CSIR-CENTRAL LEATHER RESEARCH INSTITUTE, ADYAR, CHENNAI.

SEO2401 Question Booklet No. : 06

Admit Card No. | | | | | | | | | —

Recruitment for the Post of Security Officer, Advt. No. 01/2024

Total Time Allowed : 03 hours 30 minutes **Total Marks : 200**

Read the following instructions carefully before you begin to answer the questions.

IMPORTANT INSTRUCTIONS

1. The Competitive Written Examination has the following two Papers :

Paper I (Time Allotted – 90 minutes)

Subject	No. of Questions	Maximum Marks	Negative Marks
Mental Ability and Personality Assessment Test	100	100 (one mark for every correct answer)	There will be no negative marks in this paper

Paper II (Time Allotted – 120 minutes)

Subject	Maximum Marks	Negative Marks
Comprehension	25	There will be no negative marks in this paper
Report Writing	25	
Security Regulations, Firefighting etc.	25	
General Awareness	25	

2. **The schedule of Written Examination is as follows,:**
   Paper I – from 02:00 P.M. to 03:30 P.M. (OMR based: The candidates will be provided with a Question Paper and OMR Answer Sheets)
   Paper II – from 04:00 P.M. to 06:00 P.M. (The candidates will be provided with Question Paper with blank answer sheets)
   The OMR Answer Sheets and Paper II Question Paper will have to be returned to Invigilator after end of Paper I & Paper II respectively.
3. The Paper I Question Booklet will be supplied 10 minutes prior to the commencement of the Written Test. The Candidates may take with them Question Booklet of Paper I on conclusion of examination.
4. **The candidates shall have to return the Answer Sheets of Paper I and Paper II to the Invigilator at the end each Paper.**
5. No candidates will be allowed to leave the Examination Hall before completion of both Paper I and Paper II
6. Prior to attempting answer, candidates are requested to check whether all the questions in Question Booklet of Paper I are in series and ensure that there are no blank pages in between the Question Booklet. **In case any defect in the Question Booklet is noticed, the same should be reported to the Invigilator immediately and get it replaced with a new Question Booklet of same series.**
7. Candidate must write their Admit Card Number in the space provided on the top right side of **Question Booklet of Paper I.** Do not write anything else on this Question Booklet other than the blank sheet provided for Rough Work.
8. Each question comprises of *four* responses viz. (A), (B), (C) and (D). Only one of the response is correct answer. The Candidates are required to select ONE response which they consider as correct and mark it in the OMR Answer Sheet.
9. The OMR Answer Sheet has **four** circles against each question viz Ⓐ Ⓑ Ⓒ and Ⓓ . To answer the questions, the candidates are required to blacken One circle which they consider as correct answer with **Blue or Black Ball point pen.** For *e.g.* If for any item, Ⓑ is the correct answer, the candidate have to mark as follows : Ⓐ ● Ⓒ Ⓓ The candidates are warned that if they blacken more than one circle for one question, the answer will be treated as wrong.
10. The total marks in Paper I will depend on the number of correct responses marked by the Candidate in the OMR Answer Sheet.
11. **The last page of the Question Booklet of Paper I, may be used for rough work.**
12. In all matters and in cases of doubt in Question Booklet for Paper I, the English version shall be final.
13. The candidates shall abide by the instructions issued by the Invigilator/ Exam Officials. Failure to comply with any of the instructions may render the candidate liable to such action or penalty, as may be decided by the Competent Authority, CSIR-CLRI.
14. I have read the instructions given above and the instruction given in the Notification dated 05.03.2025, 24.04.2025 & 03.06.2025 in the CSIR-CLRI website "www.clri.org" and agree to the same.

Invigilator's Signature

Candidate's Signature with date

सीएसआईआर-केन्द्रीय चर्म अनुसंधान संस्थान, अडयार, चेन्नई

SEO2401

प्रश्न पुस्तिका सं. :

प्रवेश पत्र सं. | | | | | | | | |

सुरक्षा अधिकारी के पद की भर्ती, सीएलआरआई विज्ञापन सं.: 01/2024

कुल आबंटित समय : 03 घंटे 30 मिनट

कुल अंक : 200

प्रश्नों का उत्तर देने से पहले निम्नलिखित अनुदेशों को ध्यान से पढ़ें।

महत्त्वपूर्ण अनुदेश

1. इस प्रतियोगिता लिखित परीक्षा में निम्नलिखित दो पेपर होते हैं :

पेपर–I (आबंटित समय – 90 मिनट)

विषय	प्रश्नों की संख्या	अधिकतम अंक	नेगटिव अंक
मानसिक क्षमता और व्यक्तित्व मूल्यांकन परीक्षण	100	100 (प्रत्येक सही उत्तर के लिए एक अंक)	इस पेपर में कोई नेगटिव अंक नहीं है

पेपर–II (आबंटित समय – 120 मिनट)

विषय	अधिकतम अंक	नेगटिव अंक
समझ	25	इस पेपर में कोई नेगटिव अंक नहीं है
रिपोर्ट लेखन	25	
सुरक्षा विनियम, अग्निशमन आदि	25	
सामान्य जानकारी	25	

2. **लिखित परीक्षा की समय-सारणी निम्नानुसार है:**

पेपर–I – अपराह्न 02:00 बजे से 03:30 बजे तक (OMR आधारित: उम्मीदवारों को एक प्रश्न पत्र और OMR उत्तर पत्रक प्रदान किए जाएंगे)

पेपर–II – अपराह्न 04:00 बजे से 06:00 बजे तक (उम्मीदवारों को खाली उत्तर पत्रक के साथ प्रश्न पत्र प्रदान किए जाएंगे)

OMR उत्तर पत्रक और पेपर–II प्रश्न पत्र क्रमशः पेपर–I और पेपर–II के पूरे होने के बाद अन्वीक्षक को लौटाना होगा।

3. लिखित परीक्षा शुरू होने से 10 मिनट पहले पेपर–I की प्रश्न पुस्तिका दी जाएगी। उम्मीदवार परीक्षा समाप्त होने पर पेपर–I की प्रश्न पुस्तिका अपने साथ ले जा सकते हैं।
4. **उम्मीदवारों को प्रत्येक पेपर के अंत में पेपर–I और पेपर–II की उत्तर पुस्तिकाएँ अन्वीक्षक को वापस करनी होंगी।**
5. किसी भी उम्मीदवार को पेपर–I और पेपर–II, दोनों के पूरा होने से पहले परीक्षा कक्ष छोड़ने की अनुमति नहीं दी जाएगी।
6. उत्तर देने से पहले, उम्मीदवारों से अनुरोध है कि वे जाँच लें कि पेपर–I की प्रश्न-पुस्तिका में सभी प्रश्न क्रम में हैं या नहीं और यह सुनिश्चित करें कि प्रश्न-पुस्तिका के बीच में कोई खाली पन्ने न हों। **यदि प्रश्न-पुस्तिका में कोई त्रुटि दिखाई देती है, तो उसे तुरंत अन्वीक्षक को सूचित करना होगा और उस प्रश्न-पुस्तिका को उसी श्रेणी की नई प्रश्न-पुस्तिका से बदलवाना होगा।**
7. उम्मीदवार को पेपर–I की प्रश्न-पुस्तिका के ऊपर दाईं ओर दिए गए स्थान पर अपना प्रवेश पत्र सं. लिखना होगा। रफ कार्य के लिए दिए गए खाली पन्नों के अलावा प्रश्न-पुस्तिका पर कुछ और न लिखें।
8. प्रत्येक प्रश्न के चार विकल्प (A), (B), (C) और (D) होते हैं। उनमें से केवल एक ही सही उत्तर है। उम्मीदवार केवल एक विकल्प, जिसे वे सही समझते हों, उत्तर पत्रक पर चिह्नित करें।
9. OMR उत्तर पत्रक में प्रत्येक प्रश्न के सामने चार Ⓐ Ⓑ Ⓒ Ⓓ वृत्त होंगे। प्रश्नों के उत्तर देने के लिए, उम्मीदवारों को **नीले या काले बॉल पॉइंट पेन** से एक वृत को काला करना होगा जिसे वे सही उत्तर मानते हैं। उदाहरण के लिए यदि किसी का उत्तर Ⓑ है, तो उम्मीदवार को, इस तरीके से चिह्नित करना होगा: Ⓐ ● Ⓒ Ⓓ । उम्मीदवारों को चेतावनी दी जाती है कि यदि एक प्रश्न के लिए एक से अधिक वृतों को काला करेंगे, तो उस उत्तर को गलत माना जाएगा।
10. पेपर–I में कुल अंक, उम्मीदवार द्वारा OMR उत्तर पत्रक में अंकित सही उत्तरों की संख्या पर निर्भर करेंगे।
11. **पेपर–I की प्रश्न पुस्तिका का अंतिम पृष्ठ रफ कार्य के लिए उपयोग किया जा सकता है।**
12. सभी मामलों में और पेपर–I की प्रश्न पुस्तिका में संदेह की स्थिति में, अंग्रेजी संस्करण अंतिम होगा।
13. उम्मीदवार अन्वीक्षक / परीक्षा अधिकारियों द्वारा जारी किए गए अनुदेशों का पालन करेंगे। किसी भी अनुदेश का पालन नहीं करने पर उम्मीदवार के विरुद्ध कार्रवाई या शास्ति की जा सकती है, जिसका निर्णय सक्षम प्राधिकारी, सीएसआईआर-सीएलआरआई द्वारा किया जा सकता है।
14. मैंने ऊपर दिये अनुदेशों को पढ़ लिया है, तथा www.clri.org वेबसाइट में दिनांक 05.03.2025, 24.04.2025 & 03.06.2025 को दी गई अधिसूचना के अनुदेशों को भी पढ़ लिया है और मैं उनसे समहत हूँ।

अन्वीक्षक के हस्ताक्षर

उम्मीदवार के हस्ताक्षर, दिनांक सहित

CSIR-Central Leather Research Institute

PART-II

Comprehension, Report writing, Security Regulations, Firefighting & General awareness

1. What is the role & responsibilities of Security officer and what are the registers required to be maintained in security office **(10 Marks)**

2. One of your security guards reported that he has caught a staff of the university while stealing some university property. Write a report of the theft to your Head (administration). What are good security practices to prevent **Theft** **(7 Marks)**

3. What is security patrol & its purpose? **(3 Marks)**

4. What are the objectives of conducting security Audit **(3 Marks)**

5. What are the benefits of Security lighting **(3 Marks)**

6. What is first Aid? If a student is drowned in swimming pool what First Aid you will administer **(4 Marks)**

7. What is the first aid for bleeding & Burns **(4 Marks)**

8. Name any three portable fire extinguishers **(3 Marks)**

9. What precautions / preventive action and security measures you will take as security officer during the following:(each question will carry 3 marks) **(21 Marks)**

    1. VVIP Visit
    2. Bomb threat
    3. Security arrangement for a conference/meeting :
    4. Student suicide in hostel room
    5. LPG Gas leakage from Canteen/Hostel mess
    6. Accident of two Motorcycles with the Institute
    7. Live electric wire cut due to fall of a tree

10. Write a report on "**Bomb threat, Evacuation and Search procedures** " not exceeding 1000 words/ A4 size page - **(10 Marks)**

11. **Answer the following in one word and each question will carry one mark.** **(12 Marks)**

    1. What is PSARA and when was this act enacted
    2. What is the most visible element of a security guard
    3. What is prohibited under Section IPC 144
    4. Which is the best extinguisher for oil/fuel fire
    5. Expand abbreviation UDR (under BNS/IPC)
    6. Expand the abbreviation FIR
    7. What is hacking?
    8. What is "Restricted area"
    9. What is the body colour of Hydrogen Gas Cylinder
    10. What happens in case of Excess inhalation of CO2 causes?
    11. Who is an IMPOSTER?
    12. What metal detectors are used ?

12. Comprehension. – Cyber security and Cyber attacks

Read the following passage carefully and mark the answer for the objective questions given after the passage **(20 Marks)**

In today's digital world, cybersecurity has become an important field focused on protecting computer systems, networks, and data from harmful attacks. As society relies more on technology for communication, business, and information storage, the chances of cyberattacks have increased. Cybersecurity includes various methods, technologies, and approaches aimed at keeping sensitive information safe from unapproved access,

damage, or theft. The importance of this field is highlighted by the rising number and complexity of cyber threats, which pose serious risks to individuals, businesses, and governments. Data shows that reported cyber incidents have increased over the past decade, stressing the urgent need for effective cybersecurity measures.

Cyberattacks can come in many forms, such as harmful software, phishing, denial-of-service attacks, and ransomware. Harmful software refers to any software designed to harm a computer system or network. Phishing involves tricking people into giving up personal information, like passwords or credit card numbers, by pretending to be a trustworthy source. Denial-of-service attacks try to overload a system, making it unusable, while ransomware encrypts a victim's data and demands payment for its release. Each of these methods shows the different tactics used by cybercriminals, requiring a varied approach to cybersecurity. For example, the rise in ransomware attacks has led organizations to adopt stricter data backup protocols and incident response plans.

The effects of cyberattacks go beyond immediate financial losses. A successful violation can weaken sensitive personal information, leading to identity theft and long-lasting damage to the reputation of affected organizations. Additionally, because modern systems are linked, a weakness in one area can impact many others. For example, the 2017 Equifax data breach, which exposed personal information of around 147 million people, showed how a single cyber incident can have widespread consequences. Such violations not only damage public trust but also lead to regulatory examination and possible legal issues. The aftermath often results in increased investment in cybersecurity, as organizations work to prevent future incidents.

In response to the growing threat, organizations are putting more resources into cybersecurity. These efforts include installing firewalls, intrusion detection systems, and encryption protocols to protect sensitive data. Also, employee training programs that raise awareness about cybersecurity best methods are becoming common. These initiatives are crucial since human error is one of the leading causes of security breaches. A study by IBM found that 95% of cybersecurity breaches are due to human error, highlighting the need for thorough training and awareness campaigns in organizations. Also, including artificial intelligence and machine learning into cybersecurity frameworks is gaining popularity, as these technologies can improve threat detection and response.

Even with these efforts, challenges remain in cybersecurity. The fast pace of technological change often outstrips the development of security measures,

leaving systems open to new threats. Additionally, the increasing complexity of cybercriminals, who often use advanced techniques like artificial intelligence and machine learning, makes the situation even more complicated. For instance, cybercriminals might use AI to automate attacks, making them more efficient and harder to spot. As a result, organizations must stay alert and adaptable, continually updating their security measures to counter new threats. The changing nature of cyberattacks calls for a preventive approach to cybersecurity, emphasizing the need for ongoing research and development in this area.

In conclusion, the importance of cybersecurity in today's world cannot be overstated. As cyberattacks grow in complexity and frequency, the need for strong security measures becomes more urgent. The relationship between technological progress and cybersecurity presents both challenges and opportunities for organizations and individuals. Although progress has been made in developing protective measures, the ongoing threat of cyberattacks requires a commitment to constant improvement and adaptation. Furthermore, the wider effects of cybersecurity impact national security, economic stability, and personal privacy. Therefore, building a culture of cybersecurity awareness and strength will be crucial in reducing the risks linked to our ever-changing digital landscape. Future research should also look into the ethical aspects of cybersecurity practices, especially regarding privacy and data protection.

Questions:

1. **According to paragraph 1, what is the primary focus of cybersecurity?**
    a. Protecting physical assets
    b. Safeguarding computer systems, networks, and data
    c. Safeguarding computer systems and networks
    d. Increasing business profits

2. **In paragraph 1, each of the following is mentioned as a reason for the importance of cybersecurity EXCEPT:**
    a. The rise in the number of cyber threats
    b. The increasing reliance on technology
    c. The decrease in reported cyber incidents
    d. The serious risks posed to individuals and businesses

3. **What can be inferred about the relationship between the rise in ransomware attacks and cybersecurity measures?**

a. Ransomware attacks have decreased the need for data backup protocols.
b. Organizations are becoming less concerned about cybersecurity.
c. The increase in ransomware attacks has prompted stricter cybersecurity measures.
d. Cybercriminals are less likely to use ransomware in the future.

4. **Why does the author include examples of different types of cyberattacks in paragraph 2?**
   a. To illustrate the complexity of cybersecurity
   b. To suggest that all cyber-attacks are equally harmful
   c. To emphasize the need for a single approach to cybersecurity
   d. To highlight the various tactics used by cybercriminals

5. **The word "violation" in paragraph 3 is closest in meaning to:**
   a. Breach
   b. Agreement
   c. Protection
   d. Observation

6. **What is the main purpose of paragraph 4?**
   a. To discuss the financial implications of cybersecurity
   b. To outline the measures organizations are taking to enhance cybersecurity
   c. To explain the role of technology in cyberattacks
   d. To highlight the importance of human error in cybersecurity

7. **Cybersecurity is not just a technical issue but also a societal concern. Where would the sentence best fit? The importance of cybersecurity in today's world cannot be overstated.**
   a. As cyberattacks grow in complexity and frequency, the need for strong security measures becomes more urgent.
   b. The relationship between technological progress and cybersecurity presents both challenges and opportunities for organizations and individuals.
   c. Although progress has been made in developing protective measures, the ongoing threat of cyberattacks requires a commitment to constant improvement and adaptation.
   d. Furthermore, the wider effects of cybersecurity impact national security, economic stability, and personal privacy.

सीएसआईआर-केन्द्रीय चर्म अनुसंधान संस्थान,

भाग-II

समझ, रिपोर्ट लेखन, सुरक्षा विनियम, अग्निशमन और सामान्य जागरूकता

1. सुरक्षा अधिकारी की भूमिका और जिम्मेदारियाँ क्या हैं और सुरक्षा कार्यालय में कौन से रजिस्टर बनाए रखने होते हैं? **10 अंक**

2. आपके एक सुरक्षा गार्ड ने रिपोर्ट की है कि उसने विश्वविद्यालय के एक कर्मचारी को विश्वविद्यालय की कुछ संपत्ति चोरी करते हुए पकड़ा है। अपने प्रमुख (प्रशासन) को उस चोरी की रिपोर्ट लिखें। चोरी को रोकने के लिए अच्छी सुरक्षा प्रथाएँ क्या हैं? **7 अंक**

3. सुरक्षा गश्त क्या है और इसका उद्देश्य क्या है? **3 अंक**

4. सुरक्षा ऑडिट आयोजित करने के उद्देश्य क्या हैं? **3 अंक**

5. सुरक्षा प्रकाश व्यवस्था के क्या लाभ हैं? **3 अंक**

6. प्राथमिक चिकित्सा क्या है? यदि कोई छात्र स्विमिंग पूल में डूब जाता है तो आप उसे क्या प्राथमिक चिकित्सा देंगे? **4 अंक**

7. रक्तस्राव और जलन के लिए प्राथमिक उपचार क्या है? **4 अंक**

8. किन्हीं तीन पोर्टेबल अग्निशामक यंत्रों के नाम बताइए **3 अंक**

9. निम्नलिखित कार्य के दौरान सुरक्षा अधिकारी के रूप में आप कौन-सी सावधानियाँ/निवारक कार्रवाई और सुरक्षा उपाय अपनाएंगे? **7 X 3 अंक** (प्रत्येक प्रश्न के लिए तीन अंक) **21 अंक**

    1. अति विशिष्ट जनों का दौरा
    2. बम की धमकी
    3. सम्मेलन / बैठक के लिए सुरक्षा व्यवस्था
    4. छात्रावास के कमरे में छात्र की आत्महत्या
    5. कैंटीन / छात्रावास की भोजनशाला से एलपीजी गैस का लीक होना
    6. संस्थान के साथ दो मोटरसाइकिलों की दुर्घटना
    7. पेड़ गिरने से बिजली का तार टूट जाना

10. **"बम की धमकी, निकासी और तलाशी प्रक्रियाओं"** पर एक रिपोर्ट लिखें, जो 1000 शब्दों से अधिक न हो / A4 आकार का पृष्ठ **10 अंक**

11. **निम्नलिखित प्रश्नों के उत्तर एक शब्द में दीजिए तथा प्रत्येक प्रश्न एक अंक का होगा।** **12 अंक**

    1. PSARA क्या है और यह अधिनियम कब बनाया गया?
    2. सुरक्षा गार्ड का सबसे ज़्यादा दिखाई देने वाला तत्व कौन सा है?
    3. धारा IPC 144 के तहत क्या निषिद्ध है?
    4. तेल/ईंधन की आग के लिए सबसे अच्छा अग्निशामक कौन सा है?
    5. संक्षिप्त नाम UDR (BNS/IPC के अंतर्गत) का विस्तार करें
    6. संक्षिप्त नाम FIR का विस्तार करें
    7. हैकिंग क्या है ?
    8. "प्रतिबंधित क्षेत्र" क्या है?
    9. हाइड्रोजन गैस सिलेंडर का बॉडी रंग क्या होता है?

10. CO_2 के अत्यधिक साँस लेने के कारण क्या होता है?
11. ढोंगी (IMPOSTER) कौन होता है?
12. कौन से मेटल डिटेक्टरों का उपयोग किया जाता है?

12. समझ – साइबर सुरक्षा और साइबर हमले

निम्नलिखित गद्यांश को ध्यानपूर्वक पढ़ें तथा गद्यांश के बाद दिए गए वस्तुनिष्ठ प्रश्नों के उत्तर अंकित करें **20 अंक**

आज की डिजिटल दुनिया में, साइबर सुरक्षा एक महत्वपूर्ण क्षेत्र बन गया है, जो कंप्यूटर सिस्टम, नेटवर्क और डेटा को हानिकारक हमलों से बचाने पर केंद्रित है। जैसे-जैसे समाज संचार, व्यवसाय और सूचना भंडारण के लिए प्रौद्योगिकी पर अधिक निर्भर होता जाता है, साइबर हमलों की संभावनाएँ बढ़ गई हैं। साइबर सुरक्षा में विभिन्न विधियाँ, प्रौद्योगिकियाँ और दृष्टिकोण शामिल हैं जिनका उद्देश्य संवेदनशील जानकारी को अनधिकृत पहुँच, क्षति या चोरी से सुरक्षित रखना है। इस क्षेत्र का महत्व साइबर खतरों की बढ़ती संख्या और जटिलता से उजागर होता है, जो व्यक्तियों, व्यवसायों और सरकारों के लिए गंभीर जोखिम पैदा करते हैं। आंकड़े दर्शाते हैं कि पिछले दशक में साइबर घटनाओं की संख्या में वृद्धि हुई है, जिससे प्रभावी साइबर सुरक्षा उपायों की तत्काल आवश्यकता को बल मिलता है।

साइबर हमले कई रूपों में हो सकते हैं, जैसे हानिकारक सॉफ़्टवेयर, फ़िशिंग, सेवा अस्वीकार करने वाले हमले और रैनसमवेयर। हानिकारक सॉफ़्टवेयर किसी भी ऐसे सॉफ़्टवेयर को संदर्भित करता है जिसे कंप्यूटर सिस्टम या नेटवर्क को नुकसान पहुँचाने के लिए डिज़ाइन किया गया है। फ़िशिंग में लोगों को एक भरोसेमंद स्रोत होने का दिखावा करके उनसे पासवर्ड या क्रेडिट कार्ड नंबर जैसी व्यक्तिगत जानकारी देने के लिए धोखा दिया जाता है। सेवा से इनकार करने वाले हमले सिस्टम को ओवरलोड करने की कोशिश करते हैं, जिससे यह अनुपयोगी हो जाता है, जबकि रैनसमवेयर पीड़ित के डेटा को एन्क्रिप्ट करता है और इसे जारी करने के लिए भुगतान की मांग करता है। इनमें से प्रत्येक विधि साइबर अपराधियों द्वारा इस्तेमाल की जाने वाली अलग-

अलग रणनीतियों को दर्शाती है, जिसके लिए साइबर सुरक्षा के लिए अलग-अलग दृष्टिकोण की आवश्यकता होती है। उदाहरण के लिए, रैनसमवेयर हमलों में वृद्धि ने संगठनों को सख्त डेटा बैकअप प्रोटोकॉल और घटना प्रतिक्रिया योजनाओं को अपनाने के लिए प्रेरित किया है।

साइबर हमलों के प्रभाव तत्काल वित्तीय नुकसान से कहीं ज़्यादा हैं। एक सफल उल्लंघन संवेदनशील व्यक्तिगत जानकारी को कमज़ोर कर सकता है, जिससे पहचान की चोरी हो सकती है और प्रभावित संगठनों की प्रतिष्ठा को लंबे समय तक नुकसान हो सकता है। इसके अतिरिक्त, चूँकि आधुनिक प्रणालियाँ आपस में जुड़ी हुई हैं, एक क्षेत्र में कमज़ोरी कई अन्य क्षेत्रों को प्रभावित कर सकती है। इसके अतिरिक्त, चूँकि आधुनिक प्रणालियाँ आपस में जुड़ी हुई हैं, एक क्षेत्र में कमज़ोरी कई अन्य क्षेत्रों को प्रभावित कर सकती है। उदाहरणार्थ, वर्ष 2017 में इक्विफ़ैक्स डेटा उल्लंघन, जिसमें लगभग 147 मिलियन लोगों की व्यक्तिगत जानकारी उजागर हुई, ने दिखाया कि कैसे एक अकली साइबर घटना के व्यापक परिणाम हो सकते हैं। इस तरह के उल्लंघन से न केवल लोगों का भरोसा टूट जाता है, बल्कि विनियामक जांच और संभावित कानूनी मुद्दों का भी सामना करना पड़ता है। इसके फलस्वरूप अक्सर साइबर सुरक्षा में निवेश बढ़ जाता है, क्योंकि संगठन भविष्य की घटनाओं को रोकने के लिए काम करते हैं।

बढ़ते खतरे के जवाब में, संगठन साइबर सुरक्षा में अधिक संसाधन लगा रहे हैं। इन प्रयासों में संवेदनशील डेटा की सुरक्षा के लिए फ़ायरवॉल, घुसपैठ का पता लगाने वाली प्रणालियाँ और एन्क्रिप्शन प्रोटोकॉल स्थापित करना शामिल हैं। इसके अलावा, साइबर सुरक्षा के सर्वोत्तम तरीकों के बारे में जागरूकता बढ़ाने वाले कर्मचारी प्रशिक्षण कार्यक्रम आम होते जा रहे हैं। ये पहल महत्वपूर्ण हैं क्योंकि मानवीय त्रुटि, सुरक्षा उल्लंघनों के प्रमुख कारणों में से एक है। आईबीएम द्वारा किए गए एक अध्ययन में पाया गया कि 95% साइबर सुरक्षा उल्लंघन मानवीय त्रुटि के कारण होते हैं, जिससे संगठनों में गहन प्रशिक्षण और जागरूकता अभियान की आवश्यकता को बल मिलता है। इसके अलावा, साइबर सुरक्षा ढांचे में कृत्रिम बुद्धिमत्ता और मशीन लर्निंग को शामिल करना लोकप्रियता प्राप्त कर रहा है, क्योंकि ये प्रौद्योगिकियां खतरे का पता लगाने और प्रतिक्रिया में सुधार कर सकती हैं।

इन प्रयासों के बावजूद, साइबर सुरक्षा में चुनौतियाँ बनी हुई हैं। तकनीकी परिवर्तन की तेज़ गति अक्सर सुरक्षा उपायों के विकास को पीछे छोड़ देती है, जिससे सिस्टम नए खतरों के लिए खुला रह जाते हैं। इसके अतिरिक्त, साइबर अपराधियों की बढ़ती जटिलता, जो अक्सर कृत्रिम बुद्धिमत्ता और मशीन लर्निंग जैसी उन्नत तकनीकों का उपयोग करते हैं, स्थिति को और भी जटिल बना देती है। उदाहरण के लिए, साइबर अपराधी हमलों को स्वचालित करने के लिए एआई का उपयोग कर सकते हैं, जिससे वे अधिक कुशल हो जाते हैं और उन्हें पकड़ना कठिन हो जाता है। इसके फलस्वरूप, संगठनों को सतर्क और अनुकूलनशील रहना चाहिए, नए खतरों का मुकाबला करने के लिए अपने सुरक्षा उपायों को लगातार अपडेट करते रहना चाहिए। साइबर हमलों की बदलती प्रकृति साइबर सुरक्षा के लिए निवारक दृष्टिकोण की मांग करती है, तथा इस क्षेत्र में निरंतर अनुसंधान और विकास की आवश्यकता पर बल देती है।

निष्कर्ष के तौर पर, आज की दुनिया में साइबर सुरक्षा के महत्व को कम करके नहीं आंका जा सकता। जैसे-जैसे साइबर हमलों की जटिलता और उनकी आवृत्ति बढ़ती जा रही है, मजबूत सुरक्षा उपायों की आवश्यकता और भी अधिक बढ़ रही है। प्रौद्योगिकी प्रगति और साइबर सुरक्षा के बीच का संबंध संगठनों और व्यक्तियों के लिए चुनौतियाँ और अवसर दोनों प्रस्तुत करता है। यद्यपि सुरक्षात्मक उपाय विकसित करने में प्रगति हुई है, तथापि साइबर हमलों के जारी खतरे से निपटने के लिए निरंतर सुधार और अनुकूलन के प्रति प्रतिबद्धता की आवश्यकता है। इसके अलावा, साइबर सुरक्षा के व्यापक प्रभाव राष्ट्रीय सुरक्षा, आर्थिक स्थिरता और व्यक्तिगत गोपनीयता को प्रभावित करते हैं। इसलिए, साइबर सुरक्षा जागरूकता और मजबूती की संस्कृति का निर्माण हमारे निरंतर बदलते डिजिटल परिदृश्य से जुड़े जोखिमों को कम करने में महत्वपूर्ण होगा। भावी शोध में साइबर सुरक्षा प्रथाओं के नैतिक पहलुओं पर भी ध्यान दिया जाना चाहिए, विशेषकर गोपनीयता और डेटा संरक्षण के संबंध में।

प्रश्न :

1. **पैराग्राफ 1 के अनुसार, साइबर सुरक्षा का प्राथमिक फोकस क्या है?**
    a. भौतिक संपत्तियों की सुरक्षा

b. कंप्यूटर सिस्टम, नेटवर्क और डेटा की सुरक्षा

c. कंप्यूटर सिस्टम और नेटवर्क की सुरक्षा

d. व्यावसायिक लाभ में वृद्धि

2. **पैराग्राफ 1 में, निम्नलिखित में से प्रत्येक को साइबर सुरक्षा के महत्व के कारण के रूप में उल्लेख किया गया है, सिवाय इसके कि:**

a. साइबर खतरों की संख्या में वृद्धि

b. प्रौद्योगिकी पर बढ़ती निर्भरता

c. रिपोर्ट की गई साइबर घटनाओं में कमी

d. व्यक्तियों और व्यवसायों के लिए उत्पन्न गंभीर जोखिम

3. **रैनसमवेयर हमलों में वृद्धि और साइबर सुरक्षा उपायों के बीच के संबंध के बारे में क्या अनुमान लगाया जा सकता है?**

a. रैनसमवेयर हमलों ने डेटा बैकअप प्रोटोकॉल की आवश्यकता को कम कर दिया है।

b. संगठन साइबर सुरक्षा के बारे में कम चिंतित हो रहे हैं।

c. रैनसमवेयर हमलों में वृद्धि ने सख्त साइबर सुरक्षा उपायों को प्रेरित किया है।

d. साइबर अपराधियों द्वारा भविष्य में रैनसमवेयर का उपयोग करने की संभावना कम है।

4. **लेखक ने पैराग्राफ 2 में विभिन्न प्रकार के साइबर हमलों के उदाहरण क्यों शामिल किए हैं?**

a. साइबर सुरक्षा की जटिलता को दर्शाना

b. यह सुझाव देना कि सभी साइबर हमले समान रूप से हानिकारक हैं

c. साइबर सुरक्षा के लिए एक ही दृष्टिकोण की आवश्यकता पर जोर देना

d. साइबर अपराधियों द्वारा इस्तेमाल की जाने वाली विभिन्न रणनीतियों को उजागर करना

5. **पैराग्राफ 3 में "उल्लंघन" शब्द का अर्थ किसका निकटतम है:**

   a. अतिक्रमण

   b. समझौता

   c. संरक्षण

   d. अवलोकन

6. **पैराग्राफ 4 का मुख्य उद्देश्य क्या है?**

   a. साइबर सुरक्षा के वित्तीय निहितार्थों पर चर्चा करना

   b. साइबर सुरक्षा को बढ़ाने के लिए संगठनों द्वारा किए जा रहे उपायों की रूपरेखा तैयार करना

   c. साइबर हमलों में प्रौद्योगिकी की भूमिका की व्याख्या करना

   d. साइबर सुरक्षा में मानवीय त्रुटि के महत्व को उजागर करना

7. **साइबर सुरक्षा सिर्फ़ एक तकनीकी मुद्दा नहीं है, बल्कि एक सामाजिक चिंता भी है। यह वाक्य कहाँ सबसे सही बैठेगा? आज की दुनिया में साइबर सुरक्षा के महत्व को कम करके नहीं आंका जा सकता।**

   a. जैसे-जैसे साइबर हमलों की जटिलता और उनकी आवृत्ति बढ़ती जा रही है, मजबूत सुरक्षा उपायों की आवश्यकता और अधिक बढ़ गई है।

   b. तकनीकी प्रगति और साइबर सुरक्षा के बीच का संबंध संगठनों और व्यक्तियों के लिए चुनौतियाँ और अवसर दोनों प्रस्तुत करता है।

   c. यद्यपि सुरक्षात्मक उपाय विकसित करने में प्रगति हुई है, तथापि साइबर हमलों के जारी खतरे से निपटने के लिए निरंतर सुधार और अनुकूलन के प्रति प्रतिबद्धता की आवश्यकता है।

   d. इसके अलावा, साइबर सुरक्षा के व्यापक प्रभाव राष्ट्रीय सुरक्षा, आर्थिक स्थिरता और व्यक्तिगत गोपनीयता को प्रभावित करते हैं।