

नई शिक्षा नीति के अनुसार

**2024**



TM

विश्वविद्यालय प्रकाशन (नति.)

स्वास्तिभर  
द्वारा प्रकाशित

**20 प्रश्न**

( परीक्षेपूर्वकी महत्वपूर्ण मॉडल प्रश्नोत्तर )

डिजिटल जागरूकता

साइबर सुरक्षा

आधार पाठ्यक्रम



श्रीविष वर्ष

नवीन पाठ्यक्रम

[अधिकतम अंक - 50 अंक]

डिजिटल जागरूकता - साइबर सुरक्षा

इकाई-1.

कम्प्यूटर और वेब- प्रौद्योगिकी का अवलोकन, साइबरसेस का आर्किटेक्चर, वर्ल्ड वाइड वेब, इंटरनेट का आगमन, डेटा ट्रांसफर और गवर्नेंस के लिए इंटरनेट इंफ्रास्ट्रक्चर, इंटरनेट समाज।

इंटरनेट का उपयोग- वेब ब्राउज़र, सर्व इंजन और चैटबॉट्स। वेबसाइट और पोर्टल, ई-मेल के बीच अन्तर, ई-मेल खंता खोलना, ई-मेल भेजना और प्राप्त करना, कॉन्फ़िग्यूर और फ़ोल्डर का प्रबंधन।

कम्प्यूटर सुरक्षा- मुद्दे और सुरक्षा, फायरवॉल और एंटीवायरस, सुरक्षित ऑनलाइन लेनदेन करना। इंटरनेट सुरक्षा और डिजिटल सुरक्षा। डिजिटल संसाधनों का नैतिक उपयोग, ऑनलाइन आम सुरक्षा के उपाय।

### इकाई-2.

डिजिटल भुगतान और ई-कॉमर्स- इंटरनेट बैंकिंग, नेशनल इलेक्ट्रॉनिक फंड ट्रांसफर (एनईएफटी), रीयल टाइम ग्रॉस सेंटलमेंट (आरटीजीएस), तत्काल भुगतान सेवा (आईएमपीएस) डिजिटल वित्तीय उपकरण, (वन टाइम पासवर्ड), क्यूआर (क्विक रिस्पॉन्स) कोड, यूपीआई (यूनिफाइड पैमेंट इंटरफेस), एड्डीएस (आधार सक्षम भुगतान प्रणाली) को समझना, USSD (अनस्ट्रक्चर्ड सलीमेट्री सर्विस डेटा), कार्ड (क्रेडिट/डेबिट), ई-वॉलेट, POS (प्राइंट ऑफ सेल)

ई-कॉमर्स की परिभाषा- ई-कॉमर्स के मुख्य घटक, ई-कॉमर्स सुरक्षा के तत्व, ई-कॉमर्स सम्बन्धी खतरे, ई-कॉमर्स सुरक्षा सर्वोत्तम प्रथाएँ, ऑनलाइन बिल भुगतान। डिजिटल भुगतान से सम्बन्धित आम धोखाधड़ी और निवारक उपाय। आरबीआई के दिशा-निर्देश और भुगतान नियमन अधिनियम, 2007 के प्रावधान।

### इकाई-3.

ई-गवर्नेंस सर्विस- रेलवे आरक्षण, पासपोर्ट, ई-अस्पताल जैसी ई-गवर्नेंस सेवाओं का अवलोकन, 'उमंग ऐप' का उपयोग करके मोबाइल पर विभिन्न ई-गवर्नेंस सेवाओं तक पहुँचना। भारत सरकार के पोर्टल (<https://www.mysgov.in/>) की सेवाओं और संसाधनों की खोज करना।

डिजी-लॉकर- डिजिटलॉकर के बारे में, डिजिटलॉकर की विशेषताएँ और लाभ, डिजिटलॉकर पर विभिन्न प्रमाणपत्रों और मार्कशीट को पंजीकृत करना, एक्सेस करना और प्राप्त करना।

अकादमिक बैंक ऑफ़ क्रेडिट (एबीसी)- एबीसी का विवरण, एबीसी की विशेषताएँ और लाभ, पंजीकरण, पढ़ाव, अकादमिक क्रेडिट प्राप्त करना और साक्षात करना।

ऑनलाइन शिक्षण संसाधनों की खोज- SWAYAM Central (<https://swayam.gov.in/>) और ई-पाठशाला (<https://epathshala.nic.in/>) के माध्यम से ऑनलाइन शिक्षण।

### इकाई-4.

साइबर सुरक्षा का परिचय- साइबरसेस का विनियमन, साइबर सुरक्षा की अवधारणा, साइबर सुरक्षा के मुद्दे और चुनौतियाँ।

साइबर अपराध और उल्लंघनों की परिभाषा, कम्प्यूटर और मोबाइल को लक्षित साइबर अपराध, महिलाओं और बच्चों के खिलाफ साइबर अपराध, साइबर बुलिंग। विस्तीय

धोखाधड़ी, सोशल इंजीनियरिंग हमले, मैलवेयर और रैसमवेयर हमले, जीरो डे और जीरो क्लिक अटैक।

साइबर अपराधियों की कार्यप्रणाली, साइबर अपराधों की रिपोर्टिंग, उपचारालोक और शपन उपाय, साइबर अपराध का कानूनी परिप्रेक्ष्य, आईटी अधिनियम 2000 और इसके संशोधन, भारत में साइबर अपराध और साइबर सुरक्षा से निपटने वाले संगठन, केस स्टडी।

### इकाई-5.

सोशल मीडिया अवलोकन और सुरक्षा- सोशल नेटवर्क का परिचय, सोशल मीडिया के प्रकार, सोशल मीडिया लोटेफॉर्म, सोशल मीडिया मोनिटरिंग, हैशटैग, वायरल कंटेंट, सोशल मीडिया मार्केटिंग, सोशल मीडिया प्राइवेंसी, ऑनलाइन सोशल नेटवर्क में चुनौतियाँ, अवसर और चुकसान, सोशल मीडिया से संबंधित सुरक्षा मुद्दे, फ़्लैगिंग और अनुपयुक्त सामग्री की रिपोर्टिंग, अनुपयुक्त सामग्री पोस्ट करने के संबंध में कानून, सोशल मीडिया के उपयोग के लिए प्रथाएँ, केस स्टडी।

### अनुशंसित मूल्यांकन विधियाँ

वस्तुनिष्ठ प्रश्न

50 × 1 = 50 अंक

□ ध्यान दें: 'डिजिटल जागरूकता - साइबर सुरक्षा' विषय आधार पाठ्यक्रम में रखा गया है। नई शिक्षा नीति के अन्तर्गत इस विषय पर परीक्षा में सभी वस्तुनिष्ठ प्रश्न ही पूरे जायेंगे। इस पुस्तक में अनेक वस्तुनिष्ठ प्रश्नों के साथ ही सम्बन्धित पाठ्यक्रम के प्रत्येक टॉपिक पर कुछ दीर्घ एवं लघुउत्तरीय प्रश्नों का भी दिष्ट गये हैं। इनके अद्यतन से आप इस विषय को भली-भाँति समझ सकेंगे और किसी भी वस्तुनिष्ठ प्रश्न का उत्तर देने की स्वयं क्षमता विकसित कर सकेंगे।

### कृपया ध्यान दें

विश्वविद्यालय प्रकाशन, ग्वालियर द्वारा प्रकाशित बी.ए., बी.कॉम. तथा बी.एस.-सी. की '20 प्रश्न' पुस्तकें खरीदते समय प्रत्येक पेज पर 2024 तथा देखकर सही तथा असली पुस्तक ही खरीदें। ये बी.ए., बी.कॉम. तथा बी.एस.-सी. कक्षाओं के अंग्रेजी माध्यम में भी प्रकाशित हैं।

# द्वितीय जगत्कला

## साइबर सुरक्षा

(आधार पाठ्यक्रम)

### इकाई-1

## कम्प्यूटर और वेब, इंटरनेट का उपयोग, कम्प्यूटर सुरक्षा

दीर्घ एवं लघु उत्तरीय प्रश्न-

प्रश्न-1. Internet से आप क्या समझते हैं? इसकी Services को समझाइये।

अथवा  
इंटरनेट के आगमन पर संक्षिप्त टिप्पणी लिखिए।

अथवा  
निम्न को संक्षेप में समझाइए-

(1) इंटरनेट सेवाएँ (2) इंटरनेट का उपयोग

उत्तर- Internet : इंटरनेट 'इंटरनेशनल नेटवर्क' का संक्षिप्त रूप है। इसे डॉ. विन्टन जी सर्फ ने विकसित किया था। यह विश्वव्यापी कम्प्यूटर नेटवर्क है, जिसमें सभी प्रकार की सूचनायें संग्रहित की जाती हैं। दुनियाँ के विभिन्न स्थानों पर स्थापित टेलीफोन लाईन्स अथवा उपग्रह की सहायता से एक-दूसरे के साथ जुड़े computers का नेटवर्क ही Internet कहलाता है।

Internet system में सभी सूचनायें जिस computer में store होती हैं, उसे web server कहा जाता है, कभी-कभी इसे www (World-Wide-Web) के नाम से जाना जाता है। Internet के द्वारा प्रयोक्ता को कई महत्वपूर्ण services प्रदान की जाती हैं, जो निम्नलिखित हैं-

(1) E-mail (Electronic-Mail) - E-mail computer के द्वारा भेजी जाने वाली Electronic डाक सेवा का संक्षिप्त रूप है। इसके द्वारा एक व्यक्ति विश्व के किसी भी कोने में दूसरे व्यक्ति तक संदेश पहुँचा सकता है। यह सामान्य डाक सेवा की तुलना में अत्यधिक सस्ती तथा तीव्र होती है।

(2) FTP (File Transfer Protocol) - यह protocol एक computer network से दूसरे computer network पर file को भेजने का कार्य करता है। FTP connect कनेक्शन दो प्रकार के होते हैं-

(i) Anonymous (ii) Non-Anonymous

यदि आप किसी Anonymous services से connect हैं तो आपको login के समय user name के रूप में Anonymous तथा password के रूप में 'E-mail Address' ईसर्ट करना होगा जबकि Non-anonymous FTP server में

2024

द्वितीय जगत्कला - साइबर सुरक्षा

5

आपको एक व्यक्तिगत user name तथा password दिया गया होता है। File transfer दो प्रकार के हो सकते हैं। ASCII और Binary। ASCII का प्रयोग केवल text को transfer कराने के लिये किया जाता है। जबकि Binary का प्रयोग text के अतिरिक्त कुछ भी transfer करवाने के लिये किया जाता है।

(3) गोफर (Gopher) - यह एक यूजर फ्रेंडली इन्टरफेस प्रदान करता है। गोफर के माध्यम से कोई यूजर Internet पर सूचनाओं को प्राप्त कर सकता है। गोफर वांछित सूचनाओं को search करके सामने ला देता है। इसके अलावा गोफर कई Internet services को आपस में जोड़ने में भी सहायक होता है।

(4) Telnet - Telnet protocol यूजर को Remote computer से संयोजन करने में सहायक होता है। Telnet के माध्यम से आप विश्वभर के पुस्तकालयों, शैक्षणिक संस्थानों तथा अन्य सार्वजनिक सेवाओं का प्रयोग कर सकते हैं। www आपको Telnet के द्वारा वेब साइट एक्सेस करने की तथा FTP के द्वारा फाइल Transfer करने की सुविधा देता है।

(5) Use net - यूजनेट एक ऐसा नेटवर्क है जो किसी यूजर user को विभिन्न समूहों से सलाह करने में सहायता प्रदान करता है। यह विभिन्न News group का एक ऐसा समूह है जो सूचनाओं के विशेष क्षेत्र को कवर करता है। उदाहरण के लिए यदि कोई user sports के बारे में जानना चाहता है तो यूजनेट काजो समूह sports को कवर करता है, उसे sports के बारे में जानकारी प्रदान करेगा।

(6) www (World wide-web) - www एक प्रकार का डाटाबेस है जो पूरे विश्व में फैला हुआ है। यूजर इसी के माध्यम से सूचनाओं का आदान-प्रदान करता है। इसे सन् 1989 में टिम बर्नर ली द्वारा जेनेवा, स्विट्जरलैण्ड में स्थापित किया गया था। किसी भी www सिस्टम में एक computer निश्चित तौर पर होता है, जिसे हम web server कहते हैं। user को दिखाई जाने वाली Information को इन वेब सर्विस में वेब पेज के रूप में रखा जाता है। इन webpages को कई तरह के प्रोग्राम या Tools का प्रयोग करके तैयार किया जा सकता है। इन Tools में सर्वाधिक प्रचलित भाषा HTML (Hyper Text Markup Language) है। इन वेब पेज को वेब ब्राउजर नामक यूपैरिस्की के द्वारा देखा जाता है। वेब ब्राउजर एक प्रोग्राम होता है जो world wide web को एक्सेस करना आसान बना देता है। Netscape Navigator, Microsoft, Internet Explorer तथा Mosaic तीन प्रचलित वेब ब्राउजर के उदाहरण हैं।

(7) आर्ची (Archie) - आर्ची एक ऐसा system है जो FTP server में store files को search करता है। आर्ची आमतौर पर servers का एक ऐसा संग्रह है जिसके प्रत्येक server में जानकारी रहती है कि कौन-सी file किस server में है तथा यह किस विषय से सम्बन्धित है।

(8) वेरोनिका (Veronica) - यह एक ऐसा प्रोग्राम है जो गोफर के माध्यम से कार्य करता है। इसके माध्यम से शीघ्रतापूर्वक आवश्यक सूचनाएँ प्राप्त की जा सकती

है। यूजर गोफर सर्वर और वेरोनिका server को एक्सेस करके किसी Database तक आसानी से पहुँच सकता है।

(9) **Wide Area Information System (WAIS)**— यह एक प्रकार का search इंजन है जो कि यूजर द्वारा मांगी गयी सूचना file को server से ढूँढकर यूजर को प्रदान करता है। WAIS उस Address के बारे में बताता है जहाँ file उपलब्ध है। यदि user द्वारा मांगी गयी FILE किसी एक WAIS सर्वर पर नहीं मिलती तब यह WAIS सर्वर किसी अन्य WAIS सर्वर की सहायता लेता है।

(10) **Internet Relay Chat— IRC (Internet Relay Chat)** को सामान्य Language में chat के रूप में जाना जाता है। इसका प्रयोग user एक-दूसरे से online संवाद स्थापित करने में करते हैं। एक user दूसरे side के user से संवाद text या voice के रूप में स्थापित करते हैं।

प्रश्न-2. **World Wide Web क्या है? www का इतिहास समझाइये।**

अथवा

वर्ल्ड वाइड वेब क्या है?

उत्तर— **World Wide Web (www)** : वर्ल्ड वाइड वेब सर्वर की एक शृंखला है जो हायपर टेक्स्ट के माध्यम से आपस में संयोजित होता है। हायपर text सूचना को प्रस्तुत करने का वैसा तरीका है, जिससे कुछ खास आयटम डाउनलोड होते हैं। उस डाउनलोड text को चुनने पर आप उससे सम्बन्धित विस्तृत जानकारी प्राप्त करते हैं जो आपको एक document से दूसरे document में जाने में सहायता करता है तथा जो इंटरनेट पर किसी भी सर्वर में उपलब्ध हो सकते हैं। वेब को विशेष बनाने में प्रमुख यह है आप इंटरनेट पर इनके माध्यम से कहीं भी भ्रमण कर सकते हैं। जैसे आप किसी एक टी.पी. साइट, गोफर, Veronica या किसी अन्य दस्तावेज में डाल सकते हैं। web को भ्रमण करने के लिए आप ब्राउजर सॉफ्टवेयर जैसे (Mosaic), मौजिक नेटस्केप नेवीगेटर (Netscape Navigator) या इंटरनेट एक्सप्लोरर का प्रयोग करते हैं। वेब हायपर टेक्स्ट के साथ उच्च स्तरीय ग्राफिक्स का उत्तम प्रयोग करता है। FTP तथा Telnet जैसे Text पर आधारित सेवाओं के साथ ही web में अच्छी मात्रा में ग्राफिक्स का प्रयोग होता है। आज हम वेब पेजों में चित्र तथा ध्वनि का समावेश आसानी से बहुतायत में देख सकते हैं।

वेब का इतिहास (History of web)— वर्ल्ड वाइड वेब के आविष्कार से पहले इंटरनेट का प्रयोग बहुत ही कठिन था। इस पर उपलब्ध सूचनाओं को खोजना तथा इसका प्रयोग में लाना और कठिन था। इंटरनेट पर उपलब्ध files को ढूँढना तथा उसे डाउनलोड करने के लिए यूनिक्स स्कालर (shaller) तथा विभिन्न tools की आवश्यकता पड़ती थी।

Com में उनके कार्य के लिए हमेशा इंटरनेट की आवश्यकता पड़ती थी। इंटरनेट का प्रयोग वह शोध, तथा अपने शोधकर्ता मित्रों के साथ सम्पर्क करने में करते थे, उन्हें इंटरनेट को उपयोग किये जाने में आने वाली कठिनाइयों ने इस बात के लिए उनके अन्दर ऐसी "गली का विकास करने पर प्रेरित किया जो उनके काम को आसान बना सके। 1989 में, होने world wide web के विकास के लिए सर्न के इलेक्ट्रॉनिक्स एंड computing and

for physics विभाग को एक प्रस्ताव दिया लेकिन इस प्रस्ताव को बहुत अधिक स्वीकृति नहीं मिली फिर जब दोबारा उन्होंने अपने मित्र रॉबर्ट कैलियो के साथ, प्रस्ताव की अस्वीकृति के कारण पर विचार करने के बाद दुबारा प्रस्तुत किया हो तो उसे स्वीकृति मिल गयी।

प्रश्न-3. **ISP की अवधारणा को समझाइये।**

उत्तर— **Internet Service Provider (ISP)**— वह कंपनी जो Internet सुविधा प्रदान करती है। इंटरनेट सेवा प्रदाता (इंटरनेट सर्विस प्रोवाइडर) कहलाती है। किसी अन्य कंपनी की तरह ही इंटरनेट सेवा प्रदाता अपनी सेवाओं के लिए प्रयोक्ता से पैसा लेती है। सामान्यतः यह शुल्क राशि इंटरनेट सेवा प्रदाता द्वारा दो प्रकार से ली जाती है—

(i) इंटरनेट प्रयोग करने के लिये, (ii) इंटरनेट कनेक्शन देने के लिये।

इंटरनेट पर किए जाने वाले कार्य के बदले प्रत्येक प्रयोक्ता अपने हिस्से का भुगतान करता है। नेटवर्क एक साथ संयोजित होते हैं तथा कैसे आपस में जोड़ें यह निर्णय करते हैं। विद्यालय या विश्वविद्यालय अथवा एक कंपनी अपने संयोजन का भुगतान क्षेत्रीय नेटवर्क को करती है तथा वह क्षेत्रीय नेटवर्क इस एक्सेस के लिए राष्ट्रीय प्रदाता को भुगतान करता है।

ISP के सभी ग्राहकों को इंटरनेट प्रयोग के बदले में शुल्क राशि का भुगतान करना ही होता है। अधिकतर मामलों में आई.एस.पी. ग्राहक पर एक निश्चित मासिक शुल्क लगाती है। इसमें कस्टमर को समयावधि, संचार की दूरी तथा डाटा डाउनलोड या अपडेट की मात्रा के लिए स्वतंत्रता दी जाती है। प्रयोग शुल्क के बदले आई.एस.पी. ग्राहक के computer से गंतव्य स्थान तक अन्य स्थानों से ग्राहक के computer तक डाटा को ले जाने और लाने पर सहमत होता है।

ISP एक व्यावसायिक प्रतिष्ठान (organization) से एक व्यक्ति की तुलना में अधिक शुल्क लेते हैं क्योंकि एक व्यक्तिगत प्रयोक्ता (user) इंटरनेट का प्रयोग कम्प्यूटर पर कभी-कभी करता है जबकि व्यावसायिक Organization में Internet का प्रयोग कई लोग करते हैं, वहाँ प्रतिदिन डाटा स्थानान्तरण की मात्रा अधिक होती है। इसके अलावा इंटरनेट का शुल्क इस बात पर भी निर्भर करता है कि उस ग्राहक के पास कौन-सा संयोजन है? ऐसे ग्राहक जिनके पास बड़ी मात्रा में Data को स्थानान्तरित करने के योग्य संयोजन है, को कम क्षमता के संयोजन वाले ग्राहकों की तुलना में अधिक शुल्क देना पड़ता है। अब तक अन्य प्रकार का संयोजन शुल्क की वैसे ग्राहकों के लिए निर्धारित होता है जिनके पास अनेक site तथा ISP के बीच अलग से एक समर्पित (dedicated) संयोजन होता है। BSNL, VSNL, Reliance, Sify, Bhatti भारत के कुछ Internet providers के नाम हैं।

प्रश्न-4. **E-mail प्रोटोकॉल की व्याख्या कीजिये।**

उत्तर— **E-mail Protocols** की व्याख्या : User E-mail भेजने के लिए अलग-अलग प्रकार के system का प्रयोग करते हैं। समान पद्धति वाले निर्देशों के समूह को प्रोटोकॉल (Protocols) कहते हैं। इलेक्ट्रॉनिक मेल के आवागमन में प्रयुक्त होने वाले protocols निम्नलिखित हैं—

(1) **S.M.T.P. (Simple Mail Transfer Protocol)**— System में E-mail सुविधा को क्रियान्वित करने के लिए प्रयोग किया जाने वाला यह मुख्य प्रोटोकॉल

है। इस प्रोटोकॉल की सहायता से ही mail एक system से दूसरे system तक पहुँचती है। mail को पहुँचाने का विवरण इस प्रोटोकॉल की सहायता से पूरा किया जाता है। S.M.T.P. प्रोटोकॉल TCP/IP प्रोटोकॉल का एक सदस्य है। यह E-mail प्रोसेस में ASCII केक्टर सेट का उपयोग करता है। इंटरनेट पर हजारों-लाखों सिस्टम S.M.T.P. की सहायता से E-mail भेजते व प्राप्त करते हैं।

(2) पोस्ट ऑफिस प्रोटोकॉल (Post Office Protocol) - Post office प्रोटोकॉल का प्रयोग mail box को Access करने के लिए किया जाता है। इसका प्रयोग E-mail को डाउनलोड करने के लिए भी किया जाता है। मुख्य रूप से इस प्रोटोकॉल के निम्नलिखित कार्य हैं-

- Remote mail box में log-in करने के लिए।
- Remote mail box से log-out करने के लिए।
- Remote mail box से message डिलीट करने के लिए।
- Remote mail box से message लेने के लिए।

(3) X-400 - X-400 प्रोटोकॉल का प्रयोग E-mail (connectivity) के लिए किया जाता है। इसका निर्माण मुख्य रूप से Binary file transfer जैसी समस्याओं का समाधान करने के लिए किया गया था। इस प्रोटोकॉल का कार्य असमान कम्प्यूटर प्रणाली के मध्य संदेश प्रसारण के लिए प्रत्येक कम्प्यूटर के मध्य message प्रसारण के लिए प्रत्येक कम्प्यूटर के इलेक्ट्रॉनिक मेल system के बीच एक नेटवर्क की आवश्यकता को पूरा करता है।

(4) M.I.M.E. (Multipurpose Internet Mail Extension) - M.I.M.E. एक ऐसा प्रोटोकॉल है जो असमान character sets वाले भाषाओं में Text को Interchange करता है। इसके साथ ही यह कई भिन्न computer systems के बीच मल्टीमीडिया E-mails को भी स्थानान्तरित करता है। S.M.T.P. के द्वारा केवल Text files ही भेजी जा सकती है। जबकि MIME प्रोटोकॉल के द्वारा Formatted Documents, Photos, Sound files तथा Video files इत्यादि को भी भेजा जा सकता है।

(5) U.U.C.P. (Unix to unix copy) - यह प्रोटोकॉल unix ऑपरेटिंग सिस्टम में प्रयोग किया जाता है। Unix ऑपरेटिंग सिस्टम में यह प्रोटोकॉल एक Host से दूसरे Host पर files को transfer करता है। यह यूनिक्स नेटवर्किंग में E-mail तथा यूजनेट के लिए संचार माध्यम प्रदान करता है।

(6) IMAP-4 (Interactive Mail/Access Protocol) - यह प्रोटोकॉल उन user की सहायता के लिए Design किया गया है जिन्हें विभिन्न प्रकार के कम्प्यूटर्स को प्रयोग करने की जरूरत होती है, जैसे Laptop कम्प्यूटर। इसे किसी भी Machine से Access किया जा सकता है। इस protocol में user की machine को server में एक्सेस करने की आवश्यकता होती है।

प्रश्न-5. Internet तथा Intranet में क्या अन्तर है? समझाइये।  
उत्तर - Internet तथा Intranet दोनों ही एक प्रकार के Network का नाम है। इंटरनेट और इंटरनेट में निम्नलिखित अंतर हैं-

S.No.	Internet	Intranet
(1)	Internet लोकल एरिया नेटवर्क (LAN) व वाइड एरिया नेटवर्क (WAN) दोनों को स्थापित कर सकता है।	Intranet केवल लोकल एरिया नेटवर्क (LAN) को जोड़ता है।
(2)	यह मानकों (Protocol) का प्रयोग विश्वव्यापी करता है।	इंटरनेट इंटरनेट मानकों का प्रयोग किसी निश्चित जगह या संगठन में करता है।
(3)	Internet मेल सर्वर व सूचनाओं का प्रयोग सार्वजनिक न्यूज ग्रुप बनाने में करता है।	इंटरनेट मेल सर्वर व सूचनाओं का प्रयोग निजी न्यूज ग्रुप बनाने में करता है।
(4)	किसी इंटरनेट साइट को बिना इंटरनेट साइट के बना सकते हैं।	इंटरनेट साइट को बिना इंटरनेट साइट की सहायता के नहीं बनाया जा सकता है।
(5)	इंटरनेट का प्रयोग करने वाले user की संख्या अधिक होती है।	इंटरनेट प्रयोग करने वाले users की संख्या इंटरनेट की तुलना में कम होती है।
(6)	इंटरनेट से जुड़ा हार्डवेयर इंटरनेट से जुड़े Hardware की तुलना में बहुत अधिक क्षमता वाला होता है।	इससे जुड़ा Hardware इंटरनेट से जुड़े Hardware की तुलना में कम क्षमता वाला होता है।

प्रश्न-6. Web based तथा Pop based E-mail में अन्तर बताइये।

उत्तर - Web based E-mail - वेब आधारित E-mail द्वारा हम E-mail प्रदाता की साइट पर पहुँचने के लिए Internet Browser का प्रयोग कर सकते हैं और इसके बाद user name तथा password की सहायता से Login कर सकते हैं। E-mail provider हमारे सभी संदेशों को हमारे लिए संग्रहित करके रखता है। अधिकांश विशालकाय free E-mail provider (प्रदाता) वेब बेस्ड E-mail व्यवसाय के अन्तर्गत कार्य करते हैं। क्योंकि इस प्रकार की service सरलता से कार्यान्वित हो जाती है तथा यह साइट पर visitors को बार-बार आने के लिए invite करता है। कई सेवाएँ अतिरिक्त कार्य जैसे- ऑनलाइन-वर्तनी जाँच, Personal Address book, Index आदि को भी करती है।

Pop based E-mail Services - पॉप आधारित ई-mail services हमारे E-mail को किसी Remote server पर store करती है। हम इस server से किसी भी समय जुड़ सकते हैं तथा अपने E-mail को पसंदा E-mail software पैकेज में डाउनलोड कर

सकते हैं। साधारणतः Pop E-mail के साथ अपने-अपने स्थानीय कम्प्यूटर पर एक बार में ही सभी नए संदेशों को डाउनलोड कर सकते हैं।

Pop based (Pop) mail service हमारे आने वाले messages को तब तक server पर store रखता है, जब तक हम इसे store करने के लिए तैयार नहीं हो जाते, इन्हें E-mail Download software जैसे- युडोरा (Eudora) आउटलुक आदि की सहायता से Download कर सकते हैं। एक बार जब हम message को Download कर लेते हैं तो वे अधिकांश इंटरनेट सेवा प्रदाता (ISP) में Pop-mail ही उपलब्ध रखता है। इसलिए हमारे पास पहले से ही संभवतः कम से कम एक एक Pop-mail एकाउंट होना चाहिए।

**प्रश्न-7. Portals पर विस्तृत निबन्ध लिखिये।**

**उत्तर-7. Portals :** यह एक इलेक्ट्रॉनिक पोर्टल (Portal) होता है। वह वेब साइट जो हमें सामान की खरीद-बिक्री से सम्बन्धित जानकारी या E-commerce की सुविधा प्रदान करती है, E-portal या portal कहलाती है। जैसे- Yahoo.com एक पोर्टल है जो E-mail, Chat, News, Advertisement आदि की सुविधा देती है। इसके अलावा हवाई यात्रा के लिए आरक्षण व किसी वस्तु की नीलामी में भागीदारी तक की सुविधा देती है। E-portal के माध्यम से कोई भी यूजर घर बैठे कुछ भी खरीद व बेच सकता है। आजकल कई कम्पनियों की websites इस concept को अपना रही हैं। इस तरीके के अपनाने के कारण किसी यूजर को कुछ खरीदने व बिक्री करने के लिए गए अन्य खर्चों से मुक्तकारा मिल जाता है। उदाहरण के लिए यदि कोई व्यक्ति कोई वाहन खरीदना चाहता है, तो E-portals की सहायता से वह अपना वाहन घर बैठे खरीद सकता है, इसके लिए उसे केवल वेब साइट पर लिखी प्रविष्टियाँ भरनी होंगी, व कम्पनी को अपना Address देना होगा ताकि वह अपने ऐजेंट के माध्यम से आपको वाहन उपलब्ध करा सके।

**प्रश्न-8. निःशुल्क E-mail services को विस्तार से समझाइये।**

**उत्तर- आज इंटरनेट पर E-mail सेवार्णु प्रदान करने वाली कई कंपनियाँ उपलब्ध हैं। सभी साइट प्रायः दो प्रकार की services प्रदान करती हैं-**

(1) निःशुल्क, (2) शुल्क सहित

**निःशुल्क E-mail services :** निःशुल्क E-mail सेवा यद्यपि सुविधाओं के दृष्टिकोण से सीमित होते हैं यह शुल्क न होने के कारण अधिक लोकप्रिय है। इनमें से कुछ नाम निम्नलिखित हैं-

- |                     |                        |
|---------------------|------------------------|
| (1) www.yahoo.com   | (2) www.rediffmail.com |
| (3) www.hotmail.com | (4) www.indiatimes.com |
| (5) www.sify.com    | (6) www.google.com     |

युक्त E-mail सेवा प्रदान करने का मुख्य उद्देश्य, यूजर से विभिन्न जानकारी प्राप्त करना है, जिससे उन Information को एकत्र करके एक Database तैयार कर सके। इस Database का उपयोग विभिन्न कम्पनियाँ द्वारा अपने निर्मित सामानों, सेवाओं को बेचने में किया जाता है। इसके अलावा free E-mail services देकर यह कम्पनियाँ अपना प्रचार करती हैं।

**प्रश्न-9. Chatting क्या है ? इसके प्रकार बताइये।**

**उत्तर- Chatting :** Chat का अर्थ सामान्यतः बातचीत करना होता है। जिस प्रकार हम अपने-सामने खड़े रहकर या टेलीफोन पर बातें करते हैं उसी प्रकार इंटरनेट पर चैटिंग की परिकल्पना है। इंटरनेट पर chat कई रूप में उपलब्ध है, जिसमें दो प्रमुख एवं प्रचलित हैं-

(1) Text chatting, (2) Voice chatting

(1) **Text chatting-** Text chatting में keyboard के द्वारा संदेश Input किए जाते हैं तथा दूसरी तरफ बैठा व्यक्ति हमारे प्रेषित message को पढ़ता है तथा इसका उत्तर इसी form और process के द्वारा देता है। हम एक या एक से अधिक व्यक्तियों के साथ chat कर सकते हैं। चैट पूरी तरह से इंटर एक्टिव है तथा इसमें तत्काल message प्रेषित किया जाता है या प्राप्त होता है। इसके लिये दोनों तरफ के व्यक्तियों का Online होना आवश्यक है। Text chatting के लिए कई website उपलब्ध हैं, जैसे-

- |                       |                   |
|-----------------------|-------------------|
| (i) www.yahoo.com     | (ii) www.sify.com |
| (iii) www.hotmail.com |                   |

(2) **Voice chatting-** जिस प्रकार टेलीफोन से अपने मित्रों तथा रिश्तेदारों के साथ बातचीत करते हैं ठीक उसी प्रकार voice chatting के द्वारा हम इंटरनेट पर किसी भी व्यक्ति से बात कर सकते हैं। बॉर्डस chat टेलीफोन की गुलना में सस्ती सेवा है। इसमें दूरी के आधार पर शुल्क नहीं देना होता है। voice chat के माध्यम से हम एक समय में केवल एक ही व्यक्ति के साथ सम्पर्क बना सकते हैं, परन्तु यदि हमारे पास full duplex sound card है तो हम दो व्यक्तियों के साथ एक साथ बात कर सकते हैं। इसके लिए हमारे पास एक माइक्रोफोन, एक स्पीकर तथा इसके लिए प्रयोग होने वाला विशेष प्रोग्राम होना चाहिए। इंटरनेट पर इंटरनेट फोन नाम का शैयरवेयर www.voicemail.com पर उपलब्ध है, जिसका प्रयोग voice chatting software के रूप में कर सकते हैं।

**प्रश्न-10. निम्न को समझाइये-**

(अ) URL (ब) Remote Logging

**उत्तर-(अ) URL (Uniform Resource Locator)- वर्ल्ड वाइड वेब से सवधि अन्य सर्वर पर फाइलों के स्थान को बताने के लिए यूनिफार्म रिसोर्स लोकेटर (Uniform Resource Locator) का प्रयोग करते हैं। URL में एक्सेस किए जाने वाले संसाधन के प्रकार (जैसे- वेब, गोफर, F.T.P.), सर्वर का पता (Address), तथा फाइल का स्थान (Location) होता है, इसका Syntax इस प्रकार है-**

**स्क्रीम : // होस्ट डोमेन [ : पोर्ट ]/पाथ/फाइल नेम**

जहाँ स्क्रीम (Scheme) से तात्पर्य है-

फाइल (file) - स्थानीय सिस्टम का फाइल

एफ.टी.पी. (FTP) - बेनाम FTP सर्वर का फाइल

एच.टी.टी.पी. (http) - वर्ल्ड वाइड वेब सर्वर का फाइल

गोफर (Gopher) - गोफर सर्वर का फाइल

वायस (WAIS) - वायस (WAIS) सर्वर का फाइल

न्यूज़ (News) - यूजनेट का एक न्यूज़ग्रुप टेलनेट (Telnet) - टेलनेट सेवा के साथ संयोजन

इसके द्वारा Port Number सामान्यतः समाप्त कर दिए जाते हैं।

(ब) दूरस्थ लॉग इन (Remote Login) - इंटरनेट रिमोट लॉग यह सेवा उपलब्ध कराता है, जो किसी user को दूरस्थ time-sharing कम्प्यूटर सिस्टम को इस प्रकार अभिभय करने में समर्थ बनाता है, जैसे प्रयोक्ता का की-बोर्ड (Key-Board) और मॉनीटर प्रत्यक्षतः दूरस्थ कम्प्यूटर से जुड़े हों। सेवा का उपयोग करने के लिए, एक User Local Computer पर एक application प्रोग्राम का आग्रह कराता है। एक Remote computer का नाम निर्देशित कराता है। स्थानीय एप्लीकेशन प्रोग्राम एक क्लाइंट बन जाता है जो इंटरनेट का प्रयोग दूरस्थ कम्प्यूटर से जोड़ने के लिए होता है। एक बार connection स्थापित हो जाने पर Remote computer user के Display को takeover कर लेता है और इन Login तथा password देने का आग्रह करता है जैसे ही जैसे यह प्रत्यक्ष तौर पर जुड़ने वाले टर्मिनल के साथ करता है।

प्रश्न-11. VSAT पर संक्षिप्त टिप्पणी लिखिये।

उत्तर- Very Small Aperture Terminal (VSAT) : VSAT वैरी स्मॉल अपचर टर्मिनल (Very small Aperture Terminal) का संक्षिप्त रूप है। इसको एक दुष्टिमान भू-स्टेशन के रूप में वर्णन किया जा सकता है जो जियो सिन्क्रोनस उपग्रह (geo-synchronous satellite) से जुड़ा होता है तथा द्वि-मार्गी दूर संचार (two-way telecommunication) तथा सूचना सेवाओं जैसे- ध्वनि, डाटा तथा वीडियो को सपोर्ट करने के लिए उपयुक्त होता है।

यह छोटे टर्मिनल एक मीटर के एंटीना रखते हैं तथा लगभग एक वाट के होते हैं; अपलिक सामान्यतः 19.2 kilo bile per second के लिये बढिया होता है। लेकिन डाउन GNK प्रायः 512 किलो बाइट प्रति सेकण्ड (kpbs) से अधिक होता है। बहुत से VSAT प्रणाली के अन्तर्गत माइक्रो-स्टेशन किसी और स्टेशन से (satellite) के द्वारा सीधे जुड़ने की क्षमता नहीं रखते हैं। वह एक विशेष प्रकार ग्राउण्ड स्टेशन जो कि बहुत बड़े एंटीना रखते हैं, जिन्के द्वारा VSAT, के मध्य सूचनाओं का आदान-प्रदान होता है। इस प्रकार की क्रियाओं में सूचना भेजने वाले (sender) और प्राप्त करने वाले (receiver) के पास बहुत बड़े एंटीना तथा अत्यधिक क्षमता वाले एम्पलीफायर (Amplifier) होते हैं। इन प्रक्रियाओं में user तक सूचना पहुँचने में अधिक समय लगता है।

प्रश्न-12. Domain name की सार्थकता पर प्रकाश डालिये।

उत्तर- Domain name : डॉमेन नाम एक ऐसा पता है जिसके जरिये internet प्रयोक्ता आपको web पर देखेंगे, web प्रकाश का पहला चरण है।

Domain name planning and registration डॉमेन का नाम निर्वाचित करवाते समय कुछ बातें आपको दिमाग में रखनी चाहिए। सबसे पहले जो चीज आपको करने की आवश्यकता होती है वह है प्रस्तावित साइट के लिये एक Domain नाम प्राप्त करना। Domain name वह name है जिसे आप अपने साइट पर देना चाहते हैं। उदाहरण के लिये

harmarabinaron cine.com एक domain name है। एक domain name प्राप्त करने के लिए आपको एक registrar को एक वार्षिक शुल्क उस नाम का प्रयोग करने देने की अनुमति को पहले देना पड़ता है। एक नाम प्राप्त कर लेने से आपको website नहीं मिल पाता है। यह सिर्फ एक नाम है। यह ठीक वैसा है जैसे नकल से बचने के लिए किसी सरकारी संस्था के अधीन किसी व्यावसायिक नाम का निवर्धन कराना।

एक डॉमेन नाम का चयन करना (Choosing a Domain Name) - इसे पूर्व की आप शीघ्रता बरतते हुए अपना डॉमेन नाम चुनें और website का नामकरण करें। आपको निम्न बातों पर ध्यान देने की आवश्यकता है-

आपका डॉमेन नाम ही आपके वेब साइट का नाम होना चाहिए (Your Domain Name should be your website name) - ऐसा Domain name जो आपके ब्रांड से मेल खाता है, बहुत महत्वपूर्ण है। वह नेम जिसका प्रयोग आप अपने उत्पाद के विज्ञापन में करते हैं। आप अपने डॉमेन के लिये भी चाहेंगे क्योंकि यही वह पहली चीज होगी जिसे लोग अपने Browser में डालकर देखेंगे। आपका डॉमेन नाम बहुत लम्बा नहीं होना चाहिए।

आपका डॉमेन नाम बहुत लम्बा नहीं होना चाहिए (Your Domain name should not be too long) - Domain 67 अक्षर (character) तक किसी भी लम्बाई के हो सकते हैं। आपको एक अस्पष्ट और दुर्बोध Domain नाम जैसे- nbo.com से ही संतोष कर लेने की आवश्यकता नहीं है। जबकि आप जो चाहते हैं, वह है। hamarabinaronline.com यद्यपि आप एक छोटा Domain name प्राप्त करने में सफल हो जाते हैं। जो मुख्य बात यह सुनिश्चित करता है कि यह अक्षरों का एक सार्थक मेल या संयोजन है या नहीं।

आपके डॉमेन नाम को hyphen मुक्त होना चाहिए (Your Domain name should be hyphen free) - Hyphenation मुक्त Domain Name के कुछ-कुछ अपने फायदे हैं और नुकसान भी। यदि hyphen सहित है। तो search इंजन आपके keywords के बेहतर रूप से पहचान सकते हैं। नुकसान यह है कि नाम Type करते समय hyphen को भूल जाना अत्यन्त आम बात है। इसके अलावा यदि कोई व्यक्ति मौखिक रूप आपके साइट को अपने किसी मित्र को recommend करता है तो आपके Domain name में hyphen होना गलती होने की संभावना बढ़ता है।

डॉमेन नाम में बहुवचन शब्द नहीं होना चाहिए (Your domain should not contain plural words) - Domain name का बहुवचन नाम (forex website.com) हमेशा ही नुकसान का कारण बनता है। चूँकि आप क्रम द्वारा नाम में 'S' Type की बात भूल जाने की संभावना बहुत रहती है। उदाहरण के लिये मान लीजिए कोई व्यक्ति website.com को log on करना चाहता है, किन्तु गलती से website.com log on कर देता है तो बहुत संभव है इससे cinenet नुकसान होने का खतरा रहेगा यदि दोनों ही डॉमेन के उत्पाद समान हों।

प्रश्न-13. E-mail भेजने तथा प्राप्त करने की विधि बताइये।

उत्तर- ई-मेल की अवधारणा (Concept of E-mail) : E-mail एक ऐसा system होता है, जिसमें एक computer प्रयोगकर्ता किसी अन्य computer प्रयोगकर्ता को संदेश एवं सूचनाओं का आदान-प्रदान कर सकता है। इन सूचनाओं के लिये कम्प्यूटरीकेशन नेटवर्क का प्रयोग होता है।

ई-मेल का यूज करने के लिये विभिन्न सॉफ्टवेयर प्रयोग में लाये जाते हैं। ई-मेल करने के लिये यह आवश्यक नहीं कि भेजने वाले व प्राप्त करने वाले के पास समान कम्प्यूटर हो यदि हम किसी ऑफिस में काम कर रहे हैं व ऑफिस के अन्य व्यक्ति को E-mail के माध्यम से यह संदेश देना चाहते हैं तो हमारे ऑफिस नेटवर्क में इंटरनेट के लिए एक गेटवे (Gateway) होता है जो हमारे संदेश को इंटरनेट के माध्यम से भेजता है।

ई-मेल के साथ कार्य करना (Working with E-mail)- ई-मेल पर कार्य करने में निम्नलिखित गतिविधियाँ शामिल हैं-

- (1) ई-मेल प्रोग्राम प्रारम्भ करना
- (2) ई-मेल संदेश लिखना
- (3) ई-मेल संदेश भित्ताना
- (4) ई-मेल संदेश पढ़ना
- (5) ई-मेल का उत्तर देना
- (6) ई-मेल प्रोग्राम से बाहर आना

ई-मेल प्रोग्राम प्रारम्भ करना (Starting the main program)- ई-मेल प्रोग्राम को प्रारम्भ करने के लिये आपके कम्प्यूटर पर ब्राउजर जैसे- इंटरनेट एक्सप्लोरर या नेटस्केप होना चाहिए तथा आपको इंटरनेट से जुड़े होना चाहिए। ई-मेल को प्रारम्भ करने के लिये निम्न पदों का अनुसरण करें-

- इंटरनेट एक्सप्लोरर के Icon को Desktop पर click करें या फिर Start → Program → Internet Explorer का चयन करें।
  - उस साइट का एड्रेस या U.R.L. एड्रेस बॉक्स में टाइप करें जिसमें आपका ई-मेल Account है। उदा. के लिए आपका ई-मेल आई.डी.
  - Exe. : prsionofmanoor@yahoo.com है तो यू.आर.एल. box में <http://www.yahoo.com> टाइप करें ऐसा करने पर चित्र की भाँति उस साइट का होम पेज खुलेगा।
  - Mail Icon को homepage से click करें।
  - अब yahoo.ID text box में अपना मेल ID टाइप करें तथा पासवर्ड बॉक्स में सही-सही password टाइप करें।
  - Sign in पर click करें या Enter key दबायें।
- मेल को पढ़ना (Reading the mail)**- जब कोई user E-mail program खोलता है तब वह सबसे पहले आये हुए मेल (message) को मेल बॉक्स में देखता है। सामान्यतः ई-मेल जो नये होते हैं एक प्रकार का सूचक चिह्न रखते हैं। जैसे विषय का हाइलाइट रहना, नये संदेश के बगल में Bulliet या check का निशान होना ऐसा इसलिये होता है कि आप कहीं नये आये हुए मेल को खोज न पायें मेल को पढ़ने के लिए सामान्य प्रक्रिया निम्न है-
- Check mail को click करें या Inbox को click करें।

- फिर उस mail को खोलने के लिए उसके विषय जो हायपरलिंक होता है, को click करें जब आप मेल के विषय को click करते हैं तब आपका संदेश (message) खुलता है।
- Standard toolbar back बटन जो mail box में जाने के लिए click करें दूसरे mail को पढ़ने के लिए next या previous बटन आवश्यकतातुसार click कर सकते हैं।

**मेल बनाना तथा भेजना (Composing and sending a mail)**- मेल कम्पोज तथा मेल पढ़ना भी दूसरी प्रक्रिया की तरह ठीक आसान है। इस कार्य के लिए निम्नलिखित पदों को करें-

- Compose को mail box page से click करें ऐसा करने पर चित्र की भाँति compose box खुलेगा।
- To text में box में मुख्य प्राप्तकर्ता का E-mail ID टाइप करें।
- दूसरे प्राप्तकर्ता का आई.डी टाइप करने के लिए CC तथा BCC text box में संबंधित E-mail ID टाइप करें।
- Subject text box में अपना संदेश टाइप करें।
- अपनी व्यक्तिगत सूचना को मेल में जोड़ने के लिए प्रयोग my signature के check box का चुनाव करें।
- Send पर click करें।

**फाइलों को संलग्न करना (Attaching files)**- File को संलग्न (Attach) करने की सुविधा ई-मेल का बढ़िया फीचर है, जिसकी मदद से आप ई-मेल के साथ अतिरिक्त सूचना को एक फाइल के साथ store कर भेज सकते हैं।

- File को Attach करने के लिये निम्न पदों का अनुसरण करें-
- Compose box में Attach files को click करें। ऐसा करने पर Attach file डायलॉग बॉक्स चित्र की भाँति खुलेगा।
- अपने कम्प्यूटर पर file को लोकैट करने के लिए Browse पर click करें।
- फिर Attach files पर click करें।

प्रश्न-14. स्वयं का E-mail account बनाने की प्रक्रिया लिखिये।

उत्तर- E-mail account बनाने की प्रक्रिया- यह rediffmail.com पर ई-मेल Account बनाने की प्रक्रिया का वर्णन किया जा रहा है।

- (1) इंटरनेट एक्सप्लोरर खोलते हैं।
- (2) एड्रेस बार में पता [www.rediff.com](http://www.rediff.com) या [www.rediffmail.com](http://www.rediffmail.com) (दोनों समान हैं) टाइप करते हैं। रेडिफ का होम page प्रदर्शित होता है।
- (3) New user ? पर click करें।
- (4) तदुपरांत, Rediffmail के लिए पंजीकरण पत्र (Registration form) प्रकट होगा।
- (5) निर्देशानुसार form को भरते हैं। उदाहरणार्थ choose your login name text box में कोई login नाम (यथा submit for allow you) तथा choose password text box में उपयुक्त password टाइप करते हैं। पासवर्ड टाइप करने में कोई गलती नहीं हो, इसे सुनिश्चित करने के लिए Retype password

text box में दुबारा वही password टाइप कराया जाता है। अतः इस text box में उसी password का दुबारा type करें।

- (6) Password Reminder Information खण्ड में चयन करने या अपना (hint) प्रश्न बनाने को कहा जाता है। यह तब बहुत महत्वपूर्ण हो जाता है जब अपना दिया हुआ password भूल जाते हैं। यह हमसे प्रश्न तथा उसका उत्तर याद काने को कहता है तथा उसी के आधार पर हमें दूसरा password प्राप्त होता है, जिसके प्रयोग के द्वारा हम अपने password के Account को खोल सकते हैं जो प्रश्न हम याद रख सकते हैं उसे द्वारा डाउन box से choose करते हैं तथा उसका उत्तर type करते हैं। विकल्प के रूप में create your arbitration text box में (hint) प्रश्न टाइप किया जा सकता है।
- (7) इस प्रकार सभी सूचना सही-सही टाइप की जाती है।
- (8) Form के नीचे के हिस्से में हम tellus your Internets खण्ड पाते हैं। जहाँ हम अपने पसंद के अनुसार check box का चयन कर सकते हैं। इस खण्ड को छोड़ा भी जा सकता है, क्योंकि यह ऐच्छिक है।

- (9) Confirm Registration भाग में एक code का नकल करने को कहा जाता है। यह सुनिश्चित करता है कि User computer नहीं बल्कि मानव है।

- (10) जब form पूरा कर लिया जाता है तब Registration me बॉक्स को click करते हैं। कुछ क्षण बाद बता दिया जाता है कि हमारे द्वारा चाहा गया ID हमें मिलेगी या नहीं यदि मांगा गया ID किसी ने पहले से लिया होगा तो किस तरह का संदेश प्रदर्शित होगा।

- (11) सकल पंजीकरण के बाद इनबॉक्स में प्रवेश करते हैं। Account logout किया जा सकता है। या किसी को मेल किया जा सकता है।

**प्रश्न-1.5. Telnet को समझाए, इसके विभिन्न उपयोग लिखिए।**

**जवाब- Telnet :** यह protocol remote login की सुविधा प्रदान करता है। यह क्लाइंट system पर user को ऐसी सुविधा प्रदान करता है जिसके माध्यम से वह remote पर login कर सकता है जब एक बार login हो जाता है तब user के द्वारा भेजी गयी रिक्वेस्ट या data सर्वर तक पहुँचता है। यह (Telnet) program भी FTP की तरह TCP protocol का प्रयोग करता है। इसका standard RFC 854 [postal और Reynolds 1983] है।

**टेलनेट की अवधारणा-** Remote login के लिये internet standard, telnet नाम के एक protocol में पाया जाता है। इसको विनिर्देश TCP/IP दस्तावेजीकरण का हिस्सा होते हैं। Telnet protocol इस बात का सटीक विवरण देता है कि कैसे एक दूरस्थ लॉगइन क्लाइंट तथा दूर स्थित login server आपस में संवाद स्थापित करते हैं। यह मानक इस बात का विवरण देता है कि जब उदाहरण के लिए, क्लाइंट किस तरह सर्वर से संबंध स्थापित करता है। कैसे क्लाइंट सर्वर को संश्लेषण के लिये keystroke को दूर करता है।

चूँकि, दोनों telnet क्लाइंट तथा सर्वर program एक ही विनिर्देशन का पालन करते हैं। जो communication detail पर सहमत हो जाते हैं। उदाहरण के लिए, यद्यपि अधिकांश computer कुंजी पटल की एक कुंजी की व्याख्या, चल रहे program पर विचलित कर देने

के आग्रह के रूप में करते हैं। सभी computer प्रणालियाँ एक ही कुंजी का प्रयोग नहीं करती कुछ computer ATTN Level वाली एक कुंजी इस्तेमाल करती है। जबकि कुछ अन्य DEL Level वाली कुंजी telnet bids की उस कड़ी (sequence) के बारे में बताती है जिसका प्रयोग एक user abort कुंजी represent करने के लिए करता है। जब एक user local कुंजी पटल पर abort कुंजी को दबता है तो telnet क्लाइंट program, कुंजी को विशेष कड़ी के रूप में अनुदित कर देता है। इस प्रकार telnet user को दूरस्थ program को abort करने के लिए उसी कुंजी को दबाने की अनुमति दे देता है, जिसका प्रयोग वह स्थानीय program को abort करने के लिए करता है।

**दूर स्थित होस्ट से संयोजन (Connection to a remote host)-** Telnet program जो Windows-98 और 95 के साथ आता है, telnet कहलाता है। वह Windows-98 और 95 के साथ आने वाले built in telnet program को संयोजित करता है। हालाँकि Windows-XP में टेलनेट पूरी तरह वही है जो 95 तथा 98 में है, Windows 98 में telnet का प्रयोग करने के लिये निम्न पदों का अनुसरण करना चाहिये।

- (1) Start पर click करें एवं Run का चयन करें telnet type करें तथा OK पर click करें telnet windows कैसे ही प्रकट है।
- (2) Internet पर HOST computer से संयोजन करने के लिये connect पर click करें और Remote computer का चयन करें।
- (3) HOST name box में computer का HOST नाम type करें जिससे आप जुड़ना चाहते हैं।
- (4) Port, box set को telnet पर छोड़ देते हैं। दूसरे option मिन internet सेवाओं को प्रयोग करने के लिए HOST computer से जुड़ते हैं जो सिर्फ debugging के लिए उपयोगी होता है।
- (5) दूरस्थ computer को भेजने के लिए term type box, the string of character को set करें यदि यह आपसे पूछता है कि किस प्रकार के Terminal का आप प्रयोग करते हैं।
- (6) Connect पर click करें यदि आपका computer internet से संयोजित नहीं है तो आप Dial up Networking विण्डो देखेंगे जो आपको संयोजन के लिये तस्तर करेगी, एक बार online होने पर connect बटन पर click करें। telnet HOST computer से जुड़ जाता है। telnet windows में एक terminal विण्डो होता है जो आपके द्वारा HOST computer से प्राप्त text तथा आपके प्रत्युत्तर को प्रदर्शित करता है।
- (7) Login करें तथा HOST computer द्वारा चाहे गए निर्देशों को type करते हुए HOST computer का प्रयोग करें। आप windows के दाहिनी तरफ वाले scroll bar का प्रयोग करके विण्डो के ऊपरी किनारे से भी ऊपर सरक गए text की lines को देख सकते हैं।

- (8) जब आपका HOST computer का प्रयोग समाप्त हो जाए logout करें। telnet भी disconnect हो जाता है। यदि आपको disconnect करने में परेशानी होती है तो connect click करें तथा Disconnect का चयन करें ताकि telnet को sign up करने के लिए निर्देशित किया जा सके।

प्रश्न-16. Data Transmission Protocol को समझाइय।

उत्तर- Data Transmission Protocol : Data transmission protocol वे protocol होते हैं जो कि सूचनाएँ, संदेशों को data के रूप में computer या network के बीच आदान-प्रदान करने का कार्य करते हैं। data transmission protocol निम्न है-

(1) TCP/IP (Transmission Control Protocol/Internet Protocol)-

TCP/IP protocol 1980 में बनाया गया था, इसे TCP/IP सुईट भी कहते हैं, क्योंकि यह कई protocol से मिलकर बना होता है। जैसा कि हम जानते हैं कि प्रत्येक protocol की प्रत्येक परत में एक या एक से अधिक protocol होते हैं। TCP/IP protocol को चार परतों में बांटा गया है। TCP/IP एक इंटरनेट protocol है। इसके बारे में कुछ खास बातें निम्न हैं-

- यह नेटवर्क स्पेसिफिक नहीं होता है।
- यह किसी भी computer जैसे- personal computer से लेकर super computer में इस्तेमाल किया जा सकता है।
- इसका प्रयोग local Area Network तथा Wide Area Network दोनों में होता है।

(iv) इसका प्रयोग कई सरकारी तथा व्यावसायिक साइटें कर रही हैं।

(v) यदि दो computer एक कमरे से internet के माध्यम से जुड़े हैं तो वे दोनों computer भी TCP/IP protocol का प्रयोग करके ही सूचनाओं का आदान-प्रदान कर सकते हैं।

**संचार नियंत्रण प्रोटोकॉल (TCP - Transmission Control Protocol)-** यह protocol connection ऑरिएन्टेड प्रोटोकॉल हो जो यूजर process के लिए विश्वसनीय, full duplex तथा data को साइट stream में ट्रांसमिट करता है। अधिकतर इंटरनेट Application program TCP protocol का प्रयोग करते हैं। क्योंकि TCP protocol IP protocol का प्रयोग करते हैं। अतः इस protocol सूट को TCP/IP protocol कहते हैं।

प्रश्न-17. संक्षिप्त रिपण्णी लिखिये-

(1) मैसेज बोर्ड और इसके उपयोग (Message Board and its uses)

(2) वॉयज चैटिंग और text चैटिंग (Voice chatting and Text chatting)

उत्तर- (1) मैसेज बोर्ड और इसके उपयोग- यह तकनीक एक ऐसा मंच प्रदान करता है। जिस पर कोई भी अपने विचार प्रकट कर सकता है। इंटरनेट की दुनिया में message बोर्ड एक सशक्त माध्यम है। इसके द्वारा आप अपने विचारों, किसी विषय, वस्तु आदि के बारे में व्यक्त करते हैं तथा उन्हें इंटरनेट के माध्यम से अन्य लोगों के साथ बांट सकते हैं। इंटरनेट की कई साइटों पर Message Board की सुविधा विभिन्न विषयों, व्यक्तियों और वस्तुओं आदि पर प्रदान की गयी है। उस साइट के Message Board में उपस्थित विषयों पर आप अपनी राय या विचार व्यक्त कर सकते हैं तथा दूसरे व्यक्ति के विचारों को भी जान सकते हैं। यह अपने विचारों को व्यक्त करने का एक सशक्त माध्यम है।

(2) वॉयज चैटिंग और टैक्सट चैटिंग- आप जिस प्रकार टेलीफोन पर अपने मित्रों तथा पब्लिशियों के साथ ध्वनि के जरिये संवाद स्थापित करते हैं ठीक उसी प्रकार वॉयज चैटिंग के जरिये आप दूसरी ओर किसी भी व्यक्ति से बात कर सकते हैं। वॉयज चैट telephone की

अपेक्षा बहुत सस्ती सर्ვის है। इसमें दूरी के आधार पर भुगतान नहीं करना पड़ता है। Voice chatting के माध्यम से आप सामान्यतः एक समय में एक ही व्यक्ति के साथ सम्पर्क बना सकते हैं। परन्तु यदि आपके पास full duplex sound card है तो आप दो व्यक्तियों से एक समय में बात कर सकते हैं। इसके लिये आपके पास एक माइक्रोफोन और एक स्पीकर तथा इसके प्रयोग के लिये विशेष program होना चाहिये। इंटरनेट पर इंटरनेट नाम का शेयरवेयर <http://www.voicelc.com> पर उपलब्ध है। जिसका प्रयोग voice chatting program के रूप में कर सकते हैं। voice chatting को भारत में अभी तक अधिक प्रोत्साहन नहीं मिला है।

टैक्सट चैटिंग में हम संदेश Keyboard के माध्यम से प्रेषित करते हैं। तथा दूसरी ओर बैठ व्यक्ति हमारे प्रेषित संदेश को पढ़ता है तथा तुरन्त उसका जवाब देता है। चैट एक के साथ एक या एक के साथ कई लोगों के साथ एक या एक के साथ कई लोगों के सम्बन्ध पर आधारित होता है। अर्थात् आप एक साथ कई लोगों के साथ chat कर सकते हैं। Chat पूरी तरह से इंटर एक्टिव है जिसमें तत्काल संदेश प्रेषित किया जाता है या प्राप्त होता है जिसमें दोनों व्यक्ति को online होना आवश्यक है। Text chatting के लिये website उपलब्ध हैं-

- [www.yahoo.com](http://www.yahoo.com)
- [www.sify.com](http://www.sify.com)
- [www.hotmail.com](http://www.hotmail.com)

प्रश्न-18. Search Engines क्या है? Web में आप किस प्रकार से सर्व करेंगे?

उत्तर- सर्व इंजिन (Search Engines)- इंटरनेट को सूचनाओं का महासागर की उपाधि दी जाए तो यह अतिशयोक्ति न होगी। इन सूचनाओं के इस महा भंडार के साथ कठिनाई यह है कि इसका कोई केंद्रीय व्यवस्थापक नहीं है। अतः इस पर एक-एक विशेष सूचना खोजना अति मुश्किल कार्य है। इस समस्या के लिये कम्पनियों ने समाधान के रूप में ऐसे program का विकास किया है जिसे सर्व इंजिन कहते हैं। सर्व इंजिन इंटरनेट पर उपलब्ध सूचना को तलाश करने में हमारी हर संपन्न मदद करता है।

**वेब को खोजना (Searching the Web)-** वेब के माध्यम से इच्छित सूचनाओं को तलाशना हमेशा आसान नहीं होता है। ऐसा इसलिए है कि web पर लाखों की संख्या में website उपलब्ध है तथा हजारों की संख्या में समानता रखने वाले page होते हैं। इस खण्ड में हम विभिन्न प्रकार से web पर सूचनाओं को खोजने की प्रक्रिया करेंगे। Web पर दो प्रकार से सूचना को सर्व (search) किया जाता है-

(1) डायरेक्ट्री (Directories) के द्वारा (2) की-वर्ड (Key-words) के द्वारा

(1) डायरेक्ट्री के द्वारा (Using A Directory)- डायरेक्ट्री के माध्यम से आप जिस विषय पर सूचना पाना चाह रहे हो उस category का चुनाव करते हैं। Directory एक विशेष विषय को निरूपित करती है तथा वह अपने अंदर कई Sub-directory रखती है। जिसका चुनाव करते हुए आप उस खास category को चुनते हैं। जब आप उस विशेष directory को चुनते हैं तब directory उस विषय से सम्बन्धित website की सूची प्रदर्शित करती है। उदाहरण के रूप में लूकसमर्ड नामक सर्व इंजिन को देखें।

(2) की-वर्ड (Key-words) के द्वारा- सर्व इंजिन आपको की-वर्ड के आधार पर भी उससे सम्बन्धित वेबसाइट की सूची प्रदान करता है। कुछ सर्व इंजिन किसी एक key word के आधार पर सर्व करती है। जबकि अधिकतर सर्व इंजिन कई key word के आधार पर सर्व करते हैं। जैसे- "Internet and E-commerce" कई सर्व इंजिन पर आप अंग्रेजी के पूरे वाक्य या वाक्य खण्ड या प्रश्न के आधार पर एक्सेस कर सकते हैं। उदाहरण के तौर पर "Novels written by O. Henry" या "How is election held in UK" चित्र में आप इस तरह के खोज (search) को [www.lycos.com](http://www.lycos.com) में देख सकते हैं।

प्रश्न-19. Teleconferencing को समझाइये।

उत्तर- Teleconferencing- आप जिस प्रकार टेलीफोन पर अपने मित्रों तथा सम्बन्धियों के साथ ध्वनि के जरिये संवाद स्थापित करते हैं ठीक उसी प्रकार voice chatting के जरिये आप दूसरी ओर किसी भी व्यक्ति से बात कर सकते हैं। Voice chat telephone से अपेक्षाकृत सस्ती सर्विस है। इसमें दूरी के आधार पर भुगतान नहीं करना पड़ता है। Voice chat के माध्यम से सामान्यतः आप एक समय में एक ही व्यक्ति से सम्पर्क बना सकते हैं। परन्तु यदि आपके पास full duplex sound card है तो आप दो व्यक्तियों के साथ एक समय में सम्पर्क बना सकते हैं। इसके लिये आपके पास एक microphone तथा एक स्पीकर तथा इसके लिये प्रयोग होने वाला एक विशेष program होना चाहिए। इंटरनेट पर इंटरनेट जोन नाम का एक शेयरवेयर <http://www.vocal.com> पर उपलब्ध है। जिसका प्रयोग voice chatting program के रूप में कर सकते हैं। वॉयज चैटिंग को भारत में अभी तक अधिक प्रोत्साहन नहीं मिल पाया है।

प्रश्न-20. Web browsers का क्या आशय है? अपने शब्दों में समझाइये।

उत्तर- वेब ब्राउजर- इंटरनेट सर्फिंग करने के लिये या इंटरनेट पर स्थित किसी भी फाइल को पढ़ने के लिये, एक विशेष सॉफ्टवेयर की आवश्यकता होती है जिसे तकनीकी भाषा में ब्राउजर कहा जाता है। ब्राउजर एक ऐसा सॉफ्टवेयर है जो हमारे कम्प्यूटर को इंटरनेट से जोड़ने में सहायता करता है। ब्राउजर के अभाव में इंटरनेट से चित्र, टेक्स्ट, संगीत, ग्राफिक्स आदि देखने व सुनने का सोच नहीं सकते हैं।

जैसे-जैसे इंटरनेट का विकास हो रहा है वैसे-वैसे ब्राउजर्स का भी विकास हो रहा है। आज के ब्राउजर प्रोग्राम पुराने ब्राउजर्स की अपेक्षा अधिक उन्नत एवं तीव्र गति से कार्य करने वाले हैं। पुराने ब्राउजर्स में इमेज, एनीमेशन आदि का प्रयोग नहीं किया जा सकता था। ये टेक्स्ट ब्राउजर्स कहलाते हैं, परन्तु विन्डोज ऑपरेटिंग सिस्टम के आते ही ब्राउजर्स भी विन्डोज के वातावरण में कार्य करने वाले बनने लगे अर्थात् चित्र आदि का भी प्रयोग किया जाने लगा और वेब ब्राउजर का विकास हुआ।

वर्ल्ड वाइड वेब को ब्राउज करने के लिये नेटस्केप नेकीगेटर और इंटरनेट एक्सप्लोरर दो ऐसे ब्राउजर्स हैं जिनको क्रमशः नेटस्केप और माइक्रोसॉफ्ट ने विकसित किया है। इन दोनों ब्राउजर्स का कार्य हमारे कम्प्यूटर्स को इंटरनेस से जोड़ना है। ये वेब ब्राउजर्स हमें इंटरनेट से सूचनाओं को प्राप्त करने एवं इन्हें एकांकित करने की सुविधा प्रदान करता है।

आजकल के आने वाले नये ऑपरेटिंग सिस्टम में एक वेब ब्राउजर को जोड़ा जाना एक फ़ैशन सा हो गया है। ऐसा ही ऑपरेटिंग सिस्टम है विन्डोज 98 जिसमें एक वेब ब्राउजर को default रूप से जोड़ा गया है अर्थात् जब भी विन्डोज 98 को कम्प्यूटर में स्थापित किया जाता है, यह वेब ब्राउजर स्वतः ही कम्प्यूटर में स्थापित हो जाता है तथा यह सिस्टम का सारा संरूप स्वतः ही सेट कर लेता है।

प्रश्न-21. FTP से आप क्या समझते हैं? इसकी कार्यविधि लिखिये।

उत्तर- File Transfer Protocol : FTP सर्वर एक ऐसा कम्प्यूटर होता है जो अपनी डिस्क पर सूचना एकांकित करके रखता है। इस कम्प्यूटर पर एकांकित सूचना यूजर्स के लिये उपलब्ध होती है, जिन्हें वे अपने कम्प्यूटर पर ट्रांसफर कर सकते हैं। अतः हम कह सकते हैं कि सूचना तकनीक का महत्वपूर्ण विषय फाइल स्थानान्तरण से सम्बन्धित क्रियाओं पर आधारित होता है। जो इंटरनेट पर उपस्थित फाइल ट्रांसफर प्रोटोकाल (FTP) के द्वारा किया जाता है। जिसमें फाइल ट्रांसफर प्रोटोकाल (FTP) इंटरनेट से जुड़े किसी एक कम्प्यूटर की फाइल्स को इंटरनेट से जुड़े किसी अन्य कम्प्यूटर पर ट्रांसफर करता है। FTP, TCP/IP प्रोटोकाल समूह का ही एक सदस्य है। FTP का मुख्य प्रतियोगी HTTP है। HTTP दिन प्रतिदिन लोकप्रिय होता जा रहा है, क्योंकि यह वे सभी कार्य तो कर ही सकता है जो FTP कर सकता है, साथ ही वह अनेक ऐसे कार्य भी कर सकता है जो FTP नहीं कर सकता। लेकिन उल्लेखनीय है कि FTP को फाइल ट्रांसफर के लिये उपयोग में लिया जाता है। इंटरनेट से जुड़े हुये यूजर्स को फाइल ट्रांसफर करने की सुविधा प्रदान करने के लिये बहुत सारे FTP सर्वर्स पूरे विश्व में स्थापित किये गये हैं।

FTP की कार्यविधि- FTP क्लाइन्ट/सर्वर तकनीक का ही पालन करता है। कोई यूजर अपने कम्प्यूटर पर FTP प्रोग्राम चलाता है, उसे रिमोट कम्प्यूटर से कनेक्ट करने के लिये निर्देश देता है तथा उसके बाद एक या अधिक फाइल्स को स्थानान्तरित करने का निर्देश देता है। स्थानीय कम्प्यूटर पर चल रहा FTP प्रोग्राम किसी क्लाइंट के समान कार्य करता है जो FTP सर्वर प्रोग्राम से सम्पर्क बनाने के लिये TCP का उपयोग करता है। जब यूजर किसी फाइल को ट्रांसफर करना चाहता है तो क्लाइंट प्रोग्राम तथा सर्वर प्रोग्राम आपस में मिलकर इंटरनेट के माध्यम से उस फाइल की एक कॉपी स्थानान्तरित कर देते हैं। जिस फाइल को यूजर ने माँगा है, उस फाइल को FTP सर्वर ढूँढता है और फाइल के सारे कन्टेन्ट्स की कॉपी को TCP के द्वारा इंटरनेट के माध्यम से क्लाइंट तक पहुँचा देता है। जब क्लाइंट प्रोग्राम के पास डाटा आ जाता है तो वह यूजर के कम्प्यूटर की डिस्क पर उस फाइल के डाटा को लिख देता है। FTP के मुख्य दो कार्य निम्नलिखित हैं-

(1) फाइल अपलोड करना- इंटरनेट पर जब यूजर अपने कम्प्यूटर से किसी रिमोट कम्प्यूटर पर फाइल ट्रांसफर करता है तो यह प्रक्रिया फाइल अपलोडिंग कहलाती है। हम फाइल को केवल तभी अपलोड कर सकते हैं जब हम FTP सर्वर के प्रमाणिक यूजर हों।

(2) फाइल डाउनलोड करना- यह फाइल अपलोडिंग के विपरीत प्रक्रिया डाउनलोडिंग है। इसमें फाइलों को किसी रिमोट कम्प्यूटर से अपने कम्प्यूटर पर ट्रांसफर किया जाता

है। इसके लिये यूजर को FTP सर्वर पर किसी विशेष एकाउंट की आवश्यकता नहीं होती।

प्रश्न-22. इन्टरनेट फ्राइड से क्या तात्पर्य है? संक्षेप में वर्णन कीजिये।

उत्तर- इन्टरनेट फ्राइड- इन्टरनेट का चलन और उपयोग दुनिया भर में अत्यन्त तेजी से बढ़ा है। इन्टरनेट के माध्यम से आप दुनिया के एक कोने से दूसरे कोने तक सैकड़ों में ही सम्पर्क कायम कर सकते हैं। आज बातचीत, पढ़ाई आदि से लेकर कारोबार तक इन्टरनेट पर चल रहा है। पर-पर से लेकर सभी छोटे-बड़े औद्योगिक घरानों की अपनी-अपनी साइट्स हैं। बल्कि अब तो शायद ही कोई ऐसा क्षेत्र या विषय बचा हो जिस पर वेबसाइट नहीं बनी हुई है। लेकिन इसी इन्टरनेट का एक दूसरा जो महत्वपूर्ण पहलू है वह है सुरक्षा। आज तेजी से बढ़ते नेटवर्क को फुलपूरा सुरक्षा की सबसे ज्यादा आवश्यकता है। आये दिन वेबसाइट्स में सेंध लगाकर डाटा चुराने, नष्ट कर देने, साइट्स को नुकसान पहुँचाने जैसी खबरें आ रही हैं। हमलावर और घुसपैठिए, साइट्स को नष्ट कर देते हैं। इसलिए अब यह जरूरी हो गया है कि यदि आपका अपना नेटवर्क या साइट है तो आप उसे पूरी तरह सुरक्षित रखें। नेटवर्क अथवा साइट्स पर होने वाले हमलों को मुख्य रूप से तीन भागों में बाँटा जा सकता है। घुसपैठ, सेवा में इंकार और सूचना (डाटा) की चोरी। घुसपैठ में कोई भी व्यक्ति अवैध रूप से आपके कम्प्यूटर्स तक पहुँचकर उनका इस्तेमाल कर सकता है। सेवाओं की चोरी में, चोर आपके महत्वपूर्ण, गोपनीय डाटा और जानकारीयों को चुराकर उनका दुरुपयोग कर सकता है।

इसलिए साइट्स और नेटवर्क की सुरक्षा एक चिंता का विषय है। इन्टरनेट से आप सम्बन्ध जोड़ लें, यह इसका हल नहीं है। पिछले कुछ वर्षों में इसकी सुरक्षा के लिए फायरवॉल तकनीक विकसित की गई है। यह हार्डवेयर और सॉफ्टवेयर दोनों रूपों में होता है।

एकाउन्ट नेम का पता लगाने के लिए हैकर्स Finger, Ish या Puser नामक यूनिकस प्रोग्राम का इस्तेमाल कर सकते हैं। एक बार एकाउन्ट नाम पता चलने के बाद वे डिक्शनरी के उपयोग से पासवर्ड का अनुमान लगा लेते हैं।

प्रश्न-23. इंटरनेट से जुड़ी अन्य सेवाओं को समझाइये।

उत्तर- इंटरनेट से जुड़ी अन्य सेवाएँ-

(1) बातचीत- इंटरनेट से जुड़े किसी कम्प्यूटर पर कार्य कर रहे व्यक्ति द्वारा ऐसे ही किसी दूसरे कम्प्यूटर पर कार्य कर रहे व्यक्ति के साथ बातचीत की जा सकती है। इस सुविधा को ही चैटिंग कहा जाता है। इसमें दोनों व्यक्ति एक ही समय एक ही वेब साइट पर लॉग-इन करते हैं और अपने संदेश अपने-अपने कम्प्यूटर पर टाइप करते हैं, जो दूसरे कम्प्यूटर पर भी दिखायी पड़ता है। इसी का सुधरा हुआ रूप वॉयस मेल होता है, जिसमें माइक तथा स्पीकर द्वारा दूर-दूर बैठे दो व्यक्ति इस प्रकार बात कर लेते हैं, जैसे टेलीफोन पर कर रहे हों। इन सेवाओं को प्रदान करने के लिए कई निशुल्क सॉफ्टवेयर उपलब्ध हैं जैसे गूगल द्वारा जी-टॉक और याहू द्वारा याहू मैसेंजर। इसी सेवा का एक और विकसित रूप है विडियो चैटिंग जहाँ आप बात करते हुए एक-दूसरे का विडियो भी देख सकते हैं। माइक्रोसॉफ्ट का सॉफ्टवेयर स्काईप इसका एक प्रसिद्ध उदाहरण है।

(2) ई-कॉमर्स- दूर-दूर स्थित व्यक्तियों या कम्पनियों या कम्पनियों द्वारा इंटरनेट के माध्यम से आपस में सम्पर्क करके वस्तुओं और सेवाओं की खरीद-बिक्री तथा लेन-देन करना ई-कॉमर्स कहलाता है। यह इंटरनेट का एक नवीन उपयोग है, लेकिन अनुमान लगाया गया है कि भविष्य में इंटरनेट पर अन्य क्रियाओं से ज्यादा ई-कॉमर्स ही क्रिया जायेगा। ई-कॉमर्स द्वारा आप- पुस्तकें, फोन, कम्प्यूटर, टी.वी., कपड़े, जूते, खिलौने आदि कुछ भी खरीद सकते हैं। आप बस एरोलान्ड्रेन या किसी फिल्म की टिकट भी ऑनलाइन खरीद सकते हैं। इस सेवा को ई-रिजर्वेशन भी कहा जाता है।

(3) ई-बैंकिंग- ई-बैंकिंग की साइटों द्वारा ग्राहक अपने बैंक से जुड़ सकते हैं और अपना खाता देख सकते हैं, खाते में पैसे डाल अथवा निकाल सकते हैं, योजनाओं में निवेश कर सकते हैं, टैक्स जमा करावा सकते हैं, आदि। इन साइटों का यूजर-नेम और पासवर्ड गुप्त रखना चाहिए।

(4) ई-लर्निंग- ई-लर्निंग का अर्थ है इलेक्ट्रॉनिक माध्यम के द्वारा शिक्षा प्रदान करना, शिक्षा प्रदान करने के लिए- पाठ्य, विज्ञ, ऐनिमेशन, आडियो और विडियो का सहारा लिया जाता है। यह तकनीक सबसे ज्यादा वहाँ उपयोगी पाई गई है जहाँ किसी कारणवश अभी तक विद्यालय स्थापित नहीं हो पाये या जहाँ अच्छे शिक्षकों की कमी है।

इंटरनेट के जरिये जुड़ने में बरती जाने वाली सावधानियाँ-

जैसा कि हमने पढ़ा, इंटरनेट के जरिये हम दुनिया भर में फैले व्यक्तियों से जुड़ सकते हैं और सभी के सामने अपना दृष्टिकोण रख सकते हैं। परन्तु इंटरनेट के जरिये लोगों से जुड़ने में कुछ सावधानियाँ बरतनी आवश्यक हैं, जिससे कि कोई आपकी व्यक्तिगत जानकारी का दुरुपयोग न कर सके। आपके द्वारा बनाये गये ब्लॉग और सोशल नेटवर्किंग साइटों में बनाये गये प्रोफाइल केवल आपके मित्र ही नहीं, अजनबी भी सीमित या असीमित रूप में देख सकते हैं। जाहिर है आप नहीं चाहेंगे कि आपकी व्यक्तिगत जानकारी गलत हाथों में पड़े और आपको कोई हानि हो। ऐसी संभावनाओं से बचने के लिए निम्नलिखित सावधानियाँ बरतें-

(1) निजी जानकारी न दें- निजी जानकारी, जिसका दुरुपयोग हो सकता है, जैसे अपना फोन नम्बर, घर का पता, ऑफिस का पता, आदि न दें।

(2) दर्शकों और मित्रों की संख्या सीमित रखें- लगभग सभी वेबसाइटों में 'Privacy Settings' विकल्प होता है, जिससे आप यह निर्धारित कर सकते हैं कि आपका प्रोफाइल, उसमें दी गई जानकारी, आपके फोटो, संदेश आदि कौन देख सकता है। सुनिश्चित करें, कि आपके विषय में निजी जानकारी और आपका विस्तृत प्रोफाइल केवल आपके वे मित्र देख सकें, जिन्हें आप जानते हैं।

(3) नये मित्र सावधानी से बनायें- अजनबियों और नये मित्रों के साथ सावधानी से पेश आयें। जब भी आपको कोई मित्रता के लिए निवेदन भेजे, तो उस व्यक्ति के प्रोफाइल को ध्यान से देखें। यदि आप उसे नहीं जानते हैं या उसके प्रोफाइल में आपको कोई संदेह हो, तो निवेदन ठुकरा दें। आजकल इन साइटों का दुरुपयोग लोगों की जानकारी प्राप्त करने और कम्प्यूटर वायरस फैलाने में भी किया जा रहा है।

(4) लेख, टिप्पणी और वेब में कुछ भी लिखने में सावधानी बरतें— ब्लॉग के जरिये आप अपने विचार दूसरों के साथ बांट सकते हैं। याद रखें, कि वेब में लिखा हुआ एक शब्द भी विश्व भर में फैले लाखों-करोड़ों पाठकों द्वारा पढ़ा जा सकता है। इसलिए केवल वही लिखें, जिसके अनेक पाठकों द्वारा पढ़े जाने पर आपको कोई हानि न हो। कोई भी विवादास्पद टिप्पणी करने से बचें। आप बाद में लेख या टिप्पणी डिलीट करके अपनी गलती सुधार सकते हैं, परन्तु तब तक यह कई पाठकों द्वारा पढ़ा जा चुका होगा, इसलिए, पहले ही सावधान रहें।

प्रश्न-2.4. कम्प्यूटर नेटवर्क में डाटा सुरक्षा क्यों आवश्यक है तथा इसके क्या उपाय हैं?

अथवा

साइबर अपराध क्या है? इनसे किस प्रकार बचा जा सकता है?

उत्तर— (A) साइबर स्पेस— दुनियाभर में फैले कम्प्यूटर संचार नेटवर्क तथा उसके चारों ओर फैले सूचनाओं के भंडार को साइबर स्पेस का काल्पनिक नाम दिया जाता है।

साइबर स्पेस शब्द का प्रयोग पहली बार कल्पना विज्ञान के लेखक विलियम गिब्सन ने अपनी पुस्तक 'स्यूरोमैस' में 1984 में किया था। वर्तमान में इंटरनेट तथा वर्ल्ड वाइड वेब के लिए साइबर स्पेस शब्द का प्रयोग किया जाता है, पर यह सही नहीं है।

1. साइबर वारफेयर— किसी राष्ट्र द्वारा दूसरे राष्ट्र के कम्प्यूटर नेटवर्क में घुसकर गुप्त व संवेदनशील डाटा चुराना, डाटा को नष्ट या क्षतिग्रस्त करना या नेटवर्क संचार को बाधित करना साइबर वारफेयर कहलाता है। इंटरनेट के बढ़ते महत्व ने साइबर वारफेयर को युद्ध की रणनीति का एक महत्वपूर्ण हिस्सा बना दिया है। इसी कारण, इसे वायु, समुद्र, जमीन तथा अंतरिक्ष के बाद 'युद्ध का पाँचवा क्षेत्र' भी कहा जाता है।

2. साइबर क्राइम— कम्प्यूटर तथा इंटरनेट के माध्यम से किया गया कोई गैर-कानूनी कार्य या अपराध साइबर क्राइम कहलाता है। इसमें कम्प्यूटर तथा इंटरनेट का प्रयोग एक हथियार, लक्ष्य या दोनों रूप में किया जाता है। इंटरनेट के जरिये किये गये अपराध को नेट क्राइम कहा जाता है। साइबर क्राइम में कम्प्यूटर, नेटवर्क या डाटा को नुकसान पहुँचाना या कम्प्यूटर, नेटवर्क या डाटा का प्रयोग किसी अन्य अपराध में करना शामिल है।

साइबर क्राइम के कुछ उदाहरण हैं—

- नेटवर्क का अनाधिकृत तौर पर प्रयोग करना।
  - कम्प्यूटर तथा नेटवर्क का प्रयोग कर व्यक्तिगतता तथा गुप्त सूचना प्राप्त करना।
  - नेटवर्क तथा सूचना को नुकसान पहुँचाना।
  - बड़ी संख्या में ई-मेल भेजना।
  - वायरस द्वारा कम्प्यूटर तथा डाटा को नुकसान पहुँचाना।
  - इंटरनेट का उपयोग कर अधिक अपराध करना।
  - इंटरनेट पर गैरकानूनी तथा असामाजिक तथ्यों तथा चित्रों को प्रदर्शित करना।
3. साइबर अपराध से बचने के उपाय—
- Login ID तथा पासवर्ड सुरक्षित रखना तथा समय-समय पर इसे परिवर्तित करते रहना।
  - Antivirus साफ्टवेयर का प्रयोग करना।
  - Fire wall का प्रयोग करना।

• Data की back-up copy रखना।

• Proxy server का प्रयोग करना।

• Data को गुप्त कोड में बदलकर भेजना व प्राप्त करना।

(B) कम्प्यूटर सुरक्षा— कम्प्यूटर सुरक्षा का तात्पर्य कम्प्यूटर में स्टोर किए गए तथा नेटवर्क द्वारा स्थानान्तरित किए गए डाटा की सुरक्षा से है। कम्प्यूटर सुरक्षा से संघ लनाकार— डाटा का अनाधिकृत उपयोग किया जा सकता है।

⇒ उपयोगकर्ता की पहचान और निजी जानकारियाँ जैसे— पासवर्ड आदि प्राप्त किए जा सकते हैं।

⇒ डाटा में अनावश्यक परिवर्तन किया जा सकता है।

⇒ डाटा को नष्ट किया जा सकता है।

⇒ किसी साफ्टवेयर प्रोग्राम के क्रियान्वयन को रोका जा सकता है।

(C) स्पॉम— कम्प्यूटर तथा इंटरनेट का प्रयोग कर अनेक व्यक्तियों को अव्यथित तथा अवैध रूप से भेजा गया संदेश स्पॉम कहलाता है। इसे नेटवर्क के दुरुपयोग के रूप में जाना जाता है। यह ई-मेल संदेश का अभेदकारी वितरण है जो ई-मेल तंत्र में संदस्यता के overlapping के कारण संभव हो पाता है।

स्पॉम सामान्यतः कम्प्यूटर, नेटवर्क तथा डाटा को किसी तरह का नुकसान नहीं पहुँचाने। वास्तव में स्पॉम एक छोटा प्रोग्राम है जिसे हजारों की संख्या में इंटरनेट पर भेजा जाता है ताकि वे इंटरनेट उपयोगकर्ता की साइट पर बार-बार प्रदर्शित हो सकें। स्पॉम मुख्यतः विज्ञापन होते हैं जिसे सामान्यतः लोग देखना नहीं चाहते। अतः इसे बार-बार भेजकर उपयोगकर्ता का ध्यान आकृष्ट किया जाता है।

यूँकि स्पॉम भेजने का खर्च उपयोगकर्ता या सर्विस प्रोवाइडर पर पड़ता है, अतः इसे विज्ञापन के एक सस्ते माध्यम के रूप में प्रयोग किया जाता है। इंटरनेट की विशालता के कारण स्पॉम भेजने वाले को पकड़ पाना कठिन होता है। स्पॉम फिल्टर को पकड़ पाना कठिन होता है। स्पॉम फिल्टर या एंटीस्पॉम साफ्टवेयर का प्रयोग कर इससे बचा जा सकता है।

(D) कुकीज— जब हम वेब ब्राउजर की सहायता से किसी वेबसाइट का उपयोग करते हैं तो उस वेब साइट का सर्वर एक संक्षिप्त डाटा फाइल उपयोगकर्ता के ब्राउजर को भेजता है। कुकीज यह साफ्टवेयर है जिसके द्वारा कोई वेबसाइट कुछ सूचनाएँ उपयोगकर्ता के कम्प्यूटर पर स्टोर करता है। कुकीज उपयोगकर्ता की जानकारी के बिना परदे के पीछे काम करता है। इसके द्वारा सर्वर उपयोगकर्ता की प्राथमिकताएँ तथा उसके द्वारा भेजी गई वेबसाइटों का विवरण वेब ब्राउजर पर संग्रहित रखता है। अगर वही उपयोगकर्ता उसी वेबसाइट पर दोबारा जाता है, तो सर्वर कुकीज के माध्यम से उसकी प्राथमिकताओं और वेबसाइट को प्रस्तुत करता है। कुछ वेबसाइट उपयोगकर्ता के username तथा Password को याद रखते हैं जिससे बार-बार Login करने की जरूरत नहीं पड़ती। इस प्रकार, कुकीज इंटरनेट के उपयोग को आसान बनाता है। कुकीज सामान्यतः कोई नुकसान नहीं पहुँचाते। पर इनका प्रयोग उपयोगकर्ता की सचि के अनुरूप वेबसाइट पर विज्ञापन भेजने के लिए किया जाता है।

दूसरी तरफ, कुछ कुकीज उपयोगकर्ता के व्यक्तिगत सूचनाओं तथा उसके द्वारा वेबोई वेबसाइटों का विवरण रखकर गोपनीयता को खत्म करते हैं। हम वेबब्राउजर साफ्टवेयर का उपयोग करते समय कुकीज को चालू या बंद कर सकते हैं।

(E) प्राक्सी सर्वर—यह स्थानीय नेटवर्क से जुड़ा हुआ ऐसा सर्वर है जो अपने साथ जुड़े हुए कम्प्यूटरों के इंटरनेट से जुड़ने के अनुरोध की निश्चित नियमों के अनुसार जाँच करता है तथा नियमानुसार सही पाये जाने पर ही उसे मुख्य सर्वर को भेजता है। इस प्रकार, यह मुख्य सर्वर तथा उपयोगकर्ता के बीच फ़िल्टर, का कार्य करता है तथा अनाधिकृत उपयोगकर्ताओं से नेटवर्क को सुरक्षा प्रदान करता है।

प्राक्सी सर्वर हार्डवेयर (एक कम्प्यूटर सिस्टम) या साफ्टवेयर या दोनों हो सकता है। क्सी सर्वर के उद्देश्य हैं—

- ⇒ अवांछित वेब पेज या वेबसाइट 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।

(F) फायरवाल—यह एक डिवाइस है जो किसी कम्प्यूटर या नेटवर्क में अनाधिकृत व्यक्तिवों का प्रवेश रोकता है जबकि अधिकृत उपयोगकर्ता को कम्प्यूटर, नेटवर्क व डाटा उपयोग करने देता है। इस प्रकार, फायरवाल किसी कम्प्यूटर, डाटा या स्थानीय नेटवर्क को अनाधिकृत उपयोगकर्ताओं से सुरक्षा प्रदान करता है। फायरवाल हार्डवेयर या साफ्टवेयर या दोनों के रूप में हो सकता है। यह सामान्य नेटवर्क व सुरक्षित नेटवर्क के बीच गेट का काम करता है तथा कम्प्यूटर को नेटवर्क के खतरों जैसे—वायरस, वर्म, हैकर आदि से सुरक्षा प्रदान करता है। फायरवाल किसी स्थानीय नेटवर्क या LAN को इंटरनेट की सुरक्षा खामियों से बचाता है।

फायरवाल :

- ⇒ इनकमिंग डाटा की जाँच करता है।
- ⇒ Usename तथा Password के जरिए अधिकृत उपयोगकर्ता को ही नेटवर्क का प्रयोग करने देता है।
- ⇒ इंटरनेट पर लैन की गोपनीयता बनाए रखता है।

प्रश्न-2.5. कम्प्यूटर वायरस से आप क्या समझते हैं? विभिन्न प्रकार के वायरसों का विवेचन कीजिये।

उत्तर—कम्प्यूटर वायरस—यह एक छोटा दोषपूर्ण साफ्टवेयर प्रोग्राम है जो किसी वैध प्रोग्राम के साथ जुड़कर या इंटरनेट द्वारा कम्प्यूटर की मेमोरी में प्रवेश करता है तथा अपनी काफी स्वयं बनाकर उसे फैलाने में मदद करता है। यह डाटा को मिटाने, उसे खराब करने या उसमें परिवर्तन करने का कार्य कर सकता है। यह हार्ड डिस्क के बूट सेक्टर में प्रवेश कर डिस्क की क्षमता को कम व कम्प्यूटर की गति को धीमा कर सकता है या साफ्टवेयर प्रोग्राम को चलने से रोक सकता है।

किसी प्रोग्राम से जुड़ा वायरस तब तक सक्रिय नहीं होता जब तक उस प्रोग्राम को चलाया न जाए। वायरस ई-मेल मैसेज से नहीं फैलता। ई-मेल पर आने वाला वायरस ई-मेल अटैचमेंट के खोलने पर सक्रिय होता है। 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। कुछ वायरस स्वयं को कम्प्यूटर के बूट सेक्टर से जोड़ लेते हैं। कम्प्यूटर जितनी बार बूट करता है, वायरस उतना ही अधिक फैलता है। कई वायरस कार्पी समय पश्चात भी डाटा प्रोग्राम को नुकसान पहुँचाने की क्षमता रखते हैं।

कम्प्यूटर वायरस मुख्यतः इंटरनेट (ई-मेल, गेम या इंटरनेट फाइल) या मेमोरी उपकरण जैसे—फ्लॉपी डिस्क, सीडी, डीवीडी, पेन ड्राइव आदि के सहारे एक कम्प्यूटर से दूसरे कम्प्यूटर में प्रवेश करता है। इंटरनेट पर फाइल डाउनलोड करने पर उसके साथ लगा वायरस कम्प्यूटर को प्रभावित कर सकता है। वायरस एक साफ्टवेयर प्रोग्राम है, अतः यह कम्प्यूटर हार्डवेयर को प्रभावित नहीं करता। वायरस मेमोरी में घुसकर स्वयं को स्थापित करता है, अतः यह Write Protect मेमोरी तथा Compressed डाटा फाइल को प्रभावित नहीं कर सकता।

वायरस का कम्प्यूटर पर प्रभाव—कई कम्प्यूटर वायरस से प्रभावित है या नहीं, इसे निम्नलिखित लक्षणों से पहचाना जा सकता है—

- ⇒ वायरस कम्प्यूटर के कार्य करने 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 मेमोरी में स्थित कुछ फाइलें प्रभावित होती हैं तथा उनका डाटा दूषित हो जाता है।

कम्प्यूटर वायरस को मुख्यतः तीन भागों में बाँटा जाता है—

(1) प्रोग्राम वायरस (2) बूट वायरस (3) मल्टीपार्टाइट वायरस  
प्रोग्राम वायरस प्रोग्राम फाइलों को प्रभावित करता है जबकि बूट वायरस बूट रिकार्ड, फाइल एलोकेशन टेबल तथा पार्टिशन टेबल को प्रभावित करता है।

1. वर्म—यह एक प्रकार का कम्प्यूटर वायरस है जो अपनी काफी खुद ही बना लेता है तथा कम्प्यूटर की मेमोरी या हार्ड डिस्क में खाली स्थान को भरने लगता है। वर्म वायरस 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 काफी खुद बनाकर तेजी से फैलता है तथा मेमोरी में स्थान घेरता है। वर्म से प्रभावित कम्प्यूटर की गति धीमी हो जाती है तथा मेमोरी क्लेश भी हो सकती है।
2. मालवेयर—यह एक द्वेषपूर्ण साफ्टवेयर है जो उपयोगकर्ता की जानकारी के बिना कम्प्यूटर सिस्टम में घुसकर प्रोग्राम से छेड़छाड़ करता है या उसे नुकसान पहुँचाता है। सभी वायरस, वर्म, टर्जिन हार्स, साइवेयर आदि मालवेयर के उदाहरण हैं।
3. ट्रोजन हार्स—यह एक प्रकार का वायरस है जो स्वयं को एक उपयोगी साफ्टवेयर जैसे—गेम, यूटीलिटी प्रोग्राम आदि की तरह प्रस्तुत करता है। जब उस साफ्टवेयर

को चलाया जाता है तो ट्रेजनि हार्स पृष्ठभूमि में कोई अन्य कार्य संपादित करता है। इसका उपयोग अनाधिकृत व्यक्तियों द्वारा कम्प्यूटर की सूचनाओं तक पहुँचने तथा उनका इस्तेमाल करने के लिए किया जाता है। ट्रेजनि हार्स अपनी काफी स्वयं नहीं बनाता।

4. की-लॉगर- अपने नाम के अनुरूप यह एक ऐसा साफ्टवेयर है, जो कम्प्यूटर में दबाये गये बटनों का रिकार्ड रखता है। इस रिकार्ड का उपयोग बाद में किसी गुप्त सूचना कोड या पासवर्ड की अनाधिकृत जानकारी प्राप्त करने तथा उसका गलत प्रयोग करने के लिए किया जाता है। की-लॉगर प्रोग्राम स्पाइवेयर का एक प्रकार है क्योंकि इसे उपयोगकर्ता की सूचना के बिना कम्प्यूटर में चलाया जाता है।

5. स्पाइवेयर- यह एक द्वेषपूर्ण साफ्टवेयर प्रोग्राम है जिसका उद्देश्य कम्प्यूटर उपयोगकर्ता के विरुद्ध जासूस की तरह कार्य करना होता है। यह द्वेषपूर्ण प्रोग्राम कम्प्यूटर उपयोगकर्ता की जानकारी के बिना कम्प्यूटर उपयोग के बारे में छोटी-छोटी सूचनाएँ जैसे- ईमेल संदेश, यूजरनेम, पासवर्ड, पूर्व में देखी गई वेबसाइट का विवरण आदि इकट्ठा करता है। की-लॉगर स्पाइवेयर का एक उदाहरण है। कुछ कम्पनियाँ अपने कर्मचारियों की गतिविधियों पर नजर रखने के लिए जानबूझकर स्पाइवेयर का प्रयोग करती हैं।

6. हैकर- हैकर का वास्तविक अर्थ है- किसी तंत्र या प्रणाली की कार्य पद्धति को जानने के लिए उसमें छेड़छाड़ करने वाला व्यक्ति।

कम्प्यूटर में हैकर वह व्यक्ति है जो साफ्टवेयर तथा नेटवर्क में विद्यमान सुरक्षा खाभियों का पता लगाकर उनका उपयोग नेटवर्क में घुसने तथा डाटा का अनाधिकृत प्रयोग करने के लिए करता है। वह ऐसा कम्प्यूटर साफ्टवेयर तथा नेटवर्क की खाभियों को उजागर करने के लिए या जिज्ञासावश या आर्थिक लाभ के लिए करता है। नेटवर्क में घुसकर डाटा या साफ्टवेयर से छेड़छाड़ करने की प्रक्रिया हैकिंग कहलाता है। हैकिंग के कारण अधिकृत उपयोगकर्ता नेटवर्क तथा संसाधनों का सही उपयोग नहीं कर पाता। इसे Denial of Service (DoS) कहा जाता है। हैकर को कई श्रेणियों में बाँटा जाता है। साफ्टवेयर तथा नेटवर्क की सुरक्षा कमियों को दूर करने के लिए उनका पता लगाने वाला White hat hacker कहलाता है। साफ्टवेयर को उपयोग के लिए जारी करने से पहले उसकी कमियों को उजागर कर ठीक करने वाला Blue hat hacker कहलाता है। किसी अवैध कार्य के लिए इस पद्धति का प्रयोग करने वाला Black hat hacker कहलाता है।

7. क्रैकर- कम्प्यूटर तथा नेटवर्क की सुरक्षा पद्धति में संघ लागकर या अनाधिकृत साफ्टवेयर द्वारा पासवर्ड प्राप्त कर इनका इस्तेमाल किसी अवैध कार्य के लिए करने वाला क्रैकर कहलाता है। इसे Black hat hacker भी कहते हैं।

सामान्यतः हैकर तथा क्रैकर का प्रयोग एक ही संदर्भ में किया जाता है। हैकर का उद्देश्य कम्प्यूटर तथा नेटवर्क प्रणाली में कमियों को उजागर करना होता है जबकि क्रैकर अपराध या आर्थिक लाभ के लिए ऐसा करता है।

8. पासवर्ड क्रैकिंग- कम्प्यूटर तथा नेटवर्क का पासवर्ड कोड फॉर्म में स्टोर किया जाता है। क्रैकर साफ्टवेयर प्रोग्राम की मदद से कोडडे पासवर्ड का पता लगा लेते हैं तथा इसका प्रयोग अवैध कार्यों तथा अनाधिकृत उपयोग के लिए करते हैं। Password Cracker एक ऐसा ही साफ्टवेयर प्रोग्राम है।

9. पैकेट स्निफिंग- इंटरनेट पर डाटा को पैकेट में बाँटकर भेजा जाता है। डाटा पैकेट्स को अपने गंतव्य तक पहुँचाने से पहले ही उसकी पहचान कर उसे रिकॉर्ड कर लेना पैकेट स्निफिंग कहलाता है।

10. पैच- साफ्टवेयर कम्पनियों द्वारा उपयोग के लिए जारी साफ्टवेयर में कई खाभियाँ होती हैं जिनका फायदा हैकर/क्रैकर उठाते हैं। साफ्टवेयर कम्पनियों द्वारा इन कमियों में सुधार के लिए समय-समय पर छोटे साफ्टवेयर प्रोग्राम जारी किए जाते हैं, जिन्हें पैच कहा जाता है। ये पैच साफ्टवेयर मुख्य साफ्टवेयर के साथ ही कार्य करते हैं।

11. स्केअर वेयर- यह कम्प्यूटर वायरस का एक प्रकार है जो इंटरनेट से जुड़े कम्प्यूटर को प्रभावित करता है। इसमें इंटरनेट से जुड़े उपयोगकर्ता को कोई फ्री ईटीवायरस या फ्री साफ्टवेयर डाउनलोड करने का लालच दिया जाता है। यह एक अधिकृत साफ्टवेयर की तरह दिखता है, परन्तु इसे डाउनलोड करते ही वायरस कम्प्यूटर में प्रवेश कर जाता है।

प्रश्न-26. कम्प्यूटर डाटा सुरक्षा प्रदान करने वाले तत्वों के नाम लिखिए तथा संक्षेप में वर्णन कीजिये।

उत्तर- (1) फिशिंग- इंटरनेट पर इंटरनेट उपयोगकर्ताओं के यूजर नेम, पासवर्ड तथा अन्य व्यक्तिगत सूचनाओं को प्राप्त करने का प्रयास करना फिशिंग कहलाता है। इसके लिए उपयोगकर्ता को झूठे ई-मेल या संदेश भेजे जाते हैं जो दिखने में वैध वेबसाइट से आये हुए लगते हैं। इन ई-मेल या संदेश में उपयोगकर्ता को अपना यूजरनेम, लॉग इन आई डी या पासवर्ड तथा अन्य विवरण डालने को कहा जाता है जिनके आधार पर उपयोगकर्ता के गुप्त विवरणों की जानकारी प्राप्त की जा सकती है।

(2) डिजिटल हस्ताक्षर- यह कम्प्यूटर नेटवर्क पर किसी व्यक्ति की पहचान स्थापित करने, उसकी स्वीकृति प्राप्त करने तथा किसी तथ्य को सत्यापित करने की एक पद्धति है। इसमें नेटवर्क सुरक्षा का भी ध्यान रखा जाता है। डिजिटल सिग्नेचर तकनीक का प्रयोग कम्प्यूटर पर स्टोर किए गए किसी डॉक्यूमेंट का प्रिंट लिए बिना उस पर हस्ताक्षर करने के लिए किया जाता है। डिजिटल सिग्नेचर किसी मैसेज या डॉक्यूमेंट के साथ जुड़ जाता है तथा उसकी वैधता प्रमाणित करता है। डिजिटल सिग्नेचर कम्प्यूटर पर कोडडे फॉर्म में स्टोर किया जाता है ताकि उसे अनाधिकृत उपयोगकर्ताओं की पहुँच से दूर रखा जाए। ई-कामर्स तथा ई-प्रशासन में इसका प्रयोग प्रचलित हो रहा है।

(3) एंटी वायरस साफ्टवेयर- कम्प्यूटर तथा नेटवर्क पर विभिन्न साफ्टवेयर वायरस के खतरों से बचने के लिए एंटी वायरस साफ्टवेयर का प्रयोग किया जाता है। यह ऐसा

साफ्टवेयर प्रोग्राम होता है जो साफ्टवेयर में विद्यमान दृष्टपूर्ण प्रोग्राम, कर उन्हें नष्ट करता है तथा वैध साफ्टवेयर में घुसने से रोकता है।

एंटीवायरस साफ्टवेयर का आटो प्रोटेक्ट प्रोग्राम इस्तेमाल से पूर्व किसी साफ्टवेयर, ई-मेल या इंटरनेट फाइल की जाँच करता है तथा वायरस के सक्रिय होने पर तत्काल सूचित भी करता है। कम्प्यूटर को वायरस से मुक्त करने के लिए समय-समय पर सिस्टम स्कैन द्वारा कम्प्यूटर मेमोरी की जाँच की जानी चाहिए। जैसे-जैसे वायरस प्रकाश में आते हैं, वैसे ही कम्पनियाँ उसके लिए एंटी वायरस प्रोग्राम भी जारी करती हैं। इस कारण यह जरूरी है कि एंटी वायरस साफ्टवेयर का समय-समय पर नवीनीकरण किया जाए।

चूँकि एंटी वायरस साफ्टवेयर किसी भी प्रोग्राम या फाइल को चालू किए जाने से पहले उसकी जाँच करता है, अतः वह कम्प्यूटर के काम करने की गति को कम कर देता है। कुछ प्रचलित एंटी वायरस साफ्टवेयर प्रोग्राम हैं-

1. Norton
2. Bit Defender
3. McAfee
4. Kaspersky
5. AVG
6. Symantec
7. AVAST

प्रश्न-27. डिजिटल सिग्नेचर का क्या आशय है? संक्षेप में वर्णन कीजिए।

उत्तर- डिजिटल सिग्नेचर- डिजिटल सिग्नेचर एक क्रिप्टोग्राफिक तकनीक है, जो लिखित सिग्नेचर की तरह ही कार्य करती है व जिससे भेजेज के प्राथुर्भाव व अवयव दोनों की जाँच की जा सकती है। डिजिटल सिग्नेचर के तकनीकी विश्लेषण की प्रक्रिया लगभग एक दशक से जारी है। डिजिटल सिग्नेचर्स बहुत से राष्ट्रीय व अन्तर्राष्ट्रीय स्टैंडर्ड्स में स्वीकार किये जा चुके हैं, जिन्हें बहुत से व्यापारिक संगठन, बैंक्स और सरकारी एजेंसी ने निर्धारित कर रखा है।

सिग्नेचर्स के कानूनी उद्देश्य- सिग्नेचर ट्रांजेक्शन्स के सबस्टेन्स का भाग नहीं है, बल्कि उसका एक रूप है। सिग्नेचर के द्वारा निम्नलिखित उद्देश्य पूरे किये जाते हैं-

(1) एवीडेन्स (Evidence)- सिग्नेचर साइन किये डॉक्यूमेंट के साथ साइन करने वाले को पहचान कर उसकी लिपि के सही-गलत का निर्धारण करता है। यदि साइन करने वाला कुछ अलग तरीके से निशान चिन्हित करता है, तब वह चिन्ह उसकी विशेष पहचान होती है।

(2) सेरेमनी (Ceremony)- साइन करने वाला यदि डॉक्यूमेंट को साइन करता है तो यह समझा जाता है कि वह साइनर एक्ट के कानून महत्व को समझता है और अस्वीकार्य कार्यों को रोकने में मदद करता है।

(3) एप्रूवल (Approval)- कुछ विशेष संदर्भ जो लॉ व कस्टम के द्वारा परिभाषित हैं, वहाँ सिग्नेचर साइन करने वाली की अनुमति मानी जाती है और यह माना जाता है कि वह कानूनी रूप से अधिकृत किया गया है।

(4) इफिशियन्सी एण्ड लॉजिस्टिक्स (Efficiency & Logistics)- एक लिखित डॉक्यूमेंट में साइन करने से तार्कर्य ट्रांजेक्शन का स्पष्ट और पूर्ण होना माना जाता है और उससे अधिक जाँच-पड़ताल की आवश्यकता को भी कम करता है।

प्रश्न-28. डिजिटल सिग्नेचर के महत्व का वर्णन कीजिए।

उत्तर- डिजिटल सिग्नेचर के महत्व- डिजिटल सिग्नेचर का निर्माण और उसका निरीक्षण उन सभी प्रभावों को शामिल करता है जो कानूनी रूप से सिग्नेचर के लिए आवश्यक होते हैं-

(1) साइन करने वाले की पहचान- परिवर्तित साइनर (साइन करने वाले) के पास पब्लिक-की व प्रायवेट-की दोनों का समूह हो तब डिजिटल सिग्नेचर की से तब तक जालसाजी नहीं हो सकती है जब तक कि साइनर प्रायवेट-की का नियंत्रण न खा दे। जैसे या तो वह किसी को बता दे या फिर उसका मीडिया या वह उपकरण गुप्त हो जाए, जिसमें वह की शामिल है।

(2) भैसेज की पहचान- डिजिटल सिग्नेचर साइन किए हुए भैसेज की भी पहचान पेपर सिग्नेचर की तुलना में अधिक निश्चितता व शुद्धता के साथ करते हैं। जाँच किसी भी प्रकार के हेरफेर को रोकता है, क्योंकि हेरफेर रिजल्ट (एक साइन करता है तथा दूसरा जाँच करता है) की तुलना यह बताती है कि यह वही भैसेज है कि नहीं, जिसे साइन किया था।

(3) सकारात्मकता- डिजिटल सिग्नेचर बनाने की प्रक्रिया में साइनर को उसकी प्रायवेट-की का उपयोग आवश्यक होता है। यह तरीका साइनर द्वारा उस तथ्य की उस औपचारिकता को दर्शाता है कि साइनर ने अपना ट्रांजेक्शन कानूनी आधार पर पूर्ण कर दिया है।

(4) क्षमता- डिजिटल सिग्नेचर बनाने और जाँचने की प्रक्रिया उच्च-स्तर पर यह तय करती है कि यह डिजिटल सिग्नेचर संबंधित व्यक्ति के ही हैं। आधुनिक इलेक्ट्रॉनिक डेटा इन्टरेचेंज ("EDI") की परिस्थिति में निर्माण और जाँच की प्रक्रिया सम्पूर्ण रूप से स्वचालित होती है। इसे मशिनेबल भी कहते हैं, इसमें मानव का हस्तक्षेप कभी-कभी ही आवश्यक होता है।



दीर्घ एवं लघु उत्तरीय प्रश्न-

प्रश्न-1. ऑनलाइन ट्रांजेक्शन क्या है? यह किस प्रकार उपयोगी है? इसके उपयोग में क्या सावधानी बरतनी चाहिए? किसी एक राष्ट्रीयकृत बैंक का उदाहरण देकर इसका विस्तारपूर्वक वर्णन कीजिए।

उत्तर- ऑनलाइन ट्रांजेक्शन के लिए हमने राष्ट्रीयकृत बैंक 'स्टेट बैंक ऑफ इंडिया' (एस.बी.आई.) का उदाहरण प्रस्तुत किया है। यह केवल समझाने के लिए निम्नानुसार वर्णित किया गया है-

एक्स्टेंड वेलीडेशन एस्पएसएल क्या है? - स्पष्ट रूप से एक वेबसाइट की संस्थागत पहचान को पहचानने के लिए एक्स्टेंड वेलीडेशन एस्पएसएल प्रमाणपत्र उच्च-सुरक्षा वेब ब्राउजर जानकारी प्रदान करता है। उदाहरण के लिए, यदि आप एस्पएसएल प्रमाणपत्र जो एक्स्टेंड

वेलीडेसन मानक है, से सुरक्षित एक वेबसाइट पर जाने के लिए माइक्रोसॉफ्ट इंटरनेट एक्सप्लोरर का प्रयोग करते हैं, तो आईई7 यूआरएल एड्रेस बार हरे रंग में परिवर्तित हो जाएगा। हरे रंग के बार के बाद प्रमाणपत्र में सूचित संस्थान के नाम और प्रमाणपत्र प्राधिकरण (उदाहरण के लिए, Verisign) के बीच एक डिजिटल दिखवाई देगा। फायरफॉक्स 3 भी एक्स्टेंडेड वेलीडेसन एस्पएसएल का समर्थन करता है। अन्य ब्राउजर्स द्वारा आने वाले संस्करणों में एक्स्टेंडेड वेलीडेसन विजिबिलिटी प्रदान करना अपेक्षित है। पुराने ब्राउजर्स मौजूदा एस्पएसएल प्रमाणपत्रों में मौजूद सुरक्षा प्रतीक के साथ एक्स्टेंडेड वेलीडेसन एस्पएसएल प्रमाणपत्र डिसले करेगे।

ऑनलाइन धोखाधड़ी और फिशिंग से बचने के सुझाव—

- व्यक्तिगत या वित्तीय सूचना के लिए तत्काल अनुरोध वाले ई-मेल अथवा टेक्स्ट संदेशों के प्रति सावधान रहें। (एसबीआई तथा ज्यादातर अन्य वित्तीय संस्थाएँ और क्रेडिट कार्ड कम्पनियों मौजूदा ग्राहक की सूचना की पुष्टि करने के लिए सामान्यतः ई-मेल का प्रयोग नहीं करते हैं)।
- किसी विश्वसनीय स्रोत जैसे फोन बुक या बिल से टेलीफोन नंबर लेकर संगठन से संपर्क करें।
- जब आप ऑनलाइन एसबीआई और मोबाइल ऑनलाइन एसबीआई में लॉगइन करते हैं तो हमेशा पैडलॉक अवश्य देखें तथा ऑनलाइन एसबीआई के लिए यूआरएल एड्रेस <https://www.onlinedbi.com/retail/login.htm> और मोबाइल ऑनलाइन एसबीआई के लिए <https://m.onlinedbi.com/m/retail/login.htm> होना चाहिए।
- पूरी तरह निश्चित होने के लिए, ब्राउजर एड्रेस बार में [www.onlinedbi.com](http://www.onlinedbi.com) या <https://m.onlinedbi.com> टाइप करें।
- यदि आप एक ऐसा ई-मेल प्राप्त करते हैं जो भारतीय स्टेट बैंक से होने का दावा करता है और सदस्य सा प्रतीत होता है तो दिए गए किसी भी लिंक पर क्लिक न करें अथवा इसका उत्तर न दें। इसे डिलीट कर दें।
- आपको एक सुरक्षित साइट पर ले जाने का दावा करने वाले ई-मेल में दिए गए लिंक का प्रयोग न करें।
- टेक्स्ट मेसेज के माध्यम से कभी भी व्यक्तिगत सूचना, खाता संख्या, पासवर्ड या अन्य कोई संवेदनशील सूचना न दें क्योंकि इसका कपटपूर्ण उपयोग हो सकता है। यदि आप कोई ऐसा टेक्स्ट संदेश प्राप्त करते हैं जिसमें आपको तत्काल सूचना अद्यतन करने, खाता सक्रिय करने अथवा एक फोन नंबर पर कॉल करके या एक वेबसाइट पर सूचना देकर अपनी पहचान सत्यापित करने के बारे में कहा गया हो तो कृपया सावधानी बरतें। ये संदेश आपके खाते की गोपनीय सूचना को हारिल करने और धोखाधड़ी करने के लिए धोखाबाजों द्वारा संचालित फिशिंग स्कैम का एक हिस्सा हो सकता है।
- वेबसाइट की एड्रेस लाइन को देखने की आदत डालें और यदि इसमें प्रदर्शित एड्रेस ई-मेल में दिए गए एड्रेस से कुछ अलग है तो इसे सत्यापित कर लें।
- एंटी-वाइरस सॉफ्टवेयर, स्पाइवेयर फिल्टर, ई-मेल फिल्टर और फायरवाल प्रोग्रामों से नियमित रूप से अपनी कम्प्यूटर सुरक्षा को अद्यतन करते रहें।

- जब भी आप अनपेक्षित पत्र/फोन कॉल प्राप्त करते हैं जिसमें आपके व्यक्तिगत अथवा वित्तीय जानकारी के बारे में पूछा गया हो या साइट पर अद्यतन करने के लिए कहा गया हो तो एक सामान्य नियम के रूप में, इन पर विश्वास न करें। इस प्रकार के कॉलों की प्रामाणिकता सत्यापित करने के लिए उपलब्ध कार्यालयीन माध्यमों से अपने बैंक से सीधा संपर्क करें।
- संदेहपूर्ण ई-मेल, वेबसाइट, सोशल मीडिया नेटवर्क, टेक्स्ट संदेश या फोन कॉलों के जरिए किसी भी प्रकार की गोपनीय सूचना शेयर न करें।
- प्रचलित वेब ब्राउजर का उपयोग करें। एसबीआई द्वारा समर्थित ब्राउजर की प्रचलित सूची देखें।
- आपका ऑनलाइन बैंकिंग यूजरनेम या पासवर्ड अन्य ऑनलाइन अकाउंट्स जैसा नहीं होना चाहिए।
- आपके सभी लेनदेन सही हैं, इसकी पुष्टि करने के लिए अपने बैंक, क्रेडिट और डेबिट कार्ड विवरणी की नियमित रूप से जाँच करें।
- इसकी रिपोर्ट करें— यदि आप इस प्रकार का कोई संदेहजनक ई-मेल प्राप्त करें— तो इसकी सूचना को अथवा उस संस्थान जहाँ से मेल आई प्रतीत होती है, को दें। यदि आपने इस प्रकार का संदेहजनक ई-मेल प्राप्त किया है और अनजाने में ही अपनी व्यक्तिगत जानकारी और वित्तीय सूचना प्रदान कर दी है तो इन बातों का अनुसरण करें—
- स्टेप-1. अपने बैंक/वित्तीय संस्थान या क्रेडिट कार्ड कंपनी से संपर्क करें।
- स्टेप-2. अपने स्थानीय पुलिस से संपर्क करें।
- स्टेप-3. हमेशा फिशिंग की रिपोर्ट करें। यदि आपने इस प्रकार के एक संदेहजनक ई-मेल का उत्तर दे दिया है, को इसकी रिपोर्ट करें।
- आपकी ऑनलाइन सुरक्षा— भारतीय स्टेट बैंक में, हम उद्योग के उच्चतम सुरक्षा मानक का उपयोग करते हैं। और किसी प्रकार के नए सुरक्षा खतरों का सामना करने के लिए हम नियमित रूप से इसकी समीक्षा करते हैं।
- जब आप ऑनलाइन बैंकिंग करते हैं, तब आपके लेनदेनों की सुरक्षा करने के लिए हम द्वारा किए गए कुछ उपाय इस प्रकार हैं—
- जब आप लॉगइन करते हैं—
- आपको आपके खाते तक पहुँच, आपके विशिष्ट यूजरनेम और पासवर्ड द्वारा नियंत्रित है।
- तीन-गलत लॉगइन प्रयासों के पश्चात खाते तक आपकी पहुँच स्थगित कर दी जाती है।
- हम आपको आपके पिछले लॉगइन का दिनांक और समय दिखाते हैं, जिससे आपको पता चल सके कि किसी अन्य व्यक्ति ने आपके खाता तक पहुँच बनाने का प्रयास नहीं किया है।
- जब आप ऑनलाइन बैंकिंग करते हैं—
- आपको सूचना को सुरक्षित रखने के लिए हमारे पास 128 बिट एस्पएसएल इनक्रिप्शन है। इसका सीधा अर्थ यह है कि आपकी सूचना इंटरनेट पर एक दुर्बोध कोड के रूप में संचारित होती है जिसे सिर्फ हम सुलझा सकते हैं।

- ऑनलाइन भुगतान करने, अन्य पक्षकार जोड़ने आदि के समय "उच्च सुरक्षा" आपको सुरक्षा का एक अतिरिक्त स्तर प्रदान करता है। एसएमएस के रूप में प्राप्त यह वन टाइम पासवर्ड आपको पहचान को प्रमाणित करता है और लैनदेन की प्रक्रिया पूरी करता है।
- हमारे प्रत्येक सुरक्षित वेबसाइट में Verisign द्वारा जारी एक एसएसएल एक्स्टेंडेड वेलीडेसन प्रमाणपत्र है जो आपको यह जताता है कि वेबसाइट वास्तविक और सुरक्षित है।
- ऑनलाइन एसबीआई और मोबाइल ऑनलाइन एसबीआई का भी एक एक्स्टेंडेड वेलीडेसन (ईवी) एसएसएल प्रमाणपत्र है। अर्थात् यदि आप इंटरनेट एक्सप्लोरर का प्रयोग कर रहे हैं, जब आप हमारी साइट खोलेंगे आपको एड्रेस बार हरे रंग में परिवर्तित हो जाएगी। यह आपको यह सुनिश्चित करने में मदद करता है कि आप वास्तविक ऑनलाइन एसबीआई वेबसाइट पर हैं।
- एसएसएल प्रमाणपत्र के बारे में सूचना के लिए Verisign website देखें। अथवा ईवी प्रमाणपत्रों के बारे में अधिक जानकारी के लिए देखें।
- जब आपका कार्य समाप्त हो जाए—
- यदि एक निर्धारित समय तक आपका एकाउण्ट निष्क्रिय है तो आप अपने एकाउण्ट से स्वतः बाहर आ जाते हैं।
- आपके लॉगऑफ करने के पश्चात हमारी ऑनलाइन बैंकिंग वेबसाइट में आपके द्वारा देखे गए सभी पृष्ठ आपके ब्राउजर कैश से स्वतः हट जाते हैं। इससे आपके बाद उस कम्प्यूटर का प्रयोग करने वाले व्यक्ति के पास आपके व्यक्तिगत या अकाउण्ट ब्यौरा देखने का मौका नहीं होता है। उदाहरण के लिए, ब्राउजर का बैक बटन का चयन करने से या कम्प्यूटर की हार्ड-ड्राइव के विषयों को खोजना से।
- भारतीय स्टेट बैंक में पृष्ठभूमि में कार्यरत सुरक्षा विशेषज्ञ—
- हमारी समर्पित सुरक्षा टीम नई प्रौद्योगिकियों का अनुसंधान करती है, कार्यकलापों की निगरानी करती है और उभरने वाले सुरक्षा संबंधी किसी भी मुद्दे पर तत्काल कार्रवाई करती है।
- हम अपने सारे सिस्टम की सुरक्षा जाँच के लिए नियमित रूप से प्रतिष्ठित स्वतंत्र परामर्शदाताओं का उपयोग करते हैं।
- किसी संभावित सुरक्षा समस्या का पता लगाने और उस पर तत्काल कार्रवाई करने के अपने प्रयासों के एक अंग के रूप में नियमित गहन सुरक्षा ड्रिलिंग की जाती है।
- सुरक्षित ऑनलाइन बैंकिंग—उपयुक्त पासवर्ड का चयन करें—
- यूनिक कैरेक्टर (विशेष अक्षरांक) : एक स्वीकार्य पासवर्ड में कम से कम पाँच (5) विविध कैरेक्टर होने चाहिए। कैरेक्टरों को दोहराने से उलटे-सीधे एक समान वाले शब्द बन सकते हैं और जिसे आसानी से सुलझाया (क्रिक) जा सकता है।
- कैरेक्टर टाइप : एक स्वीकार्य पासवर्ड में कम से कम तीन विविध प्रकार के कैरेक्टर होने चाहिए— ऊपर केस, लोअर केस, संख्या, विराम चिह्न आदि। विविध कैरेक्टर समूह के नमूनों से बने पासवर्ड को सुलझाना (क्रिक करना) मुश्किल होता है।

- लॉग आउट सिक्वेंस (अधिवर्णय क्रम) : एक स्वीकार्य पासवर्ड में दो कैरेक्टर से ज्यादा संख्या क्रम (डिजिट सिक्वेंस) नहीं होना चाहिए।
- निर्दिष्ट कैरेक्टर : कुछ ऐसे कैरेक्टर हैं जिनका प्रयोग पासवर्ड में करने पर असुविधा हो सकती है— "delete" उसी प्रकार का एक कैरेक्टर है।
- पासवर्ड निम्नलिखित से कोई नहीं होना चाहिए—
- शब्दकोश के शब्द (विदेशी एवं तकनीकी शब्दकोशों को मिलाकर)
- किसी व्यक्ति अथवा वस्तु का नाम, स्थान, सर्वनाम, फोन नंबर अथवा वाहन नंबर की-बोर्ड पर अक्षरों की तरह सामान्य स्वरूप
- उपरोक्त में से कोई भी विलोम अथवा श्रृंखला रूप में
- एक अच्छा पासवर्ड बनाने का एक तरीका है अपना आर्द्विचिक (एकरानिम) बनाना।
- अपने पासवर्ड को हमेशा सुरक्षित रखें—
- पासवर्ड शेयर करना असुरक्षित है।
- अपना पासवर्ड किसी को न बताएँ।
- केवल निर्धारित स्थान पर ही अपना यूजर आईडी और पासवर्ड भरें— जैसा आप सामान्यतः करते हैं।
- असामान्य प्रतीत होने पर, जानकारी देने से पहले यह सुनिश्चित कर लें कि आपकी व्यक्तिगत जानकारी को चुराने का प्रयास तो नहीं है।
- ई-मेल द्वारा प्राप्त किसी एक हाइपरलिंक पर क्लिक करने पर पॉप-अप के रूप में सामने दिखाई देने वाले किसी भी पृष्ठ पर अपना यूजर आईडी और पासवर्ड न दें। यह सुनिश्चित करने के पश्चात कि खुलने वाला पृष्ठ वास्तविक सेवा प्रदाता से है, एड्रेस बार पर यूआरएल टाइप करके सेवा के लिए लॉगऑन करना बेहतर है।
- सूचना-कूटांकन (इन्क्रिपशन) के बिना पासवर्ड को कम्प्यूटर सिस्टम (पाम पर्सेटल अथवा मिलते-जुलते उपकरण) की किसी फाइल में न रखें।
- कम से कम प्रत्येक नब्बे दिन में एकबार अपना पासवर्ड बदलें।
- अपने कम्प्यूटर को अपना याद रखने न दें। अपने कम्प्यूटर/ब्राउजर द्वारा प्रदत्त आटो कम्प्लीट विकल्प का चयन न करें।
- यथा संभव किसी संवेदनशील सेवा का उपयोग करने के लिए किसी अविश्वसनीय सिस्टम का प्रयोग न करें। यदि आपको करना ही पड़े, तो तत्पश्चात तत्काल किसी विश्वसनीय सिस्टम पर पहली बार में ही अपना पासवर्ड बदल दें।
- एसएमएस के द्वारा प्राप्त वन टाइम पासवर्ड सक्रिय करना—
- "Profile" भाग में उच्च सुरक्षा सक्रिय करें। अन्य पक्षकार जोड़ना, अन्य पक्षकार अन्तरण आदि जैसे विविध लैनदेन सुरक्षित रूप से करने के लिए यह द्वितीय स्तर पर प्रमाणीकरण है।
- लॉगआउट करना न भूलें—
- ऑनलाइन बैंकिंग कार्य समाप्त होने के पश्चात "logout" पर क्लिक करके सेवा से ऑनलाइन करना सुनिश्चित करें। उसके बाद ब्राउजर विंडो बंद कर दें।

जाँच करें कि वेबसाइट सुरक्षित है—

- अपने ब्राउजर से ऑनलाइन एसबीआई/मोबाइल ऑनलाइन एसबीआई पर जाने के लिए यूआरएल एड्रेस बार पर नजर रखते हुए [www.onlinesbi.com](http://www.onlinesbi.com) या [m.onlinesbi.com](http://m.onlinesbi.com) एड्रेस टाइप करें।
- लॉगइन पृष्ठ पर, ब्राउजर विंडो में कहीं पर (प्रायः एड्रेस बार के अन्त में या बाहिने तरफ कोने में locked स्थिति में) आपको पैडलॉक दिखाई देगा जो यह संकेत करता है कि आप जिस वेबसाइट पर हैं वह वास्तविक है और हमारे साथ (ऑनलाइन एसबीआई) आपका संप्रेषण उच्च स्तर पर इंक्रिप्टेड है। सुरक्षा प्रमाणपत्र देखने के लिए पैडलॉक पर क्लिक करें।
- आपके इंटरनेट ब्राउजर के एड्रेस बार में यूआरएल एड्रेस को देखें जो "https" से आरंभ होता है, "https" के अन्त में 's' अक्षर का अर्थ है 'secured' (सुरक्षित)। ई-मेलों से सावधान रहें—

- कभी भी अनजाने स्रोतों से प्राप्त ई-मेलों के संलग्नक (अटैचमेंट) को डाउनलोड न करें और न ही उससे जुड़े हुए लिंक पर क्लिक करें। आपके व्यक्तिगत या वित्तीय जानकारी माँगने वाले ई-मेल के प्रति सावधान रहें।
- वित्तीय संशोधन से भेजने का वादा करने वाले ई-मेल की वैधता की जाँच करने के लिए उस संस्थान से व्यक्तिगत रूप से या फोन द्वारा या सुरक्षित मेल बॉक्स के माध्यम से संपर्क करें।

ग्राहक संबंधी सूचना प्राप्त करने के लिए एसबीआई कभी भी ई-मेल/एसएमएस नहीं भेजता है और ना ही फोन करता है। यदि आपके पास कोई ऐसा मेल आता है जिसमें आपके यूजरनेम या पासवर्ड या अन्य कोई व्यक्तिगत जानकारी पृथी गई है और यह मेल एसबीआई से भेजे जाने का वादा किया गया है तो तुरंत ही पर रिपोर्ट करें।

अपना कम्प्यूटर सुरक्षित रखें—

- व्यक्तिगत फायरवाल का उपयोग करें।
- एंटीवायरस सॉफ्टवेयर इंस्टाल करें और नवीनतम सिग्नेचर से इसे अद्यतन रखें।
- एंटीस्पाइवेयर सॉफ्टवेयर रखें।
- नियमित रूप से अपना ओपरेटिंग सिस्टम अद्यतन रखें।
- पब्लिक या नेटवर्क से जुड़े कम्प्यूटरों से सावधान रहें।

प्रश्न-2. सुरक्षित ऑनलाइन बैंकिंग की विशेषताएँ लिखिए। ऑनलाइन धोखाधड़ी और फ्रिशिंग के विभिन्न प्रकार संक्षेप में समझाइयें।

उत्तर— सुरक्षित ऑनलाइन बैंकिंग के लिए विशेषताएँ— ऑनलाइन एसबीआई निरापद और सुरक्षित बैंकिंग के लिए विविध अन्तर्निहित विशेषताएँ प्रदान करता है। आप प्रोफाइल टैब में सुरक्षा विकल्पों का उपयोग निम्नलिखित के लिए कर सकते हैं—

अपना व्यक्तिगत प्रोफाइल अपनी आवश्यकतानुसार बनाएँ— अपने व्यक्तिगत प्रोफाइल में आप अपना नाम प्रदर्शन, मोबाइल नंबर और ई-मेल आईडी सेट कर सकते हैं। नाम प्रदर्शन का प्रयोग स्वागत संदेश में होता है।

अन्य पक्ष का प्रबंधन— आप अपने विश्वसनीय अन्य पक्ष, जिन्हें आप निधि अन्तरण करना चाहते हैं, को परिभाषित कर सकते हैं। आप अपने विश्वस्त अन्य पक्षों की सूची में जोड़ सकते हैं, हटा सकते हैं या उसमें संशोधन भी कर सकते हैं।

राशि सीमा निर्धारित करना— प्रोफाइल अनुभाग में आप माँग ड्राफ्ट और अन्य पक्ष अन्तरण के लिए राशि सीमा निर्धारित कर सकते हैं। अपेक्षाकृत कम सीमा निर्धारित करना उपयुक्त रहेगा। जब और जैसे भी आवश्यकता हो आप इस सीमा को बढ़ा सकते हैं।

उच्च सुरक्षा सक्रिय करें— एसएमएस आधारित उच्च सुरक्षा आपके लेनदेनों के लिए प्रदत्त सुरक्षा का एक अतिरिक्त स्तर है। आप के लिए यह उपयुक्त होगा कि प्रोफाइल अनुभाग में इस विशिष्टता को सक्रिय करें। जब आप स्वयं अथवा अन्य पक्ष के खाते में निधि अन्तरण करते हैं, माँग ड्राफ्ट जारी करते हैं या पीपीएफ खाते में निधि जमा करते हैं, तो आपको एसएमएस के माध्यम से एक उच्च सुरक्षा पासवर्ड प्राप्त होगा। लेनदेन पूरा करने के लिए आपको इस पासवर्ड का प्रयोग करने की आवश्यकता है।

ऑनलाइन धोखाधड़ी और फ्रिशिंग के विविध प्रकार—

फ्रिशिंग ई-मेल और वेबसाइट— अपराधियों द्वारा व्यक्तिगत, वित्तीय और संवेदनशील सूचना हासिल करने के लिए भेजे गए तथा जो प्रतिष्ठित एवं विश्वसनीय व्यवसायियों, वित्तीय संस्थानों और सरकारी एजेंसियों से आए हुए प्रतीत होने वाले जाली ई-मेल, टेक्स्ट संदेश और वेबसाइट को सामान्य शब्दों में फ्रिशिंग कहते हैं। यह ब्रांड स्क्रिपिंग के नाम से भी जाना जाता है। यदि आप कभी भी ऐसा ई-मेल प्राप्त करते हैं, जिस पर आपको संदेह हो तो इसका उत्तर न दें या दिए गए लिंक पर क्लिक भी न करें। इसे डिलीट कर दें। कोई भी संदेहजनक ई-मेल जिसने एसबीआई के नाम का उपयोग किया हो के बारे में आप तत्काल ही पर रिपोर्ट कर सकते हैं। फ्रिशिंग के बारे में अधिक जानकारी के लिए यहाँ पढ़ें।

गोप्य विज्ञो/विज्ञापन— गोप्य-अप वे विज्ञापन है जो अलग ब्राउजर विंडो में "गोप्य अप" होते हैं। जब आप इस प्रकार के किसी भी गोप्य-अप पर क्लिक करते हैं, यह भी संभव है कि आप "स्पाईवेयर" या "एडवेयर" भी डाउनलोड कर रहे हैं।

फ्रिशिंग— वित्तीय पुरस्कार के उद्देश्य से लोगों की गोपनीय, व्यक्तिगत और वित्तीय जानकारी. तक पहुँचने के लिए अवैध रूप से सोशल इंजीनियरिंग और चॉइस ओवर आईपी (वीओआईपी) का प्रयोग करना फ्रिशिंग है। यह शब्द "चॉइस" और "फ्रिशिंग" से मिलकर बना है।

धोखेबाज एक स्वयंमूलित सिस्टम या वास्तविक व्यक्ति के माध्यम से किसी भी नम्बर पर फोन करते हैं और किसी बैंक/वित्तीय कम्पनी की तरफ से कॉल करने का वादा करते हुए आपको आपके खाते में कुछ समस्या होने का कारण बताते हुए, बैंक खाता, कार्ड ब्योरा आदि से संबंधित जानकारी अद्यतन करने के लिए कहते हैं कि उन्होंने अपने सिस्टम को अपग्रेड किया है।

स्मिशिंग— स्मिशिंग, फ्रिशिंग के समान ही सोशल इंजीनियरिंग तकनीकों का उपयोग करते हुए आपराधिक कर्माचालप का ही एक रूप है। स्मिशिंग से प्रभावित लोग एसएमएस संदेश प्राप्त करते हैं। "स्मिशिंग" नाम से कुख्यात वे टेक्स्ट संदेश प्रापकर्ता को किसी किसी

ऑनलाइन सेवा के लिए पंजीकरण करने को कहते हैं- उसके बाद प्रयोगकर्ता के डिवाइस में वायरस डालने की कोशिश करते हैं। कुछ संदेश यह चोतावनी भी देते हैं कि यदि उपभोक्ता अपना/अपनी व्यक्तिगत या वित्तीय जानकारी एक वेबसाइट में अद्यतन नहीं करता/करती है तो उसे इसका जुर्माना देना पड़ेगा, जिसके पश्चात् वे इस प्रकार की जानकारी और अन्य गोपनीय तथ्य हारिल करते हैं।

की-लोगिंग- अर्थात् की-लोगिंग सॉफ्टवेयर कम्प्यूटर पर टाइप किए गए सम्पत्त तथा रिकार्ड कर सकता है और यह जानकारी एक बाहरी व्यक्ति को भेज सकता है। ई-मेल में संलग्न वायरस या अन्य प्रकार के डाउनलोड के माध्यम से अधिकांश की-लोगिंग "स्पाइवेयर" या "एडवेयर" कम्प्यूटर को प्रभावित करते हैं।

प्रश्न-3. ऑनलाइन बैंकिंग को किस प्रकार सुरक्षित किया जा सकता है? इसके सुझाव लिखिए।

उत्तर- सुरक्षित ऑनलाइन बैंकिंग के लिए महत्वपूर्ण सुझाव-

- अपने ब्राउजर के एड्रेस बार में यूआरएल टाइप करके ही बैंक वेबसाइट तक पहुँचे।
- ऑनलाइन बैंकिंग प्रदान करने वाले मोबाइल एलिकेशन डाउनलोड करने से सावधान रहें। डाउनलोड करने से पहले कृपया अपने बैंक से सम्पर्क करके उनकी वास्तविकता की जाँच करें।
- साइट पर पहुँचने के लिए किसी ई-मेल संदेश में दिए गए लिंक पर क्लिक न करें।
- आपकी व्यक्तिगत जानकारी, पासवर्ड या वन टाइम एसएमएस (उच्च सुरक्षा) पासवर्ड प्राप्त करने के लिए एसबीआई या इसका कोई भी प्रतिनिधि कभी भी आपको न ही ई-मेल/एसएमएस भेजता है या फोन करता है। इस प्रकार का ई-मेल/एसएमएस या फोन कॉल इंटरनेट बैंकिंग के माध्यम से आपके अकाउंट तक पहुँचकर धोखे से नकदी आहरण का प्रयास है। कभी भी इस प्रकार के ई-मेल/एसएमएस या फोन कॉल का उत्तर न दें। यदि आप ऐसा कोई ई-मेल/एसएमएस या फोन कॉल प्राप्त करते हैं तो तुरंत पर रिपोर्ट करें। कृपया तत्काल अपना यूजर एक्सेस लॉक कर दें; यदि आपने अनजाने में अपनी जानकारी प्रदान कर दी है। लॉक करने के लिए यहाँ क्लिक करें।
- व्यक्तिगत जानकारी प्रदान करने या बैंक साइट में अकाउंट ब्यौरा अद्यतन करने के लिए पुरस्कार देने का वादा करने वाले ई-मेल/एसएमएस/फोन कॉल के प्रलोभन में न पड़ें।
- निम्नलिखित बातें आपकी इंटरनेट सुरक्षा को बेहतर बनाएँगी-  
• ब्राउजर का नवीनतम वर्जन (आईई 7.0 और आगे, मोजिल्ला फायरफॉक्स 3.1 और आगे, सफारी 3.5 और आगे, गूगल क्रोम आदि)
- फायरवाल सक्रिय करें
- प्रयुक्त एंटीवायरस सिग्नेचर
- सिस्टम वाइरस/ट्रोजन से मुक्त है यह सुनिश्चित करने के लिए नियमित रूप से एंटीवायरस से अपना कम्प्यूटर स्कैन करें।
- आवाधिक अन्तराल में अपने इंटरनेट बैंकिंग पासवर्ड को बदलें।
- हमेशा पोस्ट लॉगइन पृष्ठ पर पिछले लॉगइन दिनांक और समय की जाँच करें।

- साइबर बैंक या साइबा पीसी से अपने इंटरनेट बैंकिंग अकाउंट का उपयोग न करें।
- लॉगइन करने के पश्चात् आपको यूजरनेम और लॉगइन पासवर्ड देने के लिए नहीं कहा जाएगा। इंटरनेट बैंकिंग का उपयोग करते समय, आपको क्रेडिट या डेबिट कार्ड का ब्यौरा देने के लिए भी नहीं पूछा जाएगा। यदि आप कोई संदेश (जैसे- पॉप-अप के माध्यम से) प्राप्त करते हैं जिसमें इस प्रकार की जानकारी माँगी गई हो, वह पृष्ठ चाहे कितना भी वास्तविक प्रतीत क्यूं न हो, कृपया कोई सूचना प्रदान न करें। इस प्रकार के पॉप-अप ज्यादातर मालवेयर के परिणाम होते हैं जो कम्प्यूटर को प्रभावित करते हैं। कृपया अपने डिवाइस को इस प्रभाव से बचाने के लिए तत्काल कदम उठाएं।

प्रश्न-4. राष्ट्रीय इलेक्ट्रॉनिक फंड ट्रांसफर क्या होता है?

उत्तर- एनईएफटी (NEFT) - नेशनल इलेक्ट्रॉनिक फंड्स ट्रांसफर अथवा एनईएफटी एक राज्यव्यापी भुगतान प्रणाली एक बैंक खाते से दूसरे बैंक खाते में धन की आवाजाही को सक्षम बनाती है। आजकल ऑनलाइन बैंकिंग पर अधिक जोर दिए जाने के साथ, एनईएफटी धन हस्तान्तरण के सबसे व्यापक रूप से उपयोग किए जाने वाले तरीकों में से एक तरीके के रूप में उभरा है। एनईएफटी का उपयोग करके फंड ट्रांसफर करने के लिए किसी को बैंक शाखा में जाने की आवश्यकता नहीं होती है क्योंकि इसके माध्यम से इलेक्ट्रॉनिक रूप से किसी भी बैंक खाते से दूसरे बैंक खाते में राशि ट्रांसफर कर सकते हैं।

एनईएफटी (NEFT) लेनदेन की प्रक्रिया- एनईएफटी एक तात्कालिक प्रक्रिया नहीं है और फंड-ट्रांसफर अनुरोधों को बैंकों में संसाधित किया जाता है। एनईएफटी करने हेतु निम्नलिखित प्रक्रिया अपनाई जाती है-

- (1) धन हस्तान्तरित करने हेतु हमें लाभार्थी का विवरण जैसे लाभार्थी का नाम, बैंक की शाखा का नाम जहाँ लाभार्थी का खाता है, शाखा का IFSC कोड, खाता प्रकार और संख्या। विवरण भरकर एक आवेदन पत्र को बैंक को देना होगा।
- (2) मूल बैंक शाखा डेटा एकत्र करती है और एनईएफटी सर्विस सेन्टर को एक संदेश भेजती है।
- (3) एनईएफटी सर्विस सेन्टर अगले उपलब्ध बैंक में शामिल होने के लिए एनईएफटी क्लियरिंग सेंटर को संदेश भेजता है।
- (4) अब समाशोधन केन्द्र फंड ट्रांसफर लेनदेन को गंतव्य बैंक-वार क्रमबद्ध करता है और फिर मूल बैंक से धन प्राप्त करने और लाभार्थी के बैंक में धनराशि भेजने के लिए प्रविष्टियों को तैयार करता है।
- (5) इस बिन्दु तक गंतव्य बैंक समाशोधन केन्द्र से आवक प्रेषण संदेश प्राप्त करता है और लाभार्थी ग्राहक के खाते में क्रेडिट की प्रक्रिया सम्पन्न करता है।

प्रश्न-5. रियल टाइम ग्रांस सेटलमेंट से क्या समझते हैं?

उत्तर- आरटीजीएस (RTGS)- रीयल-टाइम सेटलमेंट, या आरटीजीएस, एक ऐसी प्रणाली है जो एक बचत खाते से दूसरे बचत खाते में धन हस्तान्तरण के अनुरोधों को प्रेषक बैंक द्वारा प्राप्त होते ही संसाधित करती है।

- (1) एनईएफटी के विपरीत, आरटीजीएस प्रत्येक फंड ट्रांसफर निर्देश को स्वतंत्र रूप से और क्रम में संसाधितक करता है।
  - (2) RTGS द्वारा भारत के बैंक से दूसरे बैंक में पैसा तुरंत ट्रांसफर किया जा सकता है।
  - (3) RTGS का उपयोग केवल उच्च राशि वाले लेनदेन में ही किया जाना चाहिए।
  - (4) RTGS लेनदेन न्यूनतम 2 लाख रुपये की राशि तक सीमित है। यदि राशि इससे कम है, तो व्यक्ति को एनईएफटी का उपयोग करना चाहिए।
  - (5) ये सुविधाएँ सभी बैंक अपने ग्राहकों को प्रदान करते हैं, लेकिन सभी बैंकों की प्रत्येक शाखा में ये सेवाएँ उपलब्ध नहीं हैं।
- आरटीजीएस फॉर्म (RTGS Form)**— अधिकांश निजी और राष्ट्रीयकृत भारतीय बैंक अपने शाखा स्थानों, वेबसाइटों या मोबाइल ऐप के माध्यम से आरटीजीएस धन हस्तान्तरण करने की ऑफर देते हैं। उपयोगकर्ता आरटीजीएस फॉर्म को पीडीएफ प्रारूप में प्रिंट करके, भरकर अपनी स्थानीय बैंक शाखा में जमा कर सकते हैं। उपयोगकर्ता इसका उपयोग करके ऑनलाइन धनराशि भेज सकते हैं क्योंकि यह सम्पानन योग्य प्रारूप में भी उपलब्ध है।
- भुगतानकर्ता को वास्तविक समय सकल निपटान फॉर्म में, निम्नलिखित जानकारी देनी होगी—

- (1) आवेदक या प्रेषक का नाम, खाता संख्या, जमा की गई धनराशि, फोन नम्बर, ईमेल पता और पता।
- (2) आईएफएस कोड, जमा खाता संख्या, नकद राशि और चेक नम्बर भुगतान का विवरण।
- (3) लाभार्थी की जानकारी में लाभार्थी का नाम, उसका खाता नम्बर, शाखा, पता और जमा की जाने वाली राशि भी भरनी होती है।

**प्रश्न-6.** आईएमपीएस क्या है? तत्काल भुगतान सेवा तथा इंटरनेट बैंकिंग को समझाइए।

**उत्तर—**आईएमपीएस (IMPS)— तत्काल भुगतान सेवा (आईएमपीएस) नामक एक वास्तविक समय इलेक्ट्रॉनिक नकद हस्तान्तरण तकनीक भुगतानकर्ता/लाभार्थी के खाते में तत्काल धनराशि जमा करने की अनुमति देती है। यह सुविधा रविवार और अन्य छुट्टियों सहित वर्ष के 24/7, 365 दिन उपलब्ध रहती है, और इसे किसी भी समय पूरा किया जा सकता है। भारतीय रिजर्व बैंक और नेशनल पेमेंट्स कॉरपोरेशन ऑफ इंडिया दोनों इस सेवा का प्रबंधन करते हैं।

नेट बैंकिंग के माध्यम से आईएमपीएस ट्रांसफर करने के लिए, प्रेषक को बैंक खाता या, आईएफएससी कोड, बैंक का नाम, बैंक खाता इत्यादि जैसे सभी विवरण देकर लाभार्थी को पंजीकृत करना होता है। प्रत्येक बैंक के लिए अलग-अलग लेनदेन शुल्क होता है। राशि ट्रांसफर पर शुल्क केवल भेजी गई राशि पर निर्भर करता है। शुल्क 1 रुपये से लेकर 7 रुपये तक होता है और अधिकांश मामलों में बैंक 5 रुपये से अधिक शुल्क नहीं लेते हैं।

**आईएमपीएस (IMPS) की विशेषताएँ—** ये निम्नवत हैं—

- (1) आईएमपीएस के माध्यम से धन हस्तान्तरण NEFT और RTGS की तरह ही सुरक्षित है।
- (2) किसी भी इंटरनेट कनेक्शन वाले स्मार्ट डिवाइस या फोन पर इस सुविधा का उपयोग करना आसान है।
- (3) यह बैंक खातों के बीच पैसे ट्रांसफर करने के सबसे तेज तरीकों में से एक है।
- (4) इसमें प्रेषक के सेल (मोबाइल) फोन नम्बर से किसी को भी पैसा भेजा जा सकता है।
- (5) इस विधि से प्रेषक के खाते में तुरंत धनराशि जमा हो जाती है।
- (6) इस ब्लैटफॉर्म पर फंड ट्रांसफर के लिए लोगों को अपने बैंक विवरण, विशेषतः अपने खाता नम्बर साझा करने की आवश्यकता नहीं है।
- (7) यह सेवा पूरे वर्ष (365 दिन) और 24 घंटे उपलब्ध है।
- (8) इस सेवा में किसी भी पक्ष से कोई शुल्क नहीं लिया जाता है अर्थात् ये निःशुल्क सेवा है।
- (9) इसमें लेन-देन पूरा होने के बाद दोनों पक्षों को मोबाइल पर मैसेज भेज दिए जाते हैं जिसमें लिखा होता है कि आपके खाता नम्बर को डेबिट और क्रेडिट किया गया है।
- (10) वर्तमान में इस सुविधा के लिए अधिकतम ट्रांसफर सीमा 5 लाख रुपये है।
- (11) उपयोगकर्ता के पास अपने बैंक का एटीएम सह डेबिट कार्ड होना चाहिए।
- (12) उपयोगकर्ता को एसएमएस अलर्ट हेतु अपने बैंक के साथ रजिस्टर्ड होना चाहिए।
- (13) यदि उपयोगकर्ता के पास बेसिक बैंडसेट है तो इस सेवा का उपयोग केवल एसएमएस और टेक्स्टिंग के द्वारा ही किया जा सकता है।
- (14) ऐसे मोबाइल फोन वाले ग्राहक जिनके पास उनके सेवा-प्रदाता के साथ-साथ जावा द्वारा सक्षम GPRS है, वे उच्च सुरक्षा और राशि के लिए इसका ऑनलाइन उपयोग कर सकते हैं।
- (15) कुछ बैंकों के पास स्मार्ट फोन के लिए अपने स्वयं के एप्लिकेशन हैं जहाँ आईएमपीएस शीघ्रता से किया जा सकता है।

**आईएमपीएस (IMPS) लेनदेन को पूरा करने के लिए आवश्यक विवरण—** आईएमपीएस (IMPS) भुगतान पूरा करने के लिए लाभार्थी के निम्नलिखित विवरणों में से एक आवश्यक है—

- (1) आधार नम्बर
- (2) IFS कोड और बैंक खाता संख्या
- (3) मोबाइल मनी आईडेंटिफायर और मोबाइल नम्बर।

**प्रश्न-7.** यूनिफाइड भुगतान इंटरफेस (UPI) पर दिव्यणी लिखिए।

**उत्तर—** यूनिफाइड पेमेंट्स इंटरफेस (UPI) एक स्मार्टफोन एप्लिकेशन है जो उपयोगकर्ताओं को बैंक खातों के बीच पैसे ट्रांसफर करने की अनुमति देता है। यह नेशनल

पेमेंट्स कॉरपोरेशन ऑफ इंडिया द्वारा विकसित एक सिंगल-विंडो मोबाइल भुगतान प्रणाली है। इसमें हर बार ग्राहक द्वारा लेनदेन शुरू करने पर बैंक विवरण या अन्य संबंधित जानकारी दर्ज करने की आवश्यकता नहीं रहती। जिससे यह बैंक तक पहुंचने का एक सुरक्षित तरीका बन जाता है।

(1) यूनिफाइड पेमेंट्स इंटरफेस (UPI) भारत में बैंकिंग के लिए एक स्मार्टफोन एप्लिकेशन है।

(2) भारतीय रिजर्व बैंक इंटरफेस को विनियमित करता है।

यूनिफाइड भुगतान इंटरफेस (UPI) कार्यप्रणाली- इंटरफेस (UPI) एक वारताविक समय भुगतान प्रणाली है। इसे एकल दो-किलक कारक प्रभागीकरण प्रक्रिया के माध्यम से पीयर-टू-पीयर अंतर-बैंक हस्तान्तरण को सक्षम करने के लिए डिजाइन किया गया है। इंटरफेस को भारत के केन्द्रीय बैंक भारतीय रिजर्व बैंक द्वारा विनियमित किया जाता है। यह एक मोबाइल नेटवर्क के साथ दो बैंक खातों के बीच धनराशि ट्रांसफर करने का काम करता है।

यह प्रणाली दो पक्षों के बीच धन हस्तान्तरित करने का सुरक्षित तरीका मानी जाती है और इसमें भौतिक नकदी या बैंक के माध्यम से लेनदेन की आवश्यकता नहीं है। पायलट सिस्टम को भारत में 11 अप्रैल, 2016 को लांच किया गया था। देशभर के बैंकों ने अगस्त, 2016 में अपना इंटरफेस अपलोड करना शुरू कर दिया था।

एनपीसीआई (UPI)- खातों में निर्बाध निपटान सुनिश्चित करने के लिए (UPI) तत्काल भुगतान सेवा और आधार सक्षम भुगतान प्रणाली जैसी मौजूदा प्रणालियों का उपयोग करता है। यह भुगतान (पुश) और प्राप्त (पुल) लेनदेन की सुविधा देता है और यहाँ तक कि ओवर-द-काउंटर या बारकोड भुगतान के साथ-साथ उपयोगिता बिल, स्कूल फीस और अन्य सदस्यता जैसे कई आवर्ती भुगतानों के लिए भी काम करता है।

प्रश्न-8. एनईएफटी, यूपीआई और आईटीसीएस के बीच अंतर लिखिए।

उत्तर- NEFT, UPI और RTGS में अंतर-

मापक	NEFT	UPI	RTGS
(1) न्यूनतम स्थानान्तरण मूल्य	रु. 1	रु. 1	रु. 2 लाख
(2) भुगतान विकल्प	ऑनलाइन और ऑफलाइन	ऑनलाइन	ऑनलाइन और ऑफलाइन
(3) अधिकतम अंतरण मूल्य	कोई सीमा नहीं	रु. 2 लाख	कोई सीमा नहीं
(4) स्थानान्तरण समय	30 मिनट तक	तत्काल	तत्काल
(5) सेवा समय	24x7 उपलब्ध	24x7 उपलब्ध	24x7 उपलब्ध
(6) आवक लेनदेन शुल्क	कोई शुल्क नहीं	कोई शुल्क नहीं	कोई शुल्क नहीं
(7) आवश्यक विवरण	खाता संख्या और आईएफएससी कोड	लाभार्थी का वीपीए/ क्यूआर कोड/खाता संख्या और	नाम, खाता संख्या और आईएफएस कोड, खाता संख्या

(8) लाभार्थी पंजीकरण	हाँ	नहीं	जुड़ा मोबाइल नंबर
	हाँ	नहीं	हाँ

प्रश्न-9. आधार सक्षम भुगतान प्रणाली क्या है? समझाइए।

उत्तर- आधार सक्षम भुगतान प्रणाली (AEPs)- आधार सक्षम भुगतान प्रणाली (AEPs) एक बैंक-आधारित भुगतान मॉडल है जो सभी आधार कार्ड धारकों को एक विशिष्ट पहचान संख्या (यूआईडी) का उपयोग करके माइक्रो-स्वचालित टेलर मशीन (एटीएम) या बिक्री बिन्दु (पीओएस) पर मॉडिक लेनदेन करने की अनुमति देता है।

नेशनल पेमेंट कॉरपोरेशन ऑफ इंडिया ने भारत में कैशलेस लेनदेन को बढ़ावा देने के लिए यह पहल की। उनका मुख्य उद्देश्य समाज के सभी वर्गों के लोगों को आधार के माध्यम से वित्तीय और बैंकिंग सेवाओं तक पहुंचने के लिए अधिकृत करना था। उपयोगकर्ता को अन्य सुविधाओं के साथ-साथ फंड ट्रांसफर करने, नकदी जमा करने, धैसे निकालने और खाते की शेष राशि की जांच करने की अनुमति देता है।

लोगों को एक व्यवसाय संचालना के माध्यम से बैंकिंग और वित्तीय सेवाएँ जैसे- फंड ट्रांसफर, नकद निकासी, मिनी स्टैटमेंट, बैलेस पूछताछ आदि करने के लिए सशक्त बनाने के उद्देश्य से, भारतीय रिजर्व बैंक और भारत सरकार द्वारा खुदरा भुगतान में नकदी रहित होने की योजना बनाई गई है। केन्द्रीकृत स्वचिग और समाशोधन संगठनों के माध्यम से आधार-उत्पन्न अंतरबैंक लेनदेन को सक्षम करना।

आधार का उपयोग करके किसी भी राज्य या केन्द्र सरकार के निकायों के लिए सामाजिक सुरक्षा पेंशन, विकलांग, वृद्धावस्था पेंशन, राष्ट्रीय ग्रामीण रोजगार गारंटी अधिनियम आदि जैसी सरकारी योजनाओं के भुगतान को सरल बनाने के लिए, AEPs का उपयोग किया जाता है।

बैंकिंग सेवाएँ-

- |                               |                     |
|-------------------------------|---------------------|
| (1) आधार से आधार फंड ट्रांसफर | (2) नकद निकासी      |
| (3) भीम आधार भुगतान           | (4) प्रमाणीकरण      |
| (5) नकद जमा                   | (6) शेष राशि पूछताछ |
| (7) मिनी स्टैटमेंट            |                     |

अन्य सेवाएँ-

- |                        |                       |
|------------------------|-----------------------|
| (1) आधार सीडिंग स्थिति | (2) बायोमेट्रिक पहचान |
| (3) डेमो प्राधिकरण     | (4) टोकनाइजेशन        |

(5) इलेक्ट्रॉनिक अपने ग्राहक को जानें या इकेबायसी।

प्रश्न-10. अनुपूरक सेवा शटा (USSD) पर टिप्पणी लिखिए।

उत्तर- USSD एक नोबल सिस्टम और मोबाइल क्युनिकेशन्स प्रोटोकॉल है जिसका उपयोग टेक्स्ट संदेश भेजने के लिए किया जाता है। USSD लघु संदेश सेवा के समान है।

USSD मोबाइल फोन पर उपलब्ध वर्णों से बने कोड का उपयोग करता है। एक USSD संदेश, जो 182 अक्षरों तक लम्बा हो सकता है, फोन और किसी अन्य डिवाइस-आमतौर पर, एक नेटवर्क या सर्वर के बीच एक वास्तविक समय संचार सत्र स्थापित करता है।

USSD का उपयोग वायरलेस एलिकेशन प्रोटोकॉल ब्राउजिंग, मोबाइल मनी सेवाओं, प्रीपेड कॉलबैक सेवा, मैनू-आधारित सूचना सेवाओं और लोकेट के लिए किया जा सकता है। USSD के साथ, उपयोगकर्ता विभिन्न मैनू से चयन करके अपने मोबाइल फोन से सीधे बातचीत करते हैं। एक एसएमएस संदेश के विपरीत, USSD सत्र के दौरान, एक USSD संदेश एक वास्तविक समय कनेक्शन बनाता है। अर्थात् USSD सूचना के दोतरफा संचार को सक्षम बनाता है, जब तक संचार लाइन खुली रहती है। इस प्रकार, प्रश्न और उत्तर लगभग तात्कालिक हैं।

**USSD की कार्य-प्रणाली-** आमतौर पर, USSD में मोबाइल फोन उपयोगकर्ता की एक क्वेरी शामिल होती है, जैसे बैंक खाते की शेष राशि जानने के लिए अनुरोध। एक बार जब उपयोगकर्ता अनुरोध भेजता है, तो USSD नेटवर्क इसे उपयोगकर्ता के USSD एलिकेशन को भेज देता है, जो अनुरोध का जवाब देता है।

इसके बाद प्रक्रिया को उल्टा दोहराया जाता है, अर्थात् प्रतिक्रिया USSD नेटवर्क वापस चली जाती है, जो उस प्रतिक्रिया को सामग्री को उपयोगकर्ता के मोबाइल फोन की स्क्रीन पर प्रदर्शित करती है। आमतौर पर प्रतिक्रियाएं, जिनमें अधिकतम 182 अल्फान्यूमेरिक वर्ण होते हैं, ऐसे प्राकृतिक में भेजी जाती हैं जिसे प्रदर्शित करना आसान हो। उपयोगकर्ता एक विशिष्ट शॉर्ट कोड डायल करके डेटा भेजता और प्राप्त करता है। आमतौर पर यह कोड पाँच नम्बर का होता है।

USSD एलिकेशन नेटवर्क पर चलते हैं, उपयोगकर्ता के डिवाइस पर नहीं। इस प्रकार, उन्हें उपयोगकर्ता के फोन पर इंस्टॉल करने की आवश्यकता नहीं है। यह सीमित स्टोरेज स्पेस वाले फीवर फोन वाले उपयोगकर्ताओं के लिए सुविधाजनक है। USSD एस नेटवर्क पर तैनात होते ही प्रत्येक ग्राहक के लिए तुरंत उपलब्ध हो जाते हैं।

**प्रश्न-11. क्रेडिट कार्ड क्या है?**

**उत्तर-** क्रेडिट कार्ड (Credit Card)- क्रेडिट कार्ड एक वित्तीय साधन है जो बैंकों द्वारा पूर्व-निर्धारित क्रेडिट सीमा के साथ जारी किया जाता है, जो आपको कैशलेस लेनदेन करने में सहायता करता है। कार्ड जारीकर्ता उपयोगकर्ता के क्रेडिट स्कोर, क्रेडिट इतिहास और आपकी आय के आधार पर क्रेडिट सीमा निर्धारित करता है।

भारत में अनेक प्रकार के क्रेडिट कार्ड उपलब्ध हैं। ये प्रत्येक व्यक्ति की जीवनशैली की आवश्यकताओं के अनुरूप विभिन्न लाभ और सुविधाएँ प्रदान करते हैं। क्रेडिट कार्ड की कुछ सामान्य श्रेणियाँ निम्नलिखित हैं-

- (1) शॉपिंग क्रेडिट कार्ड- ये कार्डधारक को आपकी ऑनलाइन और ऑफलाइन खरीदारी पर पुरस्कार, छूट और कैशबैक प्रदान करते हैं।
- (2) यात्रा क्रेडिट कार्ड- ये कार्ड बार-बार यात्रा करने वालों के लिए हवाई मील, लाउज पसुं, यात्रा बीमा और अन्य सुविधाएँ प्रदान करते हैं।

(3) कैशबैक क्रेडिट कार्ड- ये कार्डधारक को खर्च का एक प्रतिशत नकद पुरस्कार के रूप में प्रदान करते हैं, जिसे स्टेटमेंट क्रेडिट या वाउचर के लिए भुनाया जा सकता है।

(4) छात्र क्रेडिट कार्ड- ये कार्ड उन छात्रों के लिए डिज़ाइन किए गए हैं जो अपना क्रेडिट इतिहास बनाना चाहते हैं और कम ब्याज दरों, कोई वार्षिक शुल्क नहीं और कोई विदेशी मुद्रा मार्कअप शुल्क जैसे लाभों को लेना चाहते हैं।

**क्रेडिट कार्ड आवेदन प्रक्रिया-** यदि उपयोगकर्ता का क्रेडिट मजबूत है, तो वह पहले क्रेडिट कार्ड के लिए व्यक्तिगत रूप से, मेल द्वारा, फोन पर या ऑनलाइन आवेदन करते समय विभिन्न प्रकार के क्रेडिट कार्ड प्रदाताओं में से सुविधा अनुसार कोई भी कार्ड का चुनाव कर सकता है।

**क्रेडिट स्कोर जांचने की प्रक्रिया-** क्रेडिट कार्ड प्राप्त करने की सुविधा के लिए द्वारा भुगतान की जाने वाली ब्याज दरें और कोई भी लाभ जिसका उपयोगकर्ता पात्र हो सकता है, वह क्रेडिट स्कोर पर निर्भर करता है। इस कारण क्रेडिट स्कोर को सत्यापित करना आवश्यक है।

300-800 तक क्रेडिट स्कोर की पूरी शृंखला को जोखिम श्रेणियों में विभाजित किया गया है- खराब, उचित, अच्छा और उत्कृष्ट। अधिकांश क्रेडिट कार्डों के लिए अच्छे या बेहतर क्रेडिट स्कोर की आवश्यकता होती है। यदि स्कोर इस सीमा को पूरा नहीं करता है, तो उपयोगकर्ता क्रेडिट स्कोर को बेहतर बनाने के लिए काम कर सकते हैं या इसे क्रेडिट कार्ड पर का चयन कर सकते हैं जो उपलब्ध क्रेडिट स्कोर पर मिल सकता है।

**प्रश्न-12. डेबिट कार्ड क्या होता है?**

**उत्तर-** डेबिट कार्ड- डेबिट कार्ड, एक भुगतान कार्ड होता है जिसका उपयोग खरीदारी करने के लिए नकदी के स्थान पर किया जा सकता है। क्रेडिट कार्ड में आमतौर पर आगे या पीछे बैंक का नाम, कार्ड नम्बर, कार्डधारक का नाम और स्मार्टि लिथि होती है। कई नए कार्डों में अब एक चिप लगी होती है, जो लोगों को अपने कार्ड को स्वर्श करके या कार्ड डालकर और चुम्बकीय पट्टी को स्वाइप करके पिन डालकर उपयोग करने की अनुमति देती है। ये क्रेडिट कार्ड के समान होते हैं, लेकिन क्रेडिट कार्ड के विपरीत, खरीदारी के समय खरीदारी का पैसा कार्डधारक के बैंक खाते में होना आवश्यक होता है और खरीदारी का भुगतान करने के लिए तुरंत उस खाते से व्यापारी के खाते में ट्रांसफर कर दिया जाता है।

कुछ डेबिट कार्ड (प्रीपेड कार्ड) में एक संग्रहीत मूल्य होता है जिसका उपयोग भुगतान करने के लिए किया जा सकता है, जबकि अधिकांश कार्डधारक के बैंक को कार्डधारक के निर्दिष्ट बैंक खाते से पैसे निकालने का अनुरोध भेजते हैं। अन्य परिस्थितियों में, कोई भौतिक कार्ड मौजूद नहीं है क्योंकि भुगतान कार्ड नम्बर केवल ऑनलाइन उपयोग के लिए निर्दिष्ट किया गया है। इसे वर्चुअल कार्ड कहा जाता है।

डेबिट कार्ड अब इतने अधिक उपयोग किए जाते हैं कि अनेक देशों में उन्होंने या तो चेक को पूरी तरह से प्रतिस्थापित कर दिया है या उनके उपयोग को अल्पतम कम कर दिया है। डेबिट कार्ड ने बड़े पैमाने पर नकद लेनदेन का स्थान ले लिया है। डेबिट कार्ड का विकास,

क्रेडिट कार्ड और चार्ज कार्ड के विकास के विपरीत, आमतौर पर देश-विशिष्ट रहा है, जिसके कारण दुनियाभर में अनेक प्रकार की विविध प्रणालियाँ विकसित हुई हैं जो अक्सर असंतत होती हैं। 2000 के दशक के मध्य से, कई परियोजनाओं ने एक देश में जारी डेबिट कार्ड का दूसरे देश में उपयोग करना, साथ ही फोन और इंटरनेट पर खरीदारी करना संभव बना दिया है।

डेबिट कार्ड अक्सर त्वरित नकदी निकासी को सक्षम बनाते हैं, जिन्हें नकद अप्रिम के रूप में जाना जाता है, और इस तरह वे एटीएम कार्ड के रूप में काम करते हैं। ग्राहकों को रिटेल विक्रेताओं द्वारा कैशबैक विकल्प प्रदान किए जा सकते हैं ताकि वे अपनी खरीदारी के साथ-साथ वेसे भी निकाल सकें। निकाली जा सकने वाली नकदी की मात्रा पर आमतौर पर दैनिक सीमाएँ होती हैं। डेबिट कार्ड अक्सर वारिस्टिक के बने होते हैं, हालांकि कभी-कभी वे धातु या लकड़ी के भी बने होते हैं।

एक सामान्य डेबिट कार्ड के सामने वाले भाग का एक उदाहरण—

- |                                  |                       |
|----------------------------------|-----------------------|
| (1) जारी करने वाले बैंक का लोगो। | (2) ईएमवी चिप।        |
| (3) होलोग्राम।                   | (4) कार्ड नम्बर (धन)। |
| (5) कार्ड ब्रांड लोगो            | (6) समाप्ति तिथि      |
| (7) कार्डधारक का नाम             |                       |

एक सामान्य डेबिट कार्ड के पिछले भाग का एक उदाहरण—

- |                        |                            |
|------------------------|----------------------------|
| (1) चुम्बकीय पट्टी।    | (2) सिग्नेचर स्ट्रिप पैनल। |
| (3) कार्ड सुरक्षा कोड। |                            |

प्रश्न-13. वन टाइम पासवर्ड क्या है?

उत्तर— वन-टाइम पासवर्ड— वन-टाइम पासवर्ड (ओटीपी) एक अतिरिक्त एकल-उपयोग पासवर्ड है जो कम्प्यूटर या ऑनलाइन सेवा में लॉग इन करने के लिए आपके नियमित पासवर्ड के अतिरिक्त आवश्यक है। अनधिकृत उपयोगकर्ताओं को अन्य लोगों के खातों में लॉगइन करने से रोकने में मदद करने के लिए प्रमाणीकरण की एक अतिरिक्त परत जोड़ने के लिए कम्प्यूटर या सेवा तुरंत आपके लिए एक वन-टाइम पासवर्ड उत्पन्न करती है। ओटीपी दो-कारक प्रमाणीकरण कहलाने वाला पहला कदम है। वे अधिक सामान्य होते जा रहे हैं क्योंकि साइबर अपराधी आईडी चोरी करने के लिए ऑनलाइन उपयोगकर्ता के नाम और पासवर्ड प्राप्त कर लेते हैं।

वन-टाइम पासवर्ड वर्णों की एक स्ट्रिंग है जिसका उपयोग किसी उपयोगकर्ता को लेपटाप कम्प्यूटर डेस्कटाप कम्प्यूटर या ऑनलाइन सेवा तक पहुँच के लिए प्रमाणित करने के लिए किया जा सकता है। अधिकांश ओटीपी उपयोगकर्ता के मोबाइल फोन पर एक टेक्स्ट संदेश में भेजे गए चार से छह अंकों के होते हैं जो मोबाइल या ईमेल पते पर भेजे जाते हैं। साइबर सुरक्षा को मजबूत करने के तरीके के रूप में इन्हें आमतौर पर पारम्परिक उपयोगकर्ता के नाम और पासवर्ड के साथ संयोजन में उपयोग किया जाता है।

कुछ ओटीपी छह से अधिक संख्याओं या अल्फान्यूमेरिक वर्णों की स्ट्रिंग का उपयोग करते हैं। ओटीपी आमतौर पर एक ही बार उपयोग तक सीमित होते हैं और अक्सर थोड़े

समय के बाद समाप्त हो जाते हैं। एस्पएस टेक्स्ट संदेशों का उपयोग आमतौर पर उपयोगकर्ताओं को ओटीपी भेजने के लिए किया जाता है।

प्रश्न-14. त्वरित प्रतिक्रिया कोड क्या है?

उत्तर— त्वरित प्रतिक्रिया (क्यूआर) कोड— त्वरित प्रतिक्रिया कोड एक प्रकार का बारकोड होता है जिसे डिजिटल डिवाइस द्वारा आसानी से पढ़ा जा सकता है और जो चौकोर आकार के गिड में पिक्सेल की शृंखला के रूप में जानकारी संग्रहीत करता है। क्यूआर कोड का उपयोग अक्सर आपूर्ति शृंखला में उत्पादों के बारे में जानकारी ट्रैक करने के लिए किया जाता है। यह अक्सर विपणन और विज्ञापन अभियानों में उपयोग किया जाता है।

क्यूआर कोड को पुराने, एक-आयामी बारकोड से उन्नत माना जाता है। यह सन् 2000 में अन्तर्राष्ट्रीय मानकीकरण संगठन द्वारा एक अन्तर्राष्ट्रीय मानक के रूप में अनुमोदित किया गया था।

प्रश्न-15. बारकोड पर टिप्पणी लिखिए।

उत्तर— बारकोड— किसी उत्पाद या सेवा के बारे में दी जा सकने वाली जानकारी की मात्रा पारम्परिक रूप से उत्पाद की पैकेजिंग पर जगह की मात्रा या उसके लाभों के बारे में बताने वाले विज्ञापन द्वारा सीमित थी। यदि कोई उपभोक्ता उत्पाद के बारे में अधिक जानकारी चाहता है— उसकी उपलब्धता, कीमत, विशेषताएँ— तो उन्हें एक विक्रेता को ढूँढना होगा या अतिरिक्त दस्तावेजीकरण का अनुरोध करना होगा।

बारकोड आमतौर पर उत्पाद पैकेजों के पीछे पाए जाते हैं और समानान्तर रेखाओं की विभिन्न चौड़ाई के संयोजन का उपयोग करके डेटा सम्प्रोचित करते हैं, जिन्हें ऑप्टिकल स्कैनर वाली मशीनों द्वारा पढ़ा जा सकता है।

बारकोड ने कम्पनियों द्वारा इन्वेंट्री और मूल्य निर्धारण को प्रबंधित करने के तरीके में क्रांति ला दी और इसे पहली बार 1960 के दशक में अमेरिकी रेलमार्गों द्वारा उपकरण और कंटेनरों को ट्रैक करने के लिए व्यावहारिक उपयोग में लाया गया था। सन् 1974 में पारम्परिक, द्वि-आयामी बारकोड अमेरिकी खुदरा स्टोरों में आम उपयोग में आए। बारकोड अब कर्मचारी आईडी बैज और अस्पताल से लेकर शिपिंग कंटेनर तक प्रत्येक वस्तु में पाए जाते हैं।

प्रश्न-16. निम्न पर संक्षिप्त टिप्पणी लिखिये—

(1) इलेक्ट्रॉनिक नकद (2) स्मार्टकार्ड (3) संबंध आधारित स्मार्ट कार्ड।

उत्तर— (1) इलेक्ट्रॉनिक नकद— इलेक्ट्रॉनिक नकद (ई-नकद) ऑन लाइन भुगतान नयी अवधारणा है क्योंकि इसमें सुरक्षा तथा प्राइवैसी के साथ कम्प्यूटरीकृत सुविधा भी होती है जो कागजी मुद्रा से बेहतर है। इसकी सार्वभौमिकता नये बाजारों तथा अनुप्रयोगों को परिचित करती है। ई-नकद में कई रोचक लक्षण होते हैं जो इंटरनेट पर भुगतान के आकर्षक विकल्प के रूप में विकसित हो सकते हैं।

ई-नकद उपभोक्ता प्रदत्त इलेक्ट्रॉनिक प्रणाली में मुख्य भुगतान वाहक के रूप में नकदी भुगतान का स्थान लेने पर फोकस करता है। यद्यपि यह कुछ के लिए आश्चर्यजनक हो सकता है। नकद आज भी सबसे अधिक प्रचलित उपभोक्ता भुगतान उपकरण है। यह स्थिति 30 वर्षों

से इलेक्ट्रॉनिक भुगतान-प्रणाली में लगातार विकास होने के बाद भी है। निम्नलिखित कारणों से नकद आज भी भुगतान का सबसे प्रभावी रूप है-

- बैंकिंग प्रणाली में विश्वास की कमी
- नकदरहित व्यापार का अक्षम विपदांतर
- किसी व्यक्ति की प्रणाली।

बैंक जमा में नकारात्मक वास्तविक ब्याज दर को उपरोक्त कारणों से विकासशील देशों में प्राथमिक समस्याओं के रूप में देखा जाता है। यहाँ तक कि अधिकतर औद्योगिक देशों में, रुपये तथा सिक्कों का अनुपात सर्कुलेशन में per capita से अधिक है। अनुमानतः यह \$446 से \$2748 तक है। दुनिया के वो अत्यधिक औद्योगिक देशों यूनाइटेड स्टेट्स तथा यूनाइटेड किंगडम की स्थिति पर विचार करते हैं। यूनाइटेड स्टेट्स में 1992 में 300 अरब डॉलर रुपये तथा सिक्के सर्कुलेशन में थे। मजदूर बाता यह है कि यह संख्या कम नहीं हो रही है बल्कि 8 प्रतिशत प्रति वर्ष की दर से बढ़ रही है। वेक के द्वारा धन जमा करने की प्रक्रिया 6 प्रतिशत प्रति वर्ष की दर से बढ़ रही है।

नकद की प्रधानता, नवीन व्यापार तरीके के अवसर की ओर ईशारा करता है जो खरीददारी प्रक्रिया को स्मार्ट बनाने है जहाँ उपभोक्ता मूलतः नकद को मध्यम के रूप में प्रयोग करते हैं। नकद को प्रतिस्थापित करने के लिए इलेक्ट्रॉनिक भुगतान-प्रणाली में नकद के कुछ गुणों को समाहित करना होगा जो आज के क्रेडिट तथा डेबिट कार्ड में सम्भवतः नहीं है। उदाहरण के लिए नकद विनिमय होता है अर्थात् यह किसी और को भी दिया जा सकता है। नकद कानूनी प्रस्ताव होता है अर्थात् लेने, वाला लेने के लिए कृतज्ञ होता है। नकद धारक उपकरण होता है अर्थात् इसका अधिकार मालिकाना सबूत का प्रथम आधार होता है। अर्थात् यदि आपके पास नकद है तो इसके मालिक उस समय आप हैं। इसके साथ ही, नकद किसी के द्वारा रखा तथा प्रयोग किया जा सकता है यहाँ तक कि उनके पास भी यह हो सकता है जिनका कोई बैंक खाता नहीं है तथा प्राप्तकर्ता की ओर से नकद प्राप्त करने में कोई खतरा नहीं है अर्थात् इसमें माध्यम के अच्छे या बुरे होने का कोई खतरा नहीं है।

अब क्रेडिट तथा डेबिट कार्ड की तुलना नकद से करते हैं। पहला, ये आपके पास होने चाहिए क्योंकि ये निर्गतकर्ता, जोकि कार्ड मालिक होता है का पहचान-पत्र होता है। साथ ही यह एक विशेष प्रयोक्ता तक ही सीमित होता है। क्रेडिट तथा डेबिट कार्ड कानूनी प्रस्ताव नहीं होते हैं। अतः व्यापारियों को अधिकार होता है कि वे इसे स्वीकार करने से इंकार कर दें।

(2) स्मार्टकार्ड- इलेक्ट्रॉनिक टोकन की विशाल संभावना का विकास जैसे के ऑन लाइन इस्तेमाल संबंधी सर्वस्वीकृत और सुरक्षित साधनों के अभाव में रूकावट है। बहुत सारे प्रारूपों के विकसित किये जाने के बावजूद हम एक सर्वस्वीकृत भुगतान-प्रणाली से कोसों दूर हैं क्योंकि इसके लिए व्यापारियों और बैंकों की बड़ी संख्या जोड़ने और पैसे के इस्तेमाल के साधन को विकसित करने की आवश्यकता है। इसके अलावा ऐसी प्रणाली को इतना सुदृढ़ होना चाहिए कि बड़ी संख्या में वित्तीय आदान-प्रदान कर सके और सारी चुटियों को निकाल केन्द्र में एक मजबूत तथा विशाल परीक्षण तंत्र हो।

इसी बीच इलेक्ट्रॉनिक वाणिज्यिक सेवाओं के हजारों भावी विक्रेताओं को एक-दूसरे को भुगतान करने की आवश्यकता पड़ेगी जिसके लिए वे बहुत ही सक्रियता से भुगतान के विकल्पों की तलाश में हैं। स्मार्ट कार्ड एक ऐसा ही विकल्प है। स्मार्ट कार्ड 1980 के आरम्भ से ही अस्तित्व में है और वर्तमान ढंग का प्रयोग करते हुए सुरक्षित वित्तीय लेन-देन का वादा करता है। स्मार्ट कार्ड क्रेडिट और डेबिट कार्ड तथा माइक्रोप्रोसेसर-आधारित अन्य कार्ड होते हैं जो पारम्परिक चुम्बकीय स्ट्राइप की अपेक्षाकृत अधिक सूचना धारण कर सकने में समर्थ होते हैं। माइक्रोप्रोसेसर चिप अपने विकास की वर्तमान अवस्था में बहुत बड़ी मात्रा में डाटा संग्रहित कर सकता है, जो एक पारम्परिक चुम्बकीय स्ट्राइप से करीब 80 गुना अधिक होती है। उद्योग क्षेत्र के आकलन के अनुसार वर्ष 2010 तक दुनिया में सामान्य चुम्बकीय स्ट्राइप के बजाय इन्व्हेड माइक्रोप्रोसेसर होंगे।

स्मार्ट कार्ड तकनीक का प्रयोग व्यापक रूप से फ्रांस, जर्मनी, जापान और सिंगापुर जैसे देशों में सार्वजनिक कोन बिल, परिवहन और शॉपर्स लॉयल्टी के लिए भुगतान करने में होता है। अमेरिका में इस विचार की जड़ पकड़ने में कुछ अधिक ही लम्बा समय लग गया क्योंकि अत्यन्त भरोसेमंद और अत्यन्त सस्ती दूरसंचार प्रणाली क्रेडिट और डेबिट कार्ड के पक्ष में काम कर रही थी।

स्मार्ट कार्ड मुख्यतः संबंध आधारित स्मार्ट क्रेडिट कार्ड और इलेक्ट्रॉनिक पर्सज होते हैं जिनका व्यवहार पैसे के बदले में होता है, डेबिट कार्ड तथा इलेक्ट्रॉनिक मुद्रा के रूप में भी जाना जाता है।

(3) संबंध-आधारित स्मार्ट कार्ड- पूरी दुनिया की वित्तीय संस्थाएँ अधिक सुविज्ञ और तकनीकी रूप से स्मार्ट ग्राहकों को जरूरतों को पूरा करने तथा इलेक्ट्रॉनिक कॉमर्स की बढ़ती भुगतान संबंधी जरूरतों को पूरा करने के लिए अपनी सेवाओं के रख-रखाव तथा विस्तार हेतु नयी प्रणालियों का विकास कर रही हैं।

परम्परागत क्रेडिट कार्ड अत्यन्त शीघ्रतापूर्वक स्मार्ट कार्डों में तब्दील हो रहे हैं क्योंकि ग्राहक ऐसी भुगतान एवं वित्तीय सेवाएँ प्रदान करने वाले उत्पादों की माँग करते हैं जो उपयोगकर्ता को भिन्नवत्, सुविधाजनक तथा भरोसेमंद हो।

संबंध-आधारित स्मार्ट कार्ड वर्तमान कार्ड सेवाओं में अभिवृद्धि और/या उन नयी सेवाओं का योग है जिसे एक वित्तीय संस्थान एक चिप आधारित कार्ड या किसी अन्य उपकरण के जरिये अपने ग्राहकों को प्रदान करता है। इन नयी सेवाओं में बहुलावित्तीय अकाउण्टों का एक्सेस, बैल्यू-ऐडेड मार्केटिंग प्रोग्राम या फिर अन्य सूचनाएँ शामिल हो सकती हैं जिसे कार्ड-धारक अपने कार्ड में संग्रहित करना चाहते हैं। चिप आधारित कार्ड और कुछ नहीं बल्कि एक ऐसा टूल है जो व्यापक मार्केटिंग तकनीक को बदलकर प्रत्येक व्यक्ति के निजी वित्तीय और व्यक्तिगत आवश्यकताओं को पूरा करने में सहायता करेगी। इन्तान्ड क्रेडिट कार्ड धारक की सूचनाओं नाम, जन्मदिन, व्यक्तिगत खरीदारी प्राथमिकताएँ, और वास्तविक खरीदारी आँकड़े को धारण करता है। ये सूचना, व्यापारियों को उपभोक्ता के व्यवहार को ठीक-ठीक पता लगा पाने तथा खरीदारों की निष्ठा को बढ़ाने के लिए डिजाइन किए गए प्रमोशनल प्रोग्राम को विकसित करने में प्रयुक्त होती है।

संबंध-आधारित उत्पाद से ये आशा की जाती है कि ये उपभोक्ताओं को अधिक बढ़े विकल्प जिनमें निम्न शामिल हैं, प्रस्तावित करते हैं-

- (i) एक से अधिक अकाउंट का एक्सेस उपलब्ध कराना, जैसे एक कार्ड या इलेक्ट्रॉनिक उपकरण पर डेबिट, क्रेडिट, इन्वैस्टमेंट या इलेक्ट्रॉनिक नकदी के लिए सगृहीत मान/मूल्य।
- (ii) विविध प्रकार के फंक्शन, जैसे नकर एक्सेस, बिल भुगतान, बैलेंस संबंधी पूछताछ या चुनिया अकाउंट के लिए फण्ड हस्तान्तरण।

(iii) कई प्रकार के उपकरण का प्रयोग करते हुए बहुत-सी जगहों पर बहुत अभिन्न विकल्प जैसे एक ऑटोमैटेड टेलर मशीन, एक स्कीनफोन, एक पर्सनल कम्प्यूटर, एक पर्सनल डिजिटल सहायक (PDA), या इंटरएक्टिव टेलीविजन।

कंपनियाँ इन सेवाओं को प्रत्येक ग्राहक के लिए व्यक्तिगत बैंकिंग संबंध में समाहित करना चाह रही हैं। ये वित्तीय और अतिरिक्त सेवाओं का मूल्य-वर्धित प्रोग्रामों के साथ सुविधा-वृद्धि के लिए, निष्ठा और अवधारणा पैदा करने के लिए और नये ग्राहकों को आकर्षित करने के लिए पैकेज कर सकती हैं। बैंक ए.टी.एम. स्कीन पर आने वाली सेवाओं के ठीक समान सेवाओं की सूची प्रस्तावित करते हुए, स्मार्ट कार्ड पर सेवाएँ कस्टमाइज करने की कोशिश कर रही हैं। जैसा कि क्रेडिट कार्डों के साथ होता है, बैंक अक्सर की जा सकने वाली खरीदारों, हवाई यात्रा कार्यक्रम और अन्य सेवाएँ प्रस्तावित करने के लिए स्वास्थ्य संबंधी देखभाल प्रदान करने वालों, टेलीफोन कंपनियाँ, खुदरा विक्रेताओं और हवाई यात्रा कम्पनियों के साथ लिंक बना सकती हैं।

प्रश्न-17. निम्न पर संक्षिप्त टिप्पणी लिखिए-

(1) इलेक्ट्रॉनिक पर्स और डेबिट कार्ड (2) स्मार्ट कार्ड रीडर और स्मार्ट फोन।

उत्तर- (1) इलेक्ट्रॉनिक पर्स और डेबिट कार्ड- अपने बढ़ते हुए लचीलेपन के बावजूद, संबंध आधारित कार्ड क्रेडिट आधारित होती हैं और भुगतान-चक्र के अन्त में इसका निपटारा हो जाता है। नगद के बदले में एक वित्तीय माध्यम की जरूरत होती है। इस आवश्यकता को पूरा करने के लिए बैंक, क्रेडिट कार्ड कम्पनियाँ, और यहाँ तक कि सरकारी संस्थाएँ इलेक्ट्रॉनिक पर्स का परिव्य करने के दौर में हैं जो बटुवे के आकार की स्मार्ट कार्ड होती हैं। जिसमें अन्तःस्थापित माइक्रोचिप लगी होती है जो लोगों के उपयोग के लिए पैसे की रकम को संगृहित करती है ताकि खाने-पीने के सामान खरीदने से लेकर, छायाप्रति काराने से लेकर किराये के भुगतान तक के लिए नगदी की जरूरत न पड़े। एक इलेक्ट्रॉनिक पर्स निम्न तरीके से काम करता है। पर्स में पैसे डालने के बाद, किसी ATM पर या किसी सस्ते विशेष टेलीफोन के जरिये, इसका प्रयोग आइस्क्रीम तथा मिठाइयों का भुगतान करने के लिए भी किया जा सकता है बशर्त वॉडिंग मशीन में कार्ड रीडर लगा हो। वॉडिंग मशीन को सिर्फ यह पता लगाने की जरूरत होती है कि कार्ड असली है और एक आइस्क्रीम का दाम अदा करने लायक पर्याप्त पैसा उसमें उपलब्ध है। एक सेकण्ड में कार्ड के बैलेंस से खरीदारी की कीमत घटा ली जाती है और वॉडिंग मशीन के इलेक्ट्रॉनिक कैश बॉक्स में जोड़ दिया जाता है। कार्ड में बची हुई राशि को वॉडिंग मशीन के द्वारा प्रदर्शित किया जाता है या इसे ए.टी.एम. पर या

किसी बैलेंस रीडिंग उपकरण से जाँचा जा सकता है। इलेक्ट्रॉनिक पर्स आपके प्री-पेड मोबाइल की भाँति है जब इसके अन्तर की राशि खत्म हो जाय तो आप इसे दोबारा चार्ज कर सकते हैं। यहाँ तक विक्रेता का प्रश्न है, रसीदों को व्यक्तिगत रूप से या टेलीफोन द्वारा समय-समय पर इकट्ठा किया जा सकता है और बैंक खाते में स्थानान्तरित किया जा सकता है। हालाँकि यह तकनीक पिछले एक दशक से उपलब्ध रही है, परन्तु कार्ड से अपेक्षाकृत सस्ती है।

(2) स्मार्ट कार्ड रीडर और स्मार्ट फोन- स्मार्ट कार्ड के लाभ स्मार्ट कार्ड रीडर कहलाने वाले उपकरण की सर्वव्यापकता पर निर्भर करते हैं, जो किसी स्मार्ट कार्ड के चिप के साथ कम्प्यूनिकेट कर सकता है। किसी स्मार्ट कार्ड पर लिखी हुई चीजें पढ़ने और उस पर ऑकित करने के अलावा ये उपकरण विविध प्रकार की प्रबंधन प्रणालियों को सपोर्ट कर सकती हैं। कुछ स्मार्ट कार्ड रीडर पर्सनल कम्प्यूटर, विक्रय टर्मिनल तथा एक फोन को मिलाकर उपभोक्ताओं को घर बैठे ही वित्तीय लेन-देन में समर्थ बनाते हैं।

सरलतम रूप में, एक कार्डरीडर दो लाइनों को 16 कैरेक्टर्स के जरिये प्रदर्शित करता है जो दोनों प्रॉप्ट तथा प्रयोक्ता के द्वारा प्रिविड उत्तर को दर्शा सकता है। इसकी क्षमता को एक रंग कोडित फंक्शन कुंजियों के द्वारा बढ़ा दिया है जिसे इस प्रकार से प्रोग्राम किया जा सकता है कि यह एक कुन्जी दबाने से अत्यन्त सामान्य रूप से प्रयुक्त क्रियाओं को सम्पन्न कर सके। यह पर्सनल कम्प्यूटर तथा इलेक्ट्रॉनिक नकदी रजिस्टर जैसे ट्रेंजेक्शन ऑटोमेशन सिस्टम की पूरी शृंखला के साथ आर.एस.-232 क्रॉसक इंटरफेस के माध्यम से कम्प्यूनिकेट कर सकता है।

कार्ड रीडर, स्कीन फोन के रूप में अधिक प्रचलित हो रही हैं। स्कीन फोन अनुप्रयोग के प्रस्तावक बहुत पहले से ही बताए जा चुके हैं कि फोन के साथ उपभोक्ता की यन्त्रित स्कीन फोन को एक ऐसे रिसेशन देती है जिससे कम्प्यूटर का कोई मेल नहीं हो सकता। कुछ स्कीन आधारित फोन में एक चार पंक्ति वाला स्कीन, एक चुम्बकीय स्ट्राइप कार्ड रीडर तथा एक फोन की-बोर्ड होता है। प्रयोक्ता फोन पर के मेन्यू जो ऑटोमैटेड टेलर मशीन के मेन्यू जैसे होते हैं, की सहायता से लेन-देन करते हैं। बहुत सारे बैंक यह मानते हैं कि स्कीन आधारित फोन PC आधारित गृह-बैंकिंग अनुप्रयोग की अपेक्षा प्रयोग में अपेक्षाकृत अधिक सुविधाजनक है जिसमें प्रयोक्ता को अपने सिस्टम को बूट-अप करने की आवश्यकता होती है और लेन-देन के पूर्व एक मॉडेम कनेक्शन स्थापित करने की जरूरत होती है।

स्कीन फोन की अन्य विशेषताओं में उन्नत टेलीफोन फंक्शन जैसे द्वि-पथगामी स्पीकर फोन क्षमता, एक डायलिंग डाइरेक्टरी और कॉल्स को ट्रैक करने के लिए एक फोन लॉग शामिल हैं। वित्तीय संस्थाओं ने स्कीन फोन के मार्केटिंग टूल के रूप में इनका इस्तेमाल करने के लिए स्थानीय फोन कम्पनियों के साथ टीम बनायी है।

स्मार्ट कार्ड रीडरों को विशिष्ट वातावरणों के लिए कस्टमाइज किया जा सकता है। ऑपरेटिंग एनवायरमेंट उपकरण को सुरक्षा-प्रणाली से बिना कोई समझौता किये अनुप्रयोगों के निर्माण और सुधार के लिए प्रोग्रामरों को C प्रोग्रामिंग भाषा के प्रयोग की अनुमति देता है। अधिकांश कार्ड-रीडरों के लिए विकास-प्रणाली त्वरित अनुप्रयोग विकास पूर्व-कोडित

माइक्रोस के साथ आती है। स्मार्ट कार्ड प्रयोग को बढ़ावा देने के लिए, स्मार्ट कार्ड फोरम जो करीब 130 व्यापारिक और सरकारी एजेंसियों का समूह है, बहुप्रयोग वाले स्मार्ट कार्डों के प्रयोग को बढ़ावा देने के लिए आम निर्देश बना रही है— जो टॉल गेट्स से लेकर अस्पतालों तक सभी जगह उपयोग किये जा सकते हैं।

प्रश्न-18. क्रेडिट कार्ड आधारित इलेक्ट्रॉनिक भुगतान प्रणाली क्या है? समझाइये।

उत्तर— क्रेडिट कार्ड आधारित इलेक्ट्रॉनिक भुगतान-प्रणाली— डिजीटल कैश व इलेक्ट्रॉनिक कैश से संबंधित जटिलता से बचने के लिए उपभोक्ता व वेंडर इंटरनेट पर क्रेडिट कार्ड भुगतान को एक संगठित प्रामाणिक विकल्प के रूप में देख रहा है। आधारभूत प्रक्रिया में कुछ खास नया नहीं है। यदि उपभोक्ता कोई उत्पाद या सेवा खरीदना चाहते हैं तो वे सब्सिड सेवा-प्रदाता को अपने क्रेडिट कार्ड की जानकारी उपलब्ध कराते हैं और क्रेडिट कार्ड संगठन इस भुगतान को किसी अन्य भुगतान के प्रकार ही निबटारती है।

हम ऑन लाइन नेटवर्क पर क्रेडिट कार्ड भुगतान को निम्नलिखित तीन भागों में बाँट सकते हैं—

- (1) साधारण क्रेडिट कार्य व्योरे का प्रयोग करता हुआ भुगतान— भुगतान का सबसे आसान तरीका किसी सार्वजनिक नेटवर्क जैसे टेलीफोन लाइनों या इंटरनेट पर एन्क्रिप्शन रहित क्रेडिट कार्ड का आदान-प्रदान है। इंटरनेट के निम्न-स्तर की सुरक्षा-व्यवस्था इसे थोड़ा समस्याजनक बना देती है। प्रामाणिकरण भी एक महत्वपूर्ण समस्या है और यह सुनिश्चित करना वेंडर का दायित्व है कि क्रेडिट कार्ड का प्रयोग कर रहा व्यक्ति ही इसका मालिक है। एन्क्रिप्शन के बिना इसका कोई रास्ता नहीं है।
- (2) एन्क्रिप्टेड क्रेडिट कार्ड व्योरे का प्रयोग कर किया गया भुगतान— समझवारी की बात यह है कि भेजने से पूर्व आपके क्रेडिट कार्ड व्योरे को एन्क्रिप्ट किया जाये, पर उसमें भी कुछ कारकों पर विचार करना आवश्यक होता है। उसमें से एक क्रेडिट कार्ड आदान-प्रदान पर आने वाला खर्च है। यह खर्च, लेन-देन में अतिरिक्त खर्च जोड़कर कम मूल्य के भुगतान पर रोक लगा देगा।
- (3) तृतीय पक्ष सत्यापन का प्रयोग कर किया गया भुगतान— सत्यापन और सुरक्षा समस्या का एक समाधान तृतीय पक्ष का प्रवेश है। तृतीय पक्ष कोई ऐसी कम्पनी हो सकती है जो दो ग्राहकों के मध्य किये गये भुगतान को प्राप्त करे तथा इसे स्वीकृति प्रदान करे।

प्रश्न-19. इलेक्ट्रॉनिक भुगतान-प्रणाली के संचालन में जोखिम, भूलों और विवादां से होने वाले मुख्य खतरे समझाइये।

उत्तर— इलेक्ट्रॉनिक भुगतान-प्रणाली और जोखिम— ई-कॉमर्स की एक महत्वपूर्ण चुनौती जोखिम प्रबंधन है। भुगतान-प्रणालियों के संचालन में तीन मुख्य जोखिम-धोखाधड़ी और गलती, गोपनीयता के मामले, और क्रेडिट संबंधी जोखिम हैं। गलतियों से दूर रहने के लिए कानूनी ढांचे में सुधार की आवश्यकता है। गोपनीयता और धोखाधड़ी की समस्याओं से निबटने के लिए सुरक्षा ढांचे में सुधार की जरूरत है। क्रेडिट संबंधी जोखिम को कम करने के

लिए ऐसी प्रक्रिया का निर्माण करना ताकि क्रेडिट को संतुलित किया जा सके और बाजार में खुरा पैसों को कम किया जा सके।

भूलों और विवादां से होने वाले खतरे— परोक्ष रूप से सारे इलेक्ट्रॉनिक भुगतान-प्रणालियों को प्रमाणिक आँकड़े रखने के लिए कुछ क्षमता की आवश्यकता होती है जिसके कुछ स्पष्ट कारण हैं। तकनीकी दृष्टि से, इलेक्ट्रॉनिक प्रणालियों के लिए यह कोई समस्या नहीं है। क्रेडिट और डेबिट कार्ड ऐसा करते हैं और यहाँ तक कि कागज-आधारित बैंक एक प्रमाणिक रिकॉर्ड तैयार करते हैं। एक बार सूचना को इलेक्ट्रॉनिक रूप से ग्रहण कर लेने के बाद तो इसको बनाए रखना आसान और सस्ता भी होता है। उदाहरण के लिए, बहुत से लेन-देन प्रोसेसिंग प्रणालियों में पुराने या अवसूद्ध खातों को कभी मिटाया नहीं जाता और पुराने लेन-देन संबंधी इतिहास को चुम्बकीय फीलों पर सदा के लिए बरकरार रखा जा सकता है।

इलेक्ट्रॉनिक लेन-देन की अपूर्ण प्रकृति तथा विवाद हल करना पूरी तरह आँकड़ों पर निर्भर रहने के कारण भुगतान डायनेमिक्स और बैंकिंग तकनीक को अपनाना एक सामान्य नियम हो सकता है। किसी भी डाटा को कभी त्यागने की आवश्यकता नहीं है। इन ऑटोमेटिक रिकॉर्डों की विशेषताओं में निम्नलिखित शामिल हैं—

- (i) स्थायी संग्रहण
  - (ii) अभिगम्यता और पता लगा ले पाने की क्षमता।
  - (iii) एक भुगतान-प्रणाली डाटाबेस और
  - (iv) भुगतान करने वाले बैंक, या मौद्रिक स्वामित्व धारकों का डाटा हस्तान्तरण।
- जोखिम प्रबंधन के उद्देश्य के लिए रिकॉर्ड कीपिंग की आवश्यकता नगद राशि लेन-देन संबंधी गोपनीयता के खिलाफ जाता है। हम यह कह सकते हैं कि गोपनीयता आज इसलिए कायम है कि नगद की अवधारणा कम्प्यूटर और नेटवर्कों ने हमें हर चीज पता करने की जो क्षमता प्रदान की है उससे काफी पुराना है। हालाँकि भुगतान करने वाले सभी लोग सदा लेन-देन की गोपनीयता की इच्छा रखते हैं। बहुत से लोग यह विश्वास करते हैं कि गोपनीयता लोक-कल्याण के हित में नहीं है क्योंकि इससे कर तकरी तथा हवाला जैसी अनेक संभावनाएँ बनती हैं। गोपनीयता के मुद्दे यह प्रश्न खड़ा करते हैं कि क्या इलेक्ट्रॉनिक भुगतान बिना किसी ऑटोमेटिक रिकॉर्ड फीचर के किये जा सकते हैं?

बहुत सी हाल की भुगतान-प्रणालियाँ इस मुद्दे पर उभयभावी दिखती हैं। उदाहरण के लिए माइक्रोस इलेक्ट्रॉनिक पर्स नगद राशि के साथ समतुल्य रखते हैं, किन्तु इसके इलेक्ट्रॉनिक बटुवे को इस तरह से डिजाइन किया जाता है कि वे इन-बिल्ट स्टेटमेंट के साथ कार्ड के अन्तिम 20 लेन-देन के ऑटोमेटिक रिकॉर्ड रखता है। स्पष्टतः कार्ड रीडिंग टर्मिनल, मशीन या टेलीफोन सब सारे लेन-देन का रिकॉर्ड बनाए रख सकते हैं और शायद अन्तिम रूप से ऐसा करेंगे भी। इन आँकड़ों के साथ किसी स्मार्ट कार्ड का बैलेंस तथ्य के अनुसार पुनरहित किया जा सकता है जो कि किसी भी हानि या चोरी के बदले अतिरिक्त सुरक्षा प्रदान कर देता है।

गोपनीयता एक मुद्दा है जिसे इलेक्ट्रॉनिक लेन-देन में उपभोक्ता संरक्षण को कवर करने वाले नियम के जरिये संबंधित किया जाता है। इस मुद्दे पर गभीर परिचर्चा की

मुणाइश है। बिना स्वचालित रिकॉर्ड कीपिंग के बिना एक गोपनीय भुगतान-प्रणाली बैंकरोँ तथा सरकारों के लिए स्वीकार करना अत्यन्त कठिन होगा। यदि नियमों को लागू किया जाय तो प्रत्येक लेन-देन को रिपोर्ट करना होगा, अर्थात् इसे एक एकाउण्ट स्टेटमेंट पर प्रकट होना होगा ताकि गलतियों और विवादों का समाधान आसान हो सके। हालांकि ग्राहकों को यह लग सकता है कि यह सारी रिकॉर्ड कीपिंग गोपनीयता पर हमला है फलस्वरूप इलेक्ट्रॉनिक भुगतान-प्रणाली की स्वीकृति की गति धीमी हो सकती है।

प्रश्न-20. 'भारतीय कॉर्पोरेट में ई-कॉमर्स' को विस्तार से समझाइये।

उत्तर- भारतीय कॉर्पोरेट में ई-कॉमर्स- मनुष्य की व्यापार और वाणिज्यिक गतिविधियाँ उत्तनी ही पुरानी हैं जितनी धरती पर मानव सभ्यता, परन्तु आज दुनिया काफ़ी बदल गई है। अब ग्राहक को अपनी व्यस्त दिनचर्या में से समय निकालकर शहर के ट्रेफिक वाले डिपार्टमेंटल स्टोर, बैंक, शेयर बाजार या वित्तीय संस्थाओं तक जाने-जाने की तकलीफ नहीं करनी पड़ती, यह सब ई-कॉमर्स से सम्भव हो चुका है। विश्व में वर्ष 2000 में ई-कॉमर्स द्वारा लगभग 45 खरब रुपयों का व्यापार हुआ था।

ई-कॉमर्स का अर्थ है- टेलीफोन लाइन, नेटवर्क या अन्य किसी माध्यम से सेवाओं या उत्पादों के बारे में सूचनाओं का प्रेषण या भुगतान करना। सेवा क्षेत्र में ई-कॉमर्स एक सस्ती तथा शीघ्रता से बेहतर सेवा उपलब्ध कराती है। दूसरे शब्दों में ई-कॉमर्स से सामान व सेवाओं की ऑन लाइन खरीद-फरोख्त की जाती है। इस सेवा में सुई से लेकर हैलीकॉप्टर तक के क्रय-विक्रय के लिए वेबसाइट उपलब्ध हैं। ई-मेल की तर्ज पर ई-कॉमर्स की शुरुआत हुई है। यह सेवा 24 घण्टे उपलब्ध रहती है तथा इसमें किसी भी प्रतिनिधि से सम्पर्क की जरूरत नहीं पड़ती। ई-कॉमर्स के माध्यम से किए जाने वाले शोक व्यापार को मैक्रो ई-कॉमर्स तथा खुदरा व्यापारी को माइक्रो ई-कॉमर्स कहा जाता है।

भारत में सॉफ्टवेयर सम्बन्धी आधुनिक सूचना प्रौद्योगिक उद्योग की सर्वाच्च संस्था नेसकॉम ने ई-कॉमर्स के क्षेत्र में भारत की क्षमता का सही तरीके से प्रयोग करने के लिए भारत सरकार के साथ मिलकर कार्य किया है। इन दोनों के सहयोग से ऐसे प्रयास किए जा रहे हैं जिससे सॉफ्टवेयर क्षेत्र के अंग्रेजी के E अक्षर से शुरू होने वाले तीन क्षेत्रों का अव्यवस्था में उपलब्ध साधनों का अधिकतम प्रयोग कर भारतीय अर्थव्यवस्था की आर्थिक, सामाजिक, मौद्रिक तथा शैक्षिक नींव को मजबूत करना है।

(i) एन्चूकेशन (शिक्षा) (ii) एन्टरप्रेन्योरशिप (उद्यमिता) (iii) एम्प्लॉयमेन्ट (रोजगार) कुल मिलाकर ई-कॉमर्स विशेषज्ञों के अनुसार अगले कुछ वर्षों में विश्व में ई-कॉमर्स से क्रान्तिकारी परिवर्तन आएगा।

प्रश्न-21. इलेक्ट्रॉनिक कॉमर्स से आप क्या समझते हैं? संक्षेप में वर्णन कीजिये।

अथवा

ई-कॉमर्स से संबंधित विभिन्न तकनीकी एवं संगठनात्मक पहलुओं का वर्णन कीजिये।

उत्तर- इलेक्ट्रॉनिक कॉमर्स अथवा ई-कॉमर्स (Electronic Commerce or E-Commerce)- इलेक्ट्रॉनिक कॉमर्स अथवा ई-कॉमर्स उत्पादों और सेवाओं की ऑन लाइन व्यापार गतिविधियों को कहते हैं। इसका अर्थ है कि वह व्यापार लेनदेन जिसमें व्यापार करने

वाले भौतिक रूप से एक-दूसरे के सामने न होकर इलेक्ट्रॉनिक माध्यम से एक-दूसरे के साथ व्यापार करें। ई-कॉमर्स साधारणतः इन्टरनेट पर खरीदने और बेचने से संबंधित है अथवा कम्प्यूटर के माध्यम से नेटवर्क द्वारा वस्तुओं/उत्पादों अथवा सेवाओं के उपयोग या इनके अधिकारों में स्थानान्तरण से संबंधित गतिविधियों को ई-कॉमर्स कहा गया है।

ई-कॉमर्स की परिभाषा- ई-कॉमर्स व्यापार के लेनदेन में इलेक्ट्रॉनिक कम्प्यूटिकेशन और डिजिटल इंफॉर्मेशन प्रोसेसिंग टेक्नोलॉजी का उपयोग है जो विभिन्न संगठनों/प्रतिष्ठानों तथा व्यक्तियों के मध्य स्थित संबंधों की पुनः परिभाषा देता है या नया प्रारूप देता है।

कुछ व्यक्ति ई-कॉमर्स एवं ई-विजनेस को एक ही मानते हैं किन्तु वास्तव में ये दो विभिन्न परिकल्पनाएँ हैं। ई-कॉमर्स में इंफॉर्मेशन कम्प्यूटिकेशन टेक्नोलॉजी (ICT) व्यापार अथवा संगठनों के मध्य लेनदेन प्रतिष्ठानों/संगठनों और उपभोक्ता के मध्य होता है। इलेक्ट्रॉनिक कॉमर्स इन्टरनेट पर एक मार्केट प्लेस के समान है। इलेक्ट्रॉनिक कॉमर्स मुख्य रूप से इन्टरनेट तथा अन्य कम्प्यूटर नेटवर्क जैसे इलेक्ट्रॉनिक प्रणालियों पर सेवाओं तथा उत्पादों के वितरण, क्रय, विक्रय, विपणन तथा उत्पादों की सर्चिंग का नाम है। इंफॉर्मेशन टेक्नोलॉजी उद्योग इसे एक इलेक्ट्रॉनिक विजनेस एप्लीकेशन के रूप में देखती है जिसका उत्प्रेक्ष्य कॉर्पोरेट/व्यक्तिगत ट्रांजेक्शन हो सकता है। इसमें इलेक्ट्रॉनिक फंड ट्रांसफर, सलाई चेन मैनेजमेंट, ई-मार्केटिंग, ऑन लाइन व्यापार प्रोसेसिंग, इलेक्ट्रॉनिक डेटा इन्टरचेंज, ऑटोमेटेड इन्वैन्टरी मैनेजमेंट सिस्टम तथा ऑटोमेटेड डाटा कलेक्शन प्रयुक्त हो सकता है। सिस्टम चक्र में कहीं न कहीं वर्ल्ड वाइड वेब की कम्प्यूटिकेशन टेक्नोलॉजी का इस्तेमाल होता है। यद्यपि इलेक्ट्रॉनिक कॉमर्स बहुधा वर्ल्ड वाइड वेब की अपेक्षा कम्प्यूटर की अन्य टेक्नोलॉजी जैसे डाटाबेस, ई-मेल पर भी आश्रित है। तथापि यह गैर कम्प्यूटर तकनीक जैसे उस माल की दुलाई जिसे ई-कॉमर्स द्वारा खरीदा है, पर भी आश्रित है।

तकनीकी एवं संगठनात्मक पहलू (Technical And Organizational Aspects)- ई-कॉमर्स से संबंधित तकनीकी एवं संगठनात्मक पहलू निम्नलिखित हैं-

1. ई-कॉमर्स के लिए पर्याप्त मार्केट रिसर्च और विश्लेषण होना चाहिये। ई-कॉमर्स अच्छे व्यापार की योजना और आपूर्ति एवं आवश्यकता के मूल सिद्धान्तों से परे नहीं है। व्यापार में असफल होना अन्य व्यापार की तरह ही ई-कॉमर्स का भी एक सत्य है।
2. ई-कॉमर्स के लिए एक अच्छी मैनेजमेंट टीम आवश्यक है जिसके पास इंफॉर्मेशन टेक्नोलॉजी की रणनीति हो। कम्पनी की इंफॉर्मेशन टेक्नोलॉजी की रणनीति, व्यापार की रीडिजाइन प्रोसेस का एक भाग होना चाहिये।
3. ग्राहकों को एक सुरक्षित और सरल तरीका प्रदान करना जिससे वे अपना ट्रांजेक्शन कर सकें। क्रेडिट कार्ड, इन्टरनेट पर भुगतान करने का लोकप्रिय साधन है तथा 90 प्रतिशत ट्रांजेक्शन में यही साधन इस्तेमाल होता है। पूर्व में, कार्ड संख्याओं को सुरक्षित ढंग से ग्राहक तथा व्यापारी के मध्य स्वतंत्र भुगतान गेटवेज के माध्यम से स्थानान्तरित किया जाता था। आज भी इस तरह के स्वतंत्र गेटवेज का इस्तेमाल छोटे और गृह व्यापार कर रहे हैं। अधिकतर व्यापारी आज साइट पर

क्रेडिट कार्ड द्रांजेक्शन उन व्यापारी बैंकों या क्रेडिट कार्ड कम्पनियों के साथ करते हैं जिनके साथ उन्होंने अनुबंध कर लिया हो।

4. सुरक्षा तथा विश्वसनीयता उपलब्ध करवाना। समानान्तर सर्वर, हार्डवेयर रिडन्डेंसी, फेल सेफ टेक्नोलॉजी, इंफॉर्मेशन एनक्रिप्शन, तथा फायरवाल उपरोक्त आवश्यकताओं की पूर्ति करते हैं।

5. ग्राहक संबंधों की संपूर्ण जानकारी प्रदान करना ताकि यह सुनिश्चित किया जा सके कि कर्मचारी, सलायर्स तथा साझेदार ग्राहक का संपूर्ण तथा समान जानकारी प्राप्त कर सकें।

6. व्यापार की दृष्टि से मजबूत व्यापार मॉडल की संरचना।

7. एक ऐसे जागरूक, सजग संगठन की स्थापना करना जो आर्थिक, सामाजिक तथा भौतिक वातावरण के किसी भी परिवर्तन की दशा में शीघ्र प्रतिक्रिया दे।

8. एक आकर्षक वेबसाइट उपलब्ध करवाना। इस संबंध में सुलचिपूर्ण रंगों, ग्राफिक्स, एनीमेशन, फोटो, फॉन्ट तथा खाली जगहों का सही-सही तालमेल आवश्यक है।

9. रिये जा रहे उत्पाद या सेवाओं की पूरी समझ प्रदान करना जिसमें न केवल उत्पाद संबंधी जानकारी हो परन्तु अच्छे सलाहकार तथा चयनकर्ता से संबंधित जानकारी का होना आवश्यक है।

ई-कॉमर्स को इस प्रकार के नित्य कार्यों का सम्पन्न करने के लिए उत्पाद तथा इसकी उपलब्धता के बारे में सच्चा होना चाहिए, माल भेजने की प्रक्रिया विश्वसनीय होनी चाहिए, शिकायतों से तेजी के साथ और प्रभावी ढंग से निपटना चाहिए। इन्टरनेट वातावरण की यह खूबी है कि ग्राहक उत्पाद और उत्पाद करने वाली कम्पनी के बारे में अधिक जानकारी सूचना एकत्र करने के अन्य साधनों से भी परिचित होता है जो भौतिक दुनिया में संभव नहीं है। ई-कॉमर्स के कारक— एक सफल ई-कॉमर्स संगठन को चाहिये कि वह ग्राहक को एक आनन्ददायक और संतोषजनक अनुभव दें। इसको संभव बनाने में निम्नलिखित कारक सम्मिलित हैं—

- ग्राहक को प्राथमिकता देना।
- सेवा और निष्पादन उपलब्ध करना— ग्राहक को एक अच्छा खरीदारी का अनुभव देना ठीक वैसा ही जब वह स्वयं किसी दुकान में जाकर खरीदारी करके प्राप्त करता है।
- ग्राहक को खरीदारी का इन्सैनटिव देना— विक्रय प्रमोशन के इस उद्देश्य की प्राप्ति कूपन, स्पेशल ऑफर तथा फ्रूट से हो सकते हैं।
- स्वयं ध्यान देना— इसके लिए पर्सनलाइज्ड वेबसाइट, खरीदारी सुझाव और पर्सनाइज्ड विशेष ऑफर उपयोगी साबित हो सकते हैं। किसी विक्रय केन्द्र पर आमने-सामने किये गये खरीदारी के पारम्परिक तरीके का बदले बन सकते हैं।
- एक समुदाय की भावना देना— चैटरूम, डिस्कशन बोर्ड, कास्टमर इनपुट और लायल्टी प्रोग्राम जिन्हें कभी-कभी एफीनिटी प्रोग्राम भी कहते हैं, इस दिशा में सहायक सिद्ध हो सकते हैं।

(vi) ग्राहक को स्वयं सहायता देने के लिए एक ऐसी साइट देना जो ग्राहक सरलता से बिना सहायता के इस्तेमाल कर सके। यह तभी संभव है जब उत्पाद की समस्त जानकारी उपलब्ध हो, क्रॉस-सेल सूचना, उत्पाद के विकल्प पर सलाह तथा सलाइज एवं एक्सेसरी चयनकर्ता भी उपलब्ध हो।

प्रश्न-22. ई-कॉमर्स की परिभाषा देते हुये वर्तमान ई-कॉमर्स के उदाहरण समझाइये।

उत्तर— ई-कॉमर्स एक तरह का व्यवसाय या व्यापारिक वातावरण है जिसमें वस्तुओं की खरीद, बिक्री और उनके आवागमन की सारी सूचनाएँ उपलब्ध रहती हैं। ई-कॉमर्स में अन्य दूसरी तरह की तकनीक भी शामिल रहती हैं जिनके प्रयोग से कम्पनी अपना व्यवसाय आधुनिकतम ढंग से कर सकती है।

ई-कॉमर्स, टेलीकम्यूनिकेशन और डाटा प्रोसेसिंग तकनीक का एक उपयोग है जिससे व्यवसाय के भागीदारों के बीच लेनदेन की गुणवत्ता को बढ़ाया जाता है। ई-कॉमर्स, व्यवसाय की कार्यक्षमता में डाटा-प्रोसेसिंग व डाटाबेस के संग्रहण के माध्यम से बढ़ोतरी करता है। ई-कॉमर्स के माध्यम से मजदूरी लागत व पेपर के संग्रहण में कमी आती है। यह व्यवसाय को अपने माल की गुणवत्ता तथा सुविधाओं के जरिये अधिक प्रभावशाली बनाता है। ई-कॉमर्स के जरिये उपभोक्ता तथा व्यवसाय के बीच एक प्रभावशाली कम्प्यूटेशन स्थापित किया जाता है। उपभोक्ता सामान की खरीद व बिक्री कुछ ही समय में विश्व के किसी भी स्थान से कर सकता है।

ई-कॉमर्स, एक कम्प्यूटर कम्प्यूटेशन नेटवर्क के ऊपर वस्तु की बिक्री, उत्पाद तथा सुविधाओं सम्बन्धी सूचनाओं से जुड़ा रहता है। इसके अतिरिक्त ई-कॉमर्स पारम्परिक व्यापार में नई सूचनाओं के आदान-प्रदान को गति व प्रोत्साहन प्रदान करता है। यह सूचनाएँ विभिन्न व्यापारिक गतिविधियों से जुड़ी रहती हैं। इसके अन्तर्गत सूचनाओं का आदान-प्रदान एक कम्प्यूटर से दूसरे कम्प्यूटर पर इलेक्ट्रॉनिकली होता है तथा यह सूचना व्यवसाय को संचालित करने में काम में आती है।

इस प्रकार ई-कॉमर्स एक तरह से कागज रहित व्यापारिक सूचनाओं का आदान-प्रदान है, जो EDI, ई-मेल तथा इलेक्ट्रॉनिक फण्ड ट्रांसफर के जरिये व्यापार को गति प्रदान करता है। यह केवल एक मानवीय व पेपर लेनदेन प्रक्रिया नहीं है बल्कि इसका प्रयोग व्यापार को इलेक्ट्रॉनिक वातावरण व व्यापार को संचालित करने वाले तरीकों में बदलाव प्रदान करना है। पिछले कुछ वर्षों में व्यापारिक संगठनों ई-कॉमर्स को इन्टरनेट पर शुरू कर दिया है। ई-कॉमर्स ने व्यवसायों को एक नई दिशा व गति प्रदान की है। यह अन्य साधनों की अपेक्षाकृत सस्ता साधन भी है। ई-कॉमर्स के पास यह क्षमता होती है कि वह दूसरों की क्षमताओं के मिले-जुले रूप का उपयोग अधिक प्रभावशाली ढंग से कर सकता है। इसके माध्यम से हर प्रकार के लिए सूचनाओं का बांटना भी आसानी से संभव हो जाता है। प्राइवेट कम्पनियाँ अपने उपभोक्ताओं के बारे में सारे आंकड़ों का अध्ययन भी कर सकती हैं। ई-कॉमर्स सॉफ्टवेयर इस बात का भी परीक्षण करते हैं कि उनकी तकनीक उपभोक्ता आधारित खरीदारी तरीकों पर है कि नहीं। ई-कॉमर्स विभिन्न संप्रदायों, संस्कृतियों, जो कि एक-दूसरे से भिन्न दिखाई पड़ रही हों, को जोड़ता है।

वर्तमान ई-कॉमर्स के उदाहरण-

1. वैल्यू एडेड नेटवर्क (VAN)- हम VAN को एक टेलीकम्यूनिकेशन नेटवर्क की तरह परिभाषित कर सकते हैं जो विभिन्न सूचनाओं को व्यवसाय संबंधी सूचनाओं व सुविधाओं में परिवर्तित करता है।
2. सूचना सेवाएँ- इंटरनेट कम्प्यूटर्स और अमेरिका ऑन लाइन जैसे उदाहरण सारे विश्व को सूचना सेवाएँ प्रदान करते हैं तथा विश्व में ही रहे नये-नये प्रयोगों के बारे में अवगत करते हैं।
3. एप्लिकेशन एवं मेडीकल- ई-कॉमर्स के माध्यम से लोग इंटरनेट का प्रयोग करके शिक्षा के क्षेत्र में नये-नये प्रयोगों के बारे में जानकारी तथा वांछित सूचनाओं को आसानी से प्राप्त कर सकते हैं।
4. ट्रान्ज़ैक्शन प्रोसेसिंग सिस्टम- आदान-प्रदान से संबंधित लेन-देन को ट्रान्ज़ैक्शन प्रोसेसिंग सिस्टम कहते हैं जो कि निम्नलिखित हैं-
5. एयरलाइन्स आरक्षण
6. स्टॉक व्यापार
7. बीमा

प्रश्न-2.3. ई-कॉमर्स प्रणाली की तकनीतियों का संक्षेप में वर्णन करें।

उत्तर- ई-कॉमर्स प्रणाली की तकनीतियाँ- किसी ई-कॉमर्स निकाय के अन्तर्गत किसी कंपनी के व्यापार में होने वाली विभिन्न प्रक्रियाओं के बीच एकता, कम्प्यूटिकेशन व उनको लागू करने के लिए अप्रतिखित दो मुख्य तकनीक प्रयोग में लाई जाती हैं-

(1) इलेक्ट्रॉनिक डाटा इंटरचैन्ज (EDI-Electronic Data Interchange)

(2) एप्लिकेशन लिंक इनोबलिंग (ALE-Application Link Enabling)

इन दोनों तकनीकों की संरचना लगभग समान होती है, यह दोनों तकनीकें डाटा के दो सिस्टम के बीच में आदान-प्रदान में सहायक होती हैं। यह दोनों SAP की IDOC इंटरफ़ेस का प्रयोग करती हैं। यह इंटरफ़ेस, डाटा के फॉर्मेट और संरचना को व्यक्त करता है।

ALE तथा EDI, SAP के विभिन्न भाग जैसे- विक्री एवं वितरण, सामग्री प्रबंधन, वित्तीय प्रबंधन होते हैं।

प्रश्न-2.4. ई-कॉमर्स के लाभ को विस्तारपूर्वक समझाइये।

उत्तर- ई-कॉमर्स के लाभ- ई-कॉमर्स के निम्नलिखित प्रमुख लाभ हैं-

- (1) ई-कॉमर्स इन्वॉल्यूशन के रूप में कार्य करता है- यह शुरूआती दौर के, छोटे तथा मध्यम आकार के व्यापारियों को वैश्विक बाजार में पहुँचने में मदद करता है।
- (2) ई-कॉमर्स मास कस्टमाइजेशन को संभव करता है- इस क्षेत्र के ई-कॉमर्स एप्लीकेशन में आसानी से प्रयोग किये जाने वाले ऑडरिंग प्रणाली शामिल होती हैं, जिसकी सहायता से ग्राहक अपने इच्छा के अनुरूप उत्पादों का चयन कर ऑर्डर दे सकते हैं। उदाहरणस्वरूप, कोई कार निर्माता कम्पनी जो ई-कॉमर्स रणनीति के तहत व्यापार करती है। ऑर्डर के अनुसार गाड़ी तैयार कर सकती है जो ग्राहक के विवरण के अनुसार होगा। यह और अच्छे से कार्य कर सकता है,

यदि कम्पनी का निर्माण प्रक्रिया उन्मत्त क्रिसम का है तथा ऑडरिंग सिस्टम के साथ जुड़ा है।

- (3) ई-कॉमर्स नेटवर्क उत्पादन की अनुमति देता है- कम्पनी की उत्पादन प्रक्रिया को उन सभी ठेकेदारों को भेज देना जो भौगोलिक रूप से तो बिखरे हैं, परन्तु कम्प्यूटर नेटवर्क के माध्यम से आपस में जुड़े हैं। नेटवर्क उत्पादन के कारण लागत में कमी के साथ ही यह अधिक रणनीतिक टारगेट मार्केटिंग प्रदान करता है। इसके साथ ही इससे अतिरिक्त उत्पादों, सेवाओं तथा वैसी प्रणालियों को बेचने में मददगार होती है जो समय की माँग होती है। नेटवर्क प्रोडक्शन के कारण, कोई कम्पनी दुनिया के विभिन्न फैक्ट्रियों में अपनी आवश्यकताओं को भेज सकते हैं, जो उस क्षेत्र में विशेषज्ञता रखते हैं।

- (4) ई-कॉमर्स उपभोक्ता के लिए सहायक है- उपभोक्ता-व्यापार लेनदेन में ग्राहकों या उपभोक्ताओं का अधिक महत्व होता है। वे अपने आवश्यकताओं तथा रुचियों के अनुसार सामान को बनवा सकते हैं। तथा सेवाओं की डिलीवरी कैसे हो, यह भी सुनिश्चित हो सकता है। फलस्वरूप उपभोक्ता के लिए विकल्प अधिक होते हैं। ई-कॉमर्स में उत्पादन प्रक्रिया तेज तथा अधिक खुला होता है, जिस पर ग्राहकों का बहुत अधिक नियंत्रण होता है। ई-कॉमर्स के कारण उत्पादों का बाजार तथा उससे संबंधित सूचना हमेशा उपलब्ध रहता है तथा इनके कीमत अधिक पारदर्शी होते हैं, जिससे ग्राहक खरीदारी से संबंधित कम से कम कीमत के मामले में ज्यादा उपयुक्त निर्णय ले पाते हैं।

- (5) ई-कॉमर्स के पीछे ड्राइविंग फोर्स- कम से कम तीन ऐसी शक्तियाँ हैं जो ई-कॉमर्स में ईंधन का काम कर रही हैं। ये आर्थिक शक्तियाँ, कस्टमर और मार्केटिंग इंटरएक्शन शक्तियाँ तथा टेक्नोलॉजी विशेषकर मल्टीमीडिया कन्वर्जेंस हैं।

(a) आर्थिक शक्ति (Economic Force)- ई-कॉमर्स के सबसे स्पष्ट लाभ आर्थिक सामर्थ्य है। ई-कॉमर्स के आर्थिक सामर्थ्य है। ई-कॉमर्स के आर्थिक सामर्थ्य के मूल कारण ये हैं-

- (i) कम्प्यूटिकेशन लागत में कमी
- (ii) कम कीमत का प्रौद्योगिकी इन्फ्रास्ट्रक्चर
- (iii) सलायर्स के साथ सस्ती तथा तेज इलेक्ट्रॉनिक लेन-देन
- (iv) कम प्रचार लागत
- (v) सस्ती कस्टमर सेवा

आर्थिक एकीकरण बाहरी अथवा आन्तरिक है। आर्थिक एकीकरण से तात्पर्य कम्पनियों, सलायर्स, ग्राहकों तथा स्वतंत्र ठेकेदारों का इंटरनेट के माध्यम से एक चर्चुअल वातावरण में आपस में जुड़ा होना है। आन्तरिक एकीकरण से तात्पर्य दूसरी ओर कम्पनी के अन्दर विभागों का आपस में जुड़ा होना है। इसकी सहायता से महत्वपूर्ण व्यापार सूचना डिजीटल रूप में संग्रहित होते हैं जो इलेक्ट्रॉनिक रूप में कभी भी प्राप्त किये जा सकते हैं। आन्तरिक एकीकरण का सबसे अच्छा उदाहरण कॉर्पोरेट इंटरनेट है। प्रोक्टर व गैब्रल, आई बी एम., इण्टेल कुछ कम्पनियों के उदाहरण हैं जिनके कॉर्पोरेट इंटरनेट अत्यन्त प्रभावशाली हैं।

(b) बाजार शक्ति— छोटे तथा बड़े दोनों ही प्रकार की कम्पनियों को बाजार में उतरने तथा अन्तर्राष्ट्रीय बाजार पर कब्जा करने के लिए ई-कॉमर्स अत्यन्त शक्तिशाली कारक है। इन्टरनेट, इसीलिए, ग्राहक सेवा तथा सपोर्ट के लिए महत्वपूर्ण माध्यम है। इसके माध्यम से कम्पनियाँ अपने ग्राहकों को उत्पाद की विस्तृत जानकारी प्रदान कर सकते हैं।

(c) प्रौद्योगिकी शक्ति— ई-कॉमर्स के विकास में आई.सी.टी. (ICT) अर्थात् इंफॉर्मेशन तथा कम्प्यूटेशन प्रौद्योगिकी मुख्य कारक है। उदाहरण के लिए डिजिटल सामग्री में प्रगति, ओपन सिस्टम प्रौद्योगिकी का संश्लेषण तथा प्रोमोशन कम्प्यूटेशन सेवाओं को एक प्लेटफॉर्म पर लाने में अहम् भूमिका निभाई है। फलस्वरूप कम्प्यूटेशन अधिक प्रभावशाली हुआ है तथा इसमें गति, सहजता आई है और यह सस्ती हुई है।

(6) ग्राहकों, कर्मचारियों, सलायर्स, वितरक तथा प्रतिस्पर्धियों को जोड़ता है— ई-कॉमर्स संगठन नेटवर्क को बढ़ावा देता है जिसमें छोटी कम्पनियाँ ग्राहकों की आवश्यकताओं को ठीक ढंग से पूरा करने हेतु सलाह तथा उत्पाद वितरण के लिए पार्टनर कम्पनियों पर निर्भर करती हैं। ग्राहकों, कर्मचारियों, सलायरो, वितरकों तथा प्रतिस्पर्धियों को जोड़ने वाली नेटवर्क श्रृंखला को व्यवस्थित करने के लिए एक एकीकृत या विस्तारित सलाह चैन मैनेजमेंट समाधान की आवश्यकता होती है। सलाह चैन मैनेजमेंट या SCM को सामग्री, सूचना तथा वित्त के निरीक्षण के रूप में परिभाषित किया जाता है। यह निरीक्षण सलायार, उत्पादनकर्ता से लेकर थोक विक्रेता, खुदरा विक्रेता और उपभोक्ता तक चलता है। इसमें कम्पनियों के अन्दर तथा उनके मध्य इन प्रक्रिया के समन्वय तथा एकीकरण शामिल होते हैं। किसी भी प्रभावी सलाह चैन मैनेजमेंट का उद्देश्य चैन के अगले लिंक तक समान तथा सेवाओं का विलकुल ठीक समय पर निरीक्षण करना होता है।

प्रश्न-25. इन्टरनेट तथा ई-कॉमर्स में क्या पारस्परिक सम्बन्ध है? लिखिये।

उत्तर— इन्टरनेट तथा ई-कॉमर्स— इन्टरनेट की सहायता पूरी दुनिया के लोग एक-दूसरे से बगैर बहुत अधिक खर्च के तथा विश्वव्यापी रूप से जुड़ते हैं। टेक्नीकल इन्फ्रास्ट्रक्चर के रूप में यह वैश्विक नेटवर्क का एक संकलन है जो एक ही तरह के प्रोटोकॉल के आधार पर इससे जुड़कर सूचना का साझा करता है। इन्टरनेट लोगों तथा सूचना का एक विशाल नेटवर्क होने के कारण ई-कॉमर्स का मुख्य घटक है। इसकी सहायता से लोग अपने व्यापार का प्रदर्शन कर सकते हैं, अपने उत्पादों तथा सेवाओं को ऑन लाइन बेच सकते हैं। साथ ही, इन्टरनेट इन व्यापार तथा व्यापारिक उत्पादों तथा सेवाओं के बारे में संभावित ग्राहकों, व्यापारिक साझेदारों को सूचना एक्ससेस प्रदान करता है जो अंततः खरीदारी तक ले जाता है। व्यवसायिक उद्देश्यों के लिए जब इन्टरनेट का प्रयोग नहीं होता था, तब कम्पनियाँ इलेक्ट्रॉनिक डेटा इन्टरचेंज (EDI) जैसी निजी नेटवर्क, का प्रयोग कर एक-दूसरे के साथ व्यवसाय करती थी। उस समय यह ई-कॉमर्स का रूप था, किन्तु निजी नेटवर्क को स्थापित करना तथा उन्हें मेन्टेन करना अत्यन्त महंगा था। इन्टरनेट के उद्भव के साथ ई-कॉमर्स का तेजी से विकास हुआ। इसका कारण यह है कि इसमें लागत कम आता है तथा यह खुले मानकों पर आधारित है।

प्रश्न-26. इन्टरनेट और ई-बिजनेस में पारस्परिक सम्बन्ध का वर्णन कीजिये।

उत्तर— इन्टरनेट और ई-बिजनेस— इन्टरनेट अलग-अलग जगह पर लगे कम्प्यूटर्स को जोड़कर सूचनाओं के आवागमन के लिए बनाई गई एक विशेष प्रणाली है। कम्प्यूटर किसी भी सूचना चाहे वह शब्दों में हो या ध्वनियों में, फोटो में या दृश्यों में, अपनी अंकीय भाषा में परिवर्तित कर उन्हें इन्टरनेट के माध्यम से प्रसारित कर देते हैं।

इन्टरनेट ने व्यापार के कई नये रास्ते खोल दिये हैं। इसके माध्यम से कोई भी व्यक्ति अपने घर से भी व्यापार करवा सकता है। इन्टरनेट के माध्यम से कोई व्यक्ति ऑर्डर ले सकता है व उपभोक्ता को समय पर माल उपलब्ध करा सकता है। इन्टरनेट के माध्यम से होने वाले इस व्यापार को ई-बिजनेस या इलेक्ट्रॉनिक बिजनेस कहते हैं। ई-बिजनेस पारस्परिक व्यापारों की अपेक्षा कम खर्चीला होता है क्योंकि इसमें उत्पादक अपने उपभोक्ताओं से सीधे संबंध स्थापित कर सकता है। ई-बिजनेस को हम तीन भागों में बाँट सकते हैं—

- व्यापार से व्यापार ई-कॉमर्स (B2B)— जब कोई एक व्यापारिक संगठन किसी दूसरे व्यापारिक संगठन से इन्टरनेट के माध्यम से व्यापार करता है तो उसे व्यापार-से-व्यापार ई-बिजनेस कहते हैं।  
उदाहरण के लिए— एक व्यापार दूसरे व्यापार को कच्चा माल प्रदान कर रहा है तथा वह दूसरा व्यापार उस कच्चे माल का प्रयोग कर उसकी वस्तु बनाकर पहले व्यापार को दोबारा प्रदान करता है। इसे व्यापार से व्यापार ई-बिजनेस कहते हैं।
- उपभोक्ता-से-व्यापार ई-कॉमर्स (C2B)— जब कोई उपभोक्ता इन्टरनेट के माध्यम से किसी व्यापारिक संगठन से व्यापार करता है तो उसे उपभोक्ता से व्यापार ई-बिजनेस कहते हैं। उदाहरण के लिए— कोई उपभोक्ता किसी व्यापारिक संगठन से किसी वस्तु के संबंध में लेन-देन करता है तो यह उपभोक्ता से व्यापार ई-बिजनेस कहलाता है।
- उपभोक्ता-से-उपभोक्ता ई-कॉमर्स (C2C)— इसमें जब कोई उपभोक्ता किसी दूसरे उपभोक्ता से सीधे इन्टरनेट के माध्यम से संपर्क स्थापित करता है तो उसे उपभोक्ता से उपभोक्ता ई-कॉमर्स कहते हैं।

प्रश्न-27. ई-कॉमर्स के प्रकारों को विस्तार से वर्णन करते हुये समझाइये।  
उत्तर— ई-कॉमर्स के प्रकार— लेन-देन की प्रकृति तथा पक्षों (parties) की संलिप्तता के आधार पर ई-कॉमर्स के मुख्य प्रकार हैं—

- व्यापार-व्यापार ई-कॉमर्स (Business to Business E-Commerce)— व्यापार-व्यापार ई-कॉमर्स कम्पनियों के मध्य किये जाने वाले ई-कॉमर्स को कहते हैं। यह ई-कॉमर्स का वह प्रकार है जो दो व्यापारिक प्रतिष्ठानों के बीच या व्यापारिक प्रतिष्ठानों के मध्य संबंध को दर्शाता है। अधिकतर विशेषज्ञों का अनुमान है कि व्यापार-व्यापार ई-कॉमर्स व्यापार-उपभोक्ता ई-कॉमर्स की अपेक्षाकृत तेजी से उन्नति करेगा।

(B) व्यापार-उपभोक्ता ई-कॉमर्स (Business to Consumer E-Commerce)— व्यापार-उपभोक्ता इलेक्ट्रॉनिक कॉमर्स का वह रूप है जिसमें उत्पाद या सेवाएँ

किसी प्रतिष्ठान या कम्पनी से किसी उपभोक्ता को बेची जाती है। व्यापार-उपभोक्ता ई-कॉमर्स अथवा कम्पनियों और उपभोक्ताओं के बीच के वाणिज्य में निम्नलिखित प्रकार के ग्राहक आते हैं-

- (i) सूचना एकत्र करता हुआ  
(ii) भौतिक रूप अर्थात् ठोस या सर्श सामान जैसे पुस्तकें या अन्य उपभोक्ता वस्तु की खरीदारी करता हुआ। यह ई-कॉमर्स का दूसरा सबसे बड़ा और सबसे पुराना रूप है। ई-टेलिंग को इसका शुरुआत कहा जा सकता है। इस प्रकार, व्यापार-उपभोक्ता व्यापार मॉडल का अधिक साधारण मॉडल ऑन लाइन रिटेलिंग कम्पनियाँ जैसे अमेजन.कॉम, ईबे.कॉम (ebay.com) हैं।

प्रश्न-28. इलेक्ट्रॉनिक रिटेलिंग (ई-टेलिंग) क्या है? संक्षिप्त में समझाइये।

उत्तर- इलेक्ट्रॉनिक रिटेलिंग (E-tailing)- ई-टेलिंग या इलेक्ट्रॉनिक रिटेलिंग इन्टरनेट पर खुदरा सामान बेचने को कहते हैं। यह व्यापार-उपभोक्ता लेनदेन का सबसे सामान्य रूप है।

(A) उपभोक्ता-व्यापार ई-कॉमर्स- उपभोक्ता-व्यापार लेनदेन में उल्डी नीलामी सम्मिलित होते हैं जो उपभोक्ता को लेनदेन अंजाम देने हेतु संशकस्त बनाते हैं। इसका एक ठोस उदाहरण है जब प्रतिस्पर्धी एयरलाइन्स यात्री के सर्वश्रेष्ठ यात्रा तथा टिकट के लिए ऑफर देता है।

(B) उपभोक्ता-उपभोक्ता ई-कॉमर्स- उपभोक्ता-उपभोक्ता ई-कॉमर्स अथवा सी-2-सी (C2C) उपभोक्ता तथा उपभोक्ता के मध्य के वाणिज्य को कहते हैं। इलेक्ट्रॉनिक बाजारों तथा ऑन लाइन नीलामी में वृद्धि इस प्रकार के ई-कॉमर्स की विशेषता है। ये खासकर vertical उद्योगों में है जहाँ कम्पनियाँ विभिन्न सलायर्स से क्या चाहती हैं, इसकी बोली लगा सकती है। इसमें नये बाजारों के विकास की भयंकर संभावना है।

उपभोक्ता-उपभोक्ता ई-कॉमर्स में उपभोक्ता के मध्य किसी तीसरी पार्टी के माध्यम से लेनदेन होता है। इसका एक सबसे सीधा उदाहरण ऑन लाइन नीलामी है जिसमें उपभोक्ता बिक्री के लिए किसी आइटम को नेट पर भेजता है तथा अन्य उपभोक्ता उसे खरीदने के लिए बोली लगाते हैं तथा तीसरा पक्ष सामान्यतः सेवा शुल्क या कमीशन इस नीलामी को व्यवस्था करने के लिए लेते हैं। इस तरह के वाणिज्य में लगे हुए साइट्स बेचने तथा खरीदने वाले के बीच केवल intermediary का कार्य करते हैं। इनका काम उपभोक्ता को मिलाने का होता है। इनका कार्य उत्पाद के गुणवत्ता की जाँच करना नहीं होता।

(C) व्यापार-सरकार ई-कॉमर्स (Business-Government E-Commerce)- व्यापार-सरकार ई-कॉमर्स अथवा बी2जी को आमतौर पर कम्पनियों तथा पब्लिक सेक्टर के बीच किये जा रहे वाणिज्य के रूप में परिभाषित किया जाता है। इस प्रकार के ई-कॉमर्स के अन्तर्गत इन्टरनेट की उपयोगिता में पब्लिक अधिग्रहण, लाइसेंसिंग प्रक्रिया तथा अन्य सरकार संबंधी क्रियाएँ शामिल हैं।

इस प्रकार के ई-कॉमर्स के दो फीचर हैं। पब्लिक सेक्टर की भूमिका इस ई-कॉमर्स को स्थापित करने में अहम होता है तथा दूसरा ऐसा माना जाता है कि पब्लिक सेक्टर को इसके

अधिग्रहण तंत्र को अधिक प्रभावी बनाने की भरपूर आवश्यकता होती है। वेब आधारित खरीदारी पब्लिसी अधिग्रहण सिस्टम को अधिक पारदर्शी बनाती है तथा अनियमितताओं के खतरे को कम करती है। आजतक, किन्तु, संपूर्ण ई-कॉमर्स के घटक के रूप में बी2जी ई-कॉमर्स का आकार बहुत छोटा है। इसका कारण सरकारी अधिग्रहण प्रणाली का अभी तक टीक-टीक विकसित न हो पाना है।

(D) सरकार-व्यापार ई-कॉमर्स (Government-to-Business E-Commerce)- सरकार-व्यापार ई-कॉमर्स स्थानीय तथा केन्द्रीय सरकार और वाणिज्यिक ऑन लाइन बाताचीत का नाम है। इसमें सरकार के साथ केवल व्यापारिक कम्पनियाँ ही जुड़ती हैं। उदाहरणार्थ, <http://www.dti.gov.uk> एक सरकारी वेबसाइट है जहाँ व्यापारी ई-व्यापार के सर्वश्रेष्ठ प्रचलन पर सूचना तथा सुझाव प्राप्त कर सकते हैं।

(E) सरकार-नागरिक ई-कॉमर्स (Government-to-Citizen E-commerce)- इन्टरनेट शासन में बहुत ही सहायक है। यह अच्छे शासन के लिए एक दरवान साबित हुआ है। कई सरकारी विभागों को भारत के कई राज्यों में कम्प्यूटर तथा इन्टरनेट से जोड़ा गया है। आंध्रप्रदेश भारत में इस तरह का एक बेहतर उदाहरण है। इस राज्य में, इन्टरनेट की सहायता से लोग अपने कार्य पंचायत स्तर से लेकर मुख्य मंत्रीय कार्यालय तक करवा सकते हैं। इन्टरनेट ने कतार में घंटों लगने तथा लिफिकों व अन्य कर्मचारियों को रिश्तत देने जैसे समस्याओं को भी बहुत कम कर दिया है। इन्टरनेट ने बैंकों, विद्यालयों, महाविद्यालयों, विश्वविद्यालयों, पासपोर्ट कार्यालयों, प्रशासनिक कार्यालयों में सामान्य नागरिक जीवन को बहुत सहज बनाया है। भारत में नेशनल इन्फॉर्मेटिक्स सेन्टर ने कई सरकारी साइटें विकसित की हैं जो सामान्य आदमी को प्रधानमंत्री तथा राष्ट्रपति कार्यालयों से जोड़ती हैं।

ई-शासन इस तरह की सेवाओं को लोगों के दरवाजे पर पहुँचाने में बड़ी मदद की है। इसे जी-टू-सी अर्थात् सरकार से नागरिक भी कहा जाता है। ई-शासन या नागरिकों के लिए सरकार दुनिया के कई देशों में लोकप्रिय हुई है। अमेरिका का फर्स्टगव, ब्रिटेन का ई-इन्वाय, ताइवान का ई-ताइवान, सिंगापुर का ई-सिटीजन, ई-कोरिया, ई-मलेशिया तथा कनाडा का गर्वन्मेंट ऑन लाइन प्रचलित तथा पुरस्कृत है। इस प्रकार की सरकार ने राज्य के लोगों को एक ही छत के नीचे सभी संभव सुविधाएँ देकर लोगों को काम करवाने के लिए एक कार्यालय से दूसरे कार्यालय भटकने से रोकना है। ई-सेवा का प्रयोग कर लोग अपने पानी, बिजली तथा टेलीफोन का बिल बगैर किसी परेशानी के जमा कर सकते हैं। इसके अतिरिक्त वे जन्म प्रमाण-पत्र, मृत्यु प्रमाण-पत्र शैक्षणिक प्रमाण-पत्र ऑन लाइन प्राप्त कर सकते हैं। यह सेवा 1991 में प्रारम्भ हुई तथा यह ई-सेवा 200 केन्द्रों के माध्यम से 150 सेवाएँ प्रदान कर रही है। एक अनुमान के मुताबिक प्रत्येक माह पाँच करोड़ से भी अधिक लोग इससे लाभान्वित हो रहे हैं। ई-सेवा प्रॉपर्टी कर, आयकर आदि भी जमा करने में सहायक है। पासपोर्ट के लिए इसके माध्यम से आवेदन किया जा सकता है। रेलगाड़ी तथा हवाईजहाज की टिकटें सुरक्षित की जा सकती हैं। सिनेमा हॉलों से टिकट खरीदे जा सकते हैं। ई-शासन भारत में केरल तथा कर्नाटक में बहुत बढ़िया कार्य कर रहे हैं।

(F) मोबाइल कॉमर्स (Mobile Commerce) - मोबाइल कॉमर्स या एम. कॉमर्स तार रहित प्रौद्योगिकी यथा हैण्डहेल्ड उपकरण जैसे सेल्यूलर टेलीफोन तथा पर्सनल डिजिटल असिस्टेण्ट के माध्यम से सामानों तथा सेवाओं के क्रय-विक्रय को कहा जाता है। जापान आण दुनिया में एम. कॉमर्स के मामले में चोटी पर है।

प्रश्न-29. ई-कॉमर्स संबंधी सेवाएँ कौन-सी हैं तथा इनके क्या लाभ हैं? स्पष्ट कीजिये।

अथवा

ई-कॉमर्स संबंधी सेवा की आवश्यकता क्यों होती है? संक्षेप में वर्णन कीजिये।

उत्तर-ई-कॉमर्स संबंधी सेवाएँ-ई-कॉमर्स से सम्बन्धित सेवाएँ निम्न हो सकती हैं-

(A) ट्रान्जैक्शन प्रक्रिया प्रणाली (Transaction Processing System)- आदान-प्रदान से सम्बन्धित लेन-देनों को ट्रान्जैक्शन प्रक्रिया प्रणाली कहते हैं, जो कि निम्नलिखित हैं-

(i) टिकट और स्थान आरक्षण, (ii) स्टॉक व्यापार (iii) बीमा

(B) शिक्षा एवं विकासा-ई-कॉमर्स के माध्यम से लोग इन्टरनेट का प्रयोग करके शिक्षा के क्षेत्र में नये-नये प्रयोगों के बारे में जानकारी तथा वांछित सूचनाओं को आसानी से प्राप्त कर सकते हैं।

(C) सूचना सेवाएँ-इन्टरनेट कम्प्यूटर्स और अमेरिका ऑन लाइन जैसे उदाहरण सार विश्व को सूचना सेवाएँ प्रदान करते हैं तथा विश्व में हो रहे नये-नये प्रयोगों के बारे में अवगत कराते हैं।

(D) वैल्यू ऐडेड नेटवर्क- हम VAN को एक टेलीकम्यूनिकेशन नेटवर्क की तरह परिभाषित कर सकते हैं जो विभिन्न सूचनाओं को व्यवसाय संबंधी सूचनाओं व सुविधाओं में परिवर्तित करता है।

प्रश्न-30. ई-कॉमर्स से सम्बन्धित टेक्नोलॉजीज को समझाइये तथा इनके विभिन्न उपयोग लिखिये।

उत्तर-ई-कॉमर्स से सम्बन्धित टेक्नोलॉजीज- ऐसी अनेक टेक्नोलॉजी हैं, जो कि इलेक्ट्रॉनिक कॉमर्स के आवश्यक अंग हैं, जो कि निम्न प्रकार हैं-

(1) इलेक्ट्रॉनिक डाटा इन्टरचेंज (EDI)- यह एक ऐसी प्रक्रिया है जिसमें सूचना एक स्टैंडर्ड इलेक्ट्रॉनिक के रूप में एक कम्प्यूटर से दूसरे कम्प्यूटर को आदान-प्रदान की जाती है। कम्प्यूटर के अंदर संग्रह सूचना को एक विशेष सॉफ्टवेयर के द्वारा EDI फॉर्मेट में परिवर्तित किया जाता है, जिससे कि उसे एक या अधिक ट्रेडिंग पार्टनर्स को भेजा जा सके। ट्रेडिंग पार्टनर्स की मशीन पुनः इसे EDI फॉर्मेट से उस फॉर्मेट (सॉफ्टवेयर के द्वारा) में परिवर्तित करती है, जिसे वह समझ सके।

(2) बार-कोड-इसका उपयोग इसलिये किया जाता है कि कम्प्यूटर, प्रोडक्ट की स्वतः ही पहचान कर सके। ये आयाताकार आकार की परिवर्तित चौड़ाई व लम्बाई की लाइनें होती हैं। इस अनोखे पैटर्न को कुछ विशेष नम्बर वाले चिन्ह एसाईन (दिना) कर दिये जाते हैं। अतः इस प्रकार से एक फॉन्ट का निर्माण होता है, जिसे लेजर लाईट परावर्तन के द्वारा कम्प्यूटर पहचानता है। कन्ज्यूमर प्रोडक्ट्स बार कोड्स इसका सबसे महत्वपूर्ण उदाहरण हैं। इन कोड के

आधार पर प्रोडक्ट को चेक आउट काउंटर पर स्केन (परीक्षण) किया जाता है। जैसे ही प्रोडक्ट को पहचान लिया जाता है, केश रजिस्टर में उसका मूल्य लिख दिया जाता है और इस प्रकार से आंतरिक सिस्टम स्वतः ही परिवर्तित हो जाता है। ऐसी किसी भी प्रोसेस जिसमें कि मटेरिअल फ्लो पर कड़ा नियंत्रण रखना हो, यह तकनीक अत्यन्त प्रभावी होती है।

(3) इलेक्ट्रॉनिक मेल-यह एक ऐसी प्रक्रिया है जिसमें एक व्यक्ति अपने मैसेज को कम्पोज करके इन्टरनेट के द्वारा डिजिटल रूप में दूसरे को भेजता है। इन्टरनेट लाइव अलग-अलग कम्प्यूटर व कम्प्यूटर नेटवर्क्स का एक डिस्ट्रिब्यूटिव (विकेंद्रित) ग्लोबल नेटवर्क है।

(4) वर्ल्ड वाइड वेब (WWW)- यह ऐसे डोक्यूमेंट्स का संग्रह होता है, जो हायपर टेक्स्ट मार्कअप लैंग्वेज में लिखे व एनकोड किये जाते हैं। एक छोटे से सॉफ्टवेयर को जोड़ने पर जिसे ब्राउजर कहते हैं, यूजर इन डॉक्यूमेंट्स को माँग सकता है और पर्सनल कम्प्यूटर पर इनको देख सकता है। WWW, इन्टरनेट पर सबसे ज्यादा उपयोग किया जाने वाला एप्लिकेशन है।

(5) प्रोडक्ट डाटा एक्सचेंज (PDE)- यह डाटा के ग्राफीय रूप में आदान-प्रदान की ऐसी प्रक्रिया है जिसमें किसी प्रोडक्ट के विवरण के लिये पिक्चर, ड्राईंग व CAD फाइलों का उपयोग किया जाता है। जबकि अन्य परिस्थितियों में (जैसे स्पेसिफिकेशन्स, बिल्स ऑफ मटेरियल्स, मेन्युफेक्चरिंग इन्स्ट्रक्शन्स, इंजीनियरिंग चेंज नोटिसेस व टेस्ट रिजल्ट इत्यादि) डाटा कोरेक्टर व न्यूमेरिक चिन्हों पर आधारित होता है। PDE दूसरे प्रकार के व्यापारिक कम्प्यूरीकेशन में दो प्रकार से अलग होता है। पहला यह कि ग्राफीकल फाइल्स, विड्यो में बहुत अधिक होती है और सॉफ्टवेयर के बीच कोम्पैटिबिलिटी की समस्या होती है। दूसरा यह कि वरेशन कंट्रोल बहुत कठिन होता है। डेवलपमेंट सायकल में प्रोडक्ट की डिजाईन्स में बहुत बड़े-बड़े परिवर्तन होते हैं जबकि मेन्युफेक्चरिंग प्रोसेस में प्रोडक्ट में छोटा सा परिवर्तन प्रोडक्ट के उत्पादन में बहुत प्रभाव डालता है।

(6) इलेक्ट्रॉनिक फॉर्म-यह ऐसी तकनीक है जिसमें पेपर फॉर्म के साथ सूचनाओं को डिजिटल रूप में स्टोर किया जाता है। उदाहरणार्थ ऐसा पेपर फॉर्म जिसमें लाइन्स, बॉक्स, चेक ऑफ लिस्ट्स व लाईन के लिये जगह इत्यादि हो। किसी यूजर के लिए इलेक्ट्रॉनिक फॉर्म इसी फॉर्म के समान डिजिटल रूप में होता है जिसकी समस्त जानकारी कम्प्यूटर स्क्रीन पर दिखती है। इसे किबाई या माउस के द्वारा भरा जाता है। इस फॉर्म में अतिरिक्त कार्यों में सर्वप्रथम डाटा डिजिटल रूप में होने से डाटाबेस में स्टोर किया जा सकता है, सूचनाओं का स्वतः एक स्थान से दूसरे स्थान तक जाना व अन्य एप्लिकेशन के साथ उपयोग करना इत्यादि शामिल है। इसका सबसे अच्छा उदाहरण बहुत सी यूनिवर्सिटी के एप्लिकेशन फॉर्म हैं।

ई-बिजनेस इन्टरनेट पर व्यापार का संचालन है, जिसमें कि सेल-पर्वेज ही नहीं बल्कि इसके साथ-साथ परचेजर को सहयोग करना तथा व्यापार में दूसरे सहयोगी पार्टनर को भी सहयोग प्रदान करना शामिल होता है। ई-बिजनेस टर्म का सर्वप्रथम उपयोग IBM के द्वारा 1997 में अपने व्यापार को बढ़ाने के लिए किया गया था। आज अधिकांश कॉरपोरेशन इन्टरनेट की क्षमताओं का उपयोग कर, अपने व्यापार को बढ़ाने हेतु प्रयास कर रहे हैं।

कम्पनियों अपने उत्पादन को बेचने के लिए, व्यापार को बढ़ाने के लिए या संयुक्त खोज के लिए 'वेब' का उपयोग करती हैं।

### इ-गवर्नेंस सर्विस, डिजी-लॉकर, अकादमिक बैंक ऑफ़ टैडिट, ऑनलाइन शिक्षण संसाधनों की रोज़ोज़

दीर्घ एवं लघु उत्तरीय प्रश्न-

प्रश्न-1. ई-गवर्नेंस क्या है? विवेचना कीजिये।

उत्तर- ई-गवर्नेंस या इलेक्ट्रॉनिक गवर्नेंस- इलेक्ट्रॉनिक-गवर्नेंस या ई-गवर्नेंस गवर्निंग की प्रक्रियाओं में आईसीटी के आवेदन द्वारा शासन के क्षेत्र में एक नया प्रतिमान बदलाव विकसित किया गया है।

ई-गवर्नेंस सरकार, राष्ट्र, राज्य, नगरपालिका के बीच सरकार के भीतर सूचना तक विश्वसनीय पहुँच के संदर्भ में शासी प्रक्रिया में पारदर्शिता, जबाबदेही, दक्षता, प्रभावशीलता और समावेशिता को बढ़ाता है, और स्थानीय स्तर की सरकारें, नागरिक और व्यवसाय और सूचना के उपयोग और उपयोग के माध्यम से व्यवसाय को सशक्त बनाती हैं।

ई-गवर्नेंस या इलेक्ट्रॉनिक गवर्नेंस का मुख्य फोकस नागरिकों को पारदर्शी, न्यायसंगत और जवाबदेह सेवा प्रदान करना है। ई-गवर्नेंस का उद्देश्य शासन की गुणवत्ता में सुविधा और सुधार करता है और ई-मेल, वेबसाइट, एसएमएस कनेक्टिविटी और अन्य जैसे इलेक्ट्रॉनिक माध्यमों से लोगों की संचालन प्रक्रिया में भागीदारी सुनिश्चित करता है।

ई-गवर्नेंस केवल सरकारी वेबसाइटों या ई-मेल या वित्तीय लेनदेन के बारे में नहीं है, "यह बदल जाएगा कि नागरिक सरकार से कितना संबंधित है क्योंकि यह बताता है कि नागरिक एक-दूसरे से कैसे संबंधित हैं।" यह देश की लोकतांत्रिक प्रक्रियाओं में आईटी के उपयोग को भी संदर्भित करता है।

ई-गवर्नेंस नागरिकों को सार्वजनिक सेवा को बढ़ावा देने के लिए आईसीटी के उपयोग करता है। इसमें कुशल और लागत प्रभावी सेवाओं और शासित होने वाले नागरिकों को जानकारी और ज्ञान प्रदान करने के लिए आईसीटी का एक व्यावहारिक अनुप्रयोग और उपयोग शामिल है, जिससे नागरिकों की सेवा करने के लिए सरकार की विशाल क्षमता का अनुभव होता है। इसने राज्य और समाज, सरकार और लोगों, लोगों से लोगों, शासन और समाज के बीच संबंध बनाए हैं।

ई-गवर्नेंस के उद्देश्य- ई-गवर्नेंस के उद्देश्य इस प्रकार हैं-

(1) ई-गवर्नेंस का मूल उद्देश्य सरकार की जानकारी को जनहित में उपलब्ध कराना है।

(2) इसका एक लक्ष्य सरकार और लोगों के बीच एक सहकारी संरचना तैयार करना, लोगों से मदद और सलाह लेना तथा सरकार को लोगों की समस्याओं से अवगत कराना है।

2. शासन प्रक्रिया में लोगों की भागीदारी को बढ़ाने और प्रोत्साहित करने हेतु।

(4) ई-गवर्नेंस देश की सूचना और संचार प्रौद्योगिकी और इलेक्ट्रॉनिक मीडिया में सुधार करता है, जिसका उद्देश्य सरकारों, जनता और व्यवसायों को आधुनिक दुनिया के अनुपम रखकर देश की अर्थव्यवस्था को मजबूत करना है।

(5) इसका एक मुख्य उद्देश्य शासन प्रक्रिया में पारदर्शिता और जवाबदेही स्थापित करना है।

(6) सूचना और सेवाओं पर सरकारी व्यय को कम करने हेतु।

प्रश्न-2. रेलवे रिजर्वेशन पर सक्षिप्त टिप्पणी लिखिए।

उत्तर- रेलवे आरक्षण- ऑनलाइन रेलवे टिकट आरक्षण आजकल बहुत उपयोगी है। टिकट बुकिंग और संबंधित लेनदेन के लिए एक अच्छा काम करने वाला सिस्टम सॉफ्टवेयर डिजाइन करना बहुत महत्वपूर्ण है। इसे डिजाइन करने के लिए मॉडल के पूर्ण-ट्रेक प्रलेखन की आवश्यकता होती है क्योंकि यह सॉफ्टवेयर विकास से संबंधित है।

सिस्टम की विशेषताएँ- आरक्षण प्रणाली में निम्नलिखित विशेषताएँ होनी चाहिए-

(1) यदि कोई यात्री टिकट आरक्षित करना चाहता है तो सबसे पहले, उसे वैध क्रेडेंशियल्स के साथ रेलवे प्रणाली में लॉगइन करना होगा। फिर, यात्री को यात्रा की तारीख, यात्रियों के नाम और उनके विवरण, मूल स्टेशन विवरण, गंतव्य स्टेशन विवरण के साथ अपना विवरण प्रदान करना साथ ही आवश्यक टिकट का वर्ग प्रकार भी देना होगा।

(2) रेलवे आरक्षण उपलब्ध ट्रेन-सूची और सीट-उपलब्धता, विवरण के माध्यम से प्रदान करेगी।

(3) टिकट बुक करने के लिए यात्री ऑनलाइन/ऑफलाइन मोड के माध्यम से भुगतान कर सकते हैं। टिकट किराये के सफल भुगतान के बाद सिस्टम द्वारा टिकट और पीएनआर नं. यात्री को दिया जाएगा। सिस्टम भुगतान विवरण भी रखता है और उन्हें सिस्टम व्यवस्थापक को भेजता है।

(4) यात्री पीएनआर स्थिति सिस्टम में पीएनआर नम्बर दर्ज करके जात कर सकता है।

(5) आरक्षण प्रणाली को सभी ट्रेन विवरणों, किराया विवरणों, ट्रेनों की तारीख आदि को संग्रहीत करना चाहिए। इस रखरखाव को व्यवस्थापक द्वारा नियंत्रित किया जाता है।

(6) टिकट कैंसिल कराने पर सिस्टम में धन वापसी नियम भी हैं, जिनमें आरक्षण, टिकट किराया और वापसी योग्य प्रतिशत है। यात्री केवल पीएनआर नम्बर और रद्द टिकट अनुरोध दर्ज करके टिकट को रद्द कर सकता है। रद्द करने के बाद, व्यवस्थापक सिस्टम को वापसी योग्य राशि पारित करेगा और सिस्टम यात्री को वापसी योग्य राशि वापस देगा।

प्रश्न-3. पासपोर्ट सेवा पर प्रकाश डालिये।

उत्तर- पासपोर्ट सेवा- एक पासपोर्ट उन लोगों के लिए आवश्यक यात्रा दस्तावेज है जो शिक्षा, तीर्थयात्रा, पर्यटन, व्यावसायिक उद्देश्यों, चिकित्सा उपस्थिति और पारिवारिक

यात्राओं के लिए, विदेश यात्रा करना चाहते हैं, पिछले कुछ वर्षों के दौरान, बढ़ती अर्थव्यवस्था और वैश्वीकरण ने पासपोर्ट और संबंधित सेवाओं की मांग में बढोतरी की है। इस बढी हुई मांग को पूरा करने के लिए, विदेश मंत्रालय ने मई, 2010 में पासपोर्ट सेवा परियोजना को लॉन्च किया।

पासपोर्ट सेवा पासपोर्ट और संबंधित सेवाओं के विवरण के लिए सरल, कुशल और पारदर्शी प्रक्रियाओं को सक्षम बनाता है। यह परियोजना सरकारी कर्मचारियों के लिए एक देशव्यापी नेटवर्क वातावरण बनाती है और आवेदक की साख के भौतिक सत्यापन के लिए और पासपोर्ट के वितरण के लिए इंडिया पोस्ट के साथ राज्य पुलिस के साथ एकीकृत होती है-

- (1) पासपोर्ट की आवश्यकता
  - (2) पासपोर्ट के लिए आवेदन करने की प्रक्रिया
  - (3) तत्काल पासपोर्ट
- अन्य सेवाएँ-
- (1) मोबाइल पासपोर्ट सेवा
  - (2) प्रतिक्रिया या शिकायतें
  - (3) पासपोर्ट सेवा ग्रामीण क्षेत्र में।

पासपोर्ट की आवश्यकता- सभी भारतीय नागरिक जो भारत से विदेश प्रस्थान करने का इरादा रखते हैं उनके पास वैध पासपोर्ट या यात्रा दस्तावेज होना आवश्यक है। पासपोर्ट अधिनियम, 1967 के तहत, भारत सरकार विभिन्न प्रकार के पासपोर्ट और यात्रा दस्तावेज जारी कर सकती है जैसे कि साधारण पासपोर्ट, राजनयिक पासपोर्ट, आधिकारिक पासपोर्ट, उद्देश्य के लिए आपातकालीन प्रमाण-पत्र और पहचान का प्रमाण-पत्र।

पासपोर्ट के लिए आवेदन करने की प्रक्रिया-

- (1) ई-फॉर्म सबमिशन के माध्यम से।
- (2) ऑनलाइन फॉर्म सबमिशन के माध्यम से।
- (1) ई-फॉर्म सबमिशन के माध्यम से पासपोर्ट के लिए आवेदन-  
ई-फॉर्म सबमिशन के माध्यम से पासपोर्ट के लिए आवेदन करने के लिए, उपयोगकर्ताओं को पासपोर्ट सेवा पोर्टल पर पंजीकरण करना होगा।
- (2) पंजीकरण के बाद, पासपोर्ट सेवा पोर्टल पर लॉगइन करना होगा।
- (3) पासपोर्ट के ताजा या फिर से जारी करने के लिए ई-फॉर्म डाउनलोड करना होता है।
- (4) डाउनलोड किए गए ई-फॉर्म भरे और मान्य और सहजे बटन पर क्लिक करें। यह एक एक्सएमएल फाइल उत्पन्न करेगा जो बाद में सिस्टम में अपलोड करने के लिए आवश्यक होगा।
- (5) अपलोड ई-फॉर्म के माध्यम से एक्सएमएल फाइल अपलोड करें। इस स्तर पर पीडीएफ फॉर्म अफलोड नहीं करें क्योंकि सिस्टम द्वारा केवल एक्सएमएल फाइल स्वीकार की जाती है।

(6) पासपोर्ट के नए या पुनः जारी करने के लिए फॉर्म अपलोड करने के बाद, पासपोर्ट सेवा केन्द्र पर नियुक्ति का समय निर्धारित करने के लिए 'भुगतान और अनुसूची नियुक्ति' लिंक पर क्लिक करें।

(7) अब पासपोर्ट सेवा केन्द्र स्थान खोजें और अपना पीएसके चुनें।

(8) चयनित पीएसके पर नियुक्ति की बुकिंग के बाद, आप क्रेडिट/डेबिट कार्ड (मास्टर कार्ड और बीजा) के माध्यम से ऑनलाइन भुगतान कर सकते हैं। इंटरनेट बैंकिंग स्टेट बैंक ऑफ इंडिया चैलन।

(9) आप ऑनलाइन शुल्क पासपोर्ट सेवाओं के लिए कैलकुलेटर के माध्यम से शुल्क की गणना कर सकते हैं।

(10) उपयोगकर्ता एलिकेशन रसीद का प्रिंट ले सकते हैं जिसमें एलिकेशन संदर्भ संख्या या नियुक्ति संख्या है।

(11) पासपोर्ट सेवा केन्द्र पर जाएं जहाँ नियुक्ति बुक की गई है, साथ ही मूल दस्तावेज- बाहरी वेबसाइट जो एक नई विडिओ में खुलती है जैसे कि जन्म का प्रमाण पत्र, तस्वीर के साथ पहचान प्रमाण, निवास का प्रमाण और राष्ट्रीयता का प्रमाण।

(12) ई-फॉर्म सबमिशन के माध्यम से पासपोर्ट के लिए आवेदन करें।

(13) आवश्यक दस्तावेज- वेबसाइट पर जानकारी उपलब्ध रहती है।

(14) ट्रेकिंग आवेदन की स्थिति।

तत्काल पासपोर्ट सेवा- उन पासपोर्ट आवेदकों के लिए उपलब्ध यह एक योजना है, जिन्हें अपने पासपोर्ट की तत्काल आवश्यकता होती है। तत्काल योजना के तहत पासपोर्ट जारी करने का अंतिम अधिकार कार्यालय के पास होता है।

तत्काल पासपोर्ट योजना के तहत पासपोर्ट को एक कार्य दिवस के भीतर भेज दिया जाता है। यदि पुलिस सत्यापन की आवश्यकता नहीं है, तो आवेदन जमा करने की तारीख को छोड़कर, यदि पोस्ट-पासपोर्ट जारी करने के आधार पर पुलिस सत्यापन आवश्यक है, पुलिस सत्यापन रिपोर्ट की प्रतीक्षा किए बिना - आवेदन जमा करने की तारीख को छोड़कर तीसरे कार्य दिवस पर पासपोर्ट भेजा जाता है।

नागरिक ई-फॉर्म सबमिशन या ऑनलाइन फॉर्म सबमिशन के माध्यम से तत्काल योजना के तहत पासपोर्ट के नए पासपोर्ट या फिर से जारी करने के लिए आवेदन कर सकते हैं। तत्काल रक्रीम के तहत पासपोर्ट सेवाओं के लिए शुल्क की गणना कर सकते हैं। जो कि ऑनलाइन शुल्क कैलकुलेटर के माध्यम से की जा सकती है।

अन्य सेवाएँ- पासपोर्ट सेवा पोर्टल के माध्यम से पुलिस क्लियरेंस सर्टिफिकेट भी प्राप्त किया जा सकता है।

प्रश्न-4. ई-स्वास्थ्य को विस्तार से समझाइए।

उत्तर- स्वास्थ्य और परिवार कल्याण मंत्रालय ने सार्वजनिक स्वास्थ्य प्रणाली की दक्षता और प्रभावशीलता में सुधार के लिए सूचना और संचार प्रौद्योगिकी का उपयोग करके विभिन्न

पहल की है। मंत्रालय लगातार आईसीटी पहलों की योजना बनाने और शुरू करने पर काम कर रहा है। मंत्रालय द्वारा आईसीटी फाइलों के तहत किए जाने वाले कार्य इस प्रकार हैं-

(1) राष्ट्रीय स्वास्थ्य पोर्टल- स्वास्थ्य क्षेत्र में स्वास्थ्य, सरकारी कार्यक्रमों और सेवाओं के बारे में नागरिकों के बीच जागरूकता पैदा करने के लिए एक समग्र उद्देश्य के साथ, राष्ट्रीय स्वास्थ्य पोर्टल विभिन्न भाषाओं में नागरिकों और हितधारकों को जानकारी प्रदान करता है (वर्तमान में छह भाषाएँ हिन्दी, अंग्रेजी, तमिल, गुजराती, बंगाली और पंजाबी) एक वॉइस पोर्टल, जो टोल-फ्री नम्बर 1800-180-1104 और मोबाइल ऐप के माध्यम से जानकारी प्रदान करता है। इस हेतु भी उपलब्ध है-

वेबसाइट : <http://www.nhp.gov.in>

ऑनलाइन पंजीकरण प्रणाली- नागरिकों के लिए सेवाओं में सुधार करने के लिए जुलाई 2015 में लॉन्च की गई ऑनलाइन पंजीकरण प्रणाली ऑनलाइन पंजीकरण और नियुक्ति, शुल्क के भुगतान के लिए नागरिकों को सेवाएँ प्रदान करता है, जैसे- ऑनलाइन देखने की डैशबोर्ड रिपोर्ट, विभिन्न सार्वजनिक अस्पतालों में ऑनलाइन रक्त की उपलब्धता की पूछताछ करना आदि।

(2) रोगी प्रतिक्रिया अनुप्रयोग- अस्पतालों में सेवा की गुणवत्ता, सुविधाओं आदि पर प्रतिक्रिया प्रदान करके स्वास्थ्य सेवा वितरण में सुधार के लिए नागरिकों को सशक्त बनाने के लिए और अंततः रोगी संचालित, उत्तरदायी और जवाबदेह स्वास्थ्य प्रणाली स्थापित करने में मदद करने हेतु यह एप्लिकेशन लॉन्च किया गया है। यह एक मरूटी-वैनल दृष्टिकोण विज्ञ का उपयोग करके रोगियों के बारे में जानकारी एकत्र करने के लिए आईटी आधारित प्रतिक्रिया प्रणाली है। संतुष्टि का स्तर, एएसएमएस, आउटब्राउंड डायलिंग, वेब पोर्टल और मोबाइल ऐप, सार्वजनिक सुविधाओं में स्वास्थ्य सेवा वितरण की गुणवत्ता बढ़ाने के लिए सरकार को उचित निर्णय लेने में मदद करेगा जो रोगी के उपचार में सुधार करेगा। रोगी का प्रभावी और उचित देखभाल करने में सक्षम होगा।

वेबसाइट : <http://mvrbaaspatal.nhp.gov.in/>

(3) केन्द्रीय औषधि मानक नियंत्रण संगठन- कई हितधारकों के लिए 'सिंगल विंडो' प्रदान करने के लिए केन्द्रीय ड्रग्स मानक नियंत्रण संगठन ने संयुक्त रूप से "SUGAM" तैयार किया जो ऑनलाइन आवेदन प्रस्तुत करने में सक्षम बनाता है, उनकी ट्रेकिंग, मुख्य रूप से दवाओं, वैदिक परीक्षणों, नैतिकता समिति, चिकित्सा उपकरणों, टीकारण और सौन्दर्य प्रसाधनों के लिए ऑनलाइन अनुमोदन का प्रसंस्करण और अनुदान प्रदान करने में सहयोग करता है।

वेबसाइट : <http://www.cdscoc.nic.in/>

(4) राष्ट्रीय अंग और ऊतक प्रत्यारोपण संगठन- बड़े पैमाने पर नागरिकों के बीच अंग दान को बढ़ावा देने के लिए, राष्ट्रीय अंग और ऊतक प्रत्यारोपण संगठन अपने वेब-पोर्टल के माध्यम से अंग के लिए ऑनलाइन पंजीकरण के लिए सेवाएँ प्रदान करता है/अंग दान के लिए नागरिक द्वारा ऊतक प्रत्यारोपण या पुनर्प्राप्ति और ऑनलाइन प्रतिज्ञा पंजीकृत की जा सकती है।

मोबाइल एप्लिकेशन- मोबाइल कनेक्टिविटी की व्यापक पैठ का दोहन करने के लिए, अब तक निम्नलिखित विभिन्न मोबाइल ऐप लॉन्च किए गए हैं-

- (1) वैक्सीन ट्रेकर-
- (i) अपने बच्चों के टीकाकरण की स्थिति पर नजर रखने में माता-पिता का समर्थन करते हैं और उन्हें सटीक समय पर टीकाकरण सुनिश्चित करने में मदद करते हैं।
- (ii) इंडिया फाइट्स डेगू (डैगू के लक्षणों की जांच करने के लिए इसके उपयोगकर्ता को सक्षम बनाता है व निकटतम अस्पताल/रक्त बैंक की जानकारी प्राप्त करता है)।
- (iii) एनएचपी स्वास्थ्य भारत (रोग, जीवन शैली, प्राथमिक चिकित्सा) पर सूचना प्रसार का कार्य करता है।
- (iv) प्रधानमंत्री सुरक्षित मातृत्व अभियान मोबाइल ऐप (राज्यों से गर्भावस्था देखभाल संबंधी जानकारी की रिपोर्टिंग के लिए)।
- (v) एनएचपी निर्देशिका सेवा मोबाइल ऐप (भारत के समस्त अस्पतालों से संबंधित जानकारी प्रदान करता है)।
- (vii) Mera Aspaatal Mobile App (राज्यों से गर्भावस्था देखभाल संबंधी जानकारी की रिपोर्टिंग के लिए)।

011-22901701 को मिस्ड कॉल देकर लोगों को तम्बाकू छोड़ने के लिए परामर्श और मदद करने के लिए एक मोबाइल आधारित पारम्परिक पहल है। वर्तमान में 20 लाख से अधिक कुल मिस्ड कॉल समान कर लिये गये हैं और लगभग 15 लाख उपयोगकर्ता इस कार्यक्रम के लिए पंजीकृत हैं।

वेबसाइट : <http://www.nhp.gov.in/quit-tobacco>

(2) mDiabetes कार्यक्रम- यह 011-22901701 को मिस्ड कॉल देकर मधुमेह की रोकथाम और देखभाल के लिए एक मोबाइल-आधारित पहल है। वर्तमान में एक लाख से अधिक उपयोगकर्ता mDiabetes के लिए पंजीकृत हैं।

वेबसाइट : <http://mdiabetes.nhp.gov.in/>

(3) अस्पताल सूचना प्रणाली- सीएचसी स्तर तक सार्वजनिक स्वास्थ्य सुविधाओं में बेहतर दक्षता और सेवा वितरण प्राप्त करने के लिए अस्पताल प्रक्रियाओं के स्वचालन के लिए अस्पतालों में एचआईएस लागू किया जा सकता है। लक्षित प्रभाव में अस्पताल वर्कफ्लो प्रबंधन में सुविधा शामिल है जो रोगियों को सेवाओं की बेहतर डिजिटरी और अस्पतालों में प्रक्रियाओं की दक्षता में सुधार के लिए अग्रणी है। इस प्रणाली के कार्यान्वयन में निम्नलिखित शामिल हैं-

- (1) एनआईसी द्वारा विकसित एक ई-अस्पताल को 100 से अधिक अस्पतालों में क्लाउड क्लेटफॉर्म पर लागू किया गया है और 50 से अधिक अस्पताल स्टैंडअलोन क्लेटफॉर्म पर हैं।
- (2) C-DAC Noida का ई-सुगत अनुप्रयोग राजस्थान में कार्यात्मक रहा है (राज्य-व्यापीरू 80 सुविधाएँ) और अन्य राज्यों में यह 15 अस्पतालों से संबंधित है।

(4) अनमोल- एकीकृत आरसीएच रजिस्टर के लिए एक टैबलेट आधारित आवेदन जो एएनएम को अपने अधिकार क्षेत्र के लाभार्थियों के लिए डेटा दर्ज करने और अपडेट करने की अनुमति देता है, आंध्रप्रदेश राज्य में पायलट किया गया है। वर्तमान में लगभग 15,000 एएनएम आंध्रप्रदेश में अनमोल और MP & Telangana के पायलट जिलों में काम कर रहे हैं।

(5) इन्स और टीके वितरण प्रबंधन प्रणाली- यह राज्य/यूटी, जिला अस्पतालों (DH), CHC में उनके उप मंडार, विभिन्न जिला ड्रग गोदामों की खरीद, सूची संबंधित और विभिन्न दवाओं, टीके और सर्जिकल वस्तुओं के वितरण से संबंधित है। राज्य/यूटी स्तर में खरीद, आपूर्ति शृंखला, गुणवत्ता नियंत्रण और वित्त विभाग के वर्कफ्लो को स्वयंसेवा करके PHC आदि। DVDMS को अब तक 9 राज्यों/ UTS-आंध्रप्रदेश, गुजरात, जम्मू और कश्मीर, मध्यप्रदेश, महाराष्ट्र, ओडिशा, पंजाब, राजस्थान और तेलंगाना में लागू किया गया है और 8 राज्यों में इस प्रक्रिया में है- उत्तरप्रदेश, उत्तराखण्ड, बिहार, हिमाचल प्रदेश, मणिपुर, झारखंड, मेघालय और छत्तीसगढ़ DVDMS को सेंट्रल मीडिकल सर्विसेज सोसाइटी में भी लागू किया गया है- स्वास्थ्य और परिवार कल्याण विभाग के तहत एक केंद्रीय खरीद एजेंसी और कार्यान्वयन टीबी विभाग और के तहत- MoHFW का परिवार नियोजन प्रभाग, तमिलनाडु, त्रिपुरा, हरियाणा, कर्नाटक, केरल, दिल्ली और पश्चिम बंगाल जैसे राज्यों ने डीवीडीएमएस के अलावा आईटी आधारित आपूर्ति शृंखला प्रबंधन प्रणाली लागू की है, लेकिन इनमें समान विशेषताएँ हैं।

eRakt कोश- eRakt कोश लॉन्च किया गया है जो एक व्यापक है, ऑनलाइन रिसट्रम की मदद से कुशल और कुल गुणवत्ता प्रबंधन दृष्टिकोण और राज्यों/यूटी में सार्वजनिक और निजी स्वास्थ्य सुविधाओं में सभी लाइसेंस प्राप्त रक्त बैंकों के लिए रोल आउट किया जा रहा है। मतंज कोश दिल्ली, मध्यप्रदेश, उत्तराखण्ड और उत्तरप्रदेश के राज्यों/केंद्र शासित प्रदेशों में 7 ब्लाड बैंक में ऑनलाइन है। ब्लाड बैंक अपडेटेशन के लिए ई-रक्तकोश पोर्टल पर लगभग 124 ब्लाड बैंक पंजीकृत हैं। उत्तराखण्ड में 2 ब्लाड बैंक, यूपी में 1 और वेस्ट बंगाल में 1 एलिकेशन का उपयोग करने की प्रक्रिया में है।

वेबसाइट : <http://www.eraktkosh.in/>

स्वास्थ्य प्रबंधन सूचना प्रणाली (HMIS)- HMIS राष्ट्रीय स्वास्थ्य मिशन के तहत कार्यक्रमों की निगरानी के लिए एक वेब आधारित पोर्टल है।

कार्यक्रम की निगरानी और प्रबंधन में सुधार के लिए सार्वजनिक स्वास्थ्य सुविधाओं से मासिक सेवा वितरण डेटा रिपोर्टिंग के लिए लगभग 2 लाख स्वास्थ्य सुविधाएँ नियमित रूप से HMIS पोर्टल पर रिपोर्ट कर रही हैं। यह जीआईएस के साथ एकीकृत है और सार्वजनिक डोमेन में उपलब्ध है।

वेबसाइट : <http://nhm-nmis.nic.in/>

एकीकृत रोग निगरानी कार्यक्रम- डेटा प्रविष्टि, रिपोर्ट, डेटा विश्लेषण, प्रशिक्षण मॉड्यूल के लिए ऑनलाइन पोर्टल, जिस पर 90 जिले पोर्टल के माध्यम से साप्ताहिक निगरानी डेटा

रिपोर्ट करते हैं। टोल फ्री नम्बर पर रोग अलर्ट के लिए 24 x 7 कॉल सेंटर भी है, सत्यापन और उचित कार्रवाई शुरू करने के लिए

वेबसाइट : <http://dsp.nic.in/>

प्रश्न-5. ऑनलाइन परामर्श अथवा टेली-मेडिसिन का वर्णन कीजिये।

उत्तर- किफायती तरीके से स्वास्थ्य सेवाओं की सार्वभौमिक पहुँच के लिए, MoHFW ने नागरिकों के स्वस्थ जीवन और कल्याण को सुनिश्चित करने के लिए सतत विकास लक्ष्यों के साथ अपनी पहल को संरक्षित किया है। MoHFW ने देखभाल की निरन्तरता सुनिश्चित करने के लिए ग्रामीण और दूरदराज के क्षेत्रों में स्वास्थ्य सेवा वितरण की चुनौतियों का सामना करने के लिए मौजूदा स्वास्थ्य बुनियादी ढांचे के साथ सूचना और संचार प्रौद्योगिकियों के प्रभावी संलयन का उपयोग करने के लिए सक्रिय रूप से खलांग लगाई है। स्वास्थ्य सेवा वितरण में आसीटी नवाचारों से मिलने वाले लाभ को ध्यान में रखते हुए, MoHFW वर्तमान में जिस तरह से स्वास्थ्य सेवा कार्य कर रही है उसे बदलने के लिए नागरिक केन्द्रिय दृष्टिकोण अपनाया है। आईसीटी नवाचारों को शामिल करके, दुर्गम और ग्रामीण क्षेत्रों में अन्तिम उपयोगकर्ता के निकटतम बुनियादी और विशेष स्वास्थ्य देखभाल सेवाएँ प्रदान करने के लिए टेली-स्वास्थ्य समाधानों को बढ़ावा दिया जा रहा है। इस दिशा में विभाग की प्रमुख पहलों में नेशनल मीडिकल कॉलेज नेटवर्क, नेशनल टेलीमेडिसिन नेटवर्क टेलीमेडिसिन के लिए अन्तिम प्रौद्योगिकी का उपयोग आदि शामिल हैं। टेलीमेडिसिन प्रभाग के प्रमुख अधिकार उनके समर्पक विवरण में सम्मिलित किया है।

प्रश्न-6. डिजिटल लॉकर क्या है? डिजी-लॉकर की विशेषताएँ और लाभ लिखिए।

उत्तर- डिजिटल लॉकर- डिजिटल इंडिया कार्यक्रम के तहत प्रमुख पहलों में से एक है। इसका एक बीटा संस्करण इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी विभाग, सरकार द्वारा पहले ही जारी किया जा चुका है। भारत की डिजिटल लॉकर का उद्देश्य भौतिक दस्तावेजों के उपयोग को कम करना और सक्षम बनाना तथा सभी एजेंसियों में ई-दस्तावेजों का वितरण करना है।

इस पोर्टल की मदद से, ई-दस्तावेजों का साझाकरण पंजीकृत रिपॉजिटरी के माध्यम से किया जाएगा, जिससे दस्तावेजों की प्रामाणिकता ऑनलाइन सुनिश्चित होगी। निवासी अपने स्वयं के इलेक्ट्रॉनिक दस्तावेज भी अपलोड कर सकते हैं और ई-साइन सुविधा का उपयोग करके उन पर डिजिटल हस्ताक्षर कर सकते हैं। इन डिजिटल हस्ताक्षरित दस्तावेजों को सरकारी संगठनों या अन्य संस्थाओं के साथ साझा किया जा सकता है।

डिजिटल लॉकर का उद्देश्य-

- (1) निवासियों को क्लाउड पर डिजिटल लॉकर प्रदान करके उनके डिजिटल सशक्तिकरण को सक्षम करना।
- (2) दस्तावेजों पर ई-हस्ताक्षर सक्षम करना और उन्हें इलेक्ट्रॉनिक और ऑनलाइन उपलब्ध कराना। भौतिक दस्तावेजों का उपयोग कम से कम करना।
- (3) ई-दस्तावेजों की प्रामाणिकता सुनिश्चित करना और इस तरह नकली दस्तावेजों के उपयोग को समाप्त करना।

- (4) सरकार तक सुरक्षित पहुँचना होगा। निवासियों के लिए एक वेब पोर्टल और मोबाइल एप्लिकेशन के माध्यम से दस्तावेज जारी करना।
- (5) सरकार के प्रशासनिक ओपरहेड को कम करना। विभाग और एजेंसियाँ निवासियों के लिए सेवाएँ प्राप्त करना आसान बनाती हैं।
- (6) किसी भी समय, कहीं भी निवासी द्वारा दस्तावेजों तक पहुँच होना।
- (7) विभागों और एजेंसियों के बीच दस्तावेजों को आसानी से साझा करने के लिए एक अच्छी तरह से संरचित मानक दस्तावेज प्रारूप का समर्थन करने के लिए खुला और अन्तर-प्रचालनीय मानक आधारित आर्किटेक्चर प्रदान करना।
- (8) निवासियों के डेटा तक गोपनीयता और अधिकृत पहुँच सुनिश्चित करना। डिजिटल लॉकर पोर्टल- आधार नब्वर का उपयोग करके डिजिटल लॉकर हेतु साइन-अप करने के लिए Digitallocker.gov.in- वेबसाइट पर जाएँ जो एक नई विंडो में खुलती है। निवासी डिजिटल लॉकर सिस्टम पर पंजीकृत जारीकर्ताओं और अनुरोधकर्ताओं की सूची देख सकते हैं।

#### प्रश्न-7. डिजिटल लॉकर के अनुभाग लिखिए।

उत्तर- प्रत्येक उपयोगकर्ता के डिजिटल लॉकर में निम्नलिखित अनुभाग होते हैं-

- (1) भेरे प्रमाणपत्र- इस अनुभाग में दो उपखंड हैं।
- (2) डिजिटल दस्तावेज- इसमें सरकारी विभागों या अन्य एजेंसियों द्वारा उपयोगकर्ता को जारी किए गए दस्तावेजों का यूआरआई शामिल है।
- (3) अपलोड किए गए दस्तावेज- यह उपयोगकर्ता सभी डी को सूचीबद्ध करती है दस्तावेज जो उपयोगकर्ता द्वारा अपलोड किए गए हैं। अपलोड की जाने वाली प्रत्येक फाइल का आकार 10 एमबी से अधिक नहीं होना चाहिए। केवल पीडीएफ, जेपीजी, जेपीईजी, पीएनजी, बीएमपी और जीआईएफ फाइल प्रकार अपलोड किए जा सकते हैं।
- (4) भेरी प्रोफाइल- यह अनुभाग यूआईडीएआई डेटाबेस में उपलब्ध उपयोगकर्ता की पूरी प्रोफाइल प्रदर्शित करता है।
- (5) भेरा जारीकर्ता- यह अनुभाग जारीकर्ताओं के नाम और जारीकर्ता द्वारा उपयोगकर्ता को जारी किए गए दस्तावेजों की संख्या प्रदर्शित करता है।
- (6) भेरा अनुरोधकर्ता- यह अनुभाग अनुरोधकर्ताओं के नाम और अनुरोधकर्ताओं द्वारा उपयोगकर्ताओं से अनुरोध किए गए दस्तावेजों की संख्या प्रदर्शित करता है।
- (7) निरीक्षण- यह अनुभाग पंजीकृत जारीकर्ताओं और अनुरोधकर्ताओं की पूरी सूची उनके यूआरएल के साथ प्रदर्शित करता है।

#### प्रश्न-8. SWAYAM से क्या तात्पर्य है? लिखिए।

उत्तर- SWAYAM- यह भारत सरकार द्वारा शुरू किया गया एक कार्यक्रम है और इसे शिक्षा नीति के तीन प्रमुख सिद्धान्तों, पहुँच, समानता और गुणवत्ता को प्राप्त करने के लिए डिजाइन किया गया है। इस कार्यक्रम का उद्देश्य सर्वोत्तम शिक्षण-अधिगम संसाधनों को सभी तक पहुँचाना है, जिनमें सबसे वंचित लोग भी शामिल हैं। यह उन छात्रों के लिए

डिजिटल विभाजन को पाटना चाहता है जो अब तक डिजिटल क्रांति से अछूते रहे हैं और ज्ञान अर्थव्यवस्था की मुख्यधारा में शामिल नहीं हो पाए हैं।

यह एक ऐसे मंच के माध्यम से किया जाता है जो कक्षा 9 से लेकर स्नातकोत्तर तक कक्षाओं में पढ़ाए जाने वाले सभी पाठ्यक्रमों की मेजबानी की सुविधा प्रदान करता है, जिसे कोई भी, कहीं भी, किसी भी समय एक्सेस कर सकता है। सभी पाठ्यक्रम इंटरैक्टिव हैं। देश के सर्वश्रेष्ठ शिक्षकों द्वारा तैयार किए गए हैं और किसी भी शिक्षार्थी के लिए निःशुल्क उपलब्ध हैं। इन पाठ्यक्रमों को तैयार करने में देश भर से एक हजार से अधिक विशेष रूप से चुने गए संकाय और शिक्षकों ने भाग लिया है।

SWAYAM पर होस्ट किए गए पाठ्यक्रम 4 भागों में हैं- (1) वीडियो व्याख्यान, (2) विशेष रूप से तैयार की गई पठन सामग्री जिसे डाउनलोड/प्रिंट किया जा सकता है, (3) परीक्षण और क्विज के माध्यम से स्व-मूल्यांकन परीक्षण और (4) क्लियरिंग के लिए एक ऑनलाइन चर्चा मंच संदेह, आँडियो-वीडियो और मल्टीमीडिया और अत्याधुनिक शिक्षाशास्त्र/प्रौद्योगिकी का उपयोग करके सीखने के अनुभव को समृद्ध करने हेतु कदम उठाए गए हैं।

सर्वोत्तम गुणवत्ता वाली सामग्री का उत्पादन और वितरण किया जाए, यह सुनिश्चित करने के लिए नौ राष्ट्रीय समन्वयक नियुक्त किए गए हैं। वे हैं-

- (1) स्व-निर्देशित और अन्तर्राष्ट्रीय पाठ्यक्रमों के लिए एआईसीटीई (अखिल भारतीय तकनीकी शिक्षा परिषद)।
- (2) इंजीनियरिंग के लिए एनपीटीईएल (निशनल प्रोग्राम ऑन टेक्नोलॉजी एंडांस्ड लर्निंग)।
- (3) गैर तकनीकी स्नातकोत्तर शिक्षा के लिए यूजीसी (विश्वविद्यालय अनुदान आयोग)।
- (4) स्नातक शिक्षा के लिए सीईसी (कंसोर्टियम फॉर एजुकेशन कन्सुलिकेशन)।
- (5) स्कूली शिक्षा के लिए एनसीईआरटी (राष्ट्रीय शैक्षिक अनुसंधान और प्रशिक्षण परिषद)।
- (6) स्कूली शिक्षा के लिए एनआईओएस (निशनल इंस्टीट्यूट ऑफ ओपन स्कूलिंग)।
- (7) स्कूल न जाने वाले छात्रों के लिए इन्सू (इंडिरा गाँधी राष्ट्रीय मुक्त विश्वविद्यालय)।
- (8) प्रबंधन अध्ययन के लिए फंड (भारतीय प्रबंधन स्थान बैंगलोर)।
- (9) शिक्षक प्रशिक्षण कार्यक्रम के लिए एनआईटीटीआर (राष्ट्रीय तकनीकी शिक्षक प्रशिक्षण और अनुसंधान संस्थान)।

SWAYAM के माध्यम से दिए जाने वाले पाठ्यक्रम शिक्षार्थियों के लिए निःशुल्क उपलब्ध हैं। हालांकि SWAYAM प्रमाणपत्र चाहने वाले शिक्षार्थियों को शुल्क के साथ आने वाली अन्तिम प्रोक्टेट परीक्षाओं के लिए पंजीकरण करना चाहिए और निर्दिष्ट तिथियों पर निर्दिष्ट केन्द्रों पर व्यक्तिगत रूप से उपस्थित होना चाहिए। प्रमाणपत्र के लिए पात्रता की घोषणा पाठ्यक्रम पृष्ठ पर की जाएगी और शिक्षार्थियों को प्रमाणपत्र तभी मिलेगा जब यह

मान्यता प्राप्त होना। इन पाठ्यक्रमों के लिए क्रेडिट ट्रांसफर को मंजूरी देने वाले विश्वविद्यालय/कॉलेज इसके लिए इन पाठ्यक्रमों में प्राप्त अंकों/प्रमाणपत्र का उपयोग कर सकते हैं।

**क्रेडिट ट्रांसफर- यूजीसी ने पहले ही यूजीसी विनियमन 2016 जारी कर दिया है, जिसमें विश्वविद्यालयों को ऐसे पाठ्यक्रमों की पहचान करने की सलाह दी गई है, जहाँ SWAYAM पर किए गए पाठ्यक्रमों के क्रेडिट को छात्रों के शैक्षणिक रिकॉर्ड में स्थानान्तरित किया जा सकता है। एआईसीटी ने वर्ष 2016 में क्रेडिट ट्रांसफर के लिए इन पाठ्यक्रमों को अपनाने के लिए गजट अधिसूचना भी जारी की है।**

अपने मूल विश्वविद्यालय में क्रेडिट ट्रांसफर से संबंधित अपनी शिकायतों को इस फॉर्म में जमा करके इंगित कर सकते हैं। वर्तमान SWAYAM प्लेटफॉर्म को शिक्षा मंत्रालय और NPTEL, IIT मद्रास द्वारा Google Inc. और Persistent Systems Ltd. की मदद से विकसित किया गया है।



दीर्घ एवं लघु उत्तरीय प्रश्न-

**प्रश्न-1. Internet Security पर संक्षिप्त लेख लिखिए। Internet सुरक्षा की समस्या की विवेचना कीजिये।**

अथवा

सिक््युरिटी कंट्रोल कितने प्रकार के होते हैं? विस्तृत व्याख्या कीजिए।

**उत्तर- Internet Security :** इंटरनेट कई नेटवर्क का एक नेटवर्क है, इसलिए नेटवर्क सिक््युरिटी भी इंटरनेट सिक््युरिटी का ही एक भाग है।

**सुरक्षा की समस्या-** कम्प्यूटर सिस्टम को नुकसान पहुंचाने आक्रमण हेकरस अर्थात् डेटा चुराने वाले, उसमें परिवर्तन करने वाले और उसे नष्ट करने वाले द्वारा किये जाते हैं। ऑन लाइन कार्ड्स के कारण FBI's के नेशनल कम्प्यूटर कार्ड्स स्कैंड ने कम्प्यूटर अपराध के खिलाफ सुरक्षा कवच के रूप में फॉरवार्डाल की अनुशंसा की। साथ ही NCCS ने और भी अन्य सिक््युरिटी के पैमानों को तय किया, जो निम्नलिखित हैं-

(1) अनुचित एक्सेस के खिलाफ लॉन-इन वेनर्स द्वारा चेतावनी- यह इस बात को रक्रीन पर लॉग-इन के समय दर्शाता है कि कोई अनुचित यूजर सुरक्षित सिस्टम में प्रवेश लेने की कोशिश कर रहा है।

(2) की-स्ट्रोक लेवल मॉनिटरिंग- इसके अन्तर्गत किसी निश्चित वर्क-स्टेशन पर समस्त की-स्ट्रोक को पहचान कर किसी फाइल में रिकॉर्ड करते हैं। इन फाइलों की एडमिनिस्ट्रेटर विवेचना करके यह तय करता है कि कितनी बार उस स्टेशन द्वारा लॉग-इन करने का प्रयास किया गया।

(3) टेलीफोन कम्पनी द्वारा ट्रेप एण्ड ट्रेसिंग सर्विस- इस सर्विस के द्वारा हम सभी आने वाले टेलीफोन कॉलस को ट्रेस करके उनके स्रोत तक पहुंच सकते हैं, जो हमें दूरस्थ अनुचित एक्सेस रोकने में मदद करते हैं।

(4) कॉलर ID- इस सर्विस के द्वारा हम उस व्यक्ति के नाम और नम्बर को पहचान सकते हैं, जिसने हमें कॉल किया है।

(5) कॉल ब्लॉकर- इस सर्विस (यह भी कॉलर ID से संबंधित है) के द्वारा हम कुछ टेलीफोन नम्बर को प्रतिबंधित कर सकते हैं।

(6) डेटा एनक्रिप्शन- इसके द्वारा हम हमारे डेटा को किसी एनक्रिप्शन और डिक्लिप्शन सॉफ्टवेयर की मदद से परिवर्तित कर सकते हैं, जिससे कि अधिकारश हेकरस को सिस्टम में प्रवेश नहीं मिल सके।

(7) फॉरवार्डाल- सभी सिक््युरिटी पैमाने में फॉरवार्डाल सबसे अधिक सुरक्षित सुरक्षा कवच है क्योंकि यह हमारे सिस्टम में बहुत संवेदनशील स्थान पर स्थापित की जाती है और उपयोग की जाती है।

सिक््युरिटी कंट्रोल के प्रकार- हमारे कम्प्यूटर नेटवर्क सिस्टम को सुरक्षित करने के लिए दो तरह के सिक््युरिटी कंट्रोल होते हैं-

(1) इन्टरनल कंट्रोल, (2) एक्सटरनल कंट्रोल।

(1) इन्टरनल कंट्रोल- इन्टरनल कंट्रोल सामान्यतः ऐसे कंट्रोल होते हैं, जो कम्प्यूटर सिस्टम के लिए सामान्यतः अंदरूनी होते हैं। पासवर्ड, फॉरवार्डाल और डेटा इन्क्रिप्शन इत्यादि इन्टरनल कंट्रोल के उदाहरण हैं। इन्टरनल कंट्रोल सिर्फ सभी प्रभावी होते हैं, जबकि उनके साथ कुछ हद तक एक्सटरनल कंट्रोल लागू किए जायें।

(2) एक्सटरनल कंट्रोल- एक्सटरनल कंट्रोल सिस्टम के उस भाग को कंट्रोल करता है, जो सिस्टम स्वयं नहीं कर पाता है। एक्सटरनल कंट्रोल की तीन प्रमुख श्रेणियाँ इस प्रकार हैं-

(a) फिजीकल कंट्रोल (b) परसनल कंट्रोल (c) प्रोसीजरल कंट्रोल

(a) फिजीकल कंट्रोल- ये फिजिकल सिक््युरिटी के पैमाने होते हैं, जो कम्प्यूटर सिस्टम को सुरक्षित करते हैं। रूम को लॉक करना, एयरकंडीशन्स रुम्स (जो यह तय करता है कि सिस्टम अपने अनुरूप वातावरण में कार्य करें) और की-बोर्ड लाक्स फिजिकल कंट्रोल के मुख्य उदाहरण हैं। इन्टरनेटवर्किंग के प्रचलन के कारण फिजिकल कंट्रोल का महत्व कम होता जा रहा है। एक बड़े इन्टरनेट सिस्टम में हमारे अपने सिस्टम को छोड़कर किसी अन्य को भौतिक रूप से सुरक्षित करना असंभव है।

(b) परसनल कंट्रोल- ये ऐसे तकनीक और नियम होते हैं, जिनको अधिकारी उपयोग करके यह तय करते हैं कि आर्गनाइजेशन के कम्प्यूटर सिस्टम के लिए किस पर विश्वास किया जावे। जब एम्प्लॉयी को कम्प्यूटर सिस्टम के ऊपर वाले लेवल का एक्सेस प्रदान किया जाता है, तब एम्प्लॉयी की स्क्रूटनी बहुत अधिक होना चाहिए। इसके लिए इन्टरव्यू और पुराने क्रियाकलाप की जाँच या फिर पोलीग्राफ टेस्ट इत्यादि कार्य किये जाते हैं।

(c) प्रोसीजरल कंट्रोल- यह इस बात का निर्धारण है कि कम्प्यूटर सिस्टम पर सूचनाओं को सिर्फ वह नियंत्रित करे, जिनके लिए इसका नियंत्रण आवश्यक है। इन कंट्रोल में किसी नये सॉफ्टवेयर को इंस्टॉल करना और सिस्टम का मॉन्टिंग करना इत्यादि शामिल हैं।

नेटवर्क सिक्युरिटी की विचारधारा- सामान्यतः किसी भी नेटवर्क सिक्युरिटी से संबंधित तथ्यों को नियंत्रित करने की दो विचारधाराएँ होती हैं या तो हम किसी को कुछ एक्सेस करने की अनुमति दें या हम किसी को कुछ भी नहीं करने की अनुमति दें। इस प्रकार अनुमति या प्रतिबंध का यह आधार प्रत्येक इंस्टॉलेशन के लिए अद्वितीय होता है।

(1) एक्सेस की अनुमति प्रदान करना- यूजर को रिसोर्स एक्सेस करने की अनुमति देना, उसे शामिल करने का तरीका है। सिक्युरिटी की इस विचारधारा में हम निर्धारित करते हैं कि कोई भी यूजर एक्सेस प्राप्त करने के लिए किन गुणों को रखता है। यह आधार कुछ हद तक उन रिसोर्स स्वभाव पर निर्भर करता है, जिन्हें शेयर किया जाना है।

(2) एक्सेस के लिए अस्वीकार करना- यूजर को रिसोर्स एक्सेस करने की अनुमति नहीं देना, उसे अस्वीकार करने का तरीका है। सिक्युरिटी की इस विचारधारा में हम यह निर्धारित करते हैं कि कोई भी यूजर के अस्वीकार के लिए किन गुणों को रखता है। यूजर के एक्सेस को अस्वीकार करना कई आधार के समूह पर निर्भर करता है। ये आधार कुछ हद तक शेयर किये जाने वाले रिसोर्स के प्रतिबंध पर निर्भर करते हैं।

प्रश्न-2. इन्टरनेट सिक्युरिटी का क्या अर्थ है? नेटवर्क सिक्युरिटी के गतिरोधों के बारे में जानकारी दीजिए।

उत्तर- इन्टरनेट सिक्युरिटी- इन्टरनेट कई नेटवर्क का एक नेटवर्क है, इसलिए नेटवर्क सिक्युरिटी भी इन्टरनेट सिक्युरिटी का ही एक भाग है।

सुरक्षा की समस्या अथवा सामान्य खतरे- सन् 1996 में U.S. डिफेंस विभाग ने घोषणा की कि उनके कम्प्यूटर सिस्टम पर चालू वर्ष में लगभग 2.5 लाख बार आक्रमण हुए और यह एक आश्चर्यजनक बात है कि उनमें से अधिकतर का पता भी नहीं चल पाया। इन अनजान आक्रमणों ने राष्ट्रीय सुरक्षा को बहुत प्रभावित किया। बहुत से आक्रमण जिनका पता लगाया जा सका, वह कम्प्यूटर सिस्टम को नुकसान पहुँचाने के लिए तथा कम्प्यूटर की सूचनाओं को नष्ट करने के लिए थे। ये नुकसान पहुँचाने वाले आक्रमण हेकर्स अर्थात् डाटा चुराने वाले, उसमें परिवर्तन करने वाले और उसे नष्ट करने वाले द्वारा किये गये थे।

इस प्रकार नेटवर्क सिक्युरिटी में होने वाले बहुत से खतरे निम्नलिखित chart के द्वारा प्रदर्शित किए गये हैं-

नेटवर्क के सतह में सिक्युरिटी के गतिरोध- ऑनलाइन कार्डम के कारण FBI's, के नेशनल कम्प्यूटर कार्डम स्कॉड ने कम्प्यूटर अपराध के खिलाफ सुरक्षा कवच के रूप में फॉरेंसवाल की अनुशंसा की। साथ ही NCCS ने और भी अन्य सिक्युरिटी के पैमानों को तय किया, जो निम्नलिखित हैं-

(1) अनुचित एक्सेस के खिलाफ लॉग-इन वेतर्स द्वारा चेतावनी- यह इस बात को उकीन पर लॉग-इन के समय प्रदर्शित करता है कि कोई अनुचित यूजर सुरक्षित सिस्टम में प्रवेश लेने की कोशिश कर रहा है।

(2) की-स्ट्रोक लेवल मॉनिटरिंग- इसके तहत किसी निश्चित वर्क-स्टेशन पर सभी की-स्ट्रोक को पढ़वाना कर किसी फाइल में रिकॉर्ड करते हैं। इन फाइलों की एडमिनिस्ट्रेटर विवेचना करके यह निश्चित करता है कि कितनी बार उस स्टेशन द्वारा लॉग-इन करने का प्रयास किया गया।

(3) टेलीफोन कम्पनी द्वारा ट्रेप एण्ड ट्रेसिंग सर्विस- इस सर्विस के द्वारा हम सभी आने वाले टेलीफोन कॉल को ट्रेस करके उनके स्त्रोत तक पहुँच सकते हैं, जो हमें ट्रैसिंग अनुचित एक्सेस रोकने में मदद करते हैं।

(4) कॉलर ID- इस सर्विस के द्वारा हम उस व्यक्ति के नाम और नम्बर को पढ़वाना सकते हैं, जितने हमें कॉल किया है।

(5) कॉल ब्लॉकर- इस सर्विस के द्वारा हम कुछ टेलीफोन नम्बर को प्रतिबंधित कर सकते हैं।

(6) डाटा एनक्रिप्शन- इसके द्वारा हम हमारे डाटा को किसी एनक्रिप्शन और डिफ्रिक्शन सॉफ्टवेयर की मदद से परिवर्तित कर सकते हैं, जिससे कि अधिकांश हेकर्स को सिस्टम में प्रवेश नहीं मिल सके।

(7) फॉरेंसवाल- सभी सिक्युरिटी पैमाने में फॉरेंसवाल सबसे अधिक सुरक्षित सुरक्षा कवच है क्योंकि यह हमारे सिस्टम में बहुत संवेदनशील स्थान पर स्थापित की जाती है और उपयोग की जाती है।

प्रश्न-3. सिक्युरिटी कंट्रोल के प्रकारों की विवेचना कीजिए।

उत्तर- सिक्युरिटी कंट्रोल के प्रकार- किसी कम्प्यूटर नेटवर्क सिस्टम को सुरक्षित करने के लिए निम्नलिखित दो प्रकार के सिक्युरिटी कंट्रोल होते हैं-

(1) इन्टरनल कंट्रोल, (2) एक्सटरनल कंट्रोल।

(1) इन्टरनल कंट्रोल- इन्टरनल कंट्रोल वे कंट्रोल होते हैं, जो कम्प्यूटर सिस्टम के लिए सामान्यतः अंदरूनी होते हैं। पासवर्ड, फॉरेंसवाल और डाटा इन्कीशन इत्यादि इन्टरनल कंट्रोल के उदाहरण हैं। इन्टरनल कंट्रोल सिर्फ तभी प्रभावी होते हैं, जबकि उनके साथ कुछ हद तक एक्सटरनल कंट्रोल लागू किए जायें।

(2) एक्सटरनल कंट्रोल- एक्सटरनल कंट्रोल सिस्टम के उस भाग को कंट्रोल करता है, जिसे सिस्टम स्वयं नहीं कर पाता है। एक्सटरनल कंट्रोल के तीन प्रमुख वर्ग इस प्रकार हैं-

(a) फिजीकल कंट्रोल (b) पर्सनल कंट्रोल (c) प्रोसीजरल कंट्रोल।

(a) फिजीकल कंट्रोल- ये फिजिकल सिक्युरिटी के पैमाने होते हैं, जो कम्प्यूटर सिस्टम को सुरक्षित करते हैं। रूप को लॉक करना, एअरकंडीशनिंग रुस (जो यह तय करता है कि सिस्टम अपने अनुरूप वातावरण में कार्य करें) और की-बोर्ड लॉक्स फिजिकल कंट्रोल के मुख्य उदाहरण हैं। इन्टरनेटवर्किंग के प्रचलन के कारण फिजिकल कंट्रोल का महत्व कम होता

जा रहा है। एक बड़े इन्टरनेट सिस्टम में हमारे अपने सिस्टम को छोड़कर किसी अन्य को भौतिक रूप से सुरक्षित करना असंभव है।

(b) पर्सनल कंट्रोल- ये ऐसे तकनीक और नियम होते हैं, जिनको अधिकारी उपयोग करके यह तय करते हैं कि ऑर्गेनाइजेशन के कम्प्यूटर सिस्टम के लिए किस पर विश्वास किया जावे? जब एम्प्लॉयी को कम्प्यूटर सिस्टम के ऊपर वाले लेवल का एक्सेस प्रदान किया जाता है, तब एम्प्लॉयी की सख्ती बहुत अधिक होना चाहिए। इसके लिए इन्टरव्यू और पुराने क्रियाकलाप की जाँच या फिर पोलीग्राफ टेस्ट इत्यादि कार्य किये जाते हैं।

(c) प्रोसेबल कंट्रोल- ये कंट्रोल इस बात का निर्धारण करते हैं कि कम्प्यूटर सिस्टम पर सूचनाओं को सिर्फ वह नियंत्रित करे, जिनके लिए इसका नियंत्रण आवश्यक है। इन कंट्रोल में किसी नये सॉफ्टवेयर को इंस्टॉल करना और सिस्टम का मेन्टेनेंस करना इत्यादि शामिल हैं।

नेटवर्क सिक्युरिटी की विचारधारा- अधिकांशतः किसी भी नेटवर्क सिक्युरिटी से संबंधित तथ्यों को नियंत्रित करने की दो विचारधाराएँ होती हैं या तो हम किसी को कुछ एक्सेस करने की अनुमति दें या हम किसी को कुछ भी नहीं करने की अनुमति दें। इस प्रकार अनुमति या प्रतिबंध का यह आधार प्रत्येक इंस्टॉलेशन के लिए अद्वितीय होता है।

(1) एक्सेस की अनुमति प्रदान करना- यूजर को रिसोर्स एक्सेस करने की अनुमति देना, उसे शामिल करने का तरीका है। सिक्युरिटी की इस विचारधारा में हम यह निर्धारित करते हैं कि कोई भी यूजर एक्सेस प्राप्त करने के लिए किन गुणों को रखता है? यह आधार कुछ हद तक उन रिसोर्स स्वभाव पर निर्भर करता है, जिन्हें शेयर किया जाना है।

(2) एक्सेस के लिए अस्वीकार करना- यूजर को रिसोर्स एक्सेस करने की अनुमति नहीं देना, उसे अस्वीकार करने का तरीका है। सिक्युरिटी की इस विचारधारा में हम यह निर्धारित करते हैं कि कोई भी यूजर के अस्वीकार के लिए किन गुणों को रखता है? यूजर के एक्सेस को अस्वीकार करना कई आधार के समूह पर निर्भर करता है। ये आधार कुछ हद तक शेयर किये जाने वाले रिसोर्स के प्रतिबंध पर आधारित होते हैं।

प्रश्न-4. फायरवॉल क्या है? इसकी आवश्यकता क्यों पड़ती है? इसके प्रकारों तथा सीमाओं की विवेचना कीजिए।

उत्तर- फायरवॉल- फायरवॉल एक सॉफ्टवेयर सिस्टम या हार्डवेयर सिस्टम है या दोनों का मिश्रित सिस्टम है, जो दो नेटवर्क के मध्य एक्सेस कंट्रोल पॉलिसी को लागू करता है। इस प्रकार फायरवॉल हमारी सुरक्षा योजना का एक घाषणा-पत्र है।

फायरवॉल ही सर्वाधिक प्रचलित, स्वीकार नेटवर्क सुरक्षा के लिए प्रतिरोधक है, जो कॉरपोरेट नेटवर्क और बाहरी दुनिया (अविश्वसनीय नेटवर्क) के मध्य होती है। फायरवॉल का अर्थ अलग-अलग लोगों के लिए अलग-अलग प्रकार से हो सकता है। परन्तु साधारणतः यह एक ऐसी विधि है, जिसमें कि एक उपकरण (कम्प्यूटर या रूटर) को नेटवर्क और इन्टरनेट के बीच रखा जाता है। यह लोकल नेटवर्क और बाहरी दुनिया के बीच ट्रैफिक को देखरेख करता है। विशेष रूप से यह उपकरण नेटवर्क के अन्दर-बाहर से प्राप्त सभी सर्विसेस को एक्सेस करने की अनुमति देता है, जबकि बाह्य वातावरण को सिर्फ कुछ विशेष एक्सेस ही

प्रदान करता है, जो उसके लॉग-ऑन नेम, पासवर्ड, IP एड्रेस अथवा अन्य परिचय पर आधारित होती है।

इन्टरनेट फायरवॉल- फायरवॉल एक सुरक्षा उपकरण है, जो नेटवर्क के संवेदनशील भाग को खतरों से बचाता है। इन्टरनेट के संदर्भ में फायरवॉल एक ऐसा सिस्टम (एक रूटर, या पर्सनल कम्प्यूटर या एक होस्ट या अनेक होस्ट का समूह) है, जो किसी साइट या सर्वनेट के लिए एक कवच या निर्माण करता है। यह ऐसे प्रोटोकॉल और सर्विसेस जो नुकसान पहुँचाने का कार्य करते हैं, उनसे सुरक्षित करता है। फायरवॉल सिस्टम सामान्यतः गेटवे पाईट (जैसे साइट का इन्टरनेट से कनेक्शन वाला बिन्दु) पर स्थित होता है। परन्तु कभी-कभी यह अन्दर के गेटवे पर भी स्थित हो सकता है, जहाँ पर यह कुछ होस्ट के समूह या सर्वनेट की सुरक्षा करता है।

फायरवॉल की आवश्यकता- इन्टरनेट से जुड़े हुए नेटवर्क पर होने वाले निम्नलिखित अनेक आक्रमणों के कारण फायरवॉल की आवश्यकता पड़ती है-

- शोशल इंजीनियरिंग के कारण अर्थात् ऐसे आक्रमण जो कि साइट पर तकनीकी या नेटवर्क एडमिनिस्ट्रेशन व्यक्तियों से संबंधित हो जैसे- किसी यूजर या ऑपरेटर को टेलीफोन के द्वारा ऑथोरिज्ड यूजर बताना।
- वायरस के कारण अर्थात् स्वयं के कॉपी निर्मित करने वाले कोड सिगमेंट्स खिन्नमें कि ट्रैप डोर्स या आक्रमण प्रोग्राम होते हैं, जो बहुत छिपकर यूजर्स की मदद से हमारे डाटा को हमें पता चले बिना ही नुकसान पहुँचाते हैं।
- ट्रोजन हार्स वायरस के कारण अर्थात् एक प्रोग्राम जो बिन्कुल सामान्य दिख रहा है, हो सकता है कि उसमें ट्रैप डोर या कोई आक्रमण करने वाला प्रोग्राम हो।
- DNS स्फ़ीगिंग के कारण अर्थात् ऐसा कम्प्यूटर जिसके पास दूसरे सिस्टम का डोमेन नेम हो तब वह सिस्टम दूसरे सिस्टम का नेटवर्क एड्रेस उपयोग करके उसे नुकसान पहुँचा सकता है, यही DNS स्फ़ीगिंग है।
- डाटा ड्रिवन अटैक नॉर्मल डाटा को एनकोड करते हैं, इसके कारण डाटा ड्रिवन अटैक सुरक्षा कवच को भी भेदकर उसके पीछे (जो उससे सुरक्षित रहता है) वाले सिस्टम को नुकसान पहुँचाते हैं।
- IP स्लाईडिंग/हार्डजैकिंग या सेशन स्टीलिंग के कारण अर्थात् एक बार यदि किसी भी प्रकार से ऑथोरिज्डेशन हो जाता है तो उस परिस्थिति ने आक्रमणकारी ऑथोरिज्ड व्यक्ति के रूप में कार्य कर सकता है।

फायरवॉल टेक्नोलॉजी के प्रकार- फायरवॉल मुख्यतः दो में से किसी एक श्रेणी में आती है- नेटवर्क-लेवल फायरवॉल अथवा एप्लिकेशन-लेवल फायरवॉल/यद्यपि अधिकांश फायरवॉल प्रोडक्ट्स में दोनों के गुण शामिल होते हैं परन्तु फिर भी इन दोनों को अलग-अलग समझना जरूरी है-

(1) नेटवर्क लेवल फायरवॉल टेक्नोलॉजी- यह सम्पूर्ण नेटवर्क को अनुचित इन्स्ट्रक्शन से बचाता है। नेटवर्क लेवल फायरवॉल टेक्नोलॉजी का एक ही उदाहरण है पैकेट फिल्टरिंग इसमें नेटवर्क को प्राप्त होने वाली सम्पूर्ण सूचना का आकलन पूर्व-निर्धारित तथ्यों के आधार पर

किया जाता है और जो डाटा इन पूर्व नियमित मानदण्डों को पूरा नहीं करता है, उस डाटा को अस्वीकार कर दिया जाता है। नेटवर्क लेवल फायरवॉल में एक और तकनीक का उपयोग कर सकते हैं, वह है आयोराइजेशन सर्वर जो हमेशा यूजर के लॉगिन के समय उसके सही होने का निर्धारण करता है।

(2) एलिकेशन लेवल फायरवॉल टेक्नोलॉजी— यह एक्ससेस को प्रत्येक एलिकेशन के आधार पर नियंत्रित करता है। उदाहरण के लिए प्रॉक्सी सर्वर का उपयोग कुछ एलिकेशन्स जैसे HTTP को सेट करने के लिए जबकि अन्य एलिकेशन्स जैसे FTP को ब्लॉक करने के लिए करते हैं।

फायरवॉल की सीमाएँ— प्रायवेट नेटवर्क में ऐसे बहुत से सुरक्षा के issues होते हैं, जिन्हें फायरवॉल नियंत्रित नहीं कर पाता है, उनमें से कुछ इस प्रकार हैं—

(1) इनसाइडर्स इन्ट्रूजन— फायरवॉल प्रायवेट नेटवर्क के अन्दर ही किसी यूजर के द्वारा किये गये आक्रमण से रिसॉसेस को नहीं बचा सकती है। फायरवॉल एक ऐसा नेटवे है, जो सिर्फ प्रायवेट नेटवर्क इन्टरनेट के बीच के ट्रैफिक को ही फिल्टर करता है। ऐसी परिस्थिति में अन्दर वाला यूजर उस आर्गनाइजेशन की गोपनीय सूचना की चोरी भी कर सकता है या रिसॉसेस को नुकसान भी पहुँचा सकता है, जिसका फायरवॉल को पता भी न चल सके।

(2) डायरेक्ट इन्टरनेट ट्रैफिक— फायरवॉल सिर्फ तभी उपयोगी होती है, जबकि सम्पूर्ण इन्टरनेट ट्रैफिक को फायरवॉल नियंत्रित कर रहा हो। फायरवॉल ऐसे ट्रैफिक जो कि इन्टरनेट के द्वारा उसको वायपास (अनदेखा) करके प्रायवेट नेटवर्क को दिया जा रहा है, से नेटवर्क रिसॉसेस को सुरक्षित नहीं कर सकती है।

(3) वायरस प्रोटेक्शन— फायरवॉल विशेष रूप से बाह्य वायरस से प्रायवेट नेटवर्क को सुरक्षित नहीं कर पाता है। प्रायवेट नेटवर्क में वायरस का स्थानान्तरण FTP या अन्य माध्यम के द्वारा किया जा सकता है। इस प्रकार की सुरक्षा के लिए फायरवॉल में ऐसे लॉजिक होने चाहिए, जो डेटा स्ट्रिम में से वायरस ढूँढ सके।

प्रश्न-5. इन्टरनेट पर सुरक्षा के क्या उपाय हैं? संक्षेप में समझाइये।

उत्तर— इलेक्ट्रॉनिक सुरक्षा (Electronic Security)— इलेक्ट्रॉनिक सुरक्षा को समझने के लिए एक केस का अध्ययन करते हैं। विलियम याहू या सिफ्री डॉट कॉम से एक औपचारिक लगने वाला मेल प्राप्त करता है। इस ई-मेल में उसे एक वायरस के बारे में चेतावनी दी जाती है तथा उसके उपचार के लिए एक लिंक दिया जाता है जिसे उसको क्लिक करने की सलाह दी जाती है। समीर उस लिंक पर क्लिक करता है तथा फाइल को डाउनलोड करता है और फिर यह समझकर कि अब उसका कम्प्यूटर सिस्टम सुरक्षित है उसे बंद कर देता है।

ऐसा करने पर उसे यह अनुभव भी नहीं होता कि उसके कम्प्यूटर सिस्टम में ट्रॉजन नामक एक सॉफ्टवेयर प्रोग्राम सेंध लगा चुका है तथा अब उसका कम्प्यूटर कुछ लोगों के द्वारा एक्ससेस किया जा रहा है। अब वे लोग उसके कम्प्यूटर में संग्रहित फाइलों को देख सकते हैं, कॉपी कर सकते हैं। यहाँ तक कि जब तक वह इन्टरनेट से जुड़ा है उसकी सारी गतिविधियों की सूचना उन्हें मिल रही है तथा समीर द्वारा व्यापार में प्रयोग किया जा रहा क्रेडिट कार्ड की सख्या भी उनके कब्जे में है तथा उसका दुरुपयोग अवश्यभावी है।

हैकर्स, वायरस, लॉजिक बम, ई-मेल बम, ट्रॉजन्स, वेब बैंकिंग, आई.पी. स्फ़िकिंग, इमेल स्फ़िकिंग, इन्टरनेट के नकारात्मक पहलू तथा सुरक्षा खतरों के कुछ उदाहरण हैं।

इन्टरनेट पर सुरक्षा उपाय (Security Measures On Internet)— इन्टरनेट पर जब आप कार्य कर रहे हों तो आपको यहाँ कई महत्वपूर्ण टिप्स दिखे जा रहे हैं जो इस प्रकार हैं—

(1) सुरक्षा संस्कृति को विकसित करें— कई व्यवसायी इन्टरनेट सुरक्षा को अपने दिव्य कार्यों का एक हिस्सा नहीं बनाते। इसके लिए व्यापारिक संस्थानों को ई-सुरक्षा उपायों को अपनाने के साथ ही कर्मचारियों को भी इन उपायों के साथ अवगत कराना चाहिए तथा इन्टरनेट सुरक्षा पॉलिसी का अनुसरण भी करवाना चाहिए। ऐसा करना इसलिए आवश्यक है क्योंकि कभी-कभी हो सकता है कि आप या आपके कर्मचारी या अधिकारी लॉग-ऑफ़ करना भूल जायें, पासवर्ड न बदलें तथा नये सॉफ्टवेयर पैचेज को डाउनलोड करना तथा इंस्टॉल करना नजरअंदाज कर दें। ऑन लाइन सुरक्षा के प्रति जागरूकता आपके ऑन लाइन व्यवसाय को सुरक्षित करने का एक अभिन्न हिस्सा है। ये न समझें कि कर्मचारी सुरक्षा खतरों को भली-भाँति समझते हैं। इसके लिए कई सस्ते तथा अत्यंत सुरक्षा उपकरण आते हैं जो आपके कम्प्यूटर तथा सूचना-प्रणाली को हैकरों तथा वायरस से सुरक्षित रख सकते हैं।

(2) वायरस निरोधक सॉफ्टवेयर इंस्टॉल करें तथा इसे अपडेट करते रहें— वायरस के फैलने का मुख्य कारण ई-मेल अटैचमेंट जो वस्तुतः वायरस होते हैं या वायरस संक्रमित होते हैं, को खोलना, वेबसाइट से संक्रमित प्रोग्राम को डाउनलोड करना या संक्रमित फ्लॉपी डिस्क या सी.डी. का प्रयोग करना होता है। कुछ वायरस इस तरह से प्रोग्राम किये गये होते हैं जो कुछ समय आगे तक के लिए निष्क्रिय रहते हैं। वायरस निरोधक सॉफ्टवेयर को इंस्टॉल कर आप अपने कम्प्यूटर की सुरक्षा वायरस, वर्म तथा ट्रॉजन्स से कर सकते हैं। वायरस निरोधक सॉफ्टवेयर इस तरह के खतरों को स्कैन कर आपके कम्प्यूटर से हटा देते हैं। सॉफ्टवेयर स्थापित कर इसे विद्वेष-मूलक कोड को स्वतः स्कैन करने हेतु सेट किया जा सकता है। कम्प्यूटर को वायरस, वर्म तथा ट्रॉजन्स संक्रमण से बचाने के निम्नलिखित उपाय हैं—

- (i) आपके कम्प्यूटर पर फायरवॉल तथा वायरस निरोधक के सॉफ्टवेयर दोनों ही इंस्टॉल हों।
- (ii) आपके कम्प्यूटर पर अप-टू-डेट वायरस निरोधक सॉफ्टवेयर इंस्टॉल हों।
- (iii) आपके नेटवर्क के परिचालन तंत्र तथा एलिकेशन सॉफ्टवेयर के लिए सुरक्षा पैचेज अप-टू-डेट हों।
- (iv) अनजान स्रोत से प्राप्त फाइलों के साथ कार्य करते समय सावधानी बरतें।
- (v) वैसे ई-मेल अटैचमेंट न खोलें जिसके प्रेषक को आप नहीं पहचानते।
- (vi) अटैचमेंट खोलने से पहले वायरस निरोधक सॉफ्टवेयर के साथ इसे स्कैन कर लें।

- (vii) विश्वसनीय इंटरनेट साइटों से ही फाइल डाउनलोड करें तथा अपने मित्रों के मध्य फाइलों के अवल-बदल में सतर्क रहें।
- (viii) अज्ञात स्रोत से प्राप्त ई-मेल के हायपरलिंक को क्लिक न करें।
- (3) अपने कम्प्यूटर पर अनाधिकृत एक्सेस को ब्लॉक करने के लिए फायरवॉल को इंस्टॉल करें— फायरवॉल आपके कम्प्यूटर को सुरक्षित रखने के लिए सुरक्षा प्रहरी की भाँति कार्य करता है। फायरवॉल इंटरनेट से आपके कम्प्यूटर को अनाधिकृत रूप से एक्सेस तथा आपके कम्प्यूटर से सूचना डाउनलोड को ब्लॉक कर देता है। फायरवॉल उपयोगकर्ता फायरवॉल एक्सेस नियमों को सेट कर किस कनेक्शन को होने देना है तथा किसे रोकना है? यह निर्धारित कर सकते हैं। फायरवॉल के बगैर कम्प्यूटर बिना सिक्यूरिटी गार्ड के किसी भवन के समान है। अर्थात् आने और जाने वाले पर कोई पहरा नहीं। आपको केवल उपयुक्त फायरवॉल प्राप्त कर उसे प्रभावी ढंग से प्रयोग करना होता है। फायरवॉल सॉफ्टवेयर प्रायः कम्प्यूटर के परिचालन तंत्र के साथ आता है या फिर इसे विश्वसनीय वेबसाइट से डाउनलोड भी किया जा सकता है या फिर किसी कम्प्यूटर स्टोर से प्राप्त किया जा सकता है।

इंटरनेट सेवा-प्रदाता भी फायरवॉल हार्डवेयर तथा सॉफ्टवेयर का एक अच्छा स्रोत है। फायरवॉल को इंस्टॉल कर एक्टिवेट कर लें। फायरवॉल को इंस्टॉल करने के बाद उसे सक्रिय करना अति आवश्यक है। अपनी सुरक्षा आवश्यकतानुसार फायरवॉल विक्रेता से या इंटरनेट सुरक्षा सलाहकार से सहायता ले सकते हैं। फायरवॉल को भी वायरस निरोधक सॉफ्टवेयर की तरह ही समय-समय पर अपडेट करते रहना चाहिए। आमतौर पर फायरवॉल सॉफ्टवेयर में ऑटोमेटिक अपडेट फीचर होता है। आप केवल यह सुनिश्चित कर लें कि यह फीचर ऑन है। साथ ही यह सुनिश्चित कर लें कि आप फायरवॉल का बिल्कुल नया संस्करण प्रयोग कर रहे हैं।

- (4) हानिकारक ई-मेल से अपने को बचायें— ई-मेल इंटरनेट के माध्यम से कम्प्यूटिकेट करने का सबसे आसान तथा सबसे तेज माध्यम है। इसके साथ ही यह विद्वेष-मूलक कोड के माध्यम से हानिकारक इलेक्ट्रॉनिक वायरस, वर्म तथा ट्रॉजन भी वितरित करते हैं जो अटैचमेंट्स संदेशों के रूप में छिपे खतरनाक निर्देश हो सकते हैं।

ई-मेल जनित वायरस, वर्म तथा ट्रॉजन आपके व्यापारिक कम्प्यूटर-प्रणाली को नुकसान पहुँचाकर आपके व्यापारिक गतिविधियों को बाधित करते हैं। अपने कम्प्यूटर को सुरक्षित करने का एक तरीका यह है कि आप ई-मेल अटैचमेंट को खोलने तथा ई-मेल के अन्तर उपस्थित संदेशास्य हायपरलिंक को क्लिक करते समय सतर्कता बरतें। इसके लिए प्रभावकारी उपाय फायरवॉल को इंस्टॉल करना हो सकता है। किन्तु फायरवॉल आपके किसी ई-मेल अटैचमेंट या उसमें उपस्थित हायपरलिंक में छिपे विद्वेष-मूलक कोड की जिम्मेदारी नहीं लेता है अर्थात् ई-मेल में छिपे वायरस, वर्म तथा ट्रॉजन इस सुरक्षा घेरे को पार कर

सकते हैं। इसके लिए आपके पास उपाय के रूप में वायरस निरोधक सॉफ्टवेयर है जिसे इंस्टॉल करने के बाद आप इसे निरन्तर अपडेट करते रहें।

ई-मेल जनित विशेष मूलक कोड से बचने के उपाय निम्नलिखित हैं—

- फायरवॉल तथा वायरस निरोधक सॉफ्टवेयर का प्रयोग करें।
- कम से कम सप्ताह में एक बार अपने कम्प्यूटर को पूरी तरह से स्कैन करें।
- सभी फ़िल्टरिंग तथा सुरक्षा सॉफ्टवेयर को अप-टू-डेट रखें।
- अपने सभी परिचालन तंत्र तथा एप्लिकेशन सॉफ्टवेयर के लिए सुरक्षा पैकेज को इंस्टॉल करें तथा इन्हें अपडेट रखें।
- किसी अज्ञान ई-मेल को खोलने से पहले सामान्य बोध का प्रयोग करें तथा उसके शीर्षक को भी देख लें। अधिकतर स्थितियों में ई-मेल विषय ही नुकसानदायक ई-मेल की पुष्टि कर देते हैं।

- (5) **Minimise Spam**— स्पैम आपके लेटर बॉक्स में अंक मेल का इंटरनेट विकल्प है। स्पैम ई-मेल व्यवसायिक इलेक्ट्रॉनिक संदेश होते हैं जो आपकी मर्जी के बगैर आपको भेजे जाते हैं। भेजने वाले स्पैम के माध्यम से अपने सामान्यों, सेवाओं, जमीनों, निवेश अवसरों को खरीदने, बेचने तथा प्रचार करने की कोशिश करते हैं। स्पैम न ही केवल आपके इनबॉक्स को अनावश्यक और अनापेक्षित संदेशों से भरते हैं बल्कि उन्हें मिटाने के क्रम में आपका बहुत अधिक समय वर्बाद करते हैं। फलस्वरूप समय लगाने के बदले पैसे का भी नुकसान होता है। इसके साथ ही स्पैम में वायरस, वर्म तथा ट्रॉजन्स भी होते हैं। बाजार में ऐसे सॉफ्टवेयर हैं जो स्पैम के आने को कम कर सकते हैं। इस प्रकार के सॉफ्टवेयर अनापेक्षित मेलों की जाँच कर उन्हें आपके इनबॉक्स में आने से रोकते हैं। ये सॉफ्टवेयर कोई मेल स्पैम है इसकी जाँच इसमें समाहित कुछ शब्दों या वाक्यांशों के आधार पर करते हैं। फ़िल्टरिंग सॉफ्टवेयर इन संदेशों को एक खास मेल बॉक्स में भेज देते हैं जिन्हें आप बाद में यह जाँच कर कि कौन से स्पैम हैं जिन्हें मिटा सकते हैं। हालाँकि यह लागभग असम्भव है कि आप स्पैम को अपने मेल बॉक्स में आने से पूरा-पूरा रोक दें परन्तु इन्हें बहुत हद तक रोकना जा सकता है। इसके लिए निम्नलिखित उपाय हैं—

- स्पैम फ़िल्टर को इंस्टॉल कर लें जो स्पैम को आपके मेल बॉक्स में आने से रोकेंगे।
- जब आप स्पैम प्राप्त करें तो इस पते को स्पैम प्रेषक सूची में जोड़ दें या जंक मेल लिस्ट में उन्हें जोड़ें।
- अनापेक्षित मेल का जबाब न दें।
- अगर कोई ई-मेल संदेशास्य प्रतीत होता है तो उसके अनसम्बन्धित भाग को क्लिक न करें ताकि स्पैम भेजने वाले को आपके मेल की सक्रियता का पता न चल सके।
- संदेश के अटैचमेंट्स को क्लिक न करें यदि संदेश का स्रोत अनजान या संदेशास्यद हो।

- (6) डाटा का बैकअप लेते रहें— बैकअप डाटा तथा कुछ विशेष प्रोग्राम के कॉपी करने को कहते हैं। डाटा का कॉपी करने या बैकअप लेने के बाद आप कम्प्यूटर के साथ किसी प्रकार की विषम परिस्थिति में अपने व्यापार से संबंधित सूचना अपने कम्प्यूटर या वेबसाइट को आसानी के साथ पुनः प्राप्त करवा सकते हैं। आप प्रत्येक बार अपने सभी डाटा का बैकअप ले सकते हैं। अथवा केवल संशोधित डाटा का ही बैकअप ले सकते हैं कि विषम स्थिति में कितना बड़ा नुकसान हो सकता है तथा उसी प्रकार उसकी रणनीति तैयार करें। इन विषम परिस्थितियों से निपटने के लिए बैकअप संबंधित कुछ विशेष उपाय निम्न प्रकार हैं—

- (i) खतरों के स्तर को निर्धारित करने के पश्चात् एक आपदा रिकवरी योजना विकसित करें।
- (ii) बैकअप प्रक्रिया ठीक-ठीक तथा जाँचा हुआ है इसे सुनिश्चित कर लें तथा वास्तविक डाटा और डाटा प्रोसेस को रिस्टोर करने की जाँच करना न भूलें।
- (iii) बैकअप की प्रतियाँ आपके कम्प्यूटर से तथा सभी प्रकार की विषम परिस्थितियों से दूर हैं, यह सुनिश्चित करें।
- (iv) बैकअप प्रणाली में अनेक वित्तीय तथा पे-रोल प्रणाली को अवश्य सम्मिलित करें।
- (v) सभी तीसरी पार्टी सॉफ्टवेयर को इसके प्रयोग से पहले कॉपी कर लें।
- (vi) मास्टर कॉपियों का प्रयोग साधारण व्यापारिक गतिविधियों में न करें तथा इसे केवल रिकवरी उद्देश्यों के लिए सुरक्षित रखें।
- (7) अपने सिस्टम को सुरक्षित पासवर्ड के साथ विकसित करें— पासवर्ड अंकों तथा अक्षरों का एक समूह होता है जो कम्प्यूटर सिस्टम को लॉग-इन करने तथा वेबसाइट एक्सेस करने या इन्टरनेट पर अन्य कम्प्यूटरों को एक्सेस करते समय आपकी पहचान की जाँच करता है। यदि आप पासवर्ड का प्रयोग नहीं करते हैं या फिर आसानी से अनुमान लगा लेने वाला पासवर्ड या आसानी से क्रैक करने वाला पासवर्ड प्रयोग करते हैं तो व्यक्ति आपके कम्प्यूटर या लैपटॉप से महत्वपूर्ण सूचना तथा निजी विवरण चुरा सकता है। साथ ही, आपके कम्प्यूटर का दुरुपयोग कर सकता है। उदाहरण के लिए आपके कम्प्यूटर से कोई ई-मेल भेज सकता है, कुछ सेवाएँ सब्सक्राइब कर सकता है जिसका भुगतान आपको करना पड़ सकता है। आप जिस कम्प्यूटर पर काम करते हैं उस कम्प्यूटर पर डाटा सुरक्षा का वायित्व आप पर है। प्रभावशाली पासवर्ड बनाकर आप अपने कम्प्यूटर सिस्टम को अतिरिक्त सुरक्षा प्रदान कर सकते हैं। प्रभावशाली पासवर्ड बनाने के लिए निम्नलिखित टिप्स हैं—
- (i) वैसे पासवर्ड न बनायें जो आसानी से अनुमान लगाया जा सके जैसे अपना नाम, जन्म तिथि, अपने परिवार के किसी सदस्य का नाम पासवर्ड के रूप में प्रयोग न करें।
- (ii) पासवर्ड में अक्षर, अंक तथा विशेष कैरेक्टर का प्रयोग करें।

- (iii) अपने पासवर्ड को याद रखें तथा इस बात का ख्याल रखें कि आप अपने पासवर्ड को ऐसी जगह न लिखकर रखें कि जो आपके कम्प्यूटर के नजदीक हो तथा उसे आसानी से पता लगाया जा सके।
- (iv) जब आप पासवर्ड बदलें तो इसे पूरी तरह बदलें तथा पुराने पासवर्ड का दोबारा प्रयोग न करें।
- (v) पासवर्ड के लिए अंग्रेजी के अर्थपूर्ण शब्द या विदेशी शब्दों का प्रयोग न करें क्योंकि हैकर्स अपने प्रोग्राम में पूरी डिक्शनरी का प्रयोग पासवर्ड को मिलाने के लिए करते हैं।
- (vi) अपने पासवर्ड को किसी को न बताएं।
- (vii) पासवर्ड ई-मेल के माध्यम से न भेजें।
- (viii) एक-दो महीनों में पासवर्ड बदलते रहें।
- (8) अपने सॉफ्टवेयर को अप-टू-डेट रखें— जब छोटे व्यापारों में कम्प्यूटरों को बड़े स्तर पर परिचित कराया गया था तो उस समय प्रयोग किया जाने वाला सॉफ्टवेयर शायद वर्ष में एक या दो बार अपडेट किया जाता था। कभी-कभी सॉफ्टवेयर तब तक अपडेट नहीं होता था जब तक नया कम्प्यूटर न खरीदा जाय। यह प्रचलन 80 तथा 90 के दशक में था जब कुछ ही कम्प्यूटर इन्टरनेट से जुड़कर व्यापार करते थे। अब क्योंकि बहुत सारे कम्प्यूटर इन्टरनेट से जुड़े हैं। इसलिये डाटा सुरक्षा एक महत्वपूर्ण मुद्दा है। अतः आज कम्प्यूटर सॉफ्टवेयर को नवीनतम सिक्युरिटी पैकेज के साथ अप-टू-डेट रखना आवश्यक है। चूँकि हैकर्स इन्टरनेट से जुड़े कम्प्यूटरों में संघ लगाने के लिए अनवरत नये-नये रास्ते ढूँढते रहते हैं, सॉफ्टवेयर कम्पनियाँ उन्हें रोकने के लिए अपने वेबसाइट के माध्यम से संबंधित सॉफ्टवेयर के लिए अपडेट तथा संशोधित पैकेज रिलीज करते रहते हैं। ये अपडेट्स तथा पैकेज उन लोगों के लिए बिल्कुल निःशुल्क होते हैं जिन्होंने इसे खरीदा है।
- इस कार्य के लिए निम्नलिखित टिप्स हैं—
- (i) सभी महत्वपूर्ण सॉफ्टवेयर यथा परिचालन तंत्र, ई-मेल, फायरवॉल, स्केम फिल्टर्स, एण्टी वायरस की एक सूची तैयार करें।
- (ii) संबंधित विक्रेता वेबसाइट को एक्सेस करें तथा यह देख लें कि साइट पर नवीनतम संस्करण उपलब्ध है।
- (iii) सम्भवतः कोशिश यह करें कि वैसे ही सॉफ्टवेयर का प्रयोग हो जो स्वतः ही अपडेट करने की क्षमता रखता हो तथा इस फीचर को आप ऑन रखें। आमतौर पर इस प्रकार के सॉफ्टवेयर इन्टरनेट से जुड़ने पर संबंधित विक्रेता साइट से जुड़कर आवश्यक अपडेट्स स्वयं ही कर लेते हैं।
- (9) ऑन लाइन बैंकिंग की सुरक्षा सुनिश्चित कर लें— बैंक इन्टरनेट प्रयोगकर्ताओं के लिए उनके अकाउंट्स को ऑन लाइन व्यवस्थित करने हेतु एक सुविधाजनक तरीका प्रदान करते हैं। यदि आप ऑन लाइन बैंकिंग करते हैं तो आपको उन खतरों के प्रति सचेत रहना चाहिए क्योंकि जालसाज बड़े स्तर पर संदेशों का प्रयोग कर आपके क्रेडिटिवल्स चुराने की कोशिश करते हैं। ये वैध प्रतीत होने वाले संदेश

आपको यह अहसास दिलाते हैं कि वे अत्यन्त आवश्यक हैं तथा आपको बेवकूफ बनाकर आपसे आपका अकाउण्ट संख्या, पासवर्ड तथा क्रेडिट कार्ड संख्या प्राप्त कर लेते हैं। फिशिंग इसी तरह की तकनीक का नाम है जिसकी सहायता से आपकी पहचान सुराने हेतु आपकी निजी सूचना प्राप्त करते हैं। फिशिंग ई-मेल से आपसे आपका निजी विवरण लेने हेतु कई लोग बहुत ही शक्तिशाली तर्क पेश करते हैं। फिशिंग तथा ऑन लाइन बैंकिंग जालसाजी से बचने के निम्नलिखित उपाय हैं-

- (i) हमेशा अपने बैंक का यू.आर.एल. अपने ब्राउजर में टाइप करें।
- (ii) कभी भी अपने बैंक को किसी लिंक के माध्यम से कनेक्ट न करें।
- (iii) वैसे मेल के प्रति अधिक सजगता बरतें जो ज्यादा जल्दबाजी के लिए प्रेरित करते हैं।
- (iv) सुरक्षित पासवर्ड बनाने के लिए पिछले खण्ड में दिये गये नियमों का अनुसरण करें।
- (v) वायरस सुरक्षा, फायरवॉल तथा नुकसानदायक ई-मेल पर पिछले खण्ड में दिये गये टिप्स का अनुसरण करें।
- (vi) आपके वित्तीय संस्थान जैसे बैंक के द्वारा दिये गये सुरक्षा सुझाव के अनुसार कार्य करें।

(10) सुरक्षा पॉलिसी को विकसित करें तथा इसे मॉन्टर करें- सुरक्षा पॉलिसी विकसित करने तथा इसे मॉन्टर करने से तात्पर्य यह है कि आप अपने व्यापार के लिए कुछ बुनियादी सुरक्षा उपाय तय करें जो आपके व्यापार की जरूरतों के हिसाब से हो तथा उसे मॉन्टर रखें। यह ठीक उसी प्रकार है जिस प्रकार आप अपने घर तथा व्यापार की सुरक्षा के लिए भौतिक रूप से कुछ नियम तथा अनजान व्यक्ति के लिए दरवाजा न खोलना, किसी अविश्वस्त सर्वक्षण में अपनी निजी सूचना न देना इत्यादि होते हैं। इन्हें अपनाने पर दुर्घटना की संभावना कम रहती है। एक बार सुरक्षा पॉलिसी लागू हो जाने के बाद इसे व्यापारिक गतिविधियों तथा सामान्य व्यापार संस्कृति का एक अभिन्न अंग बनायें। साथ ही आप स्वयं तथा अपने कर्मचारियों को नवीनतम इंटरनेट सुरक्षा मुद्दों से पूरी तरह अवगत रखें ताकि आप अपने सुरक्षा-उपायों को अप-टू-डेट रख सकें। सुरक्षा पॉलिसी को मॉन्टर करना सभी लोगों के लिए प्रतिदिन का कार्य है। उदाहरणार्थ मेल में वायरस की जाँच कर लेना तथा कार्य खत्म होते ही इंटरनेट कनेक्शन बंद कर देना कुछ बुनियादी चीजें हैं जो मॉन्टर करना आवश्यक है। इसके लिए कुछ टिप्स इस प्रकार हैं-

- (i) व्यापार आवश्यकताओं का आकलन करें तथा उपयुक्त सुरक्षा उपायों को निर्धारित करें।
- (ii) सुरक्षा पॉलिसी तैयार करें तथा उसे अपने कर्मचारियों से अवगत करायें और उन्हें मॉन्टर रखने के लिए अपने कर्मचारियों को इसका प्रशिक्षण दें।
- (iii) अपने सभी नये कम्प्यूटरों पर सुरक्षा उपायों को स्थापित करें।

प्रश्न-6. इंटरनेट सुरक्षा से क्या अभिप्राय है? विस्तारपूर्वक वर्णन कीजिये।

उत्तर- इंटरनेट सुरक्षा- इंटरनेट सुरक्षा का अर्थ है- नेटवर्क तथा नेटवर्क पर उपलब्ध सूचना, डाटा या साफ्टवेयर को अनाधिकृत व्यक्तियों की पहुँच से दूर रखना तथा केवल

विश्वसनीय उपयोगकर्ताओं द्वारा ही इनका उपयोग सुनिश्चित करना। इंटरनेट सुरक्षा के मुख्यतः तीन आधार हैं-

1. उपयोगकर्ता के प्रामाणिकता की जाँच करना- उपयोगकर्ता के प्रामाणिकता की जाँच Login ID, Password, गुप्त कोड आदि द्वारा की जाती है।
2. एक्सेस कंट्रोल- कुछ विशेष डाटा या सूचना की उपलब्धता कुछ विशेष उपयोगकर्ताओं के लिए ही सुनिश्चित करना एक्सेस कंट्रोल कहलाता है। अंगुलियों के निशान इलेक्ट्रॉनिक कार्ड आदि द्वारा ऐसा किया जाता है।

3. क्रिप्टोग्राफी- सूचना या डाटा को इंटरनेट पर भेजने से पहले उसे गुप्त कोड में परिवर्तित करना तथा प्राप्तकर्ता द्वारा उसे प्रयोग से पूर्व पुनः सामान्य सूचना में परिवर्तित कराना क्रिप्टोग्राफी कहलाता है। यह इंटरनेट पर डाटा सुरक्षा का एक महत्वपूर्ण आधार है। सूचना या डाटा को गुप्त संदेशों में बदलने की प्रक्रिया Encryption कहलाती है जबकि इनक्रिप्ट किए गए डाटा या सूचना को पुनः सामान्य सूचना में बदलना Decryption कहलाता है। क्रिप्टोग्राफी से डाटा स्थानान्तरण के दौरान डाटा चोरी होने या लीक होने की संभावना नहीं रहती। इंटरनेट सुरक्षा में शामिल होता है-

- ⇒ सूचना, डाटा तथा संसाधनों का उपयोग केवल अधिकृत व्यक्तियों द्वारा किया जाना।
- ⇒ डाटा तथा संसाधन अधिकृत व्यक्तियों के लिए हमेशा उपलब्ध होना।
- ⇒ नेटवर्क पर भेजे गए डाटा के गतव्य तक पहुँचने से पहले उसे रिकॉर्ड करने तथा छेड़छाड़ या परिवर्तन करने की संभावना न होना।

कम्प्यूटर तथा नेटवर्क पर अधिकृत उपयोगकर्ता की पहचान करना User Identification कहलाता है जबकि इस पहचान को स्थापित करने की प्रक्रिया ऑथेंटिकेशन कहलाती है।

4. यूजर नेम तथा पासवर्ड- उपयोगकर्ता की पहचान स्थापित करने तथा उसे स्थापित करने की सर्वाधिक प्रचलित विधि यूजर नेम तथा पासवर्ड की है। इसके द्वारा केवल अधिकृत उपयोगकर्ता को ही कम्प्यूटर डाटा तथा नेटवर्क का उपयोग करने दिया जाता है। यूजर नेम तथा पासवर्ड उपयोगकर्ता द्वारा कम्प्यूटर सिस्टम में स्टोर किया जाता है। अगली बार कम्प्यूटर या नेटवर्क का उपयोग करने के लिए कम्प्यूटर सिस्टम यूजर नेम तथा पासवर्ड डालने का अनुरोध करता है। कम्प्यूटर पहले से स्टोर किए गए यूजर नेम तथा पासवर्ड से दी गई सूचना का मिलान करता है, तथा सही पाए जाने पर ही कम्प्यूटर तथा नेटवर्क के प्रयोग की इजाजत देता है।

5. पासवर्ड सुरक्षित रखने के उपाय- कम्प्यूटर सिस्टम तथा नेटवर्क में धोखे से या बार-बार प्रयास कर या साफ्टवेयर द्वारा पासवर्ड लीक होने की संभावना बनी रहती है। इससे बचने के लिए-

- ⇒ पासवर्ड नियमित अंतराल पर बदलते रहना चाहिए।
- ⇒ पासवर्ड बहुत छोटा होना चाहिए।
- ⇒ पासवर्ड जितना बड़ा होगा, बार-बार प्रयास कर उसे प्राप्त करना उतना ही कठिन होगा।
- ⇒ पासवर्ड में अक्षरों, अंकों तथा विशेष चिन्हों का मिश्रण होना चाहिए।

→ पासवर्ड में Capital letters तथा Small letters का मिश्रण भी प्रयोग किया जाना चाहिए।

6. बायोमैट्रिक तकनीक— मानवीय अंगों जैसे— अंगुली की छाप, आँख की पुतली, चेहरे की आकृति, आवाज आदि का प्रयोग कर उपयोगकर्ता की पहचान स्थापित करने की तकनीक बायोमैट्रिक तकनीक कहलाती है। कम्प्यूटर में अधिकृत व्यक्तियों के नमूने पहले से स्टोर कर दिए जाते हैं।

प्रश्न-7. क्रिप्टोलॉजी का क्या अर्थ है? इसके प्रकारों का वर्णन कीजिए।

अथवा

निम्नलिखित पर संक्षिप्त टिप्पणी लिखिए—

(1) एनक्रिप्शन (2) डिक्रिप्शन

उत्तर— क्रिप्टोलॉजी— 'क्रिप्टोग्राफी' शब्द ग्रीक भाषा के दो शब्द क्रिप्टो और ग्राफ से बना है, जिनका अर्थ होता है गुप्त और लिखना। क्रिप्टोग्राफी एक ऐसा विज्ञान है, जिसमें मैसेज को सिर्फ लिखने वाला और प्राप्त करने वाला ही समझ सकता है। जूलियस सीजर ने इसे सर्वप्रथम अपनाया था, क्योंकि वह संदेशों को भेजने हेतु अपने दूतों पर पूर्ण विश्वास नहीं करता था। एनक्रिप्शन और डिक्रिप्शन तकनीकों के द्वारा क्रिप्टोग्राफी विचारधारा को क्रियान्वित किया जाता है।

(1) एनक्रिप्शन— एनक्रिप्शन से तात्पर्य डाटा का सामान्य पढ़ने-योग्य रूप से ऐसे प्रारूप में परिवर्तन से होता है, जिसे सिर्फ कुछ निश्चित लोग ही पढ़ सकते हैं।

एनक्रिप्शन में इनपुट डाटा (जिसे इनक्रिप्ट करना है) और एल्गोरिथम (जिसे डाटा इनक्रिप्ट करना है) शामिल होते हैं। एनक्रिप्शन के बाद टेक्स्ट को पुनः पढ़ने-योग्य बनाने के लिए इसके विपरीत प्रक्रिया जिसे डि-क्रिप्शन कहते हैं, की जाती है।

(2) डिक्रिप्शन— डिक्रिप्शन ठीक एनक्रिप्शन प्रक्रिया के विपरीत होती है, जिसमें कि अस्पष्ट मैसेज को पढ़ने-योग्य मैसेज में बदला जाता है। यूनजर यह कार्य सिर्फ उचित विशेष की के उपयोग के द्वारा ही कर सकता है।

एनक्रिप्शन के प्रकार— एनक्रिप्शन को तीन मुख्य प्रकारों में विभाजित किया जा सकता है, वे इस प्रकार हैं—

(1) वन वे/ट्रिप डोर एनक्रिप्शन— यह एनक्रिप्ट करने का एक ऐसा तरीका है, जिसे डिक्रिप्ट नहीं किया जा सकता है। यह पासवर्ड के लिए एक आदर्श प्रक्रिया है, जिसे डिक्रिप्ट करने की जरूरत नहीं होती है, सिर्फ पहले वाले एनक्रिप्शन से उसकी तुलना ही आवश्यक होती है।

(2) सिंगल की एनक्रिप्शन— इन इनक्रिप्शन में सिर्फ एक ही की का उपयोग होता है, अर्थात् जिस की से एनक्रिप्ट किया जाता है, उसी से ही डिक्रिप्ट किया जाता है।

(3) डबल की एनक्रिप्शन— इस इनक्रिप्शन में दो की उपयोग की जाती है, जिसमें से एक की का उपयोग मैसेज को एनक्रिप्ट करने में और दूसरी की का उपयोग मैसेज को डिक्रिप्ट करने में करते हैं।

एनक्रिप्शन की— Key Encryption एक आवश्यक फार्मूला है, जिससे किसी मैसेज को एनक्रिप्ट और डिक्रिप्ट किया जाता है। अधिकृत यूजर्स सावधानीपूर्वक Key को विपरीत करते हैं सामान्यतः की को दो मुख्य भागों में विभाजित करते हैं—

(A) प्राइवेट/सीक्रेट की— प्राइवेट या सीक्रेट की किसी एक व्यक्ति के पास ही होती है।

(B) पब्लिक की— पब्लिक की किसी भी व्यक्ति को स्वीकृतपूर्वक वितरित की जाती है।

(A) सिंगल/सीक्रेट/प्राइवेट की एनक्रिप्शन— इस विधि में एक गुप्त की उपयोग की जाती है। इसे सिर्फ भेजने वाला व प्राप्त करने वाला ही जानता है। गुप्त की का उपयोग दोनों कार्यों के लिए किया जाता है— जब मैसेज भेजा जाता है तब इसे एनक्रिप्ट करने के लिए व जब इसे प्राप्त करते हैं, तब डिक्रिप्ट करने के लिए। इस एनक्रिप्शन की प्रक्रिया में मैसेज व की को गणितीय विधि से (हेशिंग या ट्रांसफार्मिंग से) मिलते हैं। इस परिस्थिति में इसे डिक्रिप्ट करना सोच में भी असंभव होता है, जब तक हमारे पास वह की ना हो। सीक्रेट की एनक्रिप्शन बहुत ही सुरक्षित है, परन्तु इसमें एक बहुत बड़ी समस्या यह होती है कि जब तक किसी के पास सीक्रेट की नहीं है तब तक वह उसे डिक्रिप्ट नहीं कर सकता है। इसके लिए पहले उसे वह की गुप्त तरीके से पहुँचाना होगी। इस समस्या के कारण इसका उपयोग नेटवर्क व डेलीक्युरिफिकेशन सर्विसेस के लिए नहीं होता है। यह सिर्फ वहाँ पर उपयोगी होता है, जहाँ भेजने वाले व प्राप्त करने वाले के पास की हो। सीक्रेट की एनक्रिप्शन सेल्युलर फोन में उपयोगी होती है, जहाँ पर सिर्फ सबस्क्राइबर (ग्राहक) व सर्विस प्रोवाइडर को ही की की आवश्यकता होती है।

#### Private Key Algorithm

(i) DES (डिटा एनक्रिप्शन स्टैंडर्ड्स)— UNIX के लिए DES को 1977 में विकसित किया गया। ठीक इसी साल इसे अमेरिकी सरकार का स्टैंडर्ड भी बनाया गया। DES एक बहुत प्रभावी प्राइवेट-की एल्गोरिथम है, जिसे IBM ने बनाया है और 1998 के पश्चात् इसके स्थान पर AES (एडवॉन्स एनक्रिप्शन स्टैंडर्ड्स) का उपयोग किया गया। UNIX में DES को एक कमांड लाइन टूल के रूप में क्रियान्वित किया जाता है, जो कि ठीक crypt के समान ही (जिसे des कहते हैं) होता है, परन्तु इसका एनक्रिप्शन एल्गोरिथम बहुत रबस्ट होता है। सिर्फ des के उपयोग के द्वारा सिस्टम पासवर्ड को एनक्रिप्ट करके/etc/passwd फाइल में रखते हैं। इसमें परिवर्तनशील एल्गोरिथम होते हैं, जिससे इन्हें भेदा नहीं जा सकता है (तब क्रेकर्स के पास पासवर्ड फाइल के लिए अन्य दूसरे तरीके ढूँढ़ने होते हैं)। यह एक सिंगल-की या सिमेट्रिक सिस्टम है, ठीक crypt की तरह ही। भेजने वाला व प्राप्त करने वाला दोनों ही एनक्रिप्टेड मैसेज से संबंधित की को जानते हैं।

(ii) AES (एडवॉन्स एनक्रिप्शन स्टैंडर्ड्स)— यह एक नया स्टैंडर्ड्स है जो 128 बिट ब्लॉक्स और 128 बिट कीज का उपयोग करता है और आजकल इसका सबसे अधिक उपयोग हो रहा है। सन् 1998 में एक्सपोर्ट्स प्रोडक्ट्स जो DES एनक्रिप्शन का उपयोग करते थे, उन्हें प्रतिबंधित किया गया। क्योंकि DES के द्वारा एनक्रिप्टेड टेक्स्ट को एक स्थान पर एनक्रिप्टेड ने 56 बटों के अन्तर भेव दिया था, जिसके कारण अमेरिकी एक्सपोर्ट्स नियंत्रक ने पुनः विचार किया कि एक इससे अधिक सशक्त स्टैंडर्ड्स बनाया जाना चाहिए। तब USA की

NIST (नेशनल एडवेंसिड एंफोर्समेंट एंड टेक्नोलॉजी) एक नयी सीक्रेट की का चुनाव करके DES का वैकल्पिक एनक्रिप्शन स्टैंडर्ड बनाया और तब AES अस्तित्व में आया। इस स्टैंडर्ड के लिए प्रतिस्पर्धात्मक बोली लगाने के कार्य की अनुमति NIST और नैर US सहभागियों ने दी।

(2) पब्लिक/डबल की एनक्रिप्शन- इस विधि का उपयोग बहुत से कम्प्यूटर नेटवर्किंग तथा टेलीकम्युनिकेशन सिस्टम में संवेदनशील सूचनाएँ भेजने में अक्सर होता है। इसमें SSL (सिक्योर सोकेट लेयर) प्रोटोकॉल का उपयोग होता है। जैसे इन्टरनेट पर क्रेडिट कार्ड नम्बर भेजने के लिए। SSL इन्टरनेट पर सिक्योर कम्प्युनिकेशन सेशन पब्लिक की की मदद से स्थापित करता है। यह प्रत्येक भाग लेने वाले यूजर को एक पब्लिक की व एक प्रायवेट की साइन करती है। यहाँ पर यूजर ही सिर्फ प्रायवेट की से परिचित होते हैं और पब्लिक की सामान्यतः उन सभी के लिए उपलब्ध होती है, जो उनसे संबंध रखना चाहते हैं। यहाँ पर मैसेज यदि यूजर की पब्लिक की की मदद से एनक्रिप्ट किया जाता है, तब वह उसी यूजर की प्रायवेट की से डिक्रिप्ट किया जाएगा।

उदाहरण के लिए यूजर A एक एनक्रिप्टेड मैसेज, यूजर B को भेजना चाहता है, तब प्रक्रिया इस प्रकार से होगी-

- (1) यूजर A, यूजर B को पब्लिक की की रिक्वेस्ट करेगा या फिर B (सर्टिफिकेट अथॉरिटी) से यह की को मांगेगा।
- (2) यूजर A इस मैसेज को यूजर B के लिए पब्लिक की की मदद से एनक्रिप्ट करेगा और इस एनक्रिप्टेड मैसेज को यूजर B को भेजेगा।
- (3) यूजर B इस एनक्रिप्टेड मैसेज को यूजर A से प्राप्त करेगा और यूजर B अपनी प्रायवेट की की मदद से इसे डिक्रिप्ट करेगा।

#### Public Key Algorithm :

**RSA** (राइस, शॉर और एडेल्मन) स्टैंडर्ड- RSA का नाम उनके बनाने वाले राइवेस्ट, शॉर और एडेल्मन के नाम पर रखा गया। DES के साथ ही RSA भी मार्केट में एक बहुत प्रभावी एनक्रिप्शन एल्गोरिथम था। RSA एक बहुत प्रसिद्ध क्रिप्टोसिस्टम था। यह एक एक्सपैट्रिक सिस्टम है अर्थात् जिसमें कि पब्लिक व प्रायवेट दोनों की होती है।

सामान्यतः RSA एक आत्मनिर्भर एनक्रिप्शन विधि नहीं है। अधिकांशतः यह DES या अन्य सीक्रेट की विधि के साथ उपयोग की जाती है। इस दोहरी पद्धति में मैसेज को भेजने वाला मैसेज की बाँड़ी को DES की मदद से बनायी गई की के द्वारा एनक्रिप्ट करता है। तत्पश्चात् सम्भावित प्राप्तकर्ता की पब्लिक की के द्वारा इस बनायी गई की को एनक्रिप्ट किया जाता है। ये दोनों भाग मिलकर मैसेज बनाते हैं। अब प्राप्तकर्ता अपनी प्रायवेट की का उपयोग करके उस बनायी गई DES की को डिक्रिप्ट करता है, उसके बाद DES की का उपयोग करके मैसेज की बाँड़ी को डिक्रिप्ट किया जाता है।

प्रश्न-8. आई.टी. एक्ट 2000 से क्या तात्पर्य है? संक्षेप में समझाइये।

उत्तर- आई.टी. एक्ट 2000 (IT Act 2000)- भारत में इन्टरनेट तथा इसके माध्यम से हो रहे व्यापार को सुचारु रूप से नियंत्रित करने के उद्देश्य से मई 2000 में

भारतीय संसद के दोनों सदनो ने सूचना प्रौद्योगिकी कानून पारित किया। इस कानून पर तत्कालीन राष्ट्रपति ने अगस्त 2000 में अपने सहमति की मुहर लगायी।

इस अधिनियम का उद्देश्य भारत में इलेक्ट्रॉनिक कॉमर्स को कानूनी इन्फ्रस्ट्रक्चर प्रदान करना था। आई.टी. एक्ट 2000 के विभिन्न पक्ष तथा इसके द्वारा दिये गये सुरक्षा का सारांश इस प्रकार है-

- (1) इस एक्ट के अध्याय-1 में ई-कॉमर्स से संबंधित कई महत्वपूर्ण शाब्दिक परिभाषाएँ दी गई हैं।
- (2) एक्ट का अध्याय-2 विशेषकर अनुबंध करता है कि कोई भी सबक्राइबर किसी इलेक्ट्रॉनिक रिकॉर्ड को प्रमाणित कर सकता है। इसके लिए उसे अपना डिजिटल हस्ताक्षर जोड़ना होता है। साथ ही इसमें यह भी स्पष्ट किया गया है कि कोई भी व्यक्ति उस इलेक्ट्रॉनिक रिकॉर्ड का परीक्षण सबक्राइबर की पब्लिक की का प्रयोग कर सकता है।
- (3) अधिनियम का तीसरा अध्याय इलेक्ट्रॉनिक शासन (electronic governance) का ब्यौरा प्रस्तुत करता है। इस अध्याय में डिजिटल हस्ताक्षर के कानूनी पहचान का भी ब्यौरा दिया गया है।
- (4) इस एक्ट के अध्याय-4 में इलेक्ट्रॉनिक रिकॉर्ड के अधिकार, प्राप्ति-सूचना तथा प्रेषण से संबंधित सूचना प्रस्तुत है।
- (5) इस एक्ट के अध्याय-5 में सुरक्षित इलेक्ट्रॉनिक रिकॉर्ड तथा डिजिटल हस्ताक्षर की चर्चा की गयी है।
- (6) इस एक्ट के अध्याय-6 में सर्टिफाइंग ऑथोरिटीज (certifying authorities) के संचालन की व्याख्या की गयी है।
- (7) इस एक्ट के अध्याय-7 में डिजिटल हस्ताक्षर प्रमाण-पत्र (Digital Signature Certificate) पर प्रकाश डाला गया है। इसके अनुसार कोई भी व्यक्ति डिजिटल हस्ताक्षर प्रमाण-पत्र के लिए सर्टिफाइंग ऑथोरिटी (Certifying authority) को सरकार के द्वारा अनुशंसित (Prescribed) फॉर्म के साथ आवेदन कर सकता है जिसके लिए शुल्क 25,000 तक हो सकता है। सर्टिफिकेट निर्गत करने तथा इसे न करने की पूरी जिम्मेदारी सर्टिफाइंग ऑथोरिटी (Certifying Authority) के हाथ में है।
- (8) इस एक्ट के अध्याय-8 में सबक्राइबरों (subscribers) के कर्तव्यों की चर्चा की गयी है।
- (9) इस एक्ट के सबसे महत्वपूर्ण अध्यायों में एक अध्याय-9 में जुमाने (penalties) तथा निर्णय (adjudication) की बात की गयी है। इसमें विभिन्न प्रकार के अपराधों की चर्चा भी की गयी है। इसमें निम्नलिखित मुख्य बिन्दु शामिल हैं-
- (1) कोई व्यक्ति कम्प्यूटर, कम्प्यूटर सिस्टम या कम्प्यूटर नेटवर्क के मालिक तथा प्रभारी की आज्ञा के बगैर इन्हें एक्सेस नहीं कर सकता, इससे डाटा प्राप्त नहीं कर सकता,

कम्प्यूटर को वायरस संक्रमण के अतिरिक्त अन्य विधियों से भी नुकसान नहीं पहुँचा सकता तथा कम्प्यूटर नेटवर्क के कार्य में किसी प्रकार का कोई अवरोध नहीं पहुँचा सकता।

(ii) कम्प्यूटर, कम्प्यूटर सिस्टम या किसी कम्प्यूटर नेटवर्क पर इस प्रकार किये गये किसी भी जुर्म का जुर्माना एक करोड़ रुपये तक हो सकता है।

इस अध्याय के पहले खण्ड में कम्प्यूटर, डेटाबेस, कम्प्यूटर वायरस, नुकसान (Damage) इत्यादि की परिभाषा भी प्रस्तुत की गयी है। इस अध्याय के अगले खण्ड में यह भी बताया गया है कि इस स्थिति में फैसला सुनाने की योग्यता किसको दी गयी है जो निम्न प्रकार से है-

(iii) निर्णय अधिकारी (Adjudicating officer) भारत सरकार के निर्देशक या फिर राज्य सरकार के इसी स्तर का कोई अधिकारी होगा तथा केन्द्र सरकार के द्वारा बनाये गियमों के अनुसार इसकी जाँच करेगा।

(iv) निर्णायक इस मामले का वही होगा जो सूचना प्रौद्योगिकी क्षेत्र का तथा न्यायपालिका (Judicial) का अनुभव रखता हो। इसमें यह भी बताया गया है कि वह किस प्रकार निर्णायक फैसला करेगा? तथा एक से अधिक निर्णायक की नियुक्ति होने पर कौन क्या करेगा? तथा जुर्माना का निर्धारण कैसे होगा?

(10) इस अधिनियम का 10वां अध्याय सायबर रेग्यूलेशन्स अपीलेट ट्रिब्यूनल (Cyber Regulations Appellate Tribunal) पर आधारित है। इसमें इस ट्रिब्यूनल के स्थापना की बात कही गयी है। इसमें यह बताया गया है कि केन्द्र सरकार एक से अधिक ट्रिब्यूनल की स्थापना कर सकता है तथा किस ट्रिब्यूनल का अधिकार क्षेत्र (Jurisdiction) क्या होगा? यह भी सम्मिलित है। इस ट्रिब्यूनल का प्रिजाइडिंग ऑफिसर (Presiding officer) वही हो सकता है जिसने उच्च न्यायालय के न्यायाधीश बनने की योग्यता प्राप्त की हो या फिर वह भारतीय लीगल सिस्टम (Indian Legal System) का सदस्य हो या रहा हो या फिर इस सेवा में प्रथम श्रेणी के पद पर तीन वर्षों तक रहा हो। प्रिजाइडिंग ऑफिसर की अधिकतम कार्यकाल की आयु 65 वर्ष की होगी। इस बॉडी का मुख्य रूप से इसलिए गठन किया गया है ताकि न्यायाधीश के द्वारा किये गये फैसले के विरुद्ध अपील की जा सके।

(11) इस अधिनियम के अध्याय-11 में अपराधों (offences) की चर्चा की गयी है। इसमें निम्नलिखित बातें हैं-

(i) कम्प्यूटर मुख्य डेटाबेस के साथ छेड़-छाड़-कोई भी व्यक्ति जो कानूनी रूप से सुरक्षित कम्प्यूटर सॉर्स कोड, कम्प्यूटर प्रोग्राम, कम्प्यूटर सिस्टम, कम्प्यूटर नेटवर्क के साथ जान-बूझकर छेड़-छाड़ करता है तो वह दो लाख रुपये तथा तीन साल तक की जेल का भागी होगा।

(ii) कम्प्यूटर सिस्टम को हैक करना- यहाँ हैकिंग की परिभाषा दी गयी है। कोई भी व्यक्ति कम्प्यूटर रिसोर्स में किसी नुकसान के उद्देश्य से संघ लगाता है, वह हैक

करता है। हैकिंग की सजा तीन साल कैद, दो लाख का जुर्माना या दोनों भी हो सकता है।

इसी प्रकार इस अध्याय में इलेक्ट्रॉनिक फॉर्म में किसी भी आपतितजनक सूचना के प्रकाशन से संबंधित अपराध तथा सजा का वर्णन है। इसके लिए दो प्रकार की सजा है। यदि कोई व्यक्ति इस तरह की सामग्री का प्रकाशन पहली बार करता है तो उसे पाँच साल की सजा तथा एक लाख रुपये तक का जुर्माना हो सकता है। तथा वही व्यक्ति इस अपराध की पुनरावृत्ति करता है तो वह दस साल की जेल और दो लाख रुपये तक के जुर्माने का भागी हो सकता है। इस अध्याय में गोपनीयता भंग करने, डिजिटल हस्ताक्षर सर्टिफिकेट गलत प्रकाशित करने, गलत उद्देश्य के लिए प्रकाशन करने इत्यादि जैसे अपराधों के लिए अनुशासित सजा की चर्चा है। इस प्रकार के अपराध की जाँच डिप्टी पुलिस अधीक्षक के नीचे के पद का कोई पुलिस अधिकारी नहीं कर सकता इसका भी वर्णन है।

(12) अध्याय-XII में नेटवर्क सर्विस प्रदाता इस अधिनियम के तहत किसी अपराध के लिए जिम्मेवार नहीं होंगे इसका वर्णन है तथा अध्याय-XIII में पुलिस अधिकारी की शक्ति (power) तथा अन्य विविध (miscellaneous) मुद्दों का वर्णन है।

आई.टी. एक्ट 2000 का मुख्य प्रयास पुराने पड़-कानूनों को बदलना तथा सायबर अपराधों से निबटने के लिए उपाय प्रदान करना है। हमें आवश्यकता थी कि ऐसे कानून बनें ताकि हम नेट पर अपने लेन-देन क्रेडिट कार्ड के साथ, इसके दुरुपयोग होने की वृत्ति किये बचकर सकें। यह अधिनियम चिर-प्रतिष्ठित लीगल फ्रेमवर्क (legal framework) प्रदान करता है ताकि किसी भी सूचना का कानूनी पक्ष इसलिए उपेक्षित न हो कि यह इलेक्ट्रॉनिक रिकॉर्ड फॉर्म में है।

इलेक्ट्रॉनिक रिकॉर्ड के माध्यम से किये जाने वाले व्यापार तथा संचार में वृद्धि होते देखकर यह अधिनियम सरकारी विभागों को सशक्त बनाना चाहता है कि ये विभागीय दस्तावेजों (Official documents) के फाइलिंग, निर्माण तथा अवरोधन (Retention) को डिजिटल फॉर्म में स्वीकार कर सकें। इस अधिनियम ने डिजिटल हस्ताक्षर के माध्यम से इलेक्ट्रॉनिक रिकॉर्ड्स/कम्प्यूनिकेशन्स के ऑथेंटिकेशन तथा ऑरिजिन (Origin) के लिए एक लीगल फ्रेमवर्क प्रस्तावित किया है। ई-कॉमर्स परिप्रेक्ष्य में आई.टी. एक्ट 2000 तथा इसके धाराओं (Provisions) के कई सकारात्मक पहलू हैं। सबसे पहले कि अब भारत में ई-मेल कम्प्यूनिकेशन का एक मान्य और कानूनी रूप होगा जो किसी भी कानून के दरबार (Court of law) में पेश किया जा सकता है। कम्पनियाँ अब अधिनियम द्वारा प्रदान किये गये लीगल इन्फ्रास्ट्रक्चर का प्रयोग करते हुए इलेक्ट्रॉनिक कॉमर्स को सुचारु रूप से कर सकती हैं। इस अधिनियम के अन्तर्गत अब कारपोरेट कम्पनियाँ सर्टिफाइंग ऑथोरिटीज बनाकर डिजिटल हस्ताक्षर सर्टिफिकेट निर्गत कर सकती हैं। अधिनियम के अन्तर्गत अब सरकार वेब पर नोटिफिकेशन (Notification) निर्गत कर ई-शासन को आगे ले जायेगी। इस अधिनियम के लागू होने के बाद अब कम्पनियाँ सरकारी कार्यालयों में इलेक्ट्रॉनिक रूप से एलिकेशन तथा फॉर्म आवेदन कर सकते हैं। यह अधिनियम वैसे सुरक्षा-मुद्दों को भी संबोधित करता है जो इलेक्ट्रॉनिक लेन-देन के लिए अत्यन्त आवश्यक हैं। इस अधिनियम ने सुरक्षित डिजिटल

हस्ताक्षरों की परिकल्पना को एक कानूनी परिभाषा दी है। आई.टी. एक्ट 2000 के तहत अब कम्पनियों के पास एक वैधानिक उपचार है जो उनके कम्प्यूटर सिस्टम नेटवर्क से डाटा के साथ छेड़छाड़ या चुराये जाने की स्थिति में अत्यन्त महत्वपूर्ण है। बोधी व्यक्ति या कम्पनी पर अब प्रभावित कम्पनियों एक करोड़ तक का जुर्माना लगा सकती है।

प्रश्न-9. नई राष्ट्रीय दूरसंचार नीति से आप क्या समझते हैं? समझाइये।

उत्तर- नई राष्ट्रीय दूरसंचार नीति- केन्द्रीय मंत्रिमण्डल द्वारा 26 मार्च, 1999 को अनुमोदित नई दूरसंचार नीति (NTP'99) की घोषणा कर दी गई। नई नीति ने 1994 की दूरसंचार नीति का स्थान 1 अप्रैल, 1999 से ले लिया है।

नई नीति के तहत सन् 2002 तक माँग पर फोन (Telephone on Demand) उपलब्ध कराने का लक्ष्य रखा गया था। देश में टेलीफोन उपलब्ध (Teledensity) को सन् 2005 तक 7 प्रति हजार जनसंख्या तथा सन् 2010 तक 15 प्रति हजार जनसंख्या तक लाने का लक्ष्य है। सभी गाँवों को वर्ष 2011 तक दूरसंचार सेवाओं के दायरे में लाने का लक्ष्य रखा गया था तथा सभी जिला मुख्यालयों को भी सन् 2000 तक इन्टरनेट के दायरे में लाने का लक्ष्य रखा गया। नई नीति के तहत घरेलू लम्बी दूरी की कॉलों (STTD) को 1 मार्च, 2000 तक तथा अन्तर्राष्ट्रीय कॉलों को 1 मार्च, 2004 तक निजी क्षेत्र के लिए खोल देने का लक्ष्य था।

सरकार ने 13 अगस्त, 2000 से प्राइवेट ऑपरेटरों के लिए उनकी संख्या पर बिना किसी प्रतिबन्ध के राष्ट्रीय लम्बी दूरी की सेवा को भी खोल दिया है तथा अन्तर्राष्ट्रीय टेलीफोन सेवाओं (STD) के क्षेत्र में भी निजी कम्पनियों के मार्ग को 15 जनवरी, 2002 से खोल दिया गया है। इस प्रकार सार्वजनिक क्षेत्र की कम्पनी VSNL (विदेश संचार निगम लि.) के एकाधिकार को पूर्व निर्धारित समय (1 अक्टूबर, 2004) से दो वर्ष पूर्व ही समाप्त करने का निर्णय केन्द्र सरकार ने किया है। उल्लेखनीय है कि ISD सेवाएँ प्रदान करने के लिए दूरसंचार विभाग (DOT) ने VSNL को 1986 में लाइसेंस प्रदान किया था तथा 1994 में इसे 10 वर्ष तक के लिए (31 मार्च, 2004 तक के लिए) इस क्षेत्र में एकाधिकार प्रदान किया था।

सैलूलर फोन सेवा के मामले में नई नीति में प्रत्येक सर्किल में दो ऑपरेटरों की नीति के स्थान पर दूरसंचार विभाग/महानगर टेलीफोन निगम लि. के रूप में तीसरे ऑपरेटर को भी लाने की बात स्वीकार की गई है। किसी बोधे ऑपरेटर का प्रवेश ट्राइ (TRAI) की सिफारिशों पर निर्भर करेगा। इसी प्रकार बुनियादी फोन सेवा के मामले में द्वैधिकार (दूरसंचार विभाग/महानगर टेलीफोन निगम लि. तथा एक निजी ऑपरेटर) की नीति के स्थान पर अधिक कम्पनियों के प्रवेश की बात स्वीकार की गई है। इनकी संख्या ट्राइ द्वारा निर्धारित की जाएगी।

नई दूरसंचार नीति में ट्राइ की शक्तियों को और स्पष्ट करते हुए कहा गया है कि इसका क्षेत्र सेवा प्रदान करने वालों (Service Providers) तक सीमित रहेगा। इसमें दूरसंचार विभाग जैसी सरकारी एजेंसियाँ भी शामिल हैं। सभी सेवा प्रदान करने वाली एजेंसियों को ट्राइ निर्देश जारी कर सकेगा तथा इनके बीच के पारस्परिक विवादों को निपटारने का अधिकार भी इसे होगा। इनमें दूरसंचार विभाग व निजी ऑपरेटरों के बीच के विवाद भी शामिल हैं।

नीति में यह भी स्पष्ट किया गया है कि जिन मामलों में ट्राइ की भूमिका सलाहकारी की है, उनमें इसकी सलाह लेने के लिए सरकार बाध्य नहीं है।

दूरसंचार ऑपरेशन विभाग का मार्च 2001 तक देश के चुनिन्दा शहरों में मोबाइल फोन सेवा प्रदान करने का लक्ष्य था। बाद में अन्य शहरों व ग्रामीण क्षेत्रों में भी विभाग की मोबाइल फोन सेवा का विस्तार किया जाएगा। विभाग ने मार्च 2002 तक देश के अधिकांश भागों में मोबाइल फोन सेवा उपलब्ध करा दी थी।

उल्लेखनीय है कि दूरसंचार विभाग ने मार्च, 2002 तक पूरे देश में माँग पर फोन उपलब्ध कराने का लक्ष्य भी निर्धारित किया हुआ था। किन्तु केबलों की खरीद के लिए डेंडर प्रक्रिया पर जबलपुर उच्च न्यायालय द्वारा रोक लगा दिए जाने के कारण इस लक्ष्य की प्राप्ति में विलम्ब हो गया है।

प्रश्न-10. सूचना नीति प्रबंधन पर संक्षिप्त टिप्पणी लिखिये।

अथवा

क्रेडिट जोखिम प्रबंधन के बारे में संक्षेप में वर्णन कीजिये।

उत्तर- सूचना नीति प्रबंधन (Managing information policy)- इलेक्ट्रॉनिक भुगतान-प्रणाली की गोपनीयता या निजता को सुनिश्चित करना और बनाए रखना चाहिए। प्रत्येक बार जब कोई व्यक्ति क्रेडिट कार्ड का प्रयोग करते हुए कोई सामग्री खरीदता है या कोई भूजनीन सबक्राइब करता है या किसी सर्वर को एक्सेस करता है, तब वह सूचना एक डाटाबेस में कहीं जाती है। इसके अतिरिक्त ये सारे आँकड़े आपस में जोड़े जा सकते हैं फलस्वरूप वे एक फाइल बना लेते हैं। यह फाइल यह प्रकट करेगा कि कौन से आइटम खरीदे गए थे और कहाँ तथा कब? इससे व्यापार के एक नियम का उल्लंघन होता है वह यह कि जहाँ तक संभव हो सके ग्राहकों की निजता को सुरक्षित रखा जाना चाहिए।

एक उपभोक्ता के भुगतान को आसानी से एक साथ किया जा सकता है। कहीं, और कब, और कभी-कभी जो कुछ एक उपभोक्ता खरीदता है वह संगृहित हो जाता है। डाटा का यह संग्रह उस आदमी के बारे में बहुत कुछ बता सकता है और इससे व्यक्ति की गोपनीयता के अधिकार का हनन होता है। प्रयोक्ताओं को अवश्य ही इस बात का आश्वासन दिया जाना चाहिए कि लेन-देन की जानकारी गोपनीय होगी, जो सिर्फ सम्मिलित पार्टियों तथा उनके दलालों तक सीमित रहेगी।

गोपनीयता को नेटवर्क पर बुरे लोगों से तथा अनाधिकृत अन्दर के लोगों से बचाया जाना चाहिए। उपभोक्ताओं को इस बात का आश्वासन दिया जाना चाहिए कि उन्हें आसानी से धोखा, छल या झूठे लेन-देन में फँसाने से मुक्त रखा जाएगा। यह सुरक्षा पूरे लेन-देन प्रोटोकॉल के दौरान लागू किया जाना चाहिए जिसके तहत कोई सामग्री या सेवा खरीदी या प्रदान की जाती है। इसका मतलब यह है कि बहुत से लेन-देन के लिए विश्वसनीय तृतीय पक्ष एजेंट की आवश्यकता होगी ताकि सम्मिलित पार्टियों की प्रमाणिकता तथा विश्वास प्रदान किया जा सके।

क्रेडिट जोखिम प्रबंधन (Managing Credit Risk)- क्रेडिट या संगठित रूप से लिया गया जोखिम नेट सेटिलमेंट प्रणाली में मुख्य मुद्दे हैं क्योंकि इसके नेट स्थिति का निबटारा

करने में किसी बैंक की असफलता बैंक की कई असफलताओं का कारण बन सकती है। डिजिटल सेन्ट्रल बैंक को ऐसी नीतियों का विकास करना चाहिए जो इन संभावनाओं से निबटरे सके। बहुत से विकल्प अस्तित्व में हैं, जिनमें से प्रत्येक की खूबियाँ और खामियाँ हैं।

Settlement पर डिजिटल सेन्ट्रल बैंक की गारन्टी प्रणाली से दिवालापन जाँच को हटा देता है क्योंकि बैंक अत्यन्त आसानी से दूसरे बैंकों से क्रेडिट खतरे झेल सकते हैं। बिना ऐसी किसी गारण्टी के मुद्रा बाजार, रिलियरिंग तथा निबटारे प्रणालियाँ बाधित हो सकती हैं। मध्य मार्ग के रूप में यदि सेन्ट्रल बैंक गारंटी नहीं लेता है, तो कम से कम इसे आन्तरिक रूप से यह परिभाषित करना चाहिए कि निपटारे में शामिल बैंकों के लिए लिक्विडिटी के प्रसार की शर्तें तथा नियम क्या-क्या हो सकते हैं ?

### इकाई-3

## सोशल मीडिया अवलोकन और सुरक्षा

दीर्घ एवं लघु उत्तरीय प्रश्न-

प्रश्न-1. सोशल मीडिया पर संक्षेप टिप्पणी लिखिए।

उत्तर-1. सोशल मीडिया- आज का युग सोशल मीडिया और जनसंचार माध्यमों का युग है। आज पूरा विश्व एक छोटे से कब्जे के साथ-साथ मोबाइल के छोटे से स्क्रीन में तब्दील हो गया है। यही कारण कि एगज हर कोई अपने मनोरंजन, सूचना और शिक्षा के लिए सोशल मीडिया का उपयोग करने लगा है। सोशल मीडिया हमें स्वतंत्र रूप से कुछ भी कहने और लिखने का अधिकार देता है। यही वजह है कि सोशल मीडिया सबका पसंदीदा माध्यम बन गया है। सोशल मीडिया कुछ ही समय में बहुत ज्यादा लोकप्रिय हो गया और सबके दिलों में अपने लिए एक अलग ही जगह बना ली है, विशेषतः युवाओं के।

सोशल मीडिया एक ऐसा मीडिया है जो बाकी सारे जनसंचार माध्यमों से बिलकुल भिन्न है। सोशल मीडिया एक तरह की वेबसाइट या एप्लीकेशन होती है जो लोगों को आपस में जुड़ने का काम करती है। सोशल मीडिया को न्यू मीडिया के नाम से भी जाना जाता है। इसके अन्तर्गत बहुत सारे सोशल मीडिया एप को शामिल किया गया है, जैसे- फेसबुक, इंस्टाग्राम, ट्विटर, क्वार्ट्सएप, ब्लॉग आदि। आज के दौर में सोशल मीडिया हमारी जिंदगी का एक महत्वपूर्ण हिस्सा बना हुआ है जिसके बिना हम अपने जीवन की कल्पना भी नहीं कर सकते हैं।

प्रश्न-2. सोशल नेटवर्क क्या है? समझाइये।

उत्तर-1. सोशल नेटवर्क- ऑनलाइन मौजूद वेबसाइट्स ऐप्स और सेवाओं के व्यापक संकट्टम के साथ, सोशल नेटवर्क की कोई एक सटीक परिभाषा नहीं है। हालाँकि आमतौर पर, सोशल नेटवर्क में निम्नलिखित कुछ सामान्य विशेषताएँ होती हैं जो उन्हें अन्य से अलग करती हैं-

- (1) एक सोशल नेटवर्क उपयोगकर्ता-जनित सामग्री पर ध्यान केंद्रित करेगा। उपयोगकर्ता (यूजर) मुख्य रूप से अन्य उपयोगकर्ताओं द्वारा बनाई गई सामग्री को

देखते हैं और उनके साथ बातचीत करते हैं। उन्हें दूसरों के देखने के लिए टैग्स स्टेटस अपडेट या चित्र (इमेज) पोस्ट करने के लिए प्रोत्साहित किया जाता है।

- (2) सोशल नेटवर्क उपयोगकर्ता (यूजर) या संगठन को प्रोफाइल बनाने की परिमिशन देते हैं। प्रोफाइल में व्यक्ति के बारे में जानकारी और उनके द्वारा पोस्ट की गई सामग्री वाला एक केन्द्रीकृत पेज शामिल है। उनकी प्रोफाइल उनके वास्तविक नाम से कनेक्ट हो सकती है।

- (3) एक सोशल नेटवर्क के पास अन्य उपयोगकर्ताओं (यूजर्स) के साथ स्थायी सम्बन्ध बनाने का एक तरीका होता है। इन कनेक्शन्स को आमतौर पर दूसरे उपयोगकर्ता को भिन्न बनाना या फॉलो करना कहा जाता है। वे उपयोगकर्ताओं को अन्य उपयोगकर्ताओं को खोजने (सर्व करने) और रिश्तों का जाल बनाने की परिमिशन देते हैं। अक्सर एक एल्गोरिथम अन्य उपयोगकर्ताओं और संगठनों की सिफारिश करेगा जिनके साथ वे सम्बन्ध (कॉन्टैक्ट होना) बनाना चाहते हैं।

प्रश्न-3. सोशल मीडिया के प्रकारों का वर्णन कीजिये।

अथवा

सोशल मार्केटिंग नेटवर्क के लाभ संक्षेप में लिखिये।

उत्तर-1. सोशल मीडिया के प्रकार-1. वे प्रकार निम्नवत् हैं-

- (1) सोशल नेटवर्क : फेसबुक, ट्विटर, लिंक्डइन- इस प्रकार के सोशल मीडिया का उपयोग वेब पर व्यक्तियों से जुड़ने (कनेक्ट होने) के लिए किया जाता है। वे ब्रांडिंग, सामाजिक जागरूकता (सोशल अवेयरनेस), सम्बन्ध निर्माण, ग्राहक सेवा, लीड जनरेशन और लयान्तरण के माध्यम से आपके व्यवसाय में सहायता करते हैं। आप इन नेटवर्क पर विभिन्न प्रकार के सोशल मीडिया अभियान चला सकते हैं जो आपकी पहुंच (एचोव) बढ़ाने में सहायता करेंगे।

इन सोशल मार्केटिंग नेटवर्क के निम्नलिखित लाभ हैं-

- (i) वे पारस्परिक रूप से उत्पादक सम्बन्धों को सुनिश्चित करने के लिए व्यक्तियों और व्यवसायों को ऑनलाइन बातचीत करने और डेटा और विचार साझा (शेयर) करने के लिए प्रोत्साहित करते हैं।
- (ii) यदि आप उपलब्ध मार्केटिंग अभियानों को अनुकूलित करने के लिए सर्वोत्तम तरीकों की खोज रहे हैं तो आपको फेसबुक, ट्विटर और लिंक्डइन जैसे सोशल नेटवर्क पर ऐसा करने के लिए कई प्रकार के जैविक और भुगतान किए गए तरीके मिलेंगे।

- (2) मीडिया शेयरिंग नेटवर्क : इंस्टाग्राम, स्नैपचैट, यूट्यूब- सोशल मीडिया के मीडिया शेयरिंग प्रकारों का उपयोग वेब पर तस्वीरें, लाइव वीडियो, वीडियो और अन्य प्रकार के मीडिया को खोजने (सर्व करने) और साझा (शेयर) करने के लिए किया जाता है। वे ब्रांड निर्माण, लीड जनरेशन, टारगेटिंग आदि में भी हमारी सहायता करते हैं। वे व्यक्तियों और ब्रांड्स को मीडिया को खोजने और साझा करने के लिए स्थान देते हैं ताकि टारगेटेड दर्शकों को टारगेट किया जा सके और उन्हें एक विश्वसनीय और परिणाम-संचालित तरीके से

परिवर्तित किया जा सके। वर्तमान में सोशल नेटवर्क भी ये सुविधाएँ प्रदान करते हैं। हालांकि, मीडिया शेयरिंग नेटवर्क के लिए मीडिया साझा करना उनकी मूल भूमिका (कार्य) है।

मीडिया शेयरिंग नेटवर्क के लाभ—ये लाभ निम्नलिखित हैं—

- (i) इंस्टाग्राम, यूट्यूब और स्नेपचैट प्रकार के मीडिया नेटवर्क पर छवि या वीडियो से शुरुआत करना हमारे लिए अधिक लाभदायक होता है।
- (ii) यह निश्चित करने हेतु कि हमें अपने व्यवसाय के लिए इन नेटवर्क का उपयोग करना चाहिए या नहीं, हमें अपने संसाधनों और लक्षित (टारगेट) दर्शकों पर विचार करना चाहिए। ये चैनल हमें लीड उत्पन्न करने और अपने दर्शकों का आधार बढ़ाने के लिए सुनियोजित अभियान चलाने में मदद करते हैं।
- (3) चर्चा मंच (Reddit Quora, Digg)— इस प्रकार के सोशल मीडिया चैनल का उपयोग विभिन्न प्रकार की सूचनाओं, विचारों और समाचारों को खोजने, साझा करने और चर्चा करने हेतु किया जाता है। ये वेदाग बाजार अनुसंधान करने के लिए शीर्ष स्तर के संसाधन बनकर व्यवसायों की मदद करते हैं। ये फोरम सोशल मीडिया मार्केटिंग अभियान चलाने के सबसे पुराने तरीके हैं।

फेसबुक जैसे लोकप्रिय सोशल मीडिया प्लेटफॉर्मों के प्रवेश से पहले, ये मंच ऐसे स्थान थे जहाँ पेशेवर, विशेषज्ञ और उसाही लोग विभिन्न क्षेत्रों से सम्बन्धित विभिन्न प्रकार की चर्चा करते थे।

चर्चा मंच के लाभ—ये लाभ निम्नवत् हैं—

- (i) इन चर्चा मंचों पर बड़ी संख्या में उपयोगकर्ता (यूजर्स) हैं और यह यूजर्स के व्यवसाय के लिए अभूतपूर्व पहुँच सुनिश्चित करते हैं। ये वे स्थान हैं जो किसी भी डोमेन के विभिन्न प्रश्नों के उत्तर प्रदान करते हैं।
- (ii) यदि यूजर्स के व्यवसाय को गहन ग्राहक अनुसंधान (कस्टमर्स रिसर्च) की आवश्यकता है तो ये स्थान उनके व्यवसाय के लिए सबसे उपयुक्त होंगे।
- (iii) जानकारी साझा करने और उत्तर जानने के साथ-साथ ये मंच विज्ञापन में भी बहुत प्रभावशाली हैं।

(4) बुकमार्किंग और कंटेंट क्रूरेशन नेटवर्क (Pinterest, Flipboard)— इस प्रकार के सोशल मीडिया को चुनने से हमें विभिन्न प्रकार की नवीनतम सामग्री और मीडिया का पता लगाने, साझा करने, चर्चा करने और सहेजने में सहायता मिलेगी जो वर्तमान में ट्रेंड में हैं। वे हमारे व्यवसाय के लिए ब्रांड जागरूकता (अवेयरनेस) को प्रसारित करने में बहुत सहायक हैं, साथ ही, विभिन्न प्रकार के सोशल मीडिया मार्केटिंग अभियान चलाने के लिए इसे चुनने से हमें वेबसाइट ट्रैफिक और ग्राहक कनेक्शन पैदा करने में मदद मिलती है। यदि हम कुछ आउट-ऑफ-द-बॉक्स अत्यधिक रचनात्मक अभियान चलाना चाहते हैं जो न केवल हमारे दर्शकों को सूचित कर सके बल्कि उन्हें आकर्षित भी कर सके, तो यह सोशल मीडिया सबसे उपयुक्त है।

(i) फ्लिपबोर्ड पर सोशल मीडिया अभियान चलाने के लिए हमारे पास एक ऐसी साइट होनी चाहिए जो बुकमार्क-अनुकूल हो। हमें उन फीचर्स के लिए शीर्षकों और

इमेजेज को अनुकूलित करना चाहिए जिनका उपयोग बुकमार्किंग और कंटेंट क्रूरेशन नेटवर्क हमारी सामग्री तक पहुँचने और साझा करने के लिए करते हैं।

- (ii) फ्लिपबोर्ड हमें सबसे आकर्षक सामग्री का उपयोग करके अपनी रचय की फ्लिपबोर्ड मैक्रीन बनाने की सुविधा देता है और फिर हम उसे अपने दर्शकों को दिखा सकते हैं।

(5) उपभोक्ता समीक्षा नेटवर्क : ग्लेन, जोमैटो, ट्रिपएडवाइजर— ग्राहक समीक्षा नेटवर्क का उपयोग करने से हमारी विभिन्न सेवाओं या ब्रांडों के बारे में विभिन्न जानकारी ढूँढने, साझा करने और समीक्षा (कम्प्लाइड) करने में मदद मिलेगी। जब किसी व्यवसाय को इन नेटवर्कों पर सकारात्मक समीक्षा मिलती है, तो उनके दावे अधिक विश्वसनीय हो जाते हैं क्योंकि इन नेटवर्कों पर समीक्षाएँ सामाजिक प्रमाण के रूप में व्यवसायों के लिए इन साइट्स पर सकारात्मक समीक्षा होना बहुत महत्वपूर्ण है। इसके अलावा उन सभी मुद्दों को हल करना जो हमारे ग्राहक इन समीक्षा प्लेटफॉर्मों पर पोस्ट कर रहे हैं, यह बात हमारे व्यवसाय के सकारात्मक और उत्पादक परिणामों के लिए अति महत्वपूर्ण होगी।

लाभ—उपभोक्ता समीक्षा नेटवर्क के निम्नलिखित लाभ हैं—

- (i) ये नेटवर्क उपयोगकर्ताओं को उनके द्वारा उपयोग किए गए विभिन्न प्रकार के उत्पादों और सेवाओं की समीक्षा करने हेतु एक स्थान प्रदान करते हैं।
- (ii) समीक्षा सामग्री किसी भी ब्रांड के लिए महान मूल्य जोड़ती है क्योंकि यह हमारी सेवाओं को प्राप्त करने हेतु अधिक और नये खरीदारों की संख्या को बढ़ायेगी।
- (iii) ग्लेन और जोमैटो: ऐसे सोशल मीडिया प्लेटफॉर्म हैं जो स्थान-आधारित समीक्षा सेवाएँ प्रदान करते हैं। अतः प्लेटफॉर्म स्थान-आधारित सामाजिक अभियान चलाने में हमारी सहायता करते हैं।

(6) ब्लॉगिंग और प्रकाशन नेटवर्क : वर्डप्रेस, टम्बलर तथा मीडियम— हमें लेखों, सोशल मीडिया ब्लॉगों और वेब पर अन्य सामग्री को प्रकाशित करने, खोजने और उन पर टिप्पणी करने हेतु इस प्रकार के सोशल मीडिया नेटवर्क का चयन करना चाहिए।

कंटेंट मार्केटिंग लक्षित (टारगेट) दर्शकों को लक्षित (टारगेट) करने, इन्हें आकर्षित करने, संलग्न करने और परिवर्तित करने के सबसे शक्तिशाली तरीकों में से एक है। यह सफल ऑनलाइन मार्केटिंग अभियानों का आधार बनने जा रहा है जो डिजिटल मार्केटिंग अभियानों के रूपांतरण फलन में सर्वाधिक महत्वपूर्ण भूमिका निभाते हैं।

वर्डप्रेस और ब्लॉगर पारम्परिक ब्लॉगिंग प्लेटफॉर्म हैं जबकि टम्बलर और मीडियम नवीनतम ब्लॉगिंग और प्रकाशन नेटवर्क हैं।

लाभ—ब्लॉगिंग और प्रकाशन नेटवर्क के निम्नलिखित लाभ हैं—

- (i) ये नेटवर्क उन व्यवसायों के लिए आवश्यक हैं जो कंटेंट मार्केटिंग का प्रभावी ढंग से उपयोग करना चाहते हैं, साथ ही, हम इन सामग्री को विभिन्न सामाजिक नेटवर्क जैसे फेसबुक, ट्विटर, लिंक्डइन आदि पर साझा (शेयर) कर सकते हैं।

(ii) इन नेटवर्कों पर हम जो सामग्री उपयोग करते हैं, वह हमारे अपने व्यवसाय के लिए एक स्थान बनाने में भी मदद करेगी और जो दर्शक उस जगह से सम्बन्धित जानकारी की खोज में हैं, वे निश्चित रूप से हमारे ब्लॉग या साइट पर आएंगे।

(7) सोशल शॉपिंग नेटवर्क : पॉलीबोर, ईटीसी, फैंसी- यदि हम मार्केटिंग के सभी नवीनतम रूढ़ानों का पता लगाना चाहते हैं या शॉपिंग टिप्स जानना चाहते हैं तो उक्त प्रकार के सोशल मीडिया चैनल्स हमारे लिए उपलब्ध हैं। इसके अलावा, वे विभिन्न ब्रांडों का फॉलो करने, रिलेवन्स चीजें शेयर करने और इन सोशल शॉपिंग नेटवर्क पर खरीदारी करने में हमारी मदद करते हैं। व्यवसाय ब्रांड जागरूकता पैदा करने, कनेक्टिविटी बढ़ाने और कुछ नए और प्रभावी प्लेटफॉर्म पर उत्साह बेचने हेतु इस प्रकार के सोशल मीडिया प्लेटफॉर्म का उपयोग कर सकते हैं। ये चैनल्स कुछ रिलेवन्स सामाजिक तत्वों के माध्यम से ई-कॉमर्स को वेज कर और अधिक आकर्षक बना देते हैं।

सोशल शॉपिंग नेटवर्क के लाभ- ये निम्नवत् हैं-

(i) इन नेटवर्क का प्रभावी ढंग से उपयोग करने हेतु हमें एक ऐसी साइट बनानी चाहिए जो खरीदारी के अनुभव को सामाजिक अनुभव के साथ एकीकृत करे अथवा जुड़े।

(ii) ये नेटवर्क छोटे व्यवसायों और स्टार्टअप के लिए अधिक परिणाम-संचालित हैं क्योंकि ये बिना किसी भूमि-आधारित कार्यालय या स्टोर के अपने प्रोडक्ट बेच सकते हैं।

(8) रूचि-आधारित नेटवर्क- हम समान प्रकार के शौक या रूचि रखने वाले अन्य लोगों से कनेक्ट होने हेतु इस प्रकार के सोशल मीडिया नेटवर्क का उपयोग कर सकते हैं। इसके द्वारा हम उन दर्शकों को आसानी से खोज सकते हैं जो हमारे द्वारा प्रस्तुत किए जाने वाले उत्पादों और सेवाओं के बारे में अधिक से अधिक जानने में रूचि रखते हैं। यह इसे हमारे दर्शकों से जुड़ने (कनेक्ट होने) और ऑनलाइन विशेष ब्रांड जागरूकता (अवेयरनेस) पैदा करने हेतु सबसे अच्छे नेटवर्क में से एक बनाता है। बड़े सामाजिक नेटवर्क की तुलना में, रूचि-आधारित नेटवर्क का उपयोग करने से हमें अधिक लक्षित अभियान चलाने में सहायता मिलेगी।

(i) इन नेटवर्क को चुनने से हमें किसी विशेष विषय से सम्बन्धित केवल एक उत्पाद या सेवा पर ध्यान केन्द्रित करने में सहायता मिलेगी, उदाहरणार्थ- गृह सजावट, डिजिटल मार्केटिंग प्रशिक्षण, संगीत, किताबें, आदि।

(iii) ये नेटवर्क किसी विशेष क्षेत्र के दर्शकों से कनेक्ट होने के लिए सबसे उपयुक्त स्थान हैं।

प्रश्न-4. सोशल मीडिया प्लेटफॉर्म का संक्षेप में वर्णन कीजिये।

अथवा

उत्तर- सोशल मीडिया प्लेटफॉर्म के प्रकार- ये निम्नवत् हैं-

(1) फेसबुक- वर्तमान में इसे मेटा के नाम से जाना जाता है। फेसबुक विश्व में सबसे व्यापक रूप से उपयोग किए जाने वाले सोशल मीडिया ऐस में से एक है। यह ऐप वर्ष 2004 में लॉन्च किया गया था तब यह एक साधारण सोशल नेटवर्क के रूप में शुरू हुआ

था लेकिन अब यह विशाल मार्केटिंग मशीन में बदल गया है। फेसबुक को सक्रिय इंटरनेट प्रोमोशन वाले किसी भी उपकरण, जैसे पीसी, टैबलेट और स्मार्टफोन से एक्सेस किया जा सकता है। हम टेक्स्ट, चित्र और मल्टीमीडिया पोस्ट कर सकते हैं जिससे बाद में अन्य उपयोगकर्ताओं, हमारे दोस्त या यदि हमारे पास अलग-अलग गैपनीयता सेटिंग्स हैं, को सार्वजनिक रूप से शेयर किया जाता है। ब्रांड ऐसी कहानियाँ बताने के लिए टेक्स्ट का उपयोग कर रहे हैं जिन्हें दर्शक पसंद कर रहे हैं। आज ब्रांड, ईवेंट की मेजबानी करने, उत्पाद बेचने, अपने उत्पाद लाइन की घोषणा करने, अपने उत्पादों के बारे में एक एकाउण्ट बनाने और विभिन्न अन्य कार्यों के लिए फेसबुक का उपयोग करते हैं। निःसंदेह डिजिटल क्षेत्र में किसी ब्रांड की सहायता के लिए फेसबुक अति आवश्यक हो गया है।

(3) इंस्टाग्राम- इंस्टाग्राम को इंस्टा के नाम से भी जाना जाता है। यह एक फोटो-शेयरिंग प्लेटफॉर्म है जो एक बड़-स्तरीय संसार मंच बन गया है। इसके माध्यम से ब्रांड और लोग दूसरों के साथ बातचीत करते हैं। आज हम इंस्टाग्राम पर तस्वीरें, कहानियाँ और रीलस शेयर कर सकते हैं। इस चित्र और वीडियो-शेयरिंग सोशल नेटवर्किंग साइट की स्थापना सन् 2010 में केविन सिस्ट्रॉम और माइक केनर द्वारा की गई थी और बाद में इसे फेसबुक द्वारा अधिग्रहित कर लिया गया, जिसे मेटा प्लेटफॉर्म भी कहा जाता है। एक इंस्टाग्राम उपयोगकर्ता के रूप में, हम चित्र और लघु वीडियो अपलोड कर सकते हैं, स्थान के नाम के साथ दूसरों के फीड या जियोटैग छवियों (इमेजेज) का अनुसरण कर सकते हैं। इंस्टाग्राम व्यापक रूप से फ्लॉ हुआ है, विशेषतः उन प्रभावशाली लोगों के बीच जो आजीविका कमाने के लिए ऐप का उपयोग करते हैं। हजारों फॉलोअर्स जुटाकर, प्रभावशाली लोग ब्रांडों के लिए काम करने के लिए उनका लाभ उठाते हैं। प्रभावशाली लोगों की शुरुआत इंस्टाग्राम से हुई और अन्य ऐस ने उनका अनुसरण (फॉलो) किया।

(3) स्नैपचैट- स्नैपचैट आज उपलब्ध नए सोशल मीडिया ऐस में से एक है। अमेरिका स्थित स्नैप इंक ने स्नैपचैट को एक मेसेजिंग ऐप और संसाधन के रूप में विकसित किया है। स्नैपचैट की एक मुख्य विशेषता इसमें यह है कि फोटो और संदेश केवल थोड़े समय के लिए दिखाई देते हैं। स्नैपचैट पीयर-टू-पीयर फोटो शेयरिंग पर ध्यान केन्द्रित करने से लेकर उपयोगकर्ता की 'कहानियों' की विशेषता तक बढ़ गया है। इसमें एक 'डिस्कवर' सुविधा भी है, जो ब्रांडों को विज्ञापन द्वारा समर्थित संक्षिप्त रूप वाली सामग्री दिखाने की सुविधा देती है। स्नैपचैट एंड-टू-एंड एंक्रिप्शन का भी उपयोग करता है, इसके उपयोग का विस्तार करने की योजना है। स्नैपचैट सोशल मीडिया के लिए एक नई, मोबाइल-फर्स्ट दिशा दिखाने के लिए जाना जाता है। ब्रांड अपने दर्शकों के साथ बातचीत करने के लिए स्नैपचैट का उपयोग करते हैं। यह बहुत प्रभावी है और आज की डिजिटल आबादी द्वारा उपयोग किए जाने वाले लोकप्रिय सोशल मीडिया ऐस के बीच इसने अपनी जड़ें जमा ली हैं।

(4) लिंक्डइन- लिंक्डइन एक पेशेवर सोशल नेटवर्किंग साइट है। यह अन्य सोशल नेटवर्किंग साइट्स से बिल्कुल अलग है क्योंकि यह चिन्तों और वीडियो पर ध्यान केन्द्रित नहीं करती और न ही इसमें कोई 'कहानी' सुविधा है। यह अमेरिकी व्यापार और नौकरी-उन्मुख सेवा वेबसाइट और मोबाइल ऐप फॉर्म पर उपलब्ध है। यह ऐप मई 2003 में लॉन्च किया

गया था। मुख्य रूप से यह क्राइट-कॉलर नेटवर्किंग और नौकरी विकास के लिए उपयोग किया जाता है। इस पर नौकरी के इच्छुक अपना बायोडाटा अपलोड कर सकते हैं, और नियोजता नौकरियाँ पोस्ट कर सकते हैं। लिंक्डइन को दिसम्बर 2016 से, माइक्रोसॉफ्ट द्वारा खरीद लिया गया है।

(5) ट्विटर- ट्विटर एक माइक्रोब्लॉगिंग और सोशल नेटवर्किंग प्लेटफॉर्म है। रजिस्टर्ड उपयोगकर्ता 'ट्वीट्स' के साथ पोस्ट और इंटरैक्ट करते हैं। प्लेटफॉर्म उपयोगकर्ताओं को ट्वीट पोस्ट करने, लाइक करने या रीट्वीट करने की भी परमिशन देता है, जबकि अनरजिस्टर्ड उपयोगकर्ता सार्वजनिक ट्वीट पढ़ सकते हैं। ट्विटर उन लोगों के बीच काफी लोकप्रिय है जो ऑनलाइन बयान देना पसंद करते हैं।

ट्विटर में ट्वीट करने की 280-अक्षरों की लिमिट होती है। लेकिन अक्सर यह लिमिट सामान्य ट्विटर उपयोगकर्ता के लिए पर्याप्त होती है। ट्विटर जुलाई 2006 में लॉन्च किया गया था। अब यह उपयोगकर्ताओं को वीडियो या इमेजेंस शेयर करने और दूसरों द्वारा पोस्ट की गई सामग्री को लाइक करने की परमिशन देता है। ट्विटर सभी आयु वर्ग के लोगों विशेषतः एलोन मस्क, बिल गेट्स जैसी मशहूर हस्तियों और फिलिपी सितारों और एथलीटों के बीच लोकप्रिय है।

(6) व्हाट्सएप- स्मार्टफोन के आने के बाद से व्हाट्सएप भारतीयों के बीच अत्यन्त लोकप्रिय हो गया है। लाखों भारतीय अपने प्रियजनों के साथ सम्पर्क में रहने, चुटकुले अग्रहित करने, समाचार प्राप्त करने और बहुत कुछ करने के लिए इस मैसेजिंग प्लेटफॉर्म का उपयोग करते हैं। व्हाट्सएप का एक और लाभ यह है कि सभी बातचीत एंक्रिप्टेड हैं, जिसका आशय है कि हमारे पास पूरी गोपनीयता है, चाहे हम इस ऐप का उपयोग कभी भी और कहीं भी करें। इसके अलावा व्हाट्सएप मैसेंजर अन्ताराष्ट्रीय स्तर पर उपलब्ध है और क्रॉस-कंट्री संचार का समर्थन करता है। व्हाट्सएप ने हाल ही में, व्हाट्सएप भुगतान ऐप भी लॉन्च किया है जिसके उपयोग से ग्राहक एक-दूसरे को पैसे भेजा करते हैं।

(7) टेलीग्राम- टेलीग्राम विश्व स्तर पर उपलब्ध मल्टी-प्लेटफॉर्म क्लाउड-आधारित इंस्टेंट मैसेजिंग ऐप को संदर्भित करता है। इसके द्वारा हमें एंक्रिप्टेड चैट, वीडियो कॉलिंग, फाइल शेयरिंग और अन्य सुविधाएँ मिलती हैं। टेलीग्राम उस समय व्हाट्सएप के विकल्प के रूप में सामने आया जब व्हाट्सएप गोपनीयता सम्बन्धी समस्याओं का सामना कर रहा था। संगठनों से शुरू होकर, टेलीग्राम शीघ्र ही व्यक्तिगत उपयोगकर्ताओं के बीच बहुत लोकप्रिय हो गया। टेक्स्ट और वॉयस मैसेज और वॉयस और वीडियो कॉल के अतिरिक्त, उपयोगकर्ता असीमित इमेजेंस, दस्तावेज, स्थान, ऑडियो फाइलें और स्टिकर शेयर कर सकते हैं। टेलीग्राम अपने लॉन्च के बाद से, अपने प्लेटफॉर्म पर उपयोगकर्ताओं की संख्या में वृद्धि कर रहा है।

(8) मौज- यह डवर बैंगलुरु स्थित मोहल्ला टेक प्राइवेट लिमिटेड के स्वामित्व वाली एक सोशल नेटवर्किंग सेवा है। मौज सोशल मीडिया ऐप उपयोगकर्ताओं को अन्य चीजों के अलावा विशेष प्रभावों, इमोटिकॉन्स और स्टिकर के साथ लघु वीडियो बनाने की अनुमति देता है। डवर उपयोगकर्ता वीडियो डाउनलोड कर सकते हैं। यह ऐप 15 भाषाओं का

समर्थन करता है। टिकटॉक के दिन होने के लगभग तुरंत बाद रिलीज हुए इस ऐप के मात्र छह महीने में ही 100 मिलियन यूजरर्स हो गए।

(9) शेयरचैट- शेयरचैट एक प्रमुख भारतीय सोशल मीडिया प्लेटफॉर्म है जो उपयोगकर्ताओं को अपनी राय साझा (शेयर) करने, अपने जीवन का दस्तावेजीकरण करने और अपनी मूल भाषा में नये दोस्त बनाने की अनुमति देता है। भारत की इंटरनेट क्रॉसिंग का नेतृत्व करने के मिशन पर अग्रसर शेयरचैट अपने प्लेटफॉर्म में चेज कर रहा है जिससे आगे अरब उपयोगकर्ता इंटरनेट पर बातचीत कर सकें।

प्रश्न-5. हैशटैग पर संक्षिप्त टिप्पणी लिखिये।  
उत्तर- हैशटैग- हैशटैग # प्रतीक के बाद आने वाले वे शब्द और संख्याएँ हैं जो सोशल मीडिया पर सामग्री को वर्गीकृत और ट्रैक करते हैं। आप इंस्टाग्राम, फेसबुक, टिकटॉक, ट्विटर, लिंक्डइन, यूट्यूब और पिन्टरेस्ट सहित अधिकांश प्रमुख प्लेटफॉर्म पर सामाजिक नेट, बायोस और टिप्पणियों में हैशटैग जोड़ सकते हैं।

हैशटैग का उद्देश्य- आज के सोशल मीडिया एल्गोरिथम के नवीनतम परिष्कृत चेंजेज को देखते हुए, 2000 के दशक की शुरुआत के अराजक सामाजिक फ्रीड को याद रखना मुश्किल हो सकता है। उस समय हैशटैग के उपयोगकर्ताओं के पास इस बात पर सीमित नियंत्रण था कि उन्हें कौन सी सामग्री देखना है और वे अत्यधिक अलविचार या अप्रसंगिक नेट से निराश थे। हैशटैग का आविष्कार सोशल मीडिया उपयोगकर्ता (यूजर) के अनुभव को सुव्यवस्थित करने में सहायता हेतु किया गया था।

हैशटैग समान वार्तालापों को एक साथ समूहित (ग्रुपिंग) करते हैं ताकि लोगों को उनके लिए महत्वपूर्ण सामग्री ढूँढने में मदद मिल सके। एक बार हैशटैग प्रकाशित होने के बाद, यह एक क्लिक करने योग्य, खोजने योग्य क्लिक बन जाता है।

प्रश्न-6. निम्नलिखित पर टिप्पणी लिखिये-  
(1) वायरल सामग्री (2) सोशल मीडिया मार्केटिंग।

उत्तर- (1) वायरल सामग्री- वायरल सामग्री ऑनलाइन सामग्री है जो सोशल मीडिया नेटवर्क, समाचार वेबसाइटों, एप्लीकेशंस, ईमेल न्यूजलेटर्स और खोज (सर्व) इंजनों पर शेयर और एक्सपोजर के कारण उच्च स्तर की जागरूकता प्राप्त करती है। वायरल सामग्री का एक टुकड़ा आपकी वेबसाइट पर महत्वपूर्ण यात्रा में बांड जागरूकता और ट्रैफिक उत्पन्न कर सकता है।

वायरल सामग्री वह सामग्री है जो कुछ ही घंटों में इंटरनेट पर व्यापक रूप से साझा (शेयर) की जाती है। दूसरे शब्दों में, यह वह सामग्री है जो बहुत जल्दी लोकप्रिय हो जाती है। मीम्स से लेकर समाचार लेखों तक, किसी भी प्रकार की सामग्री वायरल हो सकती है।

वायरल सामग्री किसी कम्पनी या उपयोगकर्ता के सभी संचार (कम्युनिकेशन) हैं जो वायरल हो जाते हैं। इसे बड़ी संख्या में उपयोगकर्ताओं द्वारा विभिन्न डिजिटल चैनल्स पर साझा (शेयर) किया जाता है। यह रणनीति तब काम करती है जब कम्पनी द्वारा प्रेषित संदेश, उदाहरण के लिए कम्पनी से अधिक प्रासंगिक हो जाता है।

वायरल सामग्री के पीछे का उद्देश्य हमारे लक्षित दर्शकों के अलावा अन्य लोगों से जुड़ना होता है। हालांकि, गैर उन लोगों के साथ घुमना शुरू कर देती है जो हमारे पोस्ट या

चित्र साक्षात्कार करते हैं। इसका अर्थ है कि हमें उन प्रशंसकों और अनुयायियों को प्रभावित करने के लिए वायरल सामग्री बनाने की आवश्यकता है।

(2) सोशल मीडिया मार्केटिंग- सोशल मीडिया मार्केटिंग किसी उत्पाद या सेवा को बढ़ावा देने के लिए सोशल मीडिया प्लेटफॉर्म और वेबसाइटों का उपयोग है। हालांकि 'ई-मार्केटिंग' और 'डिजिटल मार्केटिंग' शब्द अभी भी शिक्षा जगत में प्रभावी हैं। सोशल मीडिया मार्केटिंग अभ्यासकर्ताओं और शोधकर्ताओं, दोनों के लिए अधिक लोकप्रिय हो रही है। अधिकांश सोशल मीडिया प्लेटफॉर्म ने अन्तर्निहित डेटा एनालिटिक्स टूल होते हैं, जो कम्पनियों को विज्ञापन अभियानों की प्रगति, सफलता और सहभागिता को ट्रैक करने में सक्षम बनाते हैं। कम्पनियाँ सोशल मीडिया मार्केटिंग के माध्यम से वर्तमान और संभावित ग्राहकों, वर्तमान और संभावित कर्मचारियों, पत्रकारों, ब्लॉगर्स और आम जनता सहित कई हितधारकों को सम्बोधित करती हैं, जैसे- रणनीतिक स्तर पर, सोशल मीडिया मार्केटिंग में एक मार्केटिंग अभियान का प्रबंधन, प्रशासन तथा वायरा निर्धारित करना।

सोशल मीडिया मार्केटिंग का उपयोग करते समय, कम्पनियाँ ग्राहकों और इंटरनेट उपयोगकर्ताओं को उपयोगकर्ता-जनित सामग्री दे सकती हैं, जिसे मार्केटिंग-तैयार विज्ञापन प्रति का उपयोग करने के बजाय 'अर्जित मीडिया' भी कहा जाता है।

प्रश्न-7. सोशल मीडिया प्राइवसी के बारे में आप क्या जानते हैं? संक्षेप में लिखिये।

जवाब- सोशल मीडिया प्राइवसी- सोशल मीडिया गोपनीयता से तात्पर्य उस व्यक्तिगत और संवेदनशील जानकारी से है जिसे लोग आपके खातों (एकाउन्ट्स) से आपके बारे में जान सकते हैं। यह जानकारी जानबूझकर साक्षात् (शेयर) की जा सकती है या अनजाने में साक्षात् की जा सकती है।

सामान्य सोशल मीडिया गोपनीयता मुद्दे- उपयोगकर्ता के सोशल मीडिया खातों (एकाउन्ट्स) पर बड़ी मात्रा में डेटा के साथ, जालसाज उपयोगकर्ताओं की जासूसी करने, पहचान चुराने और जालसाजी का प्रयास करने के लिए पर्याप्त जानकारी पा सकते हैं। डेटा सुरक्षा के मुद्दे और गोपनीयता नियंत्रण में खामियाँ सोशल मीडिया का उपयोग करते समय उपयोगकर्ता की जानकारी को खतरे में डाल सकती हैं। अन्य सोशल मीडिया गोपनीयता मुद्दों में निम्नलिखित शामिल हैं-

(1) पहचान की चोरी के लिए डेटा माइनिंग- किसी की पहचान चुराने के लिए जालसाजों को बहुत अधिक जानकारी की आवश्यकता नहीं होती है। वे लक्षित (Targeted) पीड़ितों की मदद के लिए सोशल मीडिया पर सार्वजनिक रूप से उपलब्ध जानकारी से शुरुआत कर सकते हैं। उदाहरण के लिए, रैंकर्स फिशिंग जालसाजी वाले उपयोगकर्ताओं को लक्षित करने के लिए उपयोगकर्ता के नाम, पते, ईमेल पते और फोन नम्बर एकत्र कर सकते हैं। यहाँ तक कि ईमेल पते या फोन नम्बर से भी, एक जालसाज अधिक जानकारी पा सकता है, जैसे लीक हुए पासवर्ड, सामाजिक सुरक्षा नम्बर और क्रेडिट कार्ड नम्बर।

(2) गोपनीयता सेंटिंग खामियाँ- सोशल मीडिया अकाउंट उतने निजी नहीं हो सकते जितना कि उपयोगकर्ता सोचते हैं। उदाहरण के लिए, यदि किसी उपयोगकर्ता ने अपने किसी मित्र के साथ कुछ साक्षात् (शेयर) किया है और उन्होंने उसे दोबारा पोस्ट किया है, तो मित्र के

मित्र भी जानकारी देख सकते हैं। मूल उपयोगकर्ता की दोबारा पोस्ट की गई जानकारी अब पूरी तरह से अलग दर्शकों के सामने है। यहाँ तक कि बन्द समूह भी पूरी तरह से निजी नहीं हो सकते क्योंकि पोस्टिंग को किसी भी टिप्पणी सहित खोजा (सर्व किया) जा सकता है।

(3) स्थान सेंटिंग- स्थान ऐप सेंटिंग अभी भी उपयोगकर्ता के टिकटों को ट्रैक कर सकती है। यहाँ तक कि अगर कोई अपनी स्थान सेंटिंग बन्द कर देता है, तो भी डिवाइस के स्थान को लक्षित (टारगेट) करने के अन्य तरीके हैं। सार्वजनिक वाई-फाई, सेलफोन टॉवरों और वेबसाइटों के उपयोग से भी उपयोगकर्ता के स्थानों को ट्रैक किया जा सकता है। अतः हमेशा यह परीक्षण करें कि जीपीएस स्थान सेवाएँ बन्द हैं कि नहीं और ट्रैक किए जाने से बचने के लिए वीपीएन के माध्यम से ब्राउज करें।

व्यक्तिगत जानकारी के साथ जोड़ा गया उपयोगकर्ता स्थान उपयोगकर्ता प्रोफाइल को सटीक जानकारी प्रदान कर सकता है। बुरे अभिनेता इस डेटा का उपयोग उपयोगकर्ताओं को शीक रूप से डूँढ़ने (सर्व करने) या उनकी आदतों के बारे में डिजिटल रूप से अधिक जानने के लिए भी कर सकते हैं।

(4) जल्डून और साइबरबुलिंग- सोशल मीडिया का इस्तेमाल साइबरबुलिंग के लिए किया जा सकता है। बुरे कलाकारों को धमकी भरे संदेश या भावनात्मक संकट पैदा करने के लिए किसी के खाते (एकाउन्ट) में जाने की जरूरत नहीं है। उदाहरण के लिए, सोशल मीडिया अकाउंट वाले बच्चों को अनुचित टिप्पणियों वाले सहपाठियों की प्रतिक्रिया का सामना करना पड़ता है।

बुक्सिंग- यह साइबरबुलिंग का ही एक रूप है। इसमें बुरे अभिनेता जानबूझकर किसी व्यक्ति को चुकसाने पट्टुवाने के लिए उसके बारे में व्यक्तिगत साक्षात् (शेयर) करते हैं, जैसे किसी व्यक्ति का पता या फोन नम्बर। वे दूसरों को इस व्यक्ति को परेशान करने के लिए प्रोत्साहित करते हैं।

(5) गलत जानकारी- लोग सोशल मीडिया पर तेजी से दुष्प्रचार को फैला सकते हैं। ट्रेल पावनाओं में हेरफेर करके अन्य उपयोगकर्ताओं को तीखी बहस के लिए उकसाने का भी प्रयास करते हैं। अधिकांश सोशल मीडिया प्लेटफॉर्म पर सामग्री मॉडरेशन दिशा-निर्देश हैं, लेकिन पोस्ट को चिन्हित करने में समय लग सकता है। सोशल मीडिया पर कुछ भी भेजने या उस पर विश्वास करने से पहले जानकारी की दोबारा जाँच कर लें।

(6) मैलवेयर और वायरस- सोशल मीडिया प्लेटफॉर्म का उपयोग मैलवेयर वितरित करने के लिए किया जा सकता है, जो कम्प्यूटर को धीमा कर सकता है, विज्ञापनों के साथ उपयोगकर्ताओं पर हमला कर सकता है और संवेदनशील डेटा चुरा सकता है। साइबर अपराधी सोशल मीडिया अकाउंट पर कब्जा कर लेते हैं और प्रभावित अकाउंट और उपयोगकर्ता के सभी दोस्तों और सम्पर्कों को मैलवेयर वितरित करते हैं।

# पर्यायिक प्रश्न

संकाई-1

- (1) वेब पेज का एक नई विसे मिलक करने पर दूसरा डायरेक्ट खुलता है, वह है-
- (अ) रेफरेन्स  
(ब) URL  
(स) हाइपरलिंक  
(द) एंकर
- उत्तर- (स) हाइपरलिंक।
- (2) इंटरनेट बैंकिंग का क्या अर्थ है?
- (अ) इंटरनेट के जरिए बैंकिंग  
(ब) नेट पर बैंकों की बैठक  
(स) विदेशों के साथ संव्यवहार  
(द) उपर्युक्त सभी।
- उत्तर- (स) विदेशों के साथ संव्यवहार।
- (3) HTML का पूरा नाम है-
- (अ) हाइपर ट्रांसफर मेल लैंग्वेज  
(ब) हाइपर टेक्स्ट मार्क अप लैंग्वेज  
(स) हाईटेक मेल लैंग्वेज  
(द) उपर्युक्त में से कोई नहीं।
- उत्तर- (ब) हाइपर टेक्स्ट मार्क अप लैंग्वेज।
- (4) वेब पेज किसका उपयोग करता है?
- (अ) सर्वर  
(ब) वर्कशीट  
(स) वर्क बुक  
(द) एच.टी.टी.पी. (HTTP)
- उत्तर- (द) एच.टी.टी.पी. (HTTP)
- (5) सैम निम्न में से क्या है?
- (अ) अन सॉलिसिटेड ई-मेल  
(ब) इनकीमिंग ई-मेल  
(स) डिजिट हेतु ई-मेल  
(द) उपर्युक्त में से कोई नहीं।
- उत्तर- (अ) अन सॉलिसिटेड ई-मेल।
- (6) वह डिवाइज कौन-सी है जो वा वा से अधिक नेटवर्कों को जोड़ता है?
- (अ) रोडवे  
(ब) बस  
(स) नेटवे  
(द) उपर्युक्त में से कोई नहीं।
- उत्तर- (स) नेटवे।
- (7) ई-मेल भेजते समय सर्वोत्तम की लाइन किसकी विषय-वस्तु बताती है?
- (अ) संदेश  
(ब) कंटेंट्स  
(स) टू  
(द) CC
- उत्तर- (अ) संदेश।
- (8) इंटरनेट का पूरा नाम क्या है?
- (अ) इंटरनल नेटवर्क  
(ब) इंटरनेशनल नेटवर्क  
(स) इंटरएक्टिव नेटवर्क  
(द) इंटरनेशनल नेटवर्क।
- उत्तर- (ब) इंटरनेशनल नेटवर्क।

2024

डिजिटल जगत्कता - साइबर सुरक्षा

109

- (9) कम्प्यूटर को इंटरनेट से जोड़ने में सहायता करता है-
- (अ) केवल  
(ब) ब्राउजर  
(स) वेब  
(द) नेट।
- उत्तर- (ब) ब्राउजर।
- (10) .com डोमेन का सम्बन्ध है-
- (अ) व्यापारिक संस्था  
(ब) सूचना से सम्बन्धित  
(स) व्यक्ति से सम्बन्धित  
(द) उपर्युक्त सभी।
- उत्तर- (अ) व्यापारिक संस्था।
- (11) .org का सम्बन्ध है-
- (अ) शिक्षा से  
(ब) संगठन से  
(स) व्यापार से  
(द) उपर्युक्त सभी।
- उत्तर- (ब) संगठन से।
- (12) भारत में इंटरनेट की शुरुआत कब से हुई?
- (अ) 8 अगस्त 1995 से  
(ब) 9 अगस्त 1995 से  
(स) 15 अगस्त 1995 से  
(द) उपर्युक्त में से कोई नहीं।
- उत्तर- (स) 15 अगस्त 1995 से।
- (13) ई-मेल का पूरा नाम क्या है?
- (अ) इलेक्ट्रॉनिक मेल  
(ब) इलेक्ट्रिक मेल  
(स) उपर्युक्त (अ) और (ब) दोनों  
(द) उपर्युक्त में से कोई नहीं।
- उत्तर- (अ) इलेक्ट्रॉनिक मेल।
- (14) वेबसाइट का एड्रेस कहलाता है-
- (अ) URL  
(ब) Web  
(स) User ID  
(द) उपर्युक्त सभी।
- उत्तर- (अ) URL
- (15) www से प्रारंभ होने वाला पता किससे सम्बन्धित है?
- (अ) इंटरनेट से  
(ब) वेबसाइट से  
(स) मॉडेम से  
(द) उपर्युक्त में से कोई नहीं।
- उत्तर- (ब) वेबसाइट से।
- (16) मॉडेम कहलाता है-
- (अ) मोड्यूलर डिस्कशन  
(ब) मोड्यूलर डिमोड्यूलर  
(स) मोड्यूलर डिमोड्यूलर  
(द) उपर्युक्त सभी।
- उत्तर- (ब) मोड्यूलर डिमोड्यूलर।
- (17) ई-मेल भेजना किसके समान है?
- (अ) पत्र लिखना  
(ब) कहानी लिखना  
(स) घटना का चित्र खींचना  
(द) उपर्युक्त में से कोई नहीं।
- उत्तर- (अ) पत्र लिखना।

(18) URL का पूरा नाम है-

- (अ) Uniform Resource Line (ब) Union Resource Line  
(स) Uniform Resource Locator (द) उपर्युक्त में से कोई नहीं।

(19) LAN का पूरा नाम है-

- (अ) Line Area Network (ब) Lower Area Network  
(स) Local Area Network (द) उपर्युक्त सभी।

(20) डोमेन के नामाकरण में शैक्षणिक संस्थाओं के लिए किसका प्रयोग होता है?

- (अ) .du (ब) .mil  
(स) .org (द) .com

(21) सबसे लोकप्रिय इंटरनेट गतिविधि कौन-सी है?

- (अ) सर्चिंग (ब) शॉपिंग  
(स) संप्रेषण (द) शोध।

(22) डोमेन के नामांकन में सरकारी संस्थाओं के लिए किस संकेत का प्रयोग होता है?

- (अ) .com (ब) .gov  
(स) .net (द) .edu

(23) DNS क्या है?

- (अ) डोमेन नेम सिस्टम (ब) डोमेन रेजिस्ट्रेशन सिस्टम  
(स) डोमेन ड्राइविंग नेम सिस्टम (द) उपर्युक्त सभी।

(24) यूजर नेम है-

- (अ) कम्प्यूटर का उपयोग करने वाले का नाम  
(ब) लॉजिंग के लिए इंटरनेट एकाउंटधारी का नाम  
(स) शॉपिंग के लिए कम्प्यूटरधारी का नाम  
(द) उपर्युक्त सभी।

उत्तर- (द) उपर्युक्त सभी।

(25) इंटरनेट एड्रेस किस प्रकार प्राप्त करते हैं?

- (अ) कम्प्यूटर विक्रेता के द्वारा (ब) कम्प्यूटर क्रेता के द्वारा  
(स) बैकबोन सर्विस प्रोवाइडर के द्वारा (द) उपर्युक्त में से कोई नहीं।

उत्तर- (स) बैकबोन सर्विस प्रोवाइडर के द्वारा।

(26) इंटरनेट पर मौजूद विभिन्न सुविधाओं का उपयोग करने की अनुमति कौन देता है?

- (अ) रूटर (ब) गेटवे

(स) सर्विस प्रोवाइडर

उत्तर- (ब) गेटवे।

(37) सर्वर है-

- (अ) सेवा करने वाला कम्प्यूटर  
(ब) एक विशेष प्रकार की सेवा प्रदान करने वाला सॉफ्टवेयर  
(स) उपर्युक्त (अ) और (ब) दोनों (द) उपर्युक्त में से कोई नहीं।

उत्तर- (ब) एक विशेष प्रकार की सेवा प्रदान करने वाला सॉफ्टवेयर।

(38) ई-मेल का जन्मदाता है-

- (अ) टिमोथी (ब) लिकन गोलिड्सबर्ग  
(स) रेटामलिसन (द) उपर्युक्त में से कोई नहीं।

उत्तर- (स) रेटामलिसन।

(39) सैम का सम्बन्ध है-

- (अ) संगीत (ब) कम्प्यूटर  
(स) रिजर्व (द) उपर्युक्त सभी।

उत्तर- (ब) कम्प्यूटर।

(40) इंटरनेट पर सर्वर से सूचना पाने वाले कम्प्यूटर के प्रोसेस को कहते हैं-

- (अ) डाउनलोडिंग (ब) पुशिंग  
(स) ट्रांसफरिंग (द) उपर्युक्त सभी।

उत्तर- (अ) डाउनलोडिंग।

(41) WWW. के प्रवर्तक एवं आविष्कारक हैं-

- (अ) टिमवर्नर्सली (ब) एन. रसेल  
(स) ली. एन. फियोव (द) उपर्युक्त में से कोई नहीं।

उत्तर- (अ) टिमवर्नर्सली।

(42) गुगल, याहू तथा MSN है-

- (अ) कम्प्यूटर विधि (ब) इंटरनेट साइट्स  
(स) कम्प्यूटर धारी (द) उपर्युक्त में से कोई नहीं।

उत्तर- (ब) इंटरनेट साइट्स।

(43) WWW. का पूरा नाम है-

- (अ) विंडोवल्ड वाइड (ब) वेब वर्किंग विंडो  
(स) वर्ल्डवाइड वेब (द) उपर्युक्त सभी।

उत्तर- (स) वर्ल्डवाइड वेब।

(44) वेब पेज को रीलोड करने के लिए कौन-सी की ब्रानी चाहिए?

- (अ) रिस्टोर (ब) रीहू  
(स) रिक्रेश (द) रीलोड।

उत्तर- (स) रिक्रेश

(45) वेब पर सूचना देखने के लिए आवश्यक है-

- (अ) वेब ब्राउजर (ब) डोमेन नें सर्वर  
(स) हाइपर टेक्स्ट ट्यूबर (द) मॉडम।

उत्तर- (अ) वेब ब्राउजर।

(46) इंटरनेट है-

- (अ) नेटवर्क का बड़ा नेटवर्क (ब) आन्तरिक संग्रहण-प्रणाली  
(स) सरकारी संग्रहण-प्रणाली (द) उपर्युक्त सभी।

उत्तर- (अ) नेटवर्क का बड़ा नेटवर्क।

(47) एक कम्प्यूटर से इंटरनेट पर कम्प्यूटर में फाइल अंतरण करने वाली प्रक्रिया को कहा जाता है?

- (अ) अपलोड (ब) डाउनलोड  
(स) एक टीपी (द) साईजिंग।

उत्तर- (ब) डाउनलोड।

(48) वेबसाइट में होम पेज का अर्थ है-

- (अ) प्रथम पेज (ब) अंतिम पेज  
(स) सबसे अच्छा पेज (द) उपर्युक्त में से कोई नहीं।

उत्तर- (अ) प्रथम पेज।

(49) URL क्या है?

- (अ) प्रोग्रामिंग ऑब्जेक्ट का एक प्रकार (ब) ई-मेल पते के दो भाग  
(ब) वर्ल्डवाइड वेब पर डॉक्यूमेंट का एड्रेस (द) उपर्युक्त में से कोई नहीं।

(स) कम्प्यूटर सॉफ्टवेयर (द) उपर्युक्त सभी।

उत्तर- (ब) वर्ल्डवाइड वेब पर डॉक्यूमेंट का एड्रेस।

(50) मोडेम का सम्बन्ध किससे होता है?

- (अ) मोडेम (ब) फोन लाइन  
(स) रिसीवर (द) इनबॉक्स।

उत्तर- (ब) फोन लाइन।

(51) यूजर नेम और डोमेन नेम है-

- (अ) इनीशियल और पासवर्ड (ब) ई-मेल पते के दो भाग  
(स) विधिक नाम और फोन (द) उपर्युक्त में से कोई नहीं।

उत्तर- (ब) ई-मेल पते के दो भाग।

(52) ब्राउजर का कार्य होता है-

- (अ) विषय-सामग्री को तेजी से पढ़ता है (ब) ई-मेल पते के दो भाग  
(ब) पुस्तकालय में पत्र एवं पत्रिकाओं को पढ़ता है। (द) उपर्युक्त में से कोई नहीं।

(स) यह वेब पेज देखने के लिए प्रयुक्त एक सॉफ्टवेयर है

(द) उपर्युक्त में से कोई नहीं।

उत्तर- (स) यह वेब पेज देखने के लिए प्रयुक्त एक सॉफ्टवेयर है।

(53) जंक ई-मेल को क्या कहते हैं?

- (अ) स्पैम (ब) फ़िकट  
(स) क्रेप (द) उपर्युक्त सभी।

उत्तर- (अ) स्पैम।

(54) आई.पी. (I.P.) का पूरा नाम है-

- (अ) इंकरजेट प्रिंटर (ब) इंटरनेशन प्रोटोकॉल  
(स) इंडियन प्रोटोकॉल (द) इंटरनेट प्रोटोकॉल।

उत्तर- (द) इंटरनेट प्रोटोकॉल।

(55) इंटरनेट एड्रेस है-

- (अ) इंटरनेट का पता (ब) सॉफ्टवेयर कम्पनी का पता  
(स) TCP/IP के जरिए सूचना के आदान-प्रदान के लिए कम्प्यूटरों को आवंटित संख्या (द) उपर्युक्त में से कोई नहीं।

(द) उपर्युक्त में से कोई नहीं।

(स) TCP/IP के जरिए सूचना के आदान-प्रदान के लिए कम्प्यूटरों को आवंटित संख्या।

उत्तर- (स) TCP/IP के जरिए सूचना के आदान-प्रदान के लिए कम्प्यूटरों को आवंटित संख्या।

(56) ISP का पूरा नाम क्या है?

- (अ) इंटरनेट सर्विस प्रोवाइडर (ब) इंटरनेशनल सर्विस  
(स) इंडियन सर्विस प्रोवाइडर (द) उपर्युक्त में से कोई नहीं।

(द) उपर्युक्त में से कोई नहीं।

उत्तर- (अ) इंटरनेट सर्विस प्रोवाइडर।

(57) ISP का क्या कार्य है?

- (अ) प्रसारण करना (ब) उपयोक्ता को इंटरनेट लिंक प्रदान करना  
(स) उपयोक्ता का पंजीकृत करना (द) उपर्युक्त में से कोई नहीं।

(द) उपर्युक्त में से कोई नहीं।

(ब) उपयोक्ता को इंटरनेट लिंक प्रदान करना।

उत्तर- (ब) उपयोक्ता को इंटरनेट लिंक प्रदान करना।

(58) निम्न में से कौन-सा ई-मेल का भाग नहीं है?

- (अ) Space ( ) (ब) Period (.)  
(स) Ai sign (@) (द) उपर्युक्त में से कोई नहीं।

उत्तर- (अ) Space ( )

(59) इंटरनेट प्रोटोकॉल का क्या कार्य है?

- (अ) डाटा ब्लॉक को छोटे-छोटे डाटा पैकेट में बाँटना (ब) डाटा पैकेट पर मंजिल को पता-सम्बन्धी सूचना लगाना  
(स) उपर्युक्त (अ) और (ब) दोनों (द) उपर्युक्त में से कोई नहीं।

(द) उपर्युक्त में से कोई नहीं।

(ब) डाटा पैकेट पर मंजिल को पता-सम्बन्धी सूचना लगाना।

उत्तर- (ब) डाटा पैकेट पर मंजिल को पता-सम्बन्धी सूचना लगाना।

(60) इंटरनेट एक्सचेंजर जैसे प्रोग्रामों को क्या कहते हैं जो वेब में नेविगेशन विंडो का कार्य करते हैं?

- (अ) इंटरनेट (ब) वेब ब्राउजर  
(स) नेटवर्क (द) हाइपरटेक्स्ट।  
उत्तर- (ब) वेब ब्राउजर।

### इकाई-2

(1) चेक जारी करने की तारीख के बाद की तारीख ..... होती है।

- (अ) उत्तर दिनांकित चेक (ब) खाली चेक  
(स) रेखांकित चेक (द) अक्राउन्ट पेयी चेक।

उत्तर- (अ) उत्तर दिनांकित चेक।

(2) चेक जारी होने की तारीख से पहले की तारीख ..... होती है।

- (अ) पूर्व दिनांकित चेक (ब) पूर्ण मूल्य चेक  
(स) प्रीसेटिव चेक (द) जाँच के लायक।

उत्तर- (अ) पूर्व दिनांकित चेक।

(3) एक दरज ..... भी हो सकती है।

- (अ) पेयी. (ब) भुगतानकर्ता  
(स) बैंकर (द) ऋणदाता।

उत्तर- (अ) पेयी.

(4) वह दर जिस पर RBI स्वीकृत विनिमय बिल पर छूट देता है उसे ..... कहते हैं।

- (अ) बैंक दर (ब) ब्याज दर  
(स) विनिमय दर (द) छूट दर।

उत्तर- (द) छूट दर।

(5) ..... ने भारतीय बैंकों में कंप्यूटीकरण पर समिति (1988) का नेतृत्व किया।

- (अ) एम. नरसिंह (ब) एम.एम. शाह  
(स) एम. वेंकट राम (द) राज फोस्टर।

उत्तर- (अ) एम. नरसिंह।

(6) वर्ड बैंक एक लैटिन शब्द से लिया गया है जिसका अर्थ है .....।

- (अ) धन रखने, उधार देने और विनिमय आदि के लिए एक पीठ  
(ब) लोगों से मिलने-जुलने की संस्था  
(स) स्थान, जहाँ व्यक्ति आराम कर सके  
(द) लोगों के समन्वय के लिए एक संस्था।

उत्तर- (अ) धन रखने, उधार देने और विनिमय आदि के लिए एक पीठ।

(7) एक कम्पनी जो भांग जमा स्वीकार करती है उसे ..... कहा जाता है।

- (अ) बैंकिंग कम्पनी (ब) संपुत्र स्टॉक कम्पनी  
(स) विनिर्माण कम्पनी (द) आई.टी. कम्पनी।

उत्तर- (अ) बैंकिंग कम्पनी।

(8) ग्राहणधिकार ..... है।

- (अ) ग्राहकों की सम्पत्ति पर शुल्क बनाने की विधि  
(ब) सम्बन्धित ग्राहकों के खातों के लिए उपयोग नहीं की जाती है  
(स) ऋण के लिए उपयोग नहीं किया गया  
(द) ऋण के लिए उपयोग किया गया।

उत्तर- (अ) ग्राहकों की सम्पत्ति पर शुल्क बनाने की विधि।

(9) एक रुपये के नोट पर ..... के हस्ताक्षर होते हैं।

- (अ) भारत के राष्ट्रपति  
(ब) भारत के प्रधानमंत्री  
(स) भारतीय रिजर्व बैंक के गवर्नर  
(द) सचिव, वित्त मंत्रालय (भारत सरकार)

उत्तर- (अ) भारत के राष्ट्रपति

(10) छोटा सिक्का डिग्री ..... की सम्पत्ति है।

- (अ) भारतीय स्टेट बैंक (ब) भारत सरकार  
(स) भारतीय रिजर्व बैंक (द) भारतीय बैंक।

उत्तर- (ब) भारत सरकार।

(11) एक बैंकिंग कम्पनी जिसका लाइसेंस रद्द कर दिया गया है वह ..... के पास

- (अ) उच्च न्यायालय (ब) सुप्रीम कोर्ट  
(स) आरबीआई (द) केन्द्र सरकार।

उत्तर- (ब) भारत सरकार।

(12) भारत में ऋण का नियंत्रण कौन करता है?

- (अ) भारत सरकार (ब) आरबीआई  
(स) एसबीआई (द) इंडियन बैंक।

उत्तर- (द) केन्द्र सरकार।

(13) कृषि उद्देश्यों के लिए आरबीआई अनुदान ..... कहलाता है।

- (अ) केवल अल्पकालिक वित्त (ब) आरबीआई  
(ब) मध्यम और दीर्घकालिक वित्त (द) इंडियन बैंक।

उत्तर- (ब) आरबीआई।

(14) कृषि वित्त में सर्वोच्च संस्था ..... है।

- (अ) केवल अल्पकालिक वित्त (ब) मध्यम और दीर्घकालिक वित्त  
(स) केवल लघु और मध्यम अवधि का वित्त  
(द) लघु, मध्यम और दीर्घकालिक वित्त।

उत्तर- (स) केवल लघु और मध्यम अवधि का वित्त।

(15) कृषि वित्त में सर्वोच्च संस्था ..... है।

- (अ) नाबार्ड (ब) एक्जिम बैंक  
(स) आरबीआई (द) आईडीबीआई।

उत्तर- (अ) नाबार्ड।

(16) कृषि वित्त में सर्वोच्च संस्था ..... है।

- (अ) नाबार्ड (ब) एक्जिम बैंक  
(स) आरबीआई (द) आईडीबीआई।

उत्तर- (अ) नाबार्ड।

- (15) विकास बैंक वे संस्थाएँ हैं जो .....।  
 (अ) विकास ऋण देते हैं  
 (ब) बैंकों के आपातकालीन ऋण प्रदान करते हैं  
 (स) आरबीआई की सहायक कम्पनियाँ हैं  
 (द) उद्योगों को सावधि वित्त प्रदान करते हैं।  
 उत्तर- (ब) बैंकों के आपातकालीन ऋण प्रदान करते हैं।
- (16) IFCI की स्थापना ..... में हुई थी।  
 (अ) 1947 (ब) 1948  
 (स) 1951 (द) 1956.  
 उत्तर- (ब) 1948
- (17) IFCI का पंजीकृत कार्यालय ..... में है।  
 (अ) मुम्बई (ब) चेन्नई  
 (स) नई दिल्ली (द) कोलकाता।  
 उत्तर- (ब) चेन्नई।
- (18) राष्ट्रीय औद्योगिक विकास निगम लिमिटेड की स्थापना ..... में हुई थी।  
 (अ) 1954 (ब) 1955  
 (स) 1956 (द) 1964  
 उत्तर- (अ) 1954
- (19) LIC की स्थापना ..... में की गई थी।  
 (अ) 1948 (ब) 1951  
 (स) 1956 (द) 1964  
 उत्तर- (स) 1956
- (20) ICICI को ..... में शामिल किया गया था।  
 (अ) 1948 (ब) 1955  
 (स) 1956 (द) 1964  
 उत्तर- (ब) 1955
- (21) परक्राम्य लिखतों को ..... के अन्तर्गत परिभाषित किया गया है।  
 (अ) बैंकिंग विनियमन अधिनियम, 1949 की धारा 52  
 (ब) भारतीय रिजर्व बैंक अधिनियम, 1934 की धारा 25  
 (स) परक्राम्य लिखत अधिनियम, 1881 की धारा 13  
 (द) कम्पनी अधिनियम, 1956 की धारा 14।  
 उत्तर- (स) परक्राम्य लिखत अधिनियम, 1881 की धारा 13।
- (22) वचन पत्र पर मुख्य रूप से कौन उत्तरदायी है?  
 (अ) होल्डर (ब) निर्माता  
 (स) अदाकर्ता (द) समर्थनकर्ता।  
 उत्तर- (ब) निर्माता।

- (23) एक चेक रूग्णशा ..... को देय होता है।  
 (अ) एक मांग  
 (ब) एक निर्दिष्ट भविष्य की तारीख  
 (स) अनुग्रह का अन्तिम दिन  
 (द) भुगतान करने वाले बैंकर की वसीयत।  
 उत्तर- (अ) एक मांग।
- (24) एक वचन पत्र ..... है।  
 (अ) सेटों में निकाला जा सकता है  
 (ब) सेटों में नहीं निकाला जा सकता  
 (स) क्षतिपूर्ति बांड भी आवश्यक है  
 (द) क्षतिपूर्ति बांड आवश्यक नहीं है।  
 उत्तर- (ब) सेटों में नहीं निकाला जा सकता।
- (25) एक वचन पत्र में शब्द या क्रम ..... होते हैं।  
 (अ) डालना आवश्यक है  
 (ब) डालना आवश्यक नहीं है  
 (स) आवश्यक नहीं है लेकिन  
 (द) डालना सामान्य है। आवश्यक है। यह सामान्य है।  
 उत्तर- (स) आवश्यक नहीं है लेकिन।
- (26) विनिमय का विल ..... देय निकाला जा सकता है।  
 (अ) मांग पर याहक को  
 (ब) या तो मांग पर या एक निश्चित समय के बाद  
 (स) उपस्थिति में याहक को  
 (द) उपस्थिति में नहीं रखने वाले को।  
 उत्तर- (ब) या तो मांग पर या एक निश्चित समय के बाद।
- (27) जब तक कोई विनिमय विल स्वीकार नहीं किया जाता, तब तक उस पर प्राथमिक दायित्व ..... का होता है।  
 (अ) पेयी (ब) ड्रावी  
 (स) दराज (द) स्वीकर्ता।  
 उत्तर- (स) दराज।
- (28) विनिमय का विल अधिकतम ..... अवधि के लिए निकाला जाता है।  
 (अ) 90 दिन (ब) 120 दिन  
 (स) 180 दिन (द) 360 दिन।  
 उत्तर- (स) 180 दिन।
- (29) HDFC का फुल फॉर्म ..... है।  
 (अ) हाउसिंग डेवलपमेंट फाइनेंस कॉर्पोरेशन  
 (ब) हाउसिंग डेवलपमेंट फाइनेंस कंपनी

- (स) हाउसिंग डेवलपमेंट फाइनेंस को-ऑपरेटिव  
(स) हाउसिंग डेवलपमेंट फाइनेंस क्युमुनिटी।  
उत्तर- (अ) हाउसिंग डेवलपमेंट फाइनेंस कॉरपोरेशन।
- (30) अंतरिती को परक्राम्य लाभ .....।  
(अ) वही शीर्षक  
(स) कोई बेहतर शीर्षक नहीं  
उत्तर- (द) बेहतर शीर्षक।
- (31) ..... एक मूल वेक है।  
(अ) पोस्ट डेटेड चेक  
(स) दिनांकित चेक  
उत्तर- (ब) बासी चेक।
- (32) RBI का तात्पर्य ..... से है।  
(अ) भारतीय रिजर्व बैंक  
(स) भारतीय रुपया बैंक  
उत्तर- (अ) भारतीय रिजर्व बैंक।
- (33) उस व्यक्ति को क्या कहा जाता है जिसे चेक को राशि देय है।  
(अ) एक दराज  
(स) अदाकर्ता  
उत्तर- (स) अदाकर्ता।
- (34) कौन सा निजी बैंक है?  
(अ) एसबीआई  
(स) आईओबी  
उत्तर- (ब) यूटीआई।
- (35) व्यापारिक समुदाय के लिए सबसे उपयुक्त जमा राशि ..... है।  
(अ) बचत जमा  
(स) सावधि जमा  
उत्तर- (ब) चालू जमा।
- (36) प्रतिज्ञा ..... के सम्बन्ध में की जा सकती है।  
(अ) एक इमारत  
(स) मोटर कार  
उत्तर- (ब) शेयर।
- (37) एक संश्लेषकर्ता बैंकर को वैधानिक सुरक्षा तभी दी जाती है जब वह ..... के रूप में कार्य करता है।  
(अ) एक धारक  
(स) मूल्य के लिए एक धारक  
उत्तर- (द) नियत समय में एक धारक।

- (38) सीमा का कानून बचत जमा खाते पर ..... की तारीख से लागू होता है।  
(अ) इसे खोलने  
(स) इसकी मांग कर रहे हैं  
उत्तर- (अ) इसे खोलने।
- (39) सबसे अधिक तरल सभ्यति ..... है।  
(अ) सोना  
(स) सरकारी बॉन्ड  
उत्तर- (द) नकद।
- (40) IBA के अनुसार अधिकतम अवधि जिसके लिए सावधि जमा प्राप्त किया जा सकता है .....।  
(अ) कोई सीमा नहीं  
(स) 7 वर्ष  
उत्तर- (स) 7 वर्ष।
- (41) सेट-ऑफ का अधिकार एक ..... के अलावा और कुछ नहीं है।  
(अ) बेचने का अधिकार  
(स) मिलापने का अधिकार  
उत्तर- (स) मिलापने का अधिकार।
- (42) विनिमय बिलों की छूट ..... है।  
(अ) स्वच्छ अग्रिम  
(स) न तो स्वच्छ अग्रिम और न ही सुरक्षित अग्रिम  
(द) असुरक्षित अग्रिम।  
उत्तर- (स) न तो स्वच्छ अग्रिम और न ही सुरक्षित अग्रिम।
- (43) रिपस्ट का विस्तार ..... है।  
(अ) विश्वव्यापी अन्तर बैंक वित्तीय दूरसंचार के लिए सोसायटी  
(ब) विश्वव्यापी अन्तर बैंक वित्तीय दूरसंचार के लिए सुरक्षा  
(स) विश्वव्यापी अन्तर बैंक वित्तीय दूरसंचार के लिए सुरक्षित  
(द) विश्वव्यापी अन्तर बैंक वित्तीय दूरसंचार के लिए असुरक्षा।  
उत्तर- (अ) विश्वव्यापी अन्तर बैंक वित्तीय दूरसंचार के लिए सोसायटी।
- (44) NEFT का विस्तार ..... है।  
(अ) राष्ट्रीय इलेक्ट्रॉनिक फंड ट्रांसफर  
(ब) न्यूट्रल इलेक्ट्रॉनिक फंड ट्रांसफर  
(स) नाममात्र इलेक्ट्रॉनिक फंड ट्रांसफर  
(द) प्राकृतिक इलेक्ट्रॉनिक फंड ट्रांसफर।  
उत्तर- (अ) राष्ट्रीय इलेक्ट्रॉनिक फंड ट्रांसफर।
- (45) EFT ..... का विस्तार।  
(अ) इलेक्ट्रॉनिक फंड ट्रांसफर  
(ब) आर्थिक फंड ट्रांसफर

- (स) यूरोपीय फंड ट्रांसफर (द) इलेक्ट्रिक फंड ट्रांसफर।
- उत्तर- (अ) इलेक्ट्रॉनिक फंड ट्रांसफर।
- (46) आईटीजीएस प्रणाली एक वर्ष में ..... दिन काम करती है।  
 (अ) 365 (ब) 362  
 (स) 300 (द) 305.
- उत्तर- (ब) 362.
- (47) KYC का अर्थ है .....।  
 (अ) अपने ग्राहक को जानने (ब) अपने ऋणदाता को जानने  
 (स) अपनी लागत जानने (द) अपना कार्ड जानने।
- उत्तर- (अ) अपने ग्राहक को जानने।
- (48) ISO प्रमाणपत्र पाने वाला भारत का पहला बैंक .....।  
 (अ) SBI (ब) केनरा बैंक  
 (स) भारत का केन्द्रीय बैंक (द) इंडियन बैंक।
- उत्तर- (ब) केनरा बैंक।
- (49) भारत के बाहर शाखा खोलने वाला पहला भारतीय बैंक ..... है।  
 (अ) बैंक ऑफ इंडिया (ब) इलाहाबाद बैंक  
 (स) साउथ इंडियन बैंक (द) इंडियन बैंक।
- उत्तर- (अ) बैंक ऑफ इंडिया।
- (50) RTGS का अर्थ है .....।  
 (अ) रियल टर्न ग्रॉस सेटलमेंट (ब) वास्तविक समय सकल निपटान  
 (स) वास्तविक तकनीक सकल निपटान (द) सकल निपटान की ओर वास्तविक।
- उत्तर- (ब) वास्तविक समय सकल निपटान।
- (51) बैंक कम्प्यूटीकरण का अध्ययन करने ..... की अभ्यक्षता में गई थी।  
 (अ) डॉ. सी. रामचन्द्रन (ब) डॉ. सी. राघवेंद्र  
 (स) डॉ. सी. राजा राजन (द) डॉ. सी. रंगराजन।
- उत्तर- (द) डॉ. सी. रंगराजन।
- (52) किस प्रणाली में कम्प्यूटर केन्द्रीकृत प्रसंस्करण अवधारणा पर आधारित होते हैं?  
 (अ) प्रोसेसिंग कम्प्यूटर सिस्टम (ब) स्टैण्ड-अलोन कम्प्यूटर नेटवर्किंग  
 (स) मल्टी-यूजर कम्प्यूटर नेटवर्किंग (द) फ्रेम कम्प्यूटर सिस्टम।
- उत्तर- (स) मल्टी-यूजर कम्प्यूटर नेटवर्किंग।
- (53) ग्राहक इंटरफेस ..... स्तर पर अधिकतम होता है।  
 (अ) शाखा (ब) आंचलिक

- (स) प्रधान कार्यालय (द) राज्य कार्यालय।
- उत्तर- (ब) आंचलिक।
- (54) बैंक का मुख्य कार्यालय ..... के लिए निर्भर करता है।  
 (अ) केवल बैंक-स्तरीय योजना (ब) केवल बैंक-स्तरीय योजना, नियंत्रण कार्य  
 (स) बैंक स्तरीय योजना, नियंत्रण कार्य और नीति निर्णय (द) केवल शाखाओं को सेवाएँ।
- उत्तर- (स) बैंक स्तरीय योजना, नियंत्रण कार्य और नीति निर्णय।
- (55) कोर बैंकिंग एक ..... शाखा कम्प्यूटीकरण मॉडल है।  
 (अ) एटीएम (ब) केन्द्रीकृत  
 (स) एकीकृत (द) विकेन्द्रीकृत।
- उत्तर- (द) विकेन्द्रीकृत।
- (56) भारत में कम्प्यूटीकरण का उद्देश्य ..... है।  
 (अ) अर्थव्यवस्था पर नियंत्रण रखें (ब) कार्य-जीवन को अधिक सार्थक बनाएं  
 (स) जनशक्ति पर नियंत्रण रखें (द) मनुष्य के स्थान पर मशीनें लाएं।
- उत्तर- (द) मनुष्य के स्थान पर मशीनें लाएं।
- (57) एटीएम का उपयोग मुख्य रूप से ..... कार्य करने के लिए किया जाता है।  
 (अ) बुनियादी ढांचा (ब) कम्प्यूटर आधारित  
 (स) बैंकिंग (द) असताल में भर्ती।
- उत्तर- (स) बैंकिंग।
- (58) 1990 के दशक की शुरुआत में, किस प्रकार के एटीएम भारत में बिबाई किए?  
 (अ) बहु-उपयोगकर्ता एटीएम (ब) नेटवर्क एटीएम  
 (स) शाखा एटीएम (द) स्टैण्ड-अलोन एटीएम।
- उत्तर- (द) स्टैण्ड-अलोन एटीएम।
- (59) ईसीएस का विस्तार ..... है।  
 (अ) इलेक्ट्रॉनिक समाशोधन प्रणाली (ब) इलेक्ट्रॉनिक केन्द्रीय प्रणाली  
 (स) इलेक्ट्रॉनिक क्रॉस सिस्टम (द) इलेक्ट्रॉनिक रूपान्तरण सिस्टम।
- उत्तर- (अ) इलेक्ट्रॉनिक समाशोधन प्रणाली।
- (60) EFT की शुरुआत ..... द्वारा की गई।  
 (अ) IRDA (ब) RBI  
 (स) सेबी (द) NSE.
- उत्तर- (ब) RBI.
- (61) कितने सार्वजनिक क्षेत्र के बैंकों के पास ईएफटी सुविधा उपलब्ध है?  
 (अ) 25 (ब) 27

- (स) 28 (द) 30  
 उत्तर- (ब) 27
- (62) कितने अनुसूचित वाणिज्यिक बैंकों के पास इण्टेटी सुविधा उपलब्ध है?  
 (अ) 35 (ब) 45 (स) 55 (द) 65  
 उत्तर- (स) 55
- (63) इण्टेटी सुविधा कितने केन्द्रों पर उपलब्ध है?  
 (अ) 14 केन्द्र (ब) 15 केन्द्र  
 (स) 16 केन्द्र (द) 18 केन्द्र  
 उत्तर- (ब) 15 केन्द्र।
- (64) व्यक्तिगत लेनदेन की राशि पर कोई इण्टेटी सीमा?  
 (अ) कोई सीमा नहीं (ब) रु. 5,00,000  
 (स) रु. 50,00,000 (द) 25,00,000  
 उत्तर- (अ) कोई सीमा नहीं।
- (65) ..... एक ऐसी तकनीक है जो आपको मोबाइल डिवाइस से अपने बैंक खाते तक पहुँचने की अनुमति देती है।  
 (अ) होम बैंकिंग (ब) मोबाइल बैंकिंग  
 (स) इंटरनेट बैंकिंग (द) टेलीविजन बैंकिंग  
 उत्तर- (ब) मोबाइल बैंकिंग।
- (66) सूचना प्रौद्योगिकी के अनुप्रयोग से क्या संभव हुआ?  
 (अ) दिनांक खनन (ब) दिनांक भंडारण  
 (स) डेटाबेस (द) समर्थन प्रणाली।  
 उत्तर- (ब) दिनांक भंडारण।
- (67) ..... डेटा वेयरहाउस में छिपी रणनीतिक जानकारी को प्रकट करने की एक तकनीक है।  
 (अ) डेटा बेस (ब) डेटा वेयरहाउसिंग  
 (स) डेटा माइनिंग (द) सपोर्ट सिस्टम।  
 उत्तर- (स) डेटा माइनिंग।
- (68) ..... ग्राहकों के बारे में जनसांख्यिकीय जानकारी है जो बैंकों को विशेष खंडों पर ध्यान केंद्रित करने में मदद करती है।  
 (अ) डेट माइनिंग (ब) डेट वेयरहाउसिंग  
 (स) डेटा विश्लेषण (द) सपोर्ट सिस्टम।  
 उत्तर- (स) डेटा विश्लेषण।
- (69) ..... प्रतिभूतियों के एक सेट के प्रदर्शन और प्रतिभूतियों को जारी करने वाली कम्पनियों के मौलिक डेटा का विश्लेषण करना है।  
 (अ) दिनांक खनन (ब) दिनांक भंडारण  
 (स) डेटा विश्लेषण

- (द) स्टॉक पोर्टफोलियो निर्माण और विश्लेषण।  
 (स) डेटा विश्लेषण।  
 उत्तर- (स) डेटा विश्लेषण।
- (70) आर्बीआई को बैंकिंग और वित्त पर डेटा वेयरहाउस स्थापित करने की सिकरिया कितने की?  
 (अ) डॉ. रंगराजन ने (ब) एम.एम. शाह ने  
 (स) एम. वेंकट राम ने (द) वासुदेवन ने।  
 उत्तर- (द) वासुदेवन ने।
- (71) EDI के लिए मानकों के सार्वभौमिक सेट को ..... के रूप में जाना जाता है।  
 (अ) ईडीआई (ब) एडिकैड  
 (स) आईएसओ (द) बीआईएस।  
 उत्तर- (ब) एडिकैड।
- (72) सेवार प्रौद्योगिकी .....।  
 (अ) डेटा के प्रसंस्करण की सुविधा प्रदान करता है।  
 (ब) डेटा के प्रसारण में मदद करता है  
 (स) निर्माण समर्थन प्रणाली को सक्षम बनाता है  
 (द) डेटा माइनिंग का एक उपकरण है।  
 उत्तर- (ब) डेटा के प्रसारण में मदद करता है।
- (73) भारत का दुनिया भर में ईडीआई सेवाओं का प्रवेश द्वार कैमसा है?  
 (अ) सत्यम ऑनलाइन (ब) बीएसएनएल  
 (स) एमटीएनएल (द) बीएसएनएल।  
 उत्तर- (द) बीएसएनएल।
- (74) भारत में SHIFT नेटवर्क कब आया?  
 (अ) 1 दिसम्बर, 1991 (ब) 2 दिसम्बर, 1991  
 (स) 3 दिसम्बर, 1991 (द) 4 दिसम्बर, 1991  
 उत्तर- (ब) 2 दिसम्बर, 1991
- (75) सिस्फ्ट में कितनी मानक संदेश श्रेणियाँ हैं?  
 (अ) 10 प्रकार (ब) 9 प्रकार  
 (स) 8 प्रकार (द) 7 प्रकार।  
 उत्तर- (ब) 9 प्रकार।
- (76) बैंकिंग परिचालन ..... कार्यालय के माध्यम से किया जाता है।  
 (अ) शाखा बैंकिंग (ब) यूनिट बैंकिंग  
 (स) वाणिज्यिक बैंकिंग (द) यूनिवर्सल बैंकिंग।  
 उत्तर- (ब) यूनिट बैंकिंग।
- (77) शाखाओं के नेटवर्क के माध्यम से किए जाने वाले बैंकिंग कार्यों को ..... कहा जाता है।  
 (अ) शाखा बैंकिंग (ब) यूनिट बैंकिंग

- (स) वाणिज्यिक बैंकिंग  
(द) यूनिवर्सल बैंकिंग।
- उत्तर- (अ) शाखा बैंकिंग।
- (78) वह बैंकिंग जो केवल अल्प अवधि के लिए जमा और आधार को आकर्षित करती है, ..... के रूप में जानी जाती है।  
(अ) वाणिज्यिक बैंकिंग  
(ब) यूनिट बैंकिंग  
(स) शाखा बैंकिंग  
(द) विकास बैंकिंग।
- उत्तर- (अ) वाणिज्यिक बैंकिंग।
- (79) जमा बैंकिंग को ..... भी कहा जाता है।  
(अ) वाणिज्यिक बैंकिंग  
(ब) यूनिट बैंकिंग  
(स) शाखा बैंकिंग  
(द) विकास बैंकिंग।
- उत्तर- (अ) वाणिज्यिक बैंकिंग।
- (80) भारत में प्रत्येक अनुसूचित बैंक को आरबीआई के पास सभी जमा देनदारियों के बराबर नकद शेष रखना होता है जिसे ..... कहा जाता है।  
(अ) खुला बाजार अनुपात  
(ब) नकद आरक्षित अनुपात  
(स) बैंक आरक्षित अनुपात  
(द) क्रेडिट आरक्षित अनुपात।
- उत्तर- (ब) नकद आरक्षित अनुपात।
- (81) 1969 के दौरान कितने बैंकों का राष्ट्रीयकरण किया गया?  
(अ) 14  
(ब) 15  
(स) 16  
(द) 17
- उत्तर- (ब) 15
- (82) 1980 के दौरान कितने बैंकों का राष्ट्रीयकरण किया गया?  
(अ) 5  
(ब) 6  
(स) 7  
(द) 8
- उत्तर- (ब) 6
- (83) ..... RBI के एजेंट के रूप में कार्य करता है।  
(अ) एसबीआई  
(ब) आईसीआईसीआई  
(स) आईओबी  
(द) एचडीएफसी।
- उत्तर- (ब) आईसीआईसीआई।
- (84) किस समिति ने भारत में निजी क्षेत्र के बैंकों की स्थापना की सिफारिश की?  
(अ) डॉ. रंगराजन समिति  
(ब) नरसिंहरम समिति  
(स) राजेन्द्र समिति  
(द) गोविन्द राजन समिति।
- उत्तर- (अ) डॉ. रंगराजन समिति।
- (85) RBI की स्थापना वर्ष ..... में की गई थी।  
(अ) 1932  
(ब) 1933  
(स) 1934  
(द) 1935

- (86) ..... का गठन एक कॉर्पोरेट निकाय के रूप में किया गया है जिसका प्रायकत उत्तराधिकार और एक सामान्य मुहर है।  
(अ) आरबीआई  
(ब) आईसीआईसीआई  
(स) एचडीएफसी  
(द) आईओबी।
- उत्तर- (अ) आरबीआई।
- (87) भारतीय ..... वह बाजार है जिसमें अल्पवधि धनराशि उधार ली और उधार दी जाती है।  
(अ) मुद्रा बाजार  
(ब) खुला बाजार  
(स) बंद बाजार  
(द) क्रेडिट बाजार।
- उत्तर- (अ) मुद्रा बाजार।
- (88) बिल बाजार सबसे पहले कहाँ विकसित हुआ?  
(अ) यूएसए  
(ब) लंदन  
(स) फ्रांस  
(द) इटली।
- उत्तर- (ब) लंदन।
- (89) एक बैंक का अपने ग्राहक के चेक का भुगतान करने का दायित्व अचलत के आदेश की प्राप्ति पर समाप्त हो जाता है, जिसे ..... के रूप में जाना जाता है।  
(अ) बैंक आदेश  
(ब) गार्निशी आदेश  
(स) आरबीआई आदेश  
(द) देनदार आदेश।
- उत्तर- (ब) गार्निशी आदेश।
- (90) गार्निशी ऑर्डर ..... द्वारा जारी किया गया एक ऑर्डर है।  
(अ) आयकर अधिकारी  
(ब) आधिकारिक परिसमापक  
(स) न्यायालय  
(द) आरबीआई।
- उत्तर- (स) न्यायालय।
- (91) एक निश्चित अवधि के लिए बैंक में जमा राशि, जो जमा करते समय निर्दिष्ट होती है ..... कहलाती है।  
(अ) बचत जमा  
(ब) थालू जमा  
(स) बैंक जमा  
(द) सावधि जमा।
- उत्तर- (द) सावधि जमा।
- (92) वह न्यूनतम अवधि जिसके लिए कोई वाणिज्यिक बैंक सावधि जमा स्वीकार कर सकता है ..... होती है।  
(अ) 7 दिन  
(ब) 15 दिन  
(स) 30 दिन  
(द) 60 दिन।
- उत्तर- (अ) 7 दिन।
- (93) सावधि जमा पर व्याज ..... संयोजित होता है।  
(अ) मासिक  
(ब) त्रैमासिक  
(स) अर्धवार्षिक  
(द) वार्षिक आधार।

उत्तर- (ब) त्रैमासिक।

(94) यदि ग्राहक ..... हो तो बैंकर को खाते का संचालन बंद नहीं करना चाहिए।

- (अ) मर जाता है  
(ब) दिवालिया हो जाता है  
(स) अपना व्यावसायिक परिसर बदल देता है  
(द) पागल हो जाता है।

उत्तर- (स) अपना व्यावसायिक परिसर बदल देता है।

(95) प्लौटिंग व्याज दर बढ़ है जो ..... है।

- (अ) बैंक द्वारा मनमाने ढंग से निर्णय लिया गया  
(ब) किसी अन्य प्रासंगिक दर से जुड़ा हुआ  
(स) भारतीय बैंक संघ द्वारा निर्धारित  
(द) भारतीय रिजर्व बैंक द्वारा अधिसूचित।

उत्तर- (ब) किसी अन्य प्रासंगिक दर से जुड़ा हुआ।

(96) एमआईसीआर ..... को संदर्भित करता है।

- (अ) चुम्बकीय स्याही चरित्र पहचान  
(ब) चुम्बकीय स्याही कम्पनी मान्यता  
(स) चुम्बकीय स्याही क्रॉस मान्यता  
(द) चुम्बकीय स्याही समुदाय मान्यता।

उत्तर- (अ) चुम्बकीय स्याही चरित्र पहचान।

(97) यदि समर्थनकर्ता अपने नाम पर हस्ताक्षर करता है तो केवल समर्थन को ..... कहा जाता है।

- (अ) अपूर्ण समर्थन  
(ब) पूर्ण समर्थन  
(स) संशर्त समर्थन  
(द) प्रतिबंधित समर्थन।

उत्तर- (ब) पूर्ण समर्थन।

(98) ऑफलाइन डेटा प्रविष्टि तब बेहतर होती है जब-

- (अ) डेटा बिना किसी त्रुटि के दर्ज किया जाए  
(ब) दर्ज किए जाने वाले डेटा की मात्रा बड़ी हो  
(स) दर्ज किए जाने वाले डेटा की मात्रा छोटी हो  
(द) सूचना को समय-समय पर संसाधित किया जाए।

उत्तर- (ब) दर्ज किए जाने वाले डेटा की मात्रा बड़ी हो।

(99) चेक पर क्रॉसिंग को कौन रद्द कर सकता है?

- (अ) भुगतानकर्ता  
(ब) भुगतान करने वाला बैंकर  
(स) समर्थनकर्ता  
(द) दराज।

उत्तर- (द) दराज।

(100) चेक प्राप्तकर्ता के लिए क्या संभव नहीं है?

- (अ) विवरर चेक को ऑर्डर चेक में बदलने के लिए

(ब) विशेष रूप से क्रॉस किए गए चेक को आमतौर पर क्रॉस किए गए चेक में बनाना।

(स) सामान्य क्रॉसिंग को विशेष क्रॉसिंग में परिवर्तित करना।

(द) एक खुले चेक को रेखांकित चेक में परिवर्तित करना।

उत्तर- (ब) विशेष रूप से क्रॉस किए गए चेक को आमतौर पर क्रॉस किए गए चेक में बनाना।

(101) एक बैंकर को चेक के भुगतान से इंकार नहीं करना चाहिए यदि .....

- (अ) चेक एक उत्तर दिनांकित चेक है  
(ब) चेक पर दो से अधिक पृष्ठांकन हैं  
(स) चेक में स्पष्ट सामग्री परिवर्तन है जो चेककर्ता द्वारा उचित रूप से प्रमाणित नहीं है  
(द) चेक उसी बैंक की दूसरी शाखा पर काटा गया है।

उत्तर- (ब) चेक पर दो से अधिक पृष्ठांकन हैं।

(102) समान स्वीकारकर्ता .....

- (अ) उस पर कोई दायित्व नहीं है क्योंकि वह विधेयक में पक्षकार नहीं है।  
(ब) उस व्यक्ति के समान दायित्व वहन करता है जिसके समान के लिए वह बिल स्वीकार करता है।  
(स) अदाकर्ता के प्रति जमानतद्वारा के रूप में कार्य करता है  
(द) कोई दायित्व नहीं है।

उत्तर- (ब) उस व्यक्ति के समान दायित्व वहन करता है जिसके समान के लिए वह बिल स्वीकार करता है।

(103) चेक अनावर का कारण .....

- (अ) दराज के हस्ताक्षर भूल जाओ  
(ब) अधूरा चेक  
(स) खाते में धन की अपर्याप्तता  
(द) कोई भी मौलिक परिवर्तन।

उत्तर- (स) खाते में धन की अपर्याप्तता।

(104) REPO सुविधा का अर्थ है .....

- (अ) बिना सुरक्षा के पैसा उधार लेना  
(ब) गारंटी के आधार पर उधार लेना  
(स) सावधि ऋण के बदले उधार लेना  
(द) पुनर्बरीद के आधार पर प्रतिभूतियों के बदले उधार लेना।

उत्तर- (द) पुनर्बरीद के आधार पर प्रतिभूतियों के बदले उधार लेना।

(105) बैंकों के लिए कुल पूंजी बाजार एक्सपोजर ..... का 40 प्रतिशत निर्धारित है।

- (अ) निवल मूल्य  
(ब) कुल समय और मांग देनदारियाँ

- (स) कुल निवेश  
(द) एक बैंकिंग कम्पनी की कुल सम्पत्ति।
- उत्तर- (अ) निवल मूल्य।
- (106) एस्वीआई का विस्तार ..... होता है।  
(अ) भारतीय स्टेट बैंक (ब) भारतीय प्रतिभूति बैंक  
(स) भारत का स्टॉक ब्रोकिंग (द) सोसायटी बैंक ऑफ इंडिया।
- उत्तर- (अ) भारतीय स्टेट बैंक।
- (107) एक परक्राम्य लिखत जो भारत में निर्मित या तैयार नहीं किया गया है उसे ..... लिखत कहा जाता है।  
(अ) अन्तर्देशीय (ब) विदेशी  
(स) समय (द) स्वच्छ।
- उत्तर- (ब) विदेशी।
- (108) एक सावधि ऋण ..... द्वारा सुरक्षित नहीं होता है।  
(अ) अचल सम्पत्तियों का कानूनी बंधक (ब) माल की गिरवी  
(स) चल सम्पत्ति का दृष्टिबंधन, सांथिक बंधक (द) सांथिक बंधक।
- उत्तर- (ब) माल की गिरवी।
- (109) बैंकिंग विनियमन अधिनियम की धारा 19(बी) के अनुसार, एक बैंक किसी कम्पनी में ..... से अधिक शेयर नहीं रख सकता है।  
(अ) 20 प्रतिशत (ब) 25 प्रतिशत  
(स) 30 प्रतिशत (द) 35 प्रतिशत।
- उत्तर- (स) 30 प्रतिशत।
- (110) बुल्किट डिमांड ड्राफ्ट जारी करने के लिए केला को क्या जमा करना आवश्यक है?  
(अ) किसी तीसरे पक्ष की गारंटी (ब) संपार्थिक सुरक्षा  
(स) क्षतिपूर्ति बांड (द) भुगतानकर्ता से वचनबद्धता।
- उत्तर- (स) क्षतिपूर्ति बांड।
- (111) लॉकर किराए पर लेने वाले और बैंकर के बीच का संबंध ..... का है।  
(अ) प्रिंसिपल और एजेंट (ब) पट्टेदार और पट्टेदार  
(स) देनदार और लेनदार (द) गिरवी रखने वाला और गिरवी रखने वाला।
- उत्तर- (स) देनदार और लेनदार।
- (112) एक क्रेडिट कार्ड धारक खरीदारी के लिए ..... भुगतान करता है।  
(अ) 15 दिन बाद (ब) 20 दिन बाद  
(स) एक महीने बाद (द) तुरंत अपने खते के माध्यम से।
- उत्तर- (द) तुरंत अपने खते के माध्यम से।

- (113) क्रेडिट सूचना रिपोर्ट में ..... शामिल है।  
(अ) एक सिकारिश (ब) पुनर्भुगतान के बारे में गारंटी  
(स) क्रेडिट निर्णय (द) उधारकर्ता कम्पनी के शेयरों की हमीदारी।
- उत्तर- (स) क्रेडिट निर्णय।
- (114) क्रेडिट सूचना कम्पनी द्वारा बैंक को दी गई क्रेडिट जानकारी का उपयोग ..... किया जा सकता है।  
(अ) किसी भी उद्देश्य के लिए  
(ब) अपनी वार्षिक रिपोर्ट में प्रकाशन के लिए  
(स) क्रेडिट निर्णय लेने के लिए  
(द) उधारकर्ता कम्पनी के शेयरों की हमीदारी के लिए।
- उत्तर- (स) क्रेडिट निर्णय लेने के लिए।
- (115) बैंकिंग विनियमन अधिनियम वर्ष ..... में पारित किया गया था।  
(अ) 1934 (ब) 1946  
(स) 1949 (द) 1948
- उत्तर- (स) 1949
- (116) आईसीआईसीआई का विस्तार ..... है।  
(अ) इंडस्ट्रियल क्रेडिट एंड इन्वेस्टमेंट कॉर्पोरेशन ऑफ इंडिया  
(ब) इंडस्ट्रियल क्रेडिट एंड इन्वेस्टमेंट कम्पनी ऑफ इंडिया  
(स) भारत का औद्योगिक ऋण और निवेश सहयोग  
(द) भारतीय औद्योगिक ऋण एवं बीमा निगम।
- उत्तर- (अ) इंडस्ट्रियल क्रेडिट एंड इन्वेस्टमेंट कॉर्पोरेशन ऑफ इंडिया।
- (117) उपभोक्ता क्रेडिट व्यूरो ..... द्वारा प्राप्त क्रेडिट को करार करता है।  
(अ) व्यक्ति (ब) निजी और सार्वजनिक लिमिटेड कम्पनियाँ  
(स) स्थानिय संबंधी विंताएँ (द) बैंक।
- उत्तर- (अ) व्यक्ति।
- (118) एक बैंकर और ग्राहक के बीच ..... संबंध है।  
(अ) एक देनदार और लेनदार का  
(ब) एक लेनदार और देनदार का  
(स) मुख्य रूप से देनदार और क्रेडिट का  
(द) देनदार और एजेंट का।
- (119) बैंकर का ..... पर ग्रहणाधिकार है।  
(अ) वसूली के लिए दिए गए बांड  
(ब) सुरक्षित अभिरक्षा के लिए दिए गए बांड

- (स) गलती से छूट गए बांड  
(द) सुरक्षित रखने के लिए दिए गए बांड।  
उत्तर- (अ) वसूली के लिए दिए गए बांड।  
(120) बैंकर का ग्राहकों के प्रति वैधानिक वायित्व है कि वे .....।  
(अ) ग्राहकों के चेक का सम्मान करें  
(ब) व्यापम ग्रहणाधिकार  
(स) अपने ग्राहकों के खातों की गोपनीयता बनाए रखें  
(द) ग्राहकों के बिलों का सम्मान करें।  
उत्तर- (अ) ग्राहकों के चेक का सम्मान करें।  
(121) ..... कोई भौतिक परिवर्तन नहीं है।  
(अ) क्रॉसिंग का परिवर्तन  
(ब) भुगतान के स्थान में परिवर्तन  
(स) रिक्त पृष्ठांकन को पूर्ण पृष्ठांकन में बदलना  
(द) भुगतानकर्ता के नाम में परिवर्तन।  
उत्तर- (स) रिक्त पृष्ठांकन को पूर्ण पृष्ठांकन में बदलना।  
(122) भुगतान करने वाले बैंकर को भौतिक रूप से परिवर्तित चेक के लिए सुरक्षा मिल सकती है, बशर्ते .....।  
(अ) परिवर्तन स्पष्ट नहीं है  
(ब) वह उचित समय पर भुगतान करता है  
(स) परिवर्तन सारहीन है  
(द) (अ) और (ब) एक साथ।  
उत्तर- (द) (अ) और (ब) एक साथ।  
(123) क्रॉसिंग का सबसे सुरक्षित तरीका ..... है।  
(अ) सामान्य क्रॉसिंग  
(ब) विशेष क्रॉसिंग  
(स) धोखा देना  
(द) ए/सी आवता क्रॉसिंग।  
उत्तर- (द) ए/सी आवता क्रॉसिंग।  
(124) पृष्ठांकन यह दर्शाता है कि .....।  
(अ) समर्थनकर्ता को एक अछा शीर्षक मिला है  
(ब) समर्थनकर्ता के हस्ताक्षर वास्तविक हैं  
(स) पिछले समर्थन वास्तविक है  
(द) उपरोक्त सभी।  
उत्तर- (द) उपरोक्त सभी।  
(125) ई-बैंकिंग में सबसे बड़ी बाधा ..... है।  
(अ) स्टार्ट-अप लागत  
(स) प्रशिक्षण लागत  
(द) स्टार्ट-अप लागत।  
(ब) रखरखाव लागत  
(द) सुरक्षा लागत।

- (126) क्रेडिट कार्ड ..... प्रदान करता है।  
(अ) निश्चित अवधि के लिए परिक्रामी क्रेडिट  
(ब) कार्ड के उपयोग की पूरी राशि का भुगतान करें  
(स) कार्ड उपयोग की राशि की ऑनलाइन वसूली  
(द) केवल राशि।  
उत्तर- (अ) निश्चित अवधि के लिए परिक्रामी क्रेडिट।  
(127) डेबिट कार्ड ..... प्रदान करता है।  
(अ) निश्चित अवधि के लिए परिक्रामी क्रेडिट  
(ब) कार्ड के उपयोग की पूरी राशि का भुगतान करें  
(स) कार्ड उपयोग की राशि की ऑनलाइन वसूली  
(द) केवल राशि।  
उत्तर- (स) कार्ड उपयोग की राशि की ऑनलाइन वसूली।  
(128) मोबाइल बैंकिंग निम्नलिखित प्रदान करती है-  
(अ) भारत में कहीं भी नकदी की निकासी  
(ब) एक विशिष्ट अवधि के लिए खाते का विवरण  
(स) एक खाते से दूसरे खाते में धनराशि का स्थानान्तरण  
(द) बैलेंस पूछताछ।  
उत्तर- (द) बैलेंस पूछताछ।  
(129) मॉबैट बैंकर ..... है।  
(अ) वित्तीय दलाल  
(ब) वित्तीय मध्यस्थ  
(स) क्रेडिट मूल्यांकक  
(द) हमीदार।  
उत्तर- (ब) वित्तीय मध्यस्थ।  
(130) मॉबैट बैंकरों की गतिविधि ..... से संबंधित है।  
(अ) इक्विटी और इक्विटी संबंधित वित्त  
(ब) ऋण और ऋण संबंधी वित्त  
(स) फंड व्यवसाय  
(द) गैर-विधि व्यवसाय।  
उत्तर- (अ) इक्विटी और इक्विटी संबंधित वित्त।  
(131) चेक ..... पर देय है।  
(अ) मांग  
(ब) उपयोग  
(स) भविष्य की तारीख तय करने  
(द) दर्शन के बाद।  
उत्तर- (अ) मांग।  
(132) ..... नीलापी स्थल का एक उदाहरण है।  
(अ) ई.वे.  
(ब) इक्विबो  
(स) फेसबुक  
(द) ऑर्कुट।  
उत्तर- (अ) ई.वे.।

(133) डेबिट कार्ड केवल ..... है।

- (अ) इलेक्ट्रॉनिक कार्ड निकासी और जमा दोनों उद्देश्यों के लिए
- (ब) इलेक्ट्रॉनिक कार्ड केवल दुकान के प्रयोजन के लिए
- (स) इलेक्ट्रॉनिक कार्ड केवल निकासी प्रयोजन के लिए
- (द) इलेक्ट्रॉनिक कार्ड केवल जमा प्रयोजन के लिए

उत्तर- (अ) इलेक्ट्रॉनिक कार्ड निकासी और जमा दोनों उद्देश्यों के लिए।  
(134) ई-कैश का आशय है-

- (अ) एक नेटवर्क पर विभिन्न पार्टियों के बीच धन हस्तांतरित करना।
- (ब) एक नेटवर्क पर विभिन्न पार्टियों के बीच चेक स्थानांतरित करना।
- (स) एक नेटवर्क पर विभिन्न पार्टियों के बीच पैसा जमा करना।
- (द) एक नेटवर्क पर विभिन्न पार्टियों के बीच क्रेडिट जांच करना।

उत्तर- (अ) एक नेटवर्क पर विभिन्न पार्टियों के बीच धन हस्तांतरित करना।  
(135) सुरक्षित इलेक्ट्रॉनिक लेनदेन प्रोटोकॉल का उपयोग ..... के लिए किया जाता है।

- (अ) क्रेडिट कार्ड से भुगतान
- (ब) चेक से भुगतान
- (स) इलेक्ट्रॉनिक नकद भुगतान
- (द) इंटरनेट सेवाओं के लिए छोटी राशि के भुगतान।

उत्तर- (स) इलेक्ट्रॉनिक नकद भुगतान।  
(136) सिफ्ट में ..... डिजिटल कोड नम्बर होता है?

- (अ) 6
- (ब) 7
- (स) 10
- (द) 11

उत्तर- (द) 11  
(137) एक डिजिटल प्रमाणपत्र .....

- (अ) एक इलेक्ट्रॉनिक संदेश है जो विशिष्ट रूप से संदेश भेजने वाले की पहचान करता है।
- (ब) एक सादे पाठ दस्तावेज का सारांश है।
- (स) एक विश्वसनीय तृतीय पक्ष है जो संदेश भेजने वाले को प्रमाणित करता है।
- (द) का उपयोग निजी कुंजी और संबंधित सार्वजनिक कुंजी के स्वामी की पहचान करने के लिए किया जाता है।

उत्तर- (द) का उपयोग निजी कुंजी और संबंधित सार्वजनिक कुंजी के स्वामी की पहचान करने के लिए किया जाता है।

(138) एक क्रेडिट कार्ड में ..... होता है।

- (अ) केवल नकद
- (ब) केवल नकद नहीं
- (स) नकदी के लिए नहीं
- (द) केवल नकदी निकालें।

उत्तर- (ब) केवल नकद नहीं।  
(139) एक डेबिट कार्ड में नकदी ..... होती है।

- (अ) केवल नकद
- (ब) केवल नकद नहीं
- (स) नकदी के लिए नहीं
- (द) केवल नकदी निकालें।

उत्तर- (अ) केवल नकद।

(140) स्मार्ट का अर्थ : विशिष्ट, मापने योग्य, ....., प्रासंगिक और मूल।

- (अ) सटीक
- (ब) कार्रवाई योग्य
- (स) जवाबदेह
- (द) साध्य।

उत्तर- (द) साध्य।

(141) इलेक्ट्रॉनिक भुगतान प्रणाली एक ..... है।

- (अ) साफ्टवेयर
- (ब) हार्डवेयर
- (स) आवेदन
- (द) बैंक।

उत्तर- (स) आवेदन।

(142) इलेक्ट्रॉनिक नकद भुगतान में .....

- (अ) डेबिट कार्ड भुगतान प्रणाली का उपयोग किया जाता है।
- (ब) ग्राहक कई इलेक्ट्रॉनिक सिक्के खरीदता है जो सिक्का जारी करने वाले बैंक द्वारा डिजिटल रूप से हस्ताक्षरित होते हैं।
- (स) क्रेडिट कार्ड भुगतान प्रणाली का उपयोग किया जाता है।
- (द) RSA क्रिप्टोग्राफी का उपयोग लेनदेन में किया जाता है।

उत्तर- (स) क्रेडिट कार्ड भुगतान प्रणाली का उपयोग किया जाता है।  
(143) इलेक्ट्रॉनिक नकद भुगतान में .....

- (अ) ग्राहक बैंक द्वारा हस्ताक्षरित विभिन्न मूल्यवर्ग के सिक्के नहीं निकालता है।
- (ब) बैंक के पास जारी किए गए सिक्कों का एक डेटाबेस है।
- (स) सिक्के जारी नहीं करता।
- (द) बैंक किसी ग्राहक का पता नहीं लगा सकता।

उत्तर- (द) बैंक किसी ग्राहक का पता नहीं लगा सकता।  
(144) एक डिजिटल हस्ताक्षर .....

- (अ) बिट स्ट्रिंग एक संवाच्यता की पहचान दे रही है।
- (ब) प्रेषक की विशिष्ट पहचान।
- (स) किसी इलेक्ट्रॉनिक रिकॉर्ड को उस कुंजी से विशिष्ट रूप से बांधकर प्रमाणीकरण करना जिसे केवल प्रेषक ही जानता हो।
- (द) प्रेषक का एक एन्क्रिप्टेड हस्ताक्षर।

उत्तर- (स) किसी इलेक्ट्रॉनिक रिकॉर्ड को उस कुंजी से विशिष्ट रूप से बांधकर प्रमाणीकरण करना जिसे केवल प्रेषक ही जानता हो।

(145) सुरक्षित इलेक्ट्रॉनिक लेनदेन प्रोटोकॉल का उपयोग ..... के लिए किया जाता है।

- (अ) क्रेडिट कार्ड से भुगतान
- (ब) चेक भुगतान
- (स) इलेक्ट्रॉनिक नकद भुगतान

- (द) इंटरनेट सेवाओं के लिए छोटी राशि का भुगतान।  
 उत्तर- (अ) क्रेडिट कार्ड से भुगतान।  
 (146) इलेक्ट्रॉनिक नकर भुगतान में .....

- (अ) डेबिट कार्ड भुगतान प्रणाली का उपयोग किया जाता है।  
 (ब) ग्राहक कई इलेक्ट्रॉनिक सिक्के खरीदता है जो सिक्का जारी करने वाले बैंक द्वारा डिजिटल रूप से हस्ताक्षरित होते हैं।  
 (स) क्रेडिट कार्ड भुगतान प्रणाली का उपयोग किया जाता है।  
 (अ) RSA क्रिप्टोग्राफी का उपयोग लेनदेन में किया जाता है।  
 उत्तर- (स) क्रेडिट कार्ड भुगतान प्रणाली का उपयोग किया जाता है।  
 (147) इलेक्ट्रॉनिक नकर भुगतान में .....

- (अ) ग्राहक बैंक द्वारा हस्ताक्षरित विभिन्न मूल्यवर्ग के सिक्के नहीं निकालता है।  
 (ब) बैंक के पास जारी किए गए सिक्कों का एक डेटाबेस है।  
 (स) सिक्के जारी नहीं करता।  
 (द) बैंक किसी ग्राहक का पता नहीं लगा सकता।  
 उत्तर- (द) बैंक किसी ग्राहक का पता नहीं लगा सकता।  
 (148) एम. बैंकिंग का अर्थ है-

- (अ) अपने मोबाइल डिवाइस पर कार्य करने के लिए।  
 (ब) अपनी इंटरनेट सेवा पर कार्रवाई करने के लिए।  
 (स) अपने वेबपेज पर कार्रवाई करने के लिए।  
 (द) अपने पीसी पर कार्य करने के लिए।  
 उत्तर- (अ) अपने मोबाइल डिवाइस पर कार्य करने के लिए।  
 (149) B2B का पूरा नाम क्या है?

- (अ) Business to Buyer (ब) Business to Builder  
 (स) Business to Business (द) Builder to Business.  
 उत्तर- (स) Business to Business.

- (150) B2C की फुल फॉर्म क्या है?  
 (अ) Business to Consumer (ब) Business to Company  
 (स) Business to Corporation (द) Builder to Buyer.  
 उत्तर- (अ) Business to Consumer.

- (151) C2C का फुल फॉर्म क्या है?  
 (अ) Company to Company (ब) Consumer to Consumer  
 (स) Corporation to Consumer (द) Company to Customer.  
 उत्तर- (ब) Consumer to Consumer.  
 (152) C2B का फुल फॉर्म क्या है?  
 (अ) Company to Buyer (ब) Consumer to Consumer  
 (ब) Consumer to Consumer

- (स) Consumer to Business  
 (द) Company to Business.  
 उत्तर- (स) Consumer to Business.  
 (153) B2A का फुल फॉर्म क्या है?  
 (अ) Business to Administration  
 (ब) Business to Automation  
 (स) Buyer to Administration  
 (द) Business to Armor.

- उत्तर- (अ) Business to Administration.  
 (154) C2A का फुल फॉर्म क्या है?  
 (अ) Company to Administration  
 (ब) Consumer to Administration  
 (स) Company to Social  
 (द) Customer to Administration.

- उत्तर- (ब) Consumer to Administration.  
 (155) इनमें से कौन e-गवर्नेंस का हिस्सा है?  
 (अ) G2B (ब) G2C  
 (स) B2G (द) C2G.

- उत्तर- (द) C2G.  
 (156) कस्टमर जब किसी वेबसाइट पर जाते हैं और वहाँ पर कुछ खरीदते हैं तो उस परसेटिज को क्या कहते हैं?  
 (अ) Affiliate Program (ब) Click-through  
 (स) Spam (द) Conversion rate.

- उत्तर- (द) Conversion rate.  
 (157) CGI की फुल फॉर्म क्या है?  
 (अ) Computer Gateway Interface  
 (ब) Common Gateway Interface  
 (स) Computer Gateway Interconnection  
 (द) Common Gateway Interconnection.

- उत्तर- (ब) Common Gateway Interface.  
 (158) Amazon किस प्रकार का ई-कॉमर्स बिजनेस है?  
 (अ) b2b (ब) g2b  
 (स) g2b (द) g2c.

- उत्तर- (ब) g2b.  
 (159) जब हम कोई प्रोडक्ट इंटरनेट पर देखते हैं तो उसके डिस्क्रिप्शन को क्या कहते हैं?  
 (अ) Online catalogue (ब) Offline catalogue

- (स) Printed catalogue  
 उत्तर- (अ) Online catalogue.  
 (160) सामान्य रेडिट और क्रेडिट कार्ड का नम्बर कितने अंकों का होता है?  
 (अ) 8  
 (स) 16  
 (ब) 12  
 (द) 20.  
 उत्तर- (स) 16.  
 (161) क्रेडिट या रेडिट कार्ड में CVV की फुलफॉर्म क्या होती है?  
 (अ) Credit Verification Value  
 (ब) Card Verification Value  
 (स) Card Validity Value  
 (द) Credit Verification Visual.  
 उत्तर- (अ) Credit Verification Value.  
 (162) OTP की फुलफॉर्म क्या होती है?  
 (अ) One Time Password  
 (ब) Only Time Password  
 (स) One Type Password  
 (द) One Tracking Password.  
 उत्तर- (अ) One Time Password.  
 (163) OTP किसके माध्यम से प्राप्त किया जा सकता है?  
 (अ) SMS द्वारा  
 (ब) email द्वारा  
 (स) (अ) एवं (ब)  
 (द) इनमें से कोई नहीं।  
 उत्तर- (स) (अ) एवं (ब)  
 (164) ई-कॉमर्स में ALE का फुलफॉर्म क्या है?  
 (अ) Application Link Embedding  
 (ब) Application Link Electronics  
 (स) Application Leakage Enabling  
 (द) इनमें से कोई नहीं।  
 उत्तर- (अ) Application Link Embedding.  
 (165) ई-कॉमर्स में EDI का फुलफॉर्म क्या है?  
 (अ) Electronic Detailed International  
 (ब) Electronic Data Interchange  
 (स) Electronic Digital Interchange  
 (द) इनमें से कोई नहीं।  
 उत्तर- (ब) Electronic Data Interchange.  
 (166) ई-कॉमर्स में BPP का फुलफॉर्म क्या है?  
 (अ) Biller Payment Provider

- (ब) Biller Provision Provider  
 (स) Biller Payment Protector  
 (द) इनमें से कोई नहीं।  
 उत्तर- (अ) Biller Payment Provider.  
 (167) ई-कॉमर्स में BSP का फुलफॉर्म क्या है?  
 (अ) Biller Service Protector  
 (ब) Biller Service Provider  
 (स) Biller Service Packer  
 (द) इनमें से कोई नहीं।  
 उत्तर- (ब) Biller Service Provider.  
 (168) ई-कॉमर्स में CSP का फुलफॉर्म क्या है?  
 (अ) Card Service Provider  
 (ब) Customer Service Provider  
 (स) Central Service Provider  
 (द) इनमें से कोई नहीं।  
 उत्तर- (ब) Customer Service Provider.  
 (169) ई-कॉमर्स में ACH का फुलफॉर्म क्या है?  
 (अ) Association of Clearing Houses  
 (ब) Anonymous Cleansing House  
 (स) Automatic Cleansing House  
 (द) इनमें से कोई नहीं।  
 उत्तर- (स) Automatic Cleansing House  
 (170) ई-कॉमर्स में BITS का फुलफॉर्म क्या है?  
 (अ) Bhartiya Institute of Technology & Society  
 (ब) Banking Industry Technology Secretariat  
 (स) Banking Institute of Technology & Society  
 (द) इनमें से कोई नहीं।  
 उत्तर- (ब) Banking Industry Technology Secretariat.  
 (171) ई-कॉमर्स में CVN का फुलफॉर्म क्या है?  
 (अ) Card Verification Number  
 (ब) Commerce Verified Number  
 (स) Consumer Verified Number  
 (द) इनमें से कोई नहीं।  
 उत्तर- (अ) Card Verification Number.  
 (172) ई-कॉमर्स वेबसाइट पर किस समय सेबैट की जा सकती है?  
 (अ) हर दिन 2 घंटे  
 (ब) सुबह 9 से शाम 5 बजे तक

- (स) 24 × 7  
 उत्तर- (स) 24 × 7  
 (173) किसने सन् 1979 में पहले ऑनलाइन शॉपिंग सिस्टम को demonstrate किया था?  
 (अ) Michael Aldrich  
 (ब) Tim Berner Lee  
 (स) Wilhelm Stinitz  
 (द) इनमें से कोई नहीं।

- उत्तर- (अ) Michael Aldrich  
 (174) CMS का फुलफॉर्म क्या है?  
 (अ) Core Managang System  
 (ब) Content Management System  
 (स) Core Management System  
 (द) Cashe Management System.

- उत्तर- (ब) Content Management System.  
 (175) ई-कॉमर्स का सही मायने में अर्थ क्या है?  
 (अ) Business  
 (ब) Goods और Services को sell करना  
 (स) Electronically Business करना  
 (द) इनमें से कोई नहीं।

- उत्तर- (स) Electronically Business करना।  
 (176) CPC का फुलफॉर्म क्या होता है?  
 (अ) Cost pay for customer  
 (ब) Cost per click  
 (स) Charge per click  
 (द) इनमें से कोई नहीं।

- उत्तर- (ब) Cost per click  
 (177) AOV का फुलफॉर्म क्या होता है?  
 (अ) All Over Value  
 (ब) Average on value  
 (स) Access over value  
 (द) Average order value.

- उत्तर- (द) Average order value.  
 (178) USA में इलेक्ट्रॉनिक फंड ट्रांसफर को किस नाम से जाना जाता है?  
 (अ) e-checks  
 (ब) Book Transfer  
 (स) Giro Transfer  
 (द) इनमें से कोई नहीं।

- उत्तर- (अ) e-checks.  
 (179) CSC का फुलफॉर्म क्या है?  
 (अ) Cash security code  
 (ब) Code security card  
 (स) Card security code  
 (द) इनमें से कोई नहीं।

- उत्तर- (स) Card security code.  
 (180) UK में EFT को किस नाम से जाना जाता है?

- (अ) e-checks  
 (स) Giro Transfer  
 (ब) Book Transfer/Payment  
 (द) Easy Transfer.

- उत्तर- (ब) Book Transfer/Payment.  
 (181) Credit Card का इस्तेमाल ATM मशीन से पैस निकालने के लिए नहीं कर सकते हैं-  
 (अ) सत्य  
 (ब) असत्य  
 (स) कभी-कभी  
 (द) कह नहीं सकते।

- उत्तर- (अ) सत्य।  
 (182) Smart Card से हम कैश withdraw कर सकते हैं?  
 (अ) सत्य  
 (ब) असत्य  
 (स) कभी-कभी  
 (द) कह नहीं सकते।

- उत्तर- (ब) असत्य।  
 (183) E-Commerce का वह प्रकार जिसमें एक कंपनी इंटरनेट के माध्यम से किसी दूसरी कंपनी को अपने प्रोडक्ट बेचती हो, कहलाता है-  
 (अ) B2G  
 (ब) B2C  
 (स) B2B  
 (द) C2B.

- उत्तर- (स) B2B.  
 (184) Electrically किया जाने वाला बिजनेस क्या कहलाता है?  
 (अ) e-commerce  
 (ब) e-company  
 (स) e-corporation  
 (द) e-customer.

- उत्तर- (अ) e-commerce.  
 (185) E-Commerce में COD का फुलफॉर्म क्या होता है?  
 (अ) Cash on Delivery  
 (ब) Cash on Demand  
 (स) Commerce on Delivery  
 (द) Card on Delivery.

- उत्तर- (अ) Cash on Delivery.  
 (186) इनमें से कौनसी एक e-कॉमर्स वेबसाइट है?  
 (अ) Yahoo  
 (ब) Bing  
 (स) Google  
 (द) Amazon.

- उत्तर- (द) Amazon.  
 (187) जब बेचने वाला और खरीदने वाला दोनों बिजनेस कंपनियाँ हों तो वह कौनसा e-कॉमर्स मॉडल होता है?  
 (अ) Consumer to Business  
 (ब) Business to Consumer  
 (स) Business to Business  
 (द) Consumer to Consumer.

उत्तर- (स) Business to Business.

इकाई-3

- (1) किस प्रकार का ई-कॉमर्स कम्पनियों के बीच में स्थापित होता है?  
 (अ) B2B (ब) B2G  
 (स) C2C (द) B2C
- उत्तर- (अ) B2B
- (2) जब कोई व्यवसाय अपने उत्पादों को इंटरनेट पर उपभोक्ताओं को बेचता है तो इस प्रकार का वाणिज्य होता है?  
 (अ) B2B (ब) C2B  
 (स) B2C (द) Enterprise Commerce.
- उत्तर- (स) B2C.
- (3) ई-कॉमर्स में उपभोक्ताओं को सामग्री बनाने और वितरित करने की क्षमता क्या है?  
 (अ) कनेक्टिविटी (ब) इंटरैक्टिव  
 (स) रिलेशनलिटी (द) रिलेशनशिप।
- उत्तर- (ब) इंटरैक्टिव।
- (4) इंटरनेट पर आपूर्ति और सेवाओं के व्यापार-से-व्यापार खरीद और बिक्री के लिए एक विधि क्या है?  
 (अ) ई-प्रोक्योरमेंट (ब) एंटरप्राइज रिसोर्स मैनेजमेंट  
 (स) सप्लाय चैन मैनेजमेंट (द) ई-टेलिंग।
- उत्तर- (द) ई-टेलिंग।
- (5) ई-कॉमर्स की परिभाषा क्या है?  
 (अ) इंटरनेट पर ईमेल का प्रसारण (ब) कैंटलॉग और टेलीफोन के माध्यम से बिक्री  
 (स) इलेक्ट्रॉनिक माध्यम से व्यवसाय और संचार लेन-देन का माध्यम (द) अमेरिकी जनगणना ब्यूरो द्वारा दी गई जानकारी।
- उत्तर- (स) इलेक्ट्रॉनिक माध्यम से व्यवसाय और संचार लेन-देन का माध्यम।
- (6) स्वास्थ्य सेवाओं को एकीकृत करने के लिए बनाए गए भारत के सरकारी सेवा पोर्टल को किसके द्वारा डिजाइन किया गया है?  
 (अ) एन.आई.सी. (ब) भेल  
 (स) एच.ए.एल. (द) उपरोक्त में से कोई नहीं।
- उत्तर- (अ) एन.आई.सी.
- (7) सार्वजनिक अस्पतालों के लिए ऑनलाइन पंजीकरण प्रणाली शुरू की गई-  
 (अ) जुलाई 2015 से (ब) अगस्त 2016 से  
 (स) जुलाई 2016 से (द) जनवरी 2015 से।
- उत्तर- (अ) जुलाई 2015 से।

(8) UMANG का फुल फॉर्म है-

- (अ) Unified Mobile Application for Old-age Governance  
 (ब) Unique Mobile Application for New-age Governance  
 (स) United Mobile Application National Governance  
 (द) Universal Mobile Application Net Goods.

उत्तर- (अ) Unified Mobile Application for Old-age Governance.

(9) UMANG App निम्न सेवाओं को सुलभ करता है-

- (अ) इनकम टैक्स फाइल करना  
 (ब) आधार और पीएफ फंड क्वैरीज को हल करना  
 (स) गैस सिलेण्डर बुक करना  
 (द) उपरोक्त सभी।

उत्तर- (द) उपरोक्त सभी।

(10) ई गवर्नेंस टेक्नोलॉजी आपको प्रोवाइड करती है-

- (अ) एक क्लेटफार्म जो इंफॉर्मेशन एक्सचेंज करता है  
 (ब) एक क्लेटफार्म जो सेवाएँ देता है  
 (स) एक क्लेटफार्म जो नागरिकों को कनेक्ट रखता है  
 (द) उपरोक्त सभी।

उत्तर- (द) उपरोक्त सभी।

(11) NeGP का सबसे सफल प्रोजेक्ट है-

- (अ) Mission-Mode Project  
 (ब) Passport Seva Project  
 (स) (अ) और (ब) दोनों  
 (द) इसमें से कोई नहीं।

उत्तर- (ब) Passport Seva Project.

(12) PSP से संबंधित इनमें से कौन सी कम्पनी एल्सीकेशन साफ्टवेयर के विकास और सरकार को अतिरिक्त करने के लिए उत्तरदायी है?

- (अ) विदेश मंत्रालय (ब) भारत सरकार  
 (स) टाटा कन्सल्टेंसी सर्विस (द) इनमें से कोई नहीं।  
 (स) टाटा कन्सल्टेंसी सर्विस।

उत्तर- (स) टाटा कन्सल्टेंसी सर्विस।

(13) UMANG एल्सीकेशन किस पहल का एक हिस्सा है?

- (अ) स्वच्छ भारत अभियान (ब) मिड-डे मील  
 (स) अटल उन्नति मिशन (द) डिजिटल इंडिया।

उत्तर- (द) डिजिटल इंडिया।

(14) UMANG App का क्या उद्देश्य है?

- (अ) फास्ट ट्रेक मोबाइल गवर्नेंस  
 (ब) फास्ट गेपिंग

- (स) रलो गेभिग  
(द) इनमें से कोई नहीं।
- उत्तर- (अ) फास्ट ट्रेक मोबाइल गवर्नेंस।
- (15) **UMANG App** कितनी भाषाओं का सपोर्ट करता है?  
(अ) 10  
(ब) 11  
(स) 12  
(द) 13
- उत्तर- (द) 13
- (16) भारतीय रेलवे द्वारा रेलवे आरक्षण का कार्य किसके सौंपा गया है?  
(अ) IRCTC  
(स) NIC  
(ब) BHEL  
(द) इनमें से कोई नहीं।
- उत्तर- (अ) IRCTC
- (17) **IRCTC** द्वारा इंटरनेट टिकटिंग ऑपरेशन किस तारीख को शुरू किया गया था?  
(अ) 3 जुलाई, 2002  
(ब) 3 अगस्त, 2002  
(स) 3 जनवरी, 2002  
(द) 12 अगस्त, 2005
- उत्तर- (ब) 3 अगस्त, 2002
- (18) **DigiLocker** में किससे अप्रुव किया जाता है?  
(अ) आधार कार्ड  
(ब) पेन कार्ड  
(स) झाड़विग लाइसेंस  
(द) पासपोर्ट।
- उत्तर- (अ) आधार कार्ड।
- (19) **SAARTHI Stand for ....**  
(अ) Synergised Advanced Application Rail Travel Help and Information  
(ब) Service for Advanced Application Rail Travel Help and Information  
(स) Saving on Advanced Application Rail Travel Help and Information  
(द) इनमें से कोई नहीं।
- उत्तर- (अ) Synergised Advanced Application Rail Travel Help and Information
- (20) **SAARTHI** कब लॉन्च हुआ?  
(अ) 14 जुलाई, 2015  
(ब) 14 जुलाई, 2016  
(स) 14 जुलाई, 2017  
(द) 14 जुलाई, 2018
- उत्तर- (स) 14 जुलाई, 2017
- (21) भारत में कुल कितने पासपोर्ट सेवा केन्द्र हैं?  
(अ) 543  
(ब) 537  
(स) 587  
(द) 550
- उत्तर- (अ) 543

- (22) **UMANG App** कब लॉन्च किया गया?  
(अ) 25 नवम्बर, 2016  
(ब) 23 नवम्बर, 2017  
(स) 23 नवम्बर, 2018  
(द) इनमें से कोई नहीं।
- उत्तर- (ब) 23 नवम्बर, 2017
- (23) प्रत्येक व्यक्ति अपने इस्कॉर्प पर भी उमंग एप को एक्सेस कर सकता है-  
(अ) सही  
(ब) गलत।
- उत्तर- (अ) सही।
- (24) अगर भारतीय कम्पनी एपआरएफ कम्पनी से टावर खरीदती है तो यह होगा-  
(अ) B2B  
(ब) B2C  
(स) C2B  
(द) C2C
- उत्तर- (अ) B2B
- (25) **Alibaba** के फाउंडर कौन हैं?  
(अ) Jack Ma  
(ब) Jeff Bezos  
(स) Mark Zuckerberg  
(द) Jack Dorsey, Noah Glass, Biz Stone
- उत्तर- (अ) Jack Ma
- (26) भारत में **IT Act** कब पास किया गया था?  
(अ) 2000  
(ब) 2001  
(स) 2002  
(द) 2004
- उत्तर- (अ) 2000
- (27) दुर्भावनापूर्ण सॉफ्टवेयर के सामूहिक शब्दों को क्या कहा जाता है, जैसे वायरस, worm और ट्रोजन?  
(अ) Spam  
(ब) Phishing  
(स) Malware  
(द) Harm.
- उत्तर- (स) Malware.
- (28) अपने डाटा को ऑनलाइन अटक, हैकर और वायरस से बचाने को क्या कहते हैं?  
(अ) Physical security  
(ब) Cyber security  
(स) Cyber attack  
(द) Virus.
- उत्तर- (ब) Cyber security.
- (29) इनमें से कौन सा एक एंटीवायरस सॉफ्टवेयर है?  
(अ) Norton  
(ब) K7  
(स) Quick heal  
(द) उपरोक्त सभी।
- उत्तर- (द) उपरोक्त सभी।
- (30) इनफॉर्मेशन security में CIA का फुल फॉर्म क्या है?  
(अ) Confidentiality Integrity Availability  
(ब) Criminal Investigation Agency

- (स) Cost Information Agency  
(द) Credit Integrity Assessment.
- उत्तर- (अ) Confidentiality Integrity Availability.
- (31) कम्प्यूटर प्रणाली में सुरक्षा श्रेयता का आवधिक मूल्यांकन क्या है?  
(अ) Threat  
(ब) Attack  
(स) Hacking  
(द) Security audit.
- उत्तर- (द) Security audit.
- (32) कौन सी गतिविधियाँ राष्ट्र की सभ्यभुता और अखण्डता को खतरे में डालती हैं?  
(अ) Cyber Terrorism  
(स) Cyber squatting  
(द) Carding.
- उत्तर- (अ) Cyber Terrorism.
- (33) कम्प्यूटर सिस्टम पर अनाधिकृत नियंत्रण/पहुँच को क्या कहा जाता है और जो डेटा को नष्ट कर देता है?  
(अ) Defamation  
(स) Hacking  
(द) Scanning.
- उत्तर- (स) Hacking.  
(द) Cyber-stalking.
- (34) कुछ असामान्य का पता लगाने के इरादे से सभी फाइलों या नेटवर्क तत्वों के माध्यम से कौन सी विधि अपनाई जाती है?  
(अ) Probing  
(स) Infecting  
(द) Scanning.
- उत्तर- (ब) Phishing  
(द) Scanning.
- (35) Virus एक कम्प्यूटर से दूसरे कम्प्यूटर में कैसे फैल सकता है?  
(अ) इन्फेक्टेड फाइल को शेयर करने से  
(ब) टच करने से  
(स) दूसरे कम्प्यूटर को पास में रखने से  
(द) दोनों एक ही नेटवर्क का इस्तेमाल करने से।
- उत्तर- (अ) इन्फेक्टेड फाइल को शेयर करने से।
- (36) Virus की कुल फॉर्म क्या है?  
(अ) Very intelligent Result Until Source  
(ब) Vital information resource under siege  
(स) Viral important Record user searched  
(द) Very interchanged resource under search.
- उत्तर- (ब) Vital information resource under siege.
- (37) निम्नलिखित में से कौन सुरक्षा तंत्र से संबंधित नहीं है?  
(अ) Encryption  
(ब) Decryption  
(स) e-cash  
(द) उपरोक्त सभी।

- उत्तर- (स) e-cash.
- (38) निम्न में से कौन सा फैलवेयर का उदाहरण है?  
(अ) spyware  
(स) trojanhorse  
(द) उपरोक्त सभी।
- उत्तर- (द) उपरोक्त सभी।
- (39) निम्न में से कौन सा सॉफ्टवेयर आपके कम्प्यूटर की जासूसी करता है एवं आपसे सम्बन्धित सूचनाओं का आदान प्रदान करता है?  
(अ) Trojan Horse  
(स) Spyware  
(द) myheebon.
- उत्तर- (स) Spyware.
- (40) https:// में 5 का अर्थ है-  
(अ) सिक्योर  
(स) सिस्टम  
(द) साधारण।
- उत्तर- (अ) सिक्योर।
- (41) एक सुरक्षित पासवर्ड बनता है?  
(अ) छोटे और बड़े अक्षर  
(स) स्पेशल सिंबल (#@!% ^ )  
(द) उपरोक्त सभी।
- उत्तर- (द) उपरोक्त सभी।
- (42) पहला कम्प्यूटर वायरस कौन सा था?  
(अ) Creeper  
(स) Worm  
(द) Blaster.
- उत्तर- (अ) Creeper.  
(ब) Rat virus
- (43) इनमें से किस के माध्यम से वायरस फैल सकता है?  
(अ) Floppy Disk  
(स) Email Attachment  
(द) उपरोक्त सभी।
- उत्तर- (द) उपरोक्त सभी।
- (44) जब कोई आपके कम्प्यूटर को बिना आपकी अनुमति के एक्सेस करता है तो उसे क्या कहते हैं?  
(अ) Defamation  
(स) Hacking  
(द) Cyber-stalking.
- उत्तर- (स) Hacking.  
(ब) Carding
- (45) कम्प्यूटर में फैलने वाला वायरस क्या है?  
(अ) यह हार्डवेयर है  
(स) यह सिस्टम सॉफ्टवेयर है  
(द) यह एक विंडो टूल है।
- उत्तर- (ब) यह एक कम्प्यूटर प्रोग्राम है।

(46) इनमें से कौन वायरस फैलाने का एक आवर्श तरीका नहीं है?

- (अ) संक्रमित वेबसाइट (ब) Official Antivirus CDs  
(स) E-mail (द) USB

उत्तर- (ब) Official Antivirus Cds.

(47) Spammer आपकी पर्यन्तल इन्फॉर्मेशन कहाँ से प्राप्त कर सकते हैं?

- (अ) Facebook (ब) Instagram  
(स) LinkedIn (द) दिए गए सभी।

उत्तर- (द) दिए गए सभी।

(48) किस प्रकार के साइबर अटैक में आपसे आपकी जानकारी मांगी जाती है जैसे आपके पासवर्ड, नाम, OTP, पिन आदि?

- (अ) Password Attack (ब) Phishing Attack  
(स) Virus Attack (द) Malware Attack.

उत्तर- (ब) Phishing Attack.

(49) व्यक्तिगतों द्वारा अपनी पहचान को गलत बताकर गोपनीय जानकारी प्राप्त करने के लिए किस तरह के प्रयास किये जाते हैं?

- (अ) Computer virus (ब) Phishing Scams  
(स) Spyware Scams (द) myhedeason Scams.

उत्तर- (ब) Phishing Scams.

(50) एक मजबूत पासवर्ड होना चाहिए-

- (अ) दोनों अक्षर केस और लोअर केस अक्षरों में  
(ब) एक शब्द जो याद रखना आसान होता है, जैसे कि पालतू जानवर का नाम  
(स) नाम जिसमें कम से कम 8 वर्ण और अक्षरों, संख्याओं और वर्णों का संयोजन हो  
(द) आपका पूरा नाम।

उत्तर- (स) नाम जिसमें कम से कम 8 वर्ण और अक्षरों, संख्याओं और वर्णों का संयोजन हो।

(51) एन्क्रिप्शन सॉफ्टवेयर में फैलने वाले वायरस को क्या कहा जाता है?

- (अ) बूट वायरस (ब) मैक्रो वायरस  
(स) एंटी वायरस (द) फ़ाइल वायरस।

उत्तर- (ब) मैक्रो वायरस।

(52) कम्प्यूटर में से दुर्भावनापूर्ण फ़ाइलों को स्कैन कर हटाता है-

- (अ) एंटीवायरस (ब) वायरस  
(स) वर्ड (द) गुगल।

उत्तर- (अ) एंटीवायरस।

(53) क्यों कोई आपके कम्प्यूटर में (हैक) बिना अनुमति प्रवेश कर सकता है?

- (अ) उन्हें आप पसंद नहीं है

(ब) अपराध करने के लिए

(स) अश्लील, दुर्भावनापूर्ण कार्यक्रमों आदि को वितरित करने के लिए  
(द) दिए गए सभी।

उत्तर- (द) दिए गए सभी।

(54) यदि आपको एक मेल प्राप्त होता है जिसमें आपसे आपके username और पासवर्ड की मांग की जाती है, ऐसी परिस्थिति में आप क्या करेंगे?

- (अ) उसे अपने ईमेल प्रदाता के माध्यम से फिशिंग/स्मैम के रूप में रिपोर्ट करेंगे  
(ब) संदेश को अपने ईमेल और पासवर्ड दे देंगे  
(स) संदेश भेजने वाले से पहले बात करेंगे  
(द) इनमें से कोई नहीं।

उत्तर- (अ) उसे अपने ईमेल प्रदाता के माध्यम से फिशिंग/स्मैम के रूप में रिपोर्ट करेंगे।

(55) भारतीय आईटी, अधिनियम 2000 नियम किस क्षेत्र को नियंत्रित करने के लिए तैयार किये गए हैं?

- (अ) आयाकर (ब) औद्योगिक प्रौद्योगिकी  
(स) सूचना प्रौद्योगिकी (द) इनसाइडर ट्रेडिंग।

उत्तर- (स) सूचना प्रौद्योगिकी।



(1) इनफॉर्मेशन security में CIA की फुल फॉर्म क्या है?

- (अ) confidentiality Integrity Availability  
(ब) Criminal Investigation Agency  
(स) Cost Information Agency  
(द) Credit Integrity Assessment.

उत्तर- (अ) confidentiality Integrity Availability.

(2) Wi-Fi को हैक करने के लिए किस टूल का इस्तेमाल किया जाता है?

- (अ) Wiresnark (ब) Nessus  
(स) Aircrack-ng (द) Snort.

उत्तर- (स) Aircrack-ng.

(3) हैकिंग गैर कानूनी है और कानून की नजर में एक दंडनीय अपराध है?

- (अ) सत्य (ब) असत्य।

उत्तर- (अ) सत्य।

(4) DES की फुल फॉर्म क्या है?

- (अ) Digital Evaluation System  
(ब) Digital Encryption Standard  
(स) Digital Encryption System  
(द) Digital Evaluation Standard.

- उत्तर- (ब) Digital Encryption Standard.
- (5) असुरक्षित **plugin** का दूसरा नाम क्या है?  
 (अ) Hardware (ब) Software  
 (स) Firmware (द) Malware.
- उत्तर- (द) Malware.
- (6) **DHA** की फुल फॉर्म क्या है?  
 (अ) Directory Harvest Attack  
 (ब) DNS Harvest Attack  
 (स) Direct Harvest Attack  
 (द) Dictionary Harvest Attack.
- उत्तर- (अ) Directory Harvest Attack.
- (7) इनमें से कौन सा एक एंटीवायरस सॉफ्टवेयर है?  
 (अ) Norton (ब) K7  
 (स) Quick heal (द) उपरोक्त सभी।
- उत्तर- (द) उपरोक्त सभी।
- (8) **Password** के इस्तेमाल से नेटवर्क की ..... बढ़ती है?  
 (अ) Performance (ब) Reliability  
 (स) Security (द) Longevity.
- उत्तर- (स) Security.
- (9) **Virus** एक कम्प्यूटर से दूसरे कम्प्यूटर में कैसे फैल सकता है?  
 (अ) इन्फेक्टेड फाइल को शेयर करने से  
 (ब) टच करने से  
 (स) दूसरे कम्प्यूटर को पास में रखने से  
 (द) दोनों में एक ही नेटवर्क का इस्तेमाल करने से।
- उत्तर- (अ) इन्फेक्टेड फाइल को शेयर करने से।
- (10) निम्न में से कौन सा मैलवेयर का उदाहरण है?  
 (अ) spyware (ब) वायरस  
 (स) trojanhorse (द) उपरोक्त सभी।
- उत्तर- (द) उपरोक्त सभी।
- (11) निम्न में से किस प्रकार की वेबसाइट पर अपनी व्यक्तिगत जानकारी दर्ज नहीं करनी चाहिए?  
 (अ) जिन वेबसाइट के एड्रेस की शुरुआत में <http://> नहीं होता है  
 (ब) जिन वेबसाइट में पैडलॉक नहीं होता है  
 (स) (अ) और (ब) दोनों  
 (द) इनमें से कोई नहीं।
- उत्तर- (स) (अ) और (ब) दोनों।

- (12) निम्न में से कौन सा सॉफ्टवेयर आपके कम्प्यूटर की जासूसी करता है एवं आपसे सम्बन्धित सूचनाओं का आदान-प्रदान करता है?  
 (अ) Trojan Horse (ब) Virus  
 (स) Spyware (द) Heelsoon.
- उत्तर- (स) Spyware.
- (13) निम्न में से कौन सा मैलवेयर का उदाहरण नहीं है?  
 (अ) Trojan Horse (ब) Virus  
 (स) Spyware (द) Antivirus.
- उत्तर- (द) Antivirus.
- (14) निम्न में से किस प्रकार के साइबर अटैक के द्वारा आपको, चाही गयी वेबसाइट की जगह अन्य वेबसाइट पर ले जाया जाता है?  
 (अ) D.N.S. पोइजनिंग (ब) फिशिंग  
 (स) सेशन हार्जैक (द) इनमें से कोई नहीं।
- उत्तर- (ब) फिशिंग।
- (15) निम्न में से कौन से साइबर अटैक के प्रकार हैं?  
 (अ) Phishing (ब) Searching  
 (स) ब्राउजिंग (द) उपरोक्त सभी।
- उत्तर- (अ) Phishing.
- (16) निम्न में से कौन साइबर अटैक है?  
 (अ) Password Attack (ब) Denial of Service  
 (स) Phishing (द) उपरोक्त सभी।
- उत्तर- (द) उपरोक्त सभी।
- (17) **Cyber** सुरक्षा को ..... भी जाना जाता है।  
 (अ) देश सुरक्षा (ब) आपातकाल सुरक्षा  
 (स) कम्प्यूटर सुरक्षा (द) इनमें से कोई नहीं।
- उत्तर- (स) कम्प्यूटर सुरक्षा।
- (18) निम्न में से हानिकारक उद्देश्य वाला सॉफ्टवेयर कौनसा है?  
 (अ) मेलवेयर (ब) वर्ड  
 (स) VLC (द) पेंट।
- उत्तर- (अ) मेलवेयर।
- (19) **Denial of service** कम्प्यूटर में क्या करता है?  
 (अ) कम्प्यूटर को ओवरलोड (ब) कम्प्यूटर को चालू  
 (स) (अ) और (ब) दोनों (द) इनमें से कोई नहीं।
- उत्तर- (अ) कम्प्यूटर को ओवरलोड।
- (20) हमलावर संक्रामित विज्ञापनों को अपलोड कर किस प्रकार का हमला करता है?  
 (अ) डिनायल ऑफ सर्विसेज (ब) वेब हमले

- (स) मेलवर टायिजन  
 उत्तर- (स) मेलवर टायिजन।
- (21) System security में सेव को कैसे पहचाना जाता है?  
 (अ) हैकिंग से  
 (स) (अ) और (ब) दोनों  
 (द) इनमें से कोई नहीं।
- उत्तर- (स) (अ) और (ब) दोनों।
- (22) हमलावर क्लाउड मशीन और सर्वर के बीच एक ऑर्थिकेशन सेशन की निगरानी कर किस तरह का हमला करता है?  
 (अ) सेशन अपहरण  
 (स) (अ) और (ब) दोनों  
 (द) इनमें से कोई नहीं।
- उत्तर- (अ) सेशन अपहरण।
- (23) यह एक अप्रारंभिक या अवांछित संदेश/ईमेल है जो आमतौर पर इंटरनेट पर विज्ञापन, फिशिंग, मैलवेयर फैलाने आदि के लिए भेजी जाती है-  
 (अ) स्पैम  
 (स) सेंड  
 (ब) इंबॉक्स  
 (द) उपरोक्त सभी।
- उत्तर- (अ) स्पैम।
- (24) समाचार पढ़ने, मनोरंजन, अनुसंधान, छुट्टियाँ बुक करने, खरीदने और बेचने, सीखने, बैंक और अन्य कार्य करने के लिए सक्षम बनाता है-  
 (अ) Internet  
 (स) Word  
 (ब) Computer  
 (द) इनमें से कोई नहीं।
- उत्तर- (अ) Internet.
- (25) निम्न में से किस मैलवेयर के रूप में जाना जाता है?  
 (अ) Virus  
 (स) (अ) और (ब) दोनों  
 (द) इनमें से कोई नहीं।
- उत्तर- (स) (अ) और (ब) दोनों।
- (26) Copyright सुरक्षित सॉफ्टवेयर, वीडियो, संगीत, फोटो या दस्तावेजों को डाउनलोड करना किस प्रकार का उल्लंघन है?  
 (अ) Copyright  
 (स) विधवासाधात  
 (ब) Hacking  
 (द) सूसिबर धोखाधड़ी।
- उत्तर- (अ) Copyright.
- (27) सुरक्षित वेब एड्रेस ब्राउजर में कोई पेडलोक नहीं है तो वेब एड्रेस की शुरुआत में ..... नहीं होता है-  
 (अ) शुरुआत में http://  
 (स) www  
 (ब) ब्राउजर पेडलोक  
 (द) (अ) और (ब) दोनों।
- उत्तर- (द) (अ) और (ब) दोनों।
- (28) Http:// में s का अर्थ है-

- (अ) सिक्वोर  
 (स) सिस्टम  
 (द) साधारण।
- उत्तर- (अ) सिक्वोर।
- (29) Website पर विश्वास का प्रतीक है-  
 (अ) ट्रस्टसील  
 (स) (अ) और (ब) दोनों  
 (ब) एक सिक्वोर सील  
 (द) इनमें से कोई नहीं।
- उत्तर- (अ) ट्रस्टसील।
- (30) Privacy Seal, Business Practice Seal, व्यापार पहचान सील, सुरक्षा सील आदि किस प्रकार की सील है?  
 (अ) एक सिक्युरिटी सील  
 (स) ट्रस्टसील  
 (ब) वेबसील  
 (द) वेब पोर्टल।
- उत्तर- (स) ट्रस्टसील।
- (31) Security Trust Seal सत्यापन का सबसे लोकप्रिय प्रकार है-  
 (अ) सर्वर सत्यापन  
 (स) (अ) और (ब) दोनों  
 (ब) वेबसाइट सत्यापन  
 (द) इनमें से कोई नहीं।
- उत्तर- (स) (अ) और (ब) दोनों।
- (32) कम्प्यूटर में से दुर्भावनापूर्ण फाइलों को स्कैन कर हटाता है-  
 (अ) एंटीवायरस  
 (स) वर्ड  
 (ब) वायरस  
 (द) गुगल।
- उत्तर- (अ) एंटीवायरस।
- (33) अन्तर्राष्ट्रीय साइबर सुरक्षा मानक है-  
 (अ) ISO 27000  
 (स) ISO 27002  
 (ब) ISO 27001  
 (द) ISO 27003.
- उत्तर- (ब) ISO 27001.
- (34) भारत में साइबर अपराध और इलेक्ट्रॉनिक कॉपर्स से सम्बन्धित कानून है-  
 (अ) IT Act, 2000  
 (स) IT Act, 2002  
 (ब) IT Act, 2001  
 (द) IT Act, 2003.
- उत्तर- (अ) IT Act, 2000.
- (35) Computer स्रोत कोड के साथ छेड़छाड़ करना किस प्रकार की घाटा है?  
 (अ) Section 65  
 (स) Section 43  
 (ब) Section 66  
 (द) Section 67.
- उत्तर- (अ) Section 65.
- (36) Electronic अभिलेखों के साथ छेड़छाड़ करना किस प्रकार की घाटा है-  
 (अ) Section 65  
 (स) Section 43  
 (ब) Section 66  
 (द) Section 67.
- उत्तर- (स) Section 43.

- (37) Hacking और कंप्यूटर अपराध किस प्रकार की घात है?  
 (अ) Section 65  
 (ब) Section 66  
 (स) Section 43  
 (द) Section 67.
- जवाब- (ब) Section 66.
- (38) Electronic रूप से अश्लील जानकारी छापना किस प्रकार की घात है?  
 (अ) Section 65  
 (ब) Section 66  
 (स) Section 43  
 (द) Section 67.
- जवाब- (द) Section 67.
- (39) भारतीय कॅपीराइट अधिनियम है-  
 (अ) Act 1954  
 (ब) Act 1955  
 (स) Act 1956  
 (द) Act 1957.
- जवाब- (द) Act 1957.
- (40) सूचना सुरक्षा प्रबंधन प्रणाली के लिए निम्न में से कौनसी एक ISO स्टैंडर्ड है?  
 (अ) ISO 9000  
 (ब) ISO 14000  
 (स) ISO 22000  
 (द) ISO 27000.
- जवाब- (द) ISO 27000.



- (1) Social Media Site Facebook कहाँ की कंपनी है?  
 (अ) भारत  
 (ब) अमेरिका  
 (स) जापान  
 (द) कनाडा।
- जवाब- (ब) अमेरिका।
- (2) फेसबुक के संस्थापक का नाम क्या है?  
 (अ) सुंदरपिचई  
 (ब) मार्क जुकरबर्ग  
 (स) बिलगेट्स  
 (द) विकलिवस।
- जवाब- (ब) मार्क जुकरबर्ग।
- (3) फेसबुक के CEO कौन हैं?  
 (अ) डेविड  
 (ब) स्टीव  
 (स) ब्राव  
 (द) मार्क जुकरबर्ग।
- जवाब- (द) मार्क जुकरबर्ग।
- (4) इनमें से कौनसी Social media साइट है?  
 (अ) फेसबुक  
 (ब) रेडियो  
 (स) टीवी  
 (द) मोबाइल।
- जवाब- (अ) फेसबुक।
- (5) मेंसेंजर किसका पार्ट है?  
 (अ) Yahoo  
 (ब) Google  
 (स) Facebook  
 (द) Bing

- जवाब- (स) Facebook.
- (6) WhatsApp किसके द्वारा खरीदा गया है?  
 (अ) माइक्रोसॉफ्ट  
 (ब) गुगल  
 (स) फेसबुक  
 (द) याहू।
- जवाब- (स) फेसबुक।
- (7) इंस्टाग्राम किसके द्वारा खरीदा गया है?  
 (अ) माइक्रोसॉफ्ट  
 (ब) गुगल  
 (स) याहू  
 (द) फेसबुक।
- जवाब- (द) फेसबुक।
- (8) Twitter कैसे सॉफ्टवेयर है?  
 (अ) माइक्रोब्लॉगिंग सॉफ्टवेयर  
 (ब) न्यूज साइट है  
 (स) डैक्ट एडिटर सॉफ्ट  
 (द) इनमें से कोई नहीं।
- जवाब- (अ) माइक्रोब्लॉगिंग सॉफ्टवेयर।
- (9) कितने कैरेक्टर Twitter पर हम टाइप कर सकते हैं?  
 (अ) 150  
 (ब) 130  
 (स) 200  
 (द) 140
- जवाब- (द) 140
- (10) Twitter का लोगो क्या है?  
 (अ) जानवर  
 (ब) मनुष्य  
 (स) मछली  
 (द) चिड़िया।
- जवाब- (द) चिड़िया।
- (11) Twitter पर एकाउन्ट कौन लोग खोल सकते हैं?  
 (अ) नेता  
 (ब) एक्टर  
 (स) आम जनता  
 (द) सभी।
- जवाब- (द) सभी।
- (12) Twitter किस तरह के मोबाइल ऑपरेटिंग सिस्टम पर आधारित है?  
 (अ) एन्ड्रॉयड  
 (ब) iphone  
 (स) Blackberry  
 (द) वे सभी।
- जवाब- (द) वे सभी।
- (13) Social media Instagram को शॉर्ट फॉर्म में कैसे लिखते हैं?  
 (अ) Ingram  
 (ब) IG  
 (स) InstaG  
 (द) वे सभी।
- जवाब- (ब) IG
- (14) Instagram के लोगो के रूप में क्या प्रयोग करते हैं?  
 (अ) चिड़िया  
 (ब) कैमरा

(स) इंस्टाग्राम शब्द  
उत्तर- (ब) कैमरा।

(15) इनमें से कौन सोशल मीडिया है?

(अ) Telegram  
(स) Snapchat  
उत्तर- (द) ये सभी।

अति लघुउत्तरीय (एक शब्द)-

(द) इनमें से कोई नहीं।

(ब) Line  
(द) ये सभी।

प्रश्न-1. उस मंत्रालय का नाम बताइए जिसने सबसे पहले फेसबुक, इंस्टाग्राम और यूट्यूब जैसे सोशल मीडिया प्लेटफॉर्म पर ऑनलाइन ईमेल विज्ञापन पर रोक लगाने का प्रस्ताव दिया?

उत्तर- इलेक्ट्रॉनिक्स और आईटी मंत्रालय ने।

प्रश्न-2. उस कम्पनी का नाम बताइए जिसके द्वारा 'ब्यू सब्सक्राइवर सर्विस' प्रीमियम सेवा लागू की गई?

उत्तर- ट्विटर।

प्रश्न-3. उस केन्द्रीय मंत्रालय का नाम बताइए जिसके द्वारा सोशल मीडिया यूजर्स की समस्याओं को हल करने के लिए 'शिकायत अपील समिति' बनाने की अनुमति दी गई?

उत्तर- इलेक्ट्रॉनिक्स और आईटी मंत्रालय।

प्रश्न-4. उस सोशल मीडिया नेटवर्क का नाम बताइए जिसने दूरस्थ शहरों में वित्तीय समवेश को बढ़ावा देने के लिए सितम्बर 2022 को इंडिया पोस्ट वेरोलनगर बैंक के साथ समझौता किया?

उत्तर- कू।

प्रश्न-5. उस राज्य का नाम बताइए जिसने सबसे ज्यादा सोशल मीडिया पर फर्जी खबरों के खिलाफ मामला दर्ज कराया?

उत्तर- पश्चिम बंगाल।

प्रश्न-6. गूगल की शुरुआत कब हुई थी?

उत्तर- सन् 1998 में।

प्रश्न-7. उस व्यक्ति का नाम बताइए जिसने गूगल की शुरुआत की थी?

उत्तर- लैरी पेज और सर्गी ब्रिन।

प्रश्न-8. उस व्यक्ति का नाम बताइए जिसने कम्प्यूटर का आविष्कार किया?

उत्तर- चार्ल्स बैबेज।

प्रश्न-9. इंटरनेट की कनेक्टिविटी में एचडीपी का सटीक विस्तृत रूप क्या है?

उत्तर- हाइपर टैकस्ट ट्रांसफर प्रोटोकॉल।

प्रश्न-10. मल्टी प्रोसेसर क्या होता है?

उत्तर- एक से अधिक प्रोसेसर।

प्रश्न-11. गूगल क्या है?

एक खोज (सर्च) इंजन है।

प्रश्न-12. गूगल की कम्पनी कहाँ पर स्थित है?

उत्तर- अमेरिका में।

प्रश्न-13. किस जगह पर गूगल की स्थापना हुई थी?

उत्तर- संयुक्त राज्य अमेरिका की कैलिफोर्निया में।

प्रश्न-14. गूगल की मूल कम्पनी का नाम बताइए।

उत्तर- वर्णमाला।

प्रश्न-15. किस सन् में फेसबुक को लांच किया गया था?

उत्तर- 4 फरवरी, 2004 में।

प्रश्न-16. उस व्यक्ति का नाम बताइए जिसने फेसबुक को लांच किया था?

उत्तर- मार्क जुकरबर्ग।

प्रश्न-17. सबसे पहले फेसबुक की शुरुआत कब हुई थी?

उत्तर- 28 अक्टूबर, 2003 में।

प्रश्न-18. सबसे पहले फेसबुक वेबसाइट का क्या नाम रखा गया था?

उत्तर- दी फेसबुक।

प्रश्न-19. किस सन् में दी फेसबुक नाम को बदलकर केवल फेसबुक रखा गया?

उत्तर- सन् 2004 में।

प्रश्न-20. किस सन् में फेसबुक ने हाई स्कूल के बच्चों के लिए लांच किया था?

उत्तर- सितम्बर, 2005 में।

प्रश्न-21. हाई स्कूल के स्टूडेंट के लिए फेसबुक को लांच तो किया गया लेकिन मार्क ने उसे नया नाम क्या दिया?

उत्तर- नेक्ट लीजिकल स्पेप।

प्रश्न-22. किस सन् में फेसबुक बुनिया की सबसे बड़ी सोशल नेटवर्किंग वेबसाइट बन गई?

उत्तर- सन् 2009 में।

प्रश्न-23. किस सन् में फेसबुक ने नोट्स का ऑप्शन लगाया?

उत्तर- 22 अगस्त, 2006 में।

प्रश्न-24. किस सन् में च्यूज फीड का फीचर लगाया गया?

उत्तर- 6 सितम्बर, 2006 में।

प्रश्न-25. किस सन् में फेसबुक चैट का फीचर आया?

उत्तर- 6 अप्रैल, 2008 में।

प्रश्न-26. किस सन् में फेसबुक ने beta version को लांच किया?

उत्तर- 20 जुलाई, 2008 को।

प्रश्न-27. किस सन् में फेसबुक ने new version को सभी यूजर के लिए लागू कर दिया गया?

उत्तर- सितम्बर 2008 में।

प्रश्न-28. किस सन् में फेसबुक ने यूजरनेस का फीचर लगाया?

उत्तर- सितम्बर 2008 में।

उत्तर- सितम्बर 2008 में।

उत्तर- सितम्बर 2008 में।

- उत्तर- 13 जुलाई, 2009 में।
- प्रश्न-29. किस सन् में फेसबुक ने लाइक का बटन लगाया?  
उत्तर- 21 अप्रैल, 2010 को।
- प्रश्न-30. किस सन् में फेसबुक ने लाइव कॉल का फीचर लगाया?  
उत्तर- 6 जुलाई, 2011 में।
- प्रश्न-31. मई 2014 में किस देश के फेसबुक यूजर सबसे ज्यादा थे?  
उत्तर- यूनाइटेड स्टेट्स (U.S.)।
- प्रश्न-32. मई 2014 में भारत के फेसबुक यूजर की संख्या कितनी थी?  
उत्तर- 108.9 मिलियन।
- प्रश्न-33. मई 2014 में ब्राजील के फेसबुक यूजर की संख्या कितनी थी?  
उत्तर- 70.5 मिलियन।
- प्रश्न-34. मई 2014 में इंडोनेशिया के फेसबुक यूजर की संख्या कितनी थी?  
उत्तर- 60.3 मिलियन।
- प्रश्न-35. मई 2014 में मैक्सिको के फेसबुक यूजर की संख्या कितनी थी?  
उत्तर- 44.4 मिलियन।
- प्रश्न-36. फेसबुक को आप कितनी भाषाओं में इस्तेमाल कर सकते हैं?  
उत्तर- 70 भाषाओं में।
- प्रश्न-37. मार्क ने फेसबुक के लाइक बटन का नाम सबसे पहले क्या रखने का निर्णय लिया था?  
उत्तर- 'ऑसम'।
- प्रश्न-38. इंस्टाग्राम की शुरुआत कब हुई थी?  
उत्तर- 6 अक्टूबर, 2010 को।
- प्रश्न-39. फेसबुक भारत में कब आया?  
उत्तर- सितम्बर, 2006 को।
- प्रश्न-40. इंस्टाग्राम की खोज किस व्यक्ति ने की?  
उत्तर- केविन सिस्ट्रॉम और माइक क्रेगर ने।
- प्रश्न-41. किस सन् में इंस्टाग्राम की खोज की गई?  
उत्तर- सन् 2010 में।
- प्रश्न-42. किस सन् में आईओएस ऑपरेटिंग सिस्टम के लिए विशेष रूप से निःशुल्क मोबाइल ऐप के रूप में लांच किया गया था?  
उत्तर- अक्टूबर, 2010 में।
- प्रश्न-43. किस सन् में इंस्टाग्राम भारत आया था?  
उत्तर- अप्रैल 2012 में।
- प्रश्न-44. किस सन् में इंस्टाग्राम का एंड्रोइड वर्जन भारत में आया?  
उत्तर- सन् 2012 में।
- प्रश्न-45. किस सन् में विशेष वर्जन आया?

- उत्तर- अक्टूबर 2016 में।
- प्रश्न-46. इंस्टाग्राम का पुराना नाम बताइए।  
उत्तर- बर्बन।
- प्रश्न-47. इंस्टाग्राम किन दो नामों से मिलकर बना है?  
उत्तर- इंस्टेट और टेलीग्राम।
- प्रश्न-48. किस जगह पर इंस्टाग्राम का मुख्यालय स्थित है?  
उत्तर- अमेरिका के कैलिफोर्निया शहर में।
- प्रश्न-49. इंस्टाग्राम का हेल्पलाइन नम्बर बताइए।  
उत्तर- 650-543-4800 या 650-308-7300
- प्रश्न-50. इंस्टाग्राम के सबसे पहले यूजर का नाम बताइए।  
उत्तर- माइक क्रैगर।
- प्रश्न-51. उस देश का नाम बताइए जो इंस्टाग्राम का सबसे ज्यादा इस्तेमाल करने वाला देश कहा जाता है?  
उत्तर- भारत।
- प्रश्न-52. उस देश का नाम बताइए जो इंस्टाग्राम का दूसरा सबसे ज्यादा इस्तेमाल करने वाला देश कहा जाता है?  
उत्तर- संयुक्त राज्य अमेरिका।
- प्रश्न-53. उस देश का नाम बताइए जो इंस्टाग्राम का तीसरा सबसे ज्यादा इस्तेमाल करने वाला देश कहा जाता है?  
उत्तर- ब्राजील।
- प्रश्न-54. उस देश का नाम बताइए जो इंस्टाग्राम का चौथा सबसे ज्यादा इस्तेमाल करने वाला देश कहा जाता है?  
उत्तर- इंडोनेशिया।
- प्रश्न-55. उस देश का नाम बताइए जो इंस्टाग्राम का पाँचवाँ सबसे ज्यादा इस्तेमाल करने वाला देश कहा जाता है?  
उत्तर- तुर्की।
- प्रश्न-56. उस देश का नाम बताइए जो इंस्टाग्राम का छठे सबसे ज्यादा इस्तेमाल करने वाला देश कहा जाता है?  
उत्तर- जापान।
- प्रश्न-57. इंस्टाग्राम का अर्थ बताइए।  
उत्तर- इंस्टाग्राम एक मोबाइल, डेस्कटॉप और इंटरनेट आधारित फोटो साझाकरण एप्लीकेशन है जो उपयोगकर्ताओं को फोटो या वीडियो को सार्वजनिक रूप से या निजी तौर पर साझा करने की अनुमति देता है।
- प्रश्न-58. इंस्टाग्राम को क्यों बरखा गया?  
उत्तर- तेज उपयोग और आसानी से इसका लाभ उठाने के लिए इसे फिर से डिजाइन किया गया।

- प्रश्न-59. 1।k इंस्टाग्राम में का क्या मतलब होता है?  
 उत्तर- एक हज़ार।
- प्रश्न-60. 10।k इंस्टाग्राम में का क्या मतलब होता है?  
 उत्तर- दस हज़ार।
- प्रश्न-61. इंस्टाग्राम का नाम के आगे लाल नम्बर का क्या अर्थ होता है?  
 उत्तर- इसका मतलब है कि इंस्टाग्राम ने पुष्टि की है कि एक खाला सार्वजनिक हस्ती, सेलिब्रिटी या ब्रांड की प्रामाणिक उपस्थिति है जिसका वह प्रतिनिधित्व करता है।
- प्रश्न-62. इंस्टाग्राम पर बैसेल का बटन कहाँ होता है?  
 उत्तर- ऊपर की तरफ दांयी ओर।
- प्रश्न-63. भारत में व्हाट्सएप किस सन् में आया था?  
 उत्तर- नवम्बर 2009 में।
- प्रश्न-64. उस व्यक्ति का नाम बताइए जिसने व्हाट्सएप की स्थापना की थी?  
 उत्तर- ब्रायन एक्टन और जन कौम ने।
- प्रश्न-65. किस सन् में व्हाट्सएप को पहली बार पेश किया गया था?  
 उत्तर- सन् 2009 में।
- प्रश्न-66. व्हाट्सएप किस देश की कम्पनी है?  
 उत्तर- अमेरिका।
- प्रश्न-67. कितने देशों में व्हाट्सएप को चलाया जाता है?  
 उत्तर- 180 देशों में।
- प्रश्न-68. व्हाट्सएप का अर्थ बताइए।  
 उत्तर- व्हाट्सएप शब्द What's up से लिया गया है जिसका हिन्दी में आशय है, क्या हाल है? WhatsApp और What's up बोलने में या समझने में कोई ज़्यादा अन्तर नहीं है।
- प्रश्न-69. व्हाट्सएप का नया नाम बताइए।  
 उत्तर- व्हाट्सएप प्लस।
- प्रश्न-70. व्हाट्सएप को कितने प्रकारों में बांटा गया है?  
 उत्तर- 3(WhatsApp, WhatsApp Business और WhatsApp web)
- प्रश्न-71. व्हाट्सएप पर 3 सर्कल का क्या अर्थ होता है?  
 उत्तर- यदि उस व्यक्ति ने आपका संदेश नहीं पढ़ा है, तो आपको पढ़े फील्ड में तीन बिन्दु दिखाई देंगे।
- प्रश्न-72. मेटा व्हाट्सएप पर क्यों लिखा जात है?  
 उत्तर- क्योंकि मेटा फेसबुक की सहयोगी कम्पनी बन चुकी है और व्हाट्सएप इंस्टाग्राम मेटा कम्पनी के अन्तर्गत आता है इसीलिए अब नीचे मेटा लिखा हुआ आता है।
- प्रश्न-73. व्हाट्सएप विजनेस क्या है?

- उत्तर- WhatsApp Business ऐप की मदद से कस्टमर्स के साथ आसानी से बातचीत की जा सकती है।
- प्रश्न-74. यूट्यूब के मालिक का नाम क्या है?  
 उत्तर- स्टीव चेन और चड हर्ले।
- प्रश्न-75. यूट्यूब किस देश की कम्पनी है?  
 उत्तर- अमेरिका।
- प्रश्न-76. यूट्यूब के सीईओ का नाम बताइए।  
 उत्तर- नील मोहन।
- प्रश्न-77. व्हाट्सएप के सीईओ का नाम बताइए।  
 उत्तर- जन कौम और ब्रायन एक्शन।
- प्रश्न-78. फेसबुक के सीईओ का नाम बताइए।  
 उत्तर- मार्क जकार्बर्ग।
- प्रश्न-79. यूट्यूब का मालिकाना अधिकार किसके पास है?  
 उत्तर- गूगल।
- प्रश्न-80. ट्विटर के सीईओ का नाम बताइए।  
 उत्तर- एलॉन मस्क।
- प्रश्न-81. किस सन् में ट्विटर की स्थापना की गई थी?  
 उत्तर- 21 मार्च, 2006 को।
- प्रश्न-82. किस जगह पर ट्विटर का मुख्यालय स्थित है?  
 उत्तर- कैलिफोर्निया (U.S.A.) में।
- प्रश्न-83. ट्विटर क्या है?  
 उत्तर- ट्विटर चिट्ठाकारी सेवा है जो अपने उपयोगकर्ताओं को अपनी जानकारियाँ, जिन्हें ट्वीट्स कहते हैं, एक दूसरे को भेजने और पढ़ने की सुविधा देता है।
- प्रश्न-84. उस व्यक्ति का नाम बताइए जिसने सबसे पहले ट्विटर एप के बारे में अपना विचार रखा था?  
 उत्तर- जैक डोरसे।
- प्रश्न-85. ट्विटर का पहला नाम क्या रखा गया था?  
 उत्तर- ट्वीट।
- प्रश्न-86. ट्विटर की फुल फॉर्म बताइए।  
 उत्तर- Typing What I'm Thinking To Everyone Reading जिसका मतलब है, मेरे मन में क्या चल रहा है, उसे टाइप करना ताकि हर कोई उसे पढ़ और जान सके।
- प्रश्न-87. ट्वीट किसने character वाला बैसेज है?  
 उत्तर- 140 character वाला।
- प्रश्न-88. Retweet क्या होता है?

उत्तर- किसी दूसरे के टवीट को क्रेडिट प्रदान करता है।

प्रश्न-89. फीड क्या होता है?

उत्तर- ये वो स्ट्रीम ऑफ टवीट्स होते हैं जिन्हें हम होम पेज पर देखते हैं। इसमें वो सारे अपडेट्स होते हैं जो कि हम उन यूजर्स से पाते हैं जिन्हें हम फॉलो करते हैं।

प्रश्न-90. Handle क्या है?

उत्तर- ये आपका यूजर नेम होता है।

प्रश्न-91. Mention क्या होता है?

उत्तर- अन्य लोगों को टैग करना या उनको मेंशन करना जिससे उन्हें वह सूचना मिल जाती है जो हमने शेयर की है।

प्रश्न-92. DM क्या है?

उत्तर- डायरेक्ट मैसेज।

प्रश्न-93. हैशटैग (#) क्या होता है?

उत्तर- हैशटैग का इस्तेमाल सोशल मीडिया साइट्स पर किसी फोटो, वीडियो, पोस्ट, कमेंट या इवेंट्स आदि को सर्च करने के लिए किया जाता है।

प्रश्न-94. Retweet Tag क्या होता है?

उत्तर- अगर हमें कोई tweet पसंद आया, तो हम उस tweet को retweet कर सकते हैं।

प्रश्न-95. Lists क्या होता है?

उत्तर- यह ट्विटर का फीचर है जिसकी मदद से लिस्ट क्रिएट की जाती है।

प्रश्न-96. रेवीग्राम की शुरुआत कब की गई थी?

उत्तर- सन् 2013 में।

