है-

(a) राष्ट्रीय साइबर एवं कम्प्यूटर केन्द्र
(b) राष्ट्रीय साइबर समन्वय केन्द्र
(c) राष्ट्रीय साइबर चलन केन्द्र
(d) राष्ट्रीय साइबर समुदाय केन्द्र

उत्तर- (b) **(MPPSC A.M.O– 2021)**

- विभिन्न स्तरों पर सूचना सुरक्षा के क्षेत्र में मानव संसाधन विकसित करने के उद्देश्य से सरकार ने **'सूचना सुरक्षा शिक्षा और जागरूकता' (Information Security Education and Awareness- ISEA) परियोजना** प्रारंभ की है।
- **'नयन' सॉफ्टवेयर**- साइबर सुरक्षा हेतु C-DAC (पुणे) द्वारा विकसित सॉफ्टवेयर।
- **राष्ट्रीय साइबर फॉरेंसिक प्रयोगशाला**- यह ऑनलाइन तथा ऑफलाइन दोनों तरीकों से सभी राज्यों एवं केन्द्र शासित प्रदेशों के **पुलिस जाँच अधिकारियों** को प्रारंभिक चरण की **साइबर फॉरेंसिक सहायता** प्रदान करती है।
- **साइट्रेन पोर्टल**- यह साइबर अपराध जाँच हेतु एक **ओपन ऑनलाइन पाठ्यक्रम मंच** है जो पुलिस अधिकारियों, न्यायिक अधिकारियों तथा अभियोजकों की क्षमता निर्माण हेतु विकसित किया गया है।
- **डिफेंस साइबर एजेंसी**- इसका **गठन मई 2019 में चीन और पाकिस्तान के हैकर्स** की ओर से होने वाले साइबर हमलों से **निपटान हेतु** किया गया है।

साइबर अपराध से संबंधित दाण्डिक प्रावधान

- **66(अ)**-संसूचना सेवा आदि द्वारा आक्रामक संदेश भेजने हेतु दंड।
- **66(ब)**-चुराए गए कम्प्यूटर या संचार युक्ति को बेईमानी से प्राप्त करने के लिए दंड।
- **66(सी)**-पहचान चोरी के लिए दंड।
- **66(डी)**-कम्प्यूटर संसाधन का उपयोग करके प्रतिरूपण द्वारा छल करने के लिए दंड।
- **66(ई)**-एकांतता के अतिक्रमण के लिए दंड।
- **66(एफ)**-साइबर आतंकवाद के लिए दंड।
- **67(ए)**-कामुकता व्यक्त करने वाले कार्य आदि सामग्री के इलेक्ट्रॉनिक रूप से प्रकाशन के लिए दंड।
- **67(बी)**-कामुकता व्यक्त करने वाले कार्य में बालकों को चित्रित करने वाली सामग्री के इलेक्ट्रॉनिक रूप से प्रकाशन के लिए दंड।
- **67(बी)(1)**-मध्यवर्तियों द्वारा सूचना का परिरक्षण और प्रतिधारण।

बुडापेस्ट कन्वेंशन

- यह **साइबर क्राइम पर आधारित एक कन्वेंशन** है।
- 8 नवम्बर, 2001 को यूरोपीय परिषद् के 109वें सत्र में मंत्रियों की समिति द्वारा रिपोर्ट प्रस्तुत की गई जिस पर **23 नवम्बर, 2001** को हस्ताक्षर किए गए तथा **1 जुलाई, 2004 को यह लागू** हुआ।
- इस कन्वेंशन में **अमेरिका और ब्रिटेन सहित कुल 64 सदस्य** हैं। (अक्टूबर, 2019 तक)

नोट

- **मध्यप्रदेश ट्रांस एसएलडीसी (SLDC)** सायबर सिक्योरिटी को लागू करने वाला देश का **पहला पावर यूटीलिटी** है।
- **साइबर क्राइसिस प्रबंधन योजना** लागू करने वाला **मध्यप्रदेश** देश का **पहला राज्य** है।

सूचना प्रौद्योगिकी अधिनियम, 2000

अध्याय, धारा तथा विषय	प्रावधान
अध्याय-1 (धारा 1-2) **प्रारंभिक**	**1.** संक्षिप्त नाम, विस्तार और लागू होना। **2.** परिभाषाएँ।
अध्याय-2 (धारा 3) **अंकीय चिह्नक और इलेक्ट्रॉनिक नियमन**	**3.** इलेक्ट्रॉनिक अभिलेख का अधिप्रमाणीकरण।
अध्याय-3 (धारा 4-10) **इलेक्ट्रॉनिक नियमन**	**4.** इलेक्ट्रॉनिक अभिलेखों की विधिमान्यता। **5.** इलेक्ट्रॉनिक चिह्नकों की विधि मान्यता। **6.** सरकार और उसके अभिकरणों में इलेक्ट्रॉनिक चिह्नकों का प्रयोग। **(क)**- सेवा प्रदाता द्वारा सेवाओं का परिदान। **7.** इलेक्ट्रॉनिक अभिलेखों का प्रतिधारण। **(क)**- इलेक्ट्रॉनिक रूप में रखे गए दस्तावेजों आदि की संपरीक्षा। **8.** इलेक्ट्रॉनिक राजपत्र में नियम, विनियम आदि का प्रकाशन। **9.** धारा-6, धारा-7 और धारा-8 इस बात पर जोर देने का अधिकार प्रदान नहीं करती कि दस्तावेज इलेक्ट्रॉनिक रूप में स्वीकार किया जाए। **10.** इलेक्ट्रॉनिक चिह्नक से संबंधित नियम बनाने की केन्द्रीय सरकार की शक्ति। **(क)**- इलेक्ट्रॉनिक साधनों के माध्यम से की गई संविदाओं की विधि मान्यता।

अध्याय-4 (धारा 11-13) इलेक्ट्रॉनिक अभिलेखों की अभिस्वीकृति और प्रेषण	**11.** इलेक्ट्रॉनिक अभिलेखों का अधिकार। **12.** प्राप्ति की अभिस्वीकृति। **13.** इलेक्ट्रॉनिक अभिलेख के प्रेषण और प्राप्ति का समय और स्थान।
अध्याय-5 (धारा-14-16) सुरक्षित इलेक्ट्रॉनिक अभिलेख और सुरक्षित इलेक्ट्रॉनिक चिह्नक	**14.** सुरक्षित इलेक्ट्रॉनिक अभिलेख। **15.** सुरक्षित इलेक्ट्रॉनिक चिह्नक। **16.** सुरक्षा प्रक्रियाएँ और पद्धतियाँ।
अध्याय-6 (धारा-17-34) प्रमाणकर्त्ता प्राधिकारियों का विनियम	**17.** नियंत्रक और अन्य अधिकारियों की नियुक्ति। **18.** नियंत्रक के कृत्य। **19.** विदेशी प्रमाणकर्त्ता प्राधिकारियों की मान्यता। **20.** नियंत्रक का कोष के रूप में काम करना। **21.** इलेक्ट्रॉनिक चिह्नक प्रमाणपत्र जारी करने के लिये अनुज्ञप्ति। **22.** अनुज्ञप्ति के लिये आवेदन। **23.** अनुज्ञप्ति का नवीकरण। **24.** अनुज्ञप्ति प्रदान करने या उसे नामंजूर करने के लिय प्रक्रिया। **25.** अनुज्ञप्ति का निलंबन। **26.** अनुज्ञप्ति के निलंबन या प्रतिसंहरण की सूचना। **27.** प्रत्यायोजन की शक्ति। **28.** उल्लंघनों का अन्वेषण करने की शक्ति। **29.** कम्प्यूटरों और डाटा तक पहुँच। **30.** प्रमाणकर्त्ता प्राधिकारी द्वारा कतिपय प्रक्रियाओं का अनुसरण किया जाना। **31.** प्रमाणकर्त्ता प्राधिकारी अधिनियम आदि के अनुपालन को सुनिश्चित करेगा। **32.** अनुज्ञप्ति का संप्रदर्शन। **33.** अनुज्ञप्ति का अभ्यर्पण। **34.** प्रकटीकरण।
अध्याय-7 (धारा-35-39) इलेक्ट्रॉनिक चिह्नक प्रमाणपत्र	**35.** प्रमाणकर्त्ता प्राधिकारी द्वारा इलेक्ट्रॉनिक चिह्नक प्रमाणपत्र जारी किया जाना। **36.** अंकीय चिह्नक प्रमाणपत्र जारी करने पर व्यपदेशन। **37.** अंकीय चिह्नक प्रमाणपत्र का निलंबन। **38.** अंकीय चिह्नक प्रमाणपत्र का प्रतिसंहरण। **39.** निलंबन या प्रतिसंहरण की सूचना।
अध्याय-8 (धारा-40-42) उपयोगकर्त्ताओं के कर्त्तव्य	**40.** कुंजी-युग्म का उत्पादित किया जाना। **41.** अंकीय चिह्नक प्रमाणपत्र की स्वीकृति। **42.** निजी कुंजी का नियंत्रण।
अध्याय-9 (धारा-43-47) शास्तियाँ, प्रतिकर और अधिनिर्णय	**43.** कम्प्यूटर, कम्प्यूटर प्रणाली आदि को नुकसान के लिये शास्ति और प्रतिकर। **(क)**- डाटा को संरक्षित रखने में असफलता के लिये प्रतिकर। **44.** जानकारी, विवरणी आदि देने में असफल रहने के लिये शास्ति। **45.** अवशिष्ट शास्ति। **46.** न्यायनिर्णयन करने की शक्ति। **47.** न्यायनिर्णायक अधिकार द्वारा विचार की जाने वाली बातें।
अध्याय-10 (धारा-48-64) साइबर अपील अधिकरण	**48.** साइबर अपील अधिकरण की स्थापना। **49.** साइबर अपील अधिकरण की संरचना। **50.** साइबर अपील अधिकरण के अध्यक्ष और सदस्यों के रूप में नियुक्ति के लिये अर्हताएँ। **51.** अध्यक्ष और सदस्यों की पदावधि, सेवा की शर्तें आदि। **52.** अध्यक्ष और सदस्यों के वेतन, भत्ते और सेवा के अन्य निबंधन और शर्तें। **53.** रिक्तियों का भरा जाना। **54.** पद त्याग और पद से हटाया जाना। **55.** अपील अधिकरण का गठन करने वाले आदेश का अंतिम होना और उसकी कार्यवाहियों का अविधिमान्य न होना। **56.** साइबर अपील अधिकरण के कर्मचारी। **57.** साइबर अपील अधिकरण को अपील। **58.** साइबर अपील अधिकरण की शक्तियाँ और प्रक्रिया। **59.** विधिक प्रतिनिधित्व का अधिकार। **60.** परिसीमा। **61.** सिविल न्यायालय की अधिकारिता का न होना। **62.** उच्च न्यायालय को अपील। **63.** अपराधों का शमन। **64.** शास्ति या प्रतिकर की वसूली।

अध्याय-11 (धारा-65-78) अपराध	**65.** कम्प्यूटर साधन कोड से छेड़छाड़ **66.** कम्प्यूटर से संबंधित अपराध। **67.** अश्लील सामग्री का इलेक्ट्रॉनिक प्रकाशन या पारेषण करने पर दंड। **(क), (ख)** कामुकता प्रदर्शन इलेक्ट्रॉनिक माध्यम से करने पर दंड। **68.** नियंत्रक की निदेश देने की शक्ति। **69.** किसी कम्प्यूटर संसाधन के माध्यम से किसी सूचना के अंतररोधन या मानिटरिंग के लिये निदेश जारी करने की शक्ति। **70.** संरक्षित प्रणाली। **(क)** राष्ट्रीय नोडल अभिकरण। **(ख)** दुर्घटना मोचन के लिये भारतीय कम्प्यूटर आपात मोचन दल का राष्ट्रीय आपात अभिकरण के रूप में सेवा करना। **71.** दुर्व्यपदशन के लिये शास्ति। **72.** गोपनीयता और एकांतता भंग के लिये शास्ति। **(क)** विधिपूर्ण सविदा का भंग करते हुए सूचना के प्रकटन के लिये दंड। **73.** इलेक्ट्रॉनिक चिह्नक प्रमाणपत्र की कतिपय विशिष्टयों को मिथ्या प्रकाशित करने के लिये शास्ति। **74.** कपटपूर्ण प्रयोजन के लिये प्रकाशन। **75.** अधिनियम का भारत से बाहर किये गए अपराधों और उल्लंघनों का लागू होना। **76.** अधिहरण। **77.** प्रतिकर शास्ति या अधिहरण का अन्य दंड में हस्तक्षेप न करना। **(क)** अपराधों का शमन। **(ख)** तीन वर्ष के कारावास वाले अपराधों का जमानतीय होना। **78.** अपराधों का अन्वेषण करने की शक्ति।
अध्याय-12 (धारा-79-90) कतिपय मामलों में मध्यवर्ती को दायित्व से छूट	**79.** कतिपय मामलों में मध्यवर्ती को दायित्व से छूट। **(क)** केन्द्रीय सरकार द्वारा इलेक्ट्रॉनिक साक्ष्य का परीक्षक अधिसूचित करना। **80.** पुलिस अधिकारी और अन्य अधिकारियों की प्रवेश करने, तलाशी लेने आदि की शक्ति। **81.** अधिनियम का अध्यारोही प्रभाव होना। **82.** अध्यक्ष, सदस्यों, अधिकारियों और कर्मचारियों, नियंत्रकों का लोकसेवक होना। **83.** निदेश देने की शक्ति। **84.** सद्भावनापूर्वक की गई कार्यवाही के लिये संरक्षण। **85.** कंपनियों द्वारा अपराध। **86.** कठिनाइयों को दूर करना। **87.** केन्द्रीय सरकार की नियम बनाने की शक्ति। **88.** सलाहकार समिति का गठन। **89.** नियंत्रक को विनियम बनाने की शक्ति। **90.** राज्य सरकार की नियम बनाने की शक्ति।

अभ्यासमाला

1. शब्द ..... का आशय है एक ऐसा व्यक्ति, जो बिना किसी प्राधिकरण के कम्प्यूटर सिस्टम में सेंध लगाकर घुसता है, जालसाजी के उद्देश्यों के लिए जानबूझकर वेब साइट को विकृत करता है।
(a) व्हाइट हैट (b) हैकर
(c) क्रैकर (d) स्टैकर

2. मूल उत्पाद या प्रति की नकल उतारकर या उसकी प्रतिलिपि को काला बाजारी के माध्यम से बाजार में बेचने को क्या कहा जाता है?
(a) स्पूफिंग (b) फिशिंग
(c) बग (d) पाइरेसी

3. 'स्पैम' किस विषय से सम्बन्धित शब्द है?
(a) कम्प्यूटर (b) कला
(c) संगीत (d) खेल

4. ब्लैक हैट कम्प्यूटर हैकर है-
(a) एक व्यक्ति जो कम्प्यूटर की सुरक्षा बनाए रखता है
(b) एक व्यक्ति जो व्यक्तिगत लाभ के दूषित इरादों से कम्प्यूटर सुरक्षा का पालन नहीं करता।
(c) कम्प्यूटर के सुरक्षित परिचालन हेतु उत्तरदायी एक व्यक्ति
(d) कम्प्यूटर सुधारने वाला एक व्यक्ति।

5. साइबर क्राइम क्या है?
(a) हैकिंग (b) स्टॉकिंग
(c) सर्विस आघात की मनाही (d) ये सभी

6. हैकिंग से आप क्या समझते हैं?
(a) सर्चिंग (b) सिक्योरिटी
(c) (a) तथा (b) दोनों (d) इनमें से कोई नहीं

7. लॉगिन नाम और पासवर्ड का सत्यापन कहलाता है-
(a) ऑथेंटिकेशन (b) एक्सेसिबिलिटी
(c) कॉन्फिगरेशन (d) लॉगिंग इन

8. मैकफी उदाहरण है-
(a) वायरस (b) क्विक हील
(c) फोटो एडिटिंग सॉफ्टवेयर (d) एंटीवायरस

9. युद्ध का पाँचवा क्षेत्र किसे कहा जाता है?
(a) अंतरिक्ष (b) समुद्र
(c) वायु (d) साइबर वारफेयर

10. एक विघटनकारी सॉफ्टवेयर, जो कम्प्यूटर से कम्प्यूटर तक फैलता है, को .... कहा जाता है।
(a) सर्च इंजन (b) चैट सॉफ्टवेयर
(c) ई-मेल (d) वायरस

11. AES का पूरा नाम क्या है?
(a) Alternative Encryption standard
(b) Advanced Encryption standard
(c) Advanced Encryption system
(d) Advanced Emission standard

12. ..... एक एंटीवायरस सॉफ्टवेयर नहीं है।
(a) मैकैफी (b) अवीरा
(c) डीबीएमएस (d) एवास्ट

13. कम्प्यूटर को हैकर से बचाने के लिए हमें इंस्टाल करना चाहिए।
(a) फायरवॉल (b) मैक्रो
(c) इनमें से कोई नहीं (d) मेलर

14. VIRUS (वायरस) का पूरा रूप क्या है?
(a) Vitalise Information Resources under Siege
(b) Vital Information Resources Uper Siege
(c) Vital Information Resources under Siege
(d) Vial Information Resoces Undead Siege

15. मालवेयर, जो कि जब तक पैसों का भुगतान न कर दिया जाए, आवश्यक डेटा को नष्ट करने अथवा प्रक्रियाओं के संचालन को बंद करने की चेतावनी को प्रदर्शित करता रहता है ..... कहलाता है।
(a) वार्म (b) ट्रोजन हॉर्स
(c) रैंसमवेयर (d) वायरस

16. कम्प्यूटर सिस्टम या नेटवर्क की सुरक्षा पर खतरे के प्रकार निम्नांक होते हैं:
i. इंटरप्शन (व्यवधान)
ii इंटरसेप्शन (अवरोधन)
iii मॉडीफिकेशन (संशोधन)
iv क्रिएशन (निर्माण)
v संरचना (फैब्रीकेशन)
निम्नलिखित में से कौन-सा विकल्प सत्य है?
(a) केवल i, ii, iii और iv
(b) केवल ii, iii, iv और v
(c) केवल i, ii, iii और v
(d) केवल i, ii, iii, iv और v सभी

17. ..... का मुख्य उद्देश्य आपके कम्प्यूटर में इंटरनेट के माध्यम से अनाधिकृत एक्सेस की रोकथाम करना होता है।
(a) पॉपअप ब्लॉकर (b) फायरवॉल
(c) स्पाईवेयर ब्लॉकर (d) स्पैम असैसिन

18. कम्प्यूटर में एंटीवायरस निम्न कारणों से इंस्टॉल किया जाता है:
(a) कम्प्यूटर को वायरस से सुरक्षित रखने के लिए
(b) कम्प्यूटर को आग से सुरक्षित रखने के लिए
(c) मेमोरी साइज बढ़ाने के लिए
(d) अन्य प्रोग्राम इंस्टॉल करने के लिए

19. एक कम्प्यूटर वायरस से कैसे संक्रमित होता है।
(a) जब एक फायरवॉल उपस्थित होता है।
(b) जब एंटीवायरस सॉफ्टवेयर एक्टिव होता है।
(c) जब इंटरनेट से अज्ञात सॉफ्टवेयर डाउनलोड किया जाता है।
(d) जब लोकल कम्प्यूटर में एमएस ऑफिस सॉफ्टवेयर पर कार्य किया जाता है।

20. निम्न में से कौन एक मालवेयर नहीं है?
(a) वार्म (b) वायरस
(c) कुकीज (d) ट्रोजन हॉर्स

21. निम्न में से कौन इंटरनेट सुरक्षा नहीं देता है-
(a) फायरवॉल (b) डेटा कम्प्रेशन
(c) डेटा एनक्रप्शन (d) यूजर ऑथेंटिकेशन

22. साइबर सुरक्षित भारत कार्यक्रम के स्तंभ कौन-से हैं?
(a) जागरूकता (b) शिक्षा
(c) सामर्थ्य (d) उपरोक्त सभी

23. निम्नलिखित में से कौन सा एक सिक्योरिटी सॉफ्टवेयर है?
(a) एनक्रिप्शन सॉफ्टवेयर
(b) एंटीवायरस सॉफ्टवेयर
(c) फायरवाल सॉफ्टवेयर
(d) उपरोक्त सभी

24. 'साइबर लॉ' शब्दावली में 'DOS' का अर्थ है?
(a) डिनायल ऑफ सर्विस
(b) दूरस्थ ऑपरेटर सेवा
(c) डेनियल ऑपरेटिंग सर्विस
(d) इनमें से कोई नहीं

25. निम्नलिखित में से किसे वायु, समुद्र, जमीन तथा अंतरिक्ष के बाद युद्ध का पांचवा क्षेत्र भी कहा जाता है?
(a) साइबर क्राइम (b) साइबर वारफेयर
(c) फायरवाल (d) स्पैम

26. कम्प्यूटर वायरस क्या है?
(a) ऐसा वायरस जो मनुष्यों के स्वास्थ्य को प्रभावित करे।
(b) ऐसा कम्प्यूटर प्रोग्राम जो स्वयं की प्रतिलिपियाँ बना सके।
(c) उपरोक्त दोनों
(d) इनमें से कोई नहीं

27. प्रॉक्सी सर्वर का प्रयोग किया जाता है?
(a) TCP/IP देने के लिये।
(b) डाटाबेस एक्सेस के लिये अनुरोध।
(c) वेब पेज के लिये क्लाइंट रिक्वेस्ट प्रोसेस करने के लिये।
(d) अनधिकृत उपयोगकर्त्ताओं के खिलाफ सुरक्षा प्रदान करने के लिये।

28. पासवर्ड के प्रयोग से उपयोगकर्त्ता-
(a) ढांचों को सरल बना सकते हैं।
(b) गोपनीयता बरकरार रख सकते हैं।
(c) समय का दक्ष प्रयोग कर सकते हैं।
(d) जल्दी सिस्टम में जा सकते हैं।

29. निम्नलिखित में से सही विकल्प को चुनिए?
(a) प्रॉक्सी सर्वर क्लाइंट से प्राप्त अनुरोध को अन्य सर्वरों को अग्रेषित करता है।
(b) प्रॉक्सी सर्वर TCP/IP एड्रेस उपलब्ध कराता है।
(c) उपरोक्त दोनों
(d) इनमें से कोई नहीं

30. फायरवॉल का मुख्य काम है?
(a) कॉपिंग (b) मूविंग
(c) डिलीटिंग (d) मॉनीटरिंग

31. इंटरनेट में फायरवॉल का प्रयोग निम्न में से किससे बचाता है?
(a) वायरस आक्रमण
(b) अनधिकृत आक्रमण
(c) डाटा ड्रिवन आक्रमण
(d) अग्नि आक्रमण

32. जंक ई-मेल को कहते है?
(a) स्पैम (b) स्पूफ
(c) स्क्रैप (d) स्क्रिप्ट

33. भारत में साइबर सुरक्षा के लिये वैधानिक फ्रेमवर्क कौन-सा अधिनियम प्रदान करता है?
(a) सूचना प्रौद्योगिकी संशोधन अधिनियम-2008
(b) सूचना प्रौद्योगिकी अधिनियम-2000
(c) सूचना प्रौद्योगिकी अधिनियम-2013
(d) इनमें से कोई नहीं

34. निम्नलिखित में से कौन-सा प्रचलित एंटीवायरस साफ्टवेयर प्रोग्राम है?
(a) Kaspersky (b) Symentac
(c) AVG (d) उपरोक्त सभी

35. एप्लीकेशन सॉफ्टवेयर में फैलने वाले वायरस को क्या कहा जाता है?
(a) एंटी वायरस (b) फाईल वायरस
(c) मैक्रो वायरस (d) मंकी वायरस

36. भारत में सूचना प्रौद्योगिकी अधिनियम कब पारित किया गया?
(a) वर्ष 2000 (b) वर्ष 2004
(c) वर्ष 1998 (d) वर्ष 2002

37. पहला कम्प्यूटर वायरस कौन-सा है?
(a) फिलिप (b) क्रीपर
(c) मेलिसा (d) पैंचकॉम

38. अपने डाटा को ऑनलाइन अटैक, हैकर और वायरस से बचाने को क्या कहते है?
(a) साइबर अटैक (b) फिजिकल सिक्यूरिटी
(c) इनमें से कोई नहीं (d) साइबर सिक्योरिटी

39. साइबर क्राइसिस प्रबंधन योजना लागू करने वाला भारत का प्रथम राज्य कौन-सा है?
(a) महाराष्ट्र (b) केरल
(c) मध्यप्रदेश (d) छत्तीसगढ़

40. हमलावर संक्रमित विज्ञापनों को अपलोड कर किस प्रकार का हमला करता है?
(a) वेब अटैक (b) डी.ओ.एस
(c) मालवेयर ट्राईएज (d) इनमें से कोई नहीं

41. निम्नलिखित में से कौन-सा द्वेषपूर्ण साफ्टवेयर प्रोग्राम जो कम्प्यूटर उपयोगकर्त्ता के विरुद्ध जासूस (Spy) की तरह कार्य करता है?
(a) पैकेट स्निफिंग (b) स्पाईवेयर
(c) वॉर्म (d) इनमें से कोई नहीं

42. राष्ट्रीय साइबर अपराध रिपोटिंग पोर्टल का प्रारंभ कब हुआ?
(a) वर्ष 2016 (b) वर्ष 2019
(c) वर्ष 2014 (d) वर्ष 2017

43. बुडापेस्ट कन्वेंशन संबंधित है?
(a) तापमान में वृद्धि से (b) शिक्षा से
(c) साइबर क्राइम से (d) इनमें से कोई नहीं

44. किस अधिनियम के तहत् CERT-IN (कम्प्यूटर इमरजेंसी रिस्पॉन्स टीम) का गठन हुआ।
(a) सूचना प्रौद्योगिकी अधिनियम-2000
(b) सूचना प्रौद्योगिकी अधिनियम-2008
(c) उपरोक्त दोनों
(d) इनमें से कोई नहीं

45. कामुकता व्यक्त करने वाले कार्य आदि सामग्री के इलेक्ट्रॉनिक रूप से प्रकाशन के लिए दण्ड का प्रावधान साइबर अपराध की किस धारा में किया गया है?
(a) 68(बी) (b) 67(ए)
(c) 66(बी) (d) 66(सी)

46. निम्नलिखित में से मालवेयर का उदाहरण है?
(a) स्पाइवेयर (b) ट्रोर्जन हार्स
(c) वॉर्म (d) उपरोक्त सभी।

47. 'वान्नाक्राई', पेट्या और इटर्नब्लू पद जो हाल ही में समाचारों में उल्लेखित थे, निम्नलिखित में से किसके साथ संबंधित है?
(a) लघु उपग्रह (b) साइबर आक्रमण
(c) क्रिप्टोकरेंसी (d) इनमें से कोई नहीं

48. निम्नलिखित में से कौन-सा कथन साइबर क्राइम से संबंधित हैं?
(a) नेटवर्क का अनाधिकृत तौर पर प्रयोग करना।
(b) ई-मेल बॅबिग।
(c) इंटरनेट का उपयोग कर आर्थिक अपराध करना।
(d) उपरोक्त सभी

49. Crime and Criminal Tracking Network and Systems (CCTNS) प्रोजेक्ट से संबंधित सत्य कथन हैं।
(a) यह प्रोजेक्ट वर्ष 2009 में पारंभ किया गया।
(b) इसका उद्देश्य पुलिस की दक्षता और प्रभावशीलता को बढ़ाने हेतु एक व्यापार और एकीकृत प्रणाली तैयार करना है।
(c) यह राष्ट्रीय ई-गवर्नेंस योजना के अंतर्गत एक मिशन मोड् प्रोजेक्ट है।
(d) उपरोक्त सभी।

50. वायरस एक कम्प्यूटर से दूसरे कम्प्यूटर में कैसे फैल सकता है?
(a) दूसरे कम्प्यूटर को पास में रखने से।
(b) इन्फेक्टेड फाइल को शेयर करने से।
(c) एक ही नेटवर्क का उपयोग करने से।
(d) इनमें से कोई नहीं।

51. इंटरनेट पर इंटरनेट उपयोगकर्त्ताओं के यूजर नेम, पासवर्ड तथा अन्य व्यक्तिगत सूचनाओं का प्राप्त करने का प्रयास करना.....कहलाता है?
(a) फिशिंग (b) पैच
(c) स्पॉम (d) स्निफिंग

52. ब्लॉकचेन तकनीक से संबंधित सही विकल्प चुनिए?
(a) ब्लॉकचेन डाटा ब्लॉकों की एक श्रृंखला होती है।
(b) भारत में तेलंगाना और आंध्रप्रदेश में पायलट परियोजना के रूप में प्रारंभ की गई।
(c) बिटकॉइन नेटवर्क, ब्लॉकचेन तकनीक का उदाहरण है।
(d) उपरोक्त सभी।

53. निम्नलिखित में कौन-सा साइबर अपराध से बचने का उपाय है?
(a) एंटीवायरस सॉफ्टवेयर का प्रयोग करना।
(b) फायरवाल का प्रयोग करना।
(c) प्रॉक्सी सर्वर का प्रयोग करना।
(d) उपरोक्त सभी।

54. यदि आपका कम्प्यूटर स्वतः रीबूट करता है तो संभावना है कि इसमें-
(a) मेमोरी पर्याप्त नहीं है। (b) वायरस है।
(c) प्रिंटर नहीं है। (d) इनमें से कोई नहीं।

55. पलाडियम प्रणाली को किस कम्पनी द्वारा विकसित किया गया है?
(a) माइक्रोसॉफ्ट (b) एप्पल
(c) सैमसंग (d) IBM

56. निम्नलिखित में से किसे कम्प्यूटर का सेफ्टी वाल्व भी कहते है?
(a) फायरवाल (b) क्रिप्टोग्राफी
(c) इनक्रिप्शन (d) इनमें से कोई नहीं

57. ऐसा दुर्भावनापूर्ण सॉफ्टवेयर जो कम्प्यूटर में फाइलों को लॉक कर देता है और उन फाइलों को अनलॉक करने के लिए उपयोगकर्त्ता से फिरौती की मॉग करता है?
(a) पेटया रैनसमवेयर (b) फिशिंग
(c) ई-मेल बॉम्बिंग (d) स्पूफिंग

58. निम्नलिखित में से कौन-सा प्रमुख कम्प्यूटर वायरस है?
(a) सी-ब्रेन (b) आई लव यू
(c) जेरूसलेम (d) उपरोक्त सभी

59. वह कम्प्यूटर वायरस जो स्वयं को किसी दूसरे कम्प्यूटर प्रोग्राम से जोड़ता है, कहलाता है?
(a) एक्सेस कंट्रोल (b) ट्रोजन हार्स
(c) वॉर्म (d) क्रैकर

60. निम्नलिखित में से किसे 'एथिकल हैकर्स' के रूप में जाना जाता है?
(a) ब्लैक हैट हैकर (b) ब्लू हैट हैकर
(c) ग्रे हैट हैकर (d) व्हाइट हैट हैकर

61. वायरस शब्द का सर्वप्रथम प्रयोग किसने किया था?
(a) वाट्सन (b) फ्रेड कोहेन
(c) माइकल एंजेलों (d) क्रीपर

62. वह गोपनीय कोड जो कुछ प्रोग्रामों में प्रविष्ट प्रतिबंधित करता है, कहलाता है?
(a) पासपोर्ट (b) एक्सेस कोड
(c) पासवर्ड (d) एंट्रीकोड

63. निम्न में से कौन-कम्प्यूटर वायरस का एक वैध फेज है?
(a) केवल प्रोपेगशन, एक्सक्यूटिंग
(b) केवल डोर्मेंट, प्रोपेगेशन, ट्रिगरिंग
(c) केवल डोर्मेंट, प्रोपेगेशन, ट्रिगरिंग, एक्सक्यूटिंग
(d) केवल ट्रिगरिंग एक्सक्यूटिंग

64. एंटी वायरस का उपयोग किया जाता है?
(a) फाइलें डिलीट करने के लिये
(b) इंस्टॉल प्रोग्राम हाटाने के लिये
(c) एक डिस्क को फ्रेग्मेंट करने के लिये
(d) इन्फेक्टेड फाइलें क्लीन करने के लिये

65. निम्नलिखित में से कौन-सा एंटीवायरस सॉफ्टवेयर है?
(a) Quick heal (b) K7
(c) Nortron (d) उपरोक्त सभी।

66. कम्प्यूटर में फैलने वाला वायरस है?
(a) ऐंट (b) हार्डवेयर
(c) कम्प्यूटर प्रोग्राम (d) सिस्टम सॉफ्टवेयर

67. एक जानबूझकर विघटनकारी सॉफ्टवेयर जो कम्प्यूटर से कम्प्टर तक फैलता है, उसे कहते है?
(a) वायरस (b) ई-मेल
(c) सर्च इंजन (d) चैट सॉफ्टवेयर

68. जब किसी वेबसाइट के ग्राहक नकली नेटवर्क यातायात के बाढ़ के कारण इसे एक्सेस करने में असमर्थ होते है तो इन्हें किस नाम से जाना जाता है?
(a) क्रेकिंग
(b) ट्रोजन हॉर्स
(c) डिनायल ऑफ सर्विस अटैक
(d) इनमें से कोई नहीं

69. सॉफ्टवेयर तथा नटवर्क की सुरक्षा कमियों को दूर करने के लिये उनका पता लगाने वाला हैकर कहलाता है?
(a) व्हाईट हैट (b) ब्लू हैट
(c) ब्लैक हैट (d) ग्रे हैट

70. निम्नलिखित में से कौन-सा प्रचलित एंटीवायरस सॉफ्टवेयर प्रोग्राम है?
(a) Nortan (b) Bit Defender
(c) McAfee (d) उपरोक्त सभी

71. निम्नलिखित में से कौन-सी साइबर अपराध की दो आवश्यक विशेषताएँ है?
(a) हार्डवेयर तथा सॉफ्टवेयर
(b) हैकर्स एवं क्रैकर्स
(c) अपराधी कम्प्यूटर दक्षता तथा कम्प्यूटर प्रौद्योगिकी की शिकार अनभिज्ञता।
(d) कार्यप्रणाली के रूप में कम्प्यूटर प्रौद्योगिक तथा पर्यावरण की अखण्डता।

72. वह कौन सा सॉफ्टवेयर है, जिसको कम्प्यूटर में इंस्टाल कर देने पर ऐसे कार्यक्रम जो बच्चों की मानसिकता पर बुरा प्रभाव डालते है, वे इंटरनेट पर नहीं आएगें?
(a) स्मार्ट डॉग (b) क्रोजर
(c) हैंड-सेक (d) इनमें से कोई नहीं

73. निम्नलिखित में से किसे 'Flow Control' के नाम से जाना जाता है?
(a) हैंड-सेक (b) स्मार्ट डॉग
(c) क्रोजर (d) पलाडियम

74. फ्राइडे थर्टीन्थ है-
(a) बूट सेक्टर वायरस (b) पॉलीमॉर्फिक वायरस
(c) फाइल वायरस (d) मल्टी पर्टाइट वायरस

75. सूचना या डाटा को गुप्त संदेशों में बदलने की क्रिया.... कहलाती है?
(a) Encryption (b) Decryption
(c) एक्सेस कंट्रोल (d) इनमें से कोई नहीं

76. अपराधियों द्वारा यूजर की पर्सनल इन्फार्मेशन प्राप्त करने चोरी करने के लिए छद्म रूप धारण करने और उनके रिसोर्स को एक्सेस करने का प्रयास कहलाता है?
(a) क्रिप्टोग्राफी (b) आइडेंटिटी थेप्ट
(c) पैच (d) पैकेट स्निफिंग

77. ऐसा सॉफ्टवेयर, जिसका उपयोग कम्प्यूटर वायरस को समाप्त करने के लिये किया जाता है?
(a) हैंड-सेक (b) पलाडियम
(c) क्रोजर (d) स्मार्टडॉग

78. निम्नलिखित में से किस प्रकार के साइबर अटैक के द्वारा आपको, चाही गयी वेबसाइट की जगह अन्य वेबसाइट पर ले जाया जाता है?
(a) सेशन हाईजैक (b) स्केअर वेयर
(c) क्रेकर (d) फिशिंग

79. एक व्यक्ति जो कम्प्यूटर को हैक करने के लिये मौजूद कम्प्यूटर कोड का उपयोग करता है, उसे क्या कहते है?
(a) स्क्रिप्ट किडीज (b) ट्रोजन हार्स
(c) स्पैम (d) वोर्म

80. वह गोपनीय कोड जो खुद प्रोग्रामों में प्रविष्ट प्रतिबंधीय करता है, कहलाता है?
(a) एक्सेस कोड (b) पासवर्ड
(c) पासपोर्ट (d) ब्लैक हैट्स हैकर

81. असुरक्षित Plugin का दूसरा नाम है?
(a) मालवेयर (b) हार्डवेयर
(c) सॉफ्टवेयर (d) फर्मवेयर

82. की-लॉगर उदाहरण है-
(a) स्पाइवेयर का (b) क्राइम वेयर का
(c) स्केअर वेयर का (d) ग्रेवेयर का

83. इंटरनेट और संबंद्ध तकनीकों का उपयोग लोगों को नुकसान पहुँचाने के लिये किया जाना कहलाता है?
(a) फ्लैम (b) साइबर बुलिंग
(c) स्पैम (d) साइबर वारफेयर

84. ऐसे प्रोग्राम जो दिखने में उपयोगी लगे लेकिन उनका प्रयोग नुकसान पहुंचाने के लिये किया जाता है क्या कहलाते है?
(a) आइडेंटिटी थेप्ट (b) साइबर बुलिंग
(c) ट्रोजन हार्स (d) मैलवेयर

85. ग्रेवेयर के अंतर्गत शामिल है-
(a) स्पाईवेयर (b) एडवेयर
(c) डायलर्स (d) उपरोक्त सभी

86. स्टक्सनेट की खोज किस वर्ष हुई?
(a) वर्ष 2007 (b) वर्ष 2008
(c) वर्ष 2009 (d) वर्ष 2010

87. साइबर सिक्योरिटी में DDOS का पूर्ण रूप क्या है?
(a) Distributed Denial of Service
(b) Digital Denial of Service
(c) Denial Digital of Service
(d) इनमें से कोई नहीं

88. वह सॉफ्टवेयर जो उपयोगकर्त्ता के ऑनलाइन होने पर बैनर या पॉपअप के रूप में बार-बार दिखाई देता है क्या कहलाता है?
(a) विंडो वेयर (b) एडवेयर
(c) पॉप-अप (d) इनमें से कोई नहीं

89. इंटरनेट पर किसी व्यक्ति के लिये लिखे हुए अपशब्द क्या कहलाते है?
(a) स्पैम (b) बुलिंग
(c) फ्लैम (d) इनमें से कोई नहीं

90. किसी प्रोग्राम या सिस्टम में रह जाने वाली गलती को क्या कहा जाता है?
(a) बग (b) डिबग
(c) फिशिंग (d) कुकीज

91. किसी प्रोग्राम में गलतियाँ पकड़ने की क्रिया कहलाती है?
(a) बग (b) डाटा डिडलिंग
(c) डिबग (d) फिशिंग

92. निम्नलिखित में से कौन-सा प्रॉक्सी सर्वर का उपयोग है?
(a) मालवेयर तथा वायरस पर नियंत्रण रखना।
(b) डाटा ट्रांसफर की गति को बढ़ाना।
(c) अंवाछित वेब पेज को प्रतिबंधित करना।
(d) उपरोक्त सभी

93. जब साइबर अपराधी बड़ी रकम बनाने के लिये कई बैंको खातों से छोटी-छोटी राशि चुराते है तो उसे क्या कहा जाता है?
(a) सलामी साइबर अटैक (b) साइबर बंबिग
(c) फिशिंग (d) साइबर बुलिंग

94. राष्ट्रीय साइबर क्राइम रिपोर्टिंग पोर्टल की शुरुआत किस मंत्रालय के अंतर्गत की गई?
(a) सूचना एवं प्रौद्योगिकी मंत्रालय
(b) गृह मंत्रालय
(c) रक्षा मंत्रालय
(d) महिला विकास मंत्रालय

95. सूचना प्रौद्योगिकी अधिनियम, 2000 में किस वर्ष संशोधन किया गया?
(a) वर्ष 2008 (b) वर्ष 2012
(c) वर्ष 2016 (d) वर्ष 2019

96. किसी व्यक्ति ने कम्प्यूटर चुराया है या उसका डाटा लीक किया गया तो उस पर साइबर अपराध की किस धारा के तहत् दण्ड का प्रावधान है?
(a) 66 अ (b) 66 ब
(c) 66 सी (d) 67 ए

97. निम्नलिखित में से कौन-सा एक प्रकार का मालवेयर है जिसे सॉफ्टवेयर सिस्टम में जानबूझ कर डाल दिया जाता है जो पूर्वनिर्धारित स्थितियाँ उत्पन्न होने पर दुराग्रहपूर्ण प्रकार्य शुरू कर देता है ?
(a) वॉर्म (b) ट्रोजन
(c) स्पाईवेयर (d) लॉजिक बम

NTA- NET June,2019

98. एक 'वायरस हॉक्स' वायरस की मिथ्या सूचना प्रदायी सचेतक ईमेल है। जब आपको निम्नानुसार एक 'वायरस हॉक्स' प्राप्त होता है तो उचित कार्रवाई क्या होगी ?

विषय : चेतावनी !
आपके कंप्यूटर में एक नए वायरस का पता चला है। अपने हार्ड डिस्क को तत्काल फॉर्मेट करें और सभी सॉफ्टवेयर को री-इंस्टॉल करें।

(a) इस ईमेल की अनदेखी करना
(b) प्रेषक को उत्तर देना
(c) अपने मित्रों को यह मेल अग्रेषित करना
(d) तत्काल अपना हार्ड डिस्क फॉर्मेट करना और सभी सॉफ्टवेयर को री-इंस्टॉल करना

99. एक नेटवर्क के किसी कंप्यूटर को किससे सुरक्षा प्रदान करने के लिये फॉयरवॉल्स का प्रयोग किया जाता है?
(a) आगजनी का हमला (b) प्राधिकृत हमला
(c) अप्राधिकृत हमला (d) आंतरिक हमला

100. निम्न में से कौन-सा इंटरनेट की सूचना सुरक्षा से संबंधित नहीं है?
(a) डेटा एंक्रिप्सन (b) वाटर मार्किंग
(c) डाटा हाइडिंग (d) इंफॉर्मेशन रिट्राइवल

उत्तरमाला

1.	c	2.	d	3.	a	4.	b	5.	d
6.	d	7.	a	8.	d	9.	d	10.	d
11.	b	12.	c	13.	a	14.	c	15.	c
16.	c	17.	b	18.	a	19.	c	20.	c
21.	b	22.	d	23.	d	24.	a	25.	b
26.	b	27.	d	28.	b	29.	a	30.	d
31.	b	32.	a	33.	b	34.	d	35.	c
36.	a	37.	b	38.	d	39.	c	40.	c
41.	b	42.	b	43.	c	44.	a	45.	b
46.	d	47.	b	48.	d	49.	d	50.	b
51.	a	52.	d	53.	d	54.	b	55.	a

56.	a	57.	a	58.	d	59.	b	60.	d
61.	b	62.	c	63.	c	64.	d	65.	d
66.	c	67.	a	68.	c	69.	a	70.	d
71.	c	72.	b	73.	a	74.	c	75.	a
76.	b	77.	d	78.	d	79.	a	80.	b
81.	a	82.	a	83.	b	84.	c	85.	d
86.	d	87.	a	88.	b	89.	c	90.	a
91.	c	92.	d	93.	a	94.	b	95.	a
96.	b	97	d	98	d	99	c	100	b

❑❑❑❑