Roll No.....

SECCS-01

Practical Guide on Cyber Security

First Semester Examination, 2024 (June)

Time : 2 Hours] **[Maximum Marks : 40**

Roll No. (in figures) : .....
अनुक्रमांक अंकों में
Roll No. (in words) : .....
अनुक्रमांक शब्दों में
Examination Centre : .....
परीक्षा केन्द्र

Invigilator's Signature

DO NOT OPEN THE BOOKLET UNTIL YOU ARE ASKED TO DO SO.

जब तक कहा न जाये, पुस्तिका न खोलें।

FIRST READ ALL THE INSTRUCTIONS / पहले सभी निर्देशों को पढ़ लें।

Important instructions / महत्वपूर्ण निर्देश

1. This paper consists of 40 multiple choice questions (M.C.Q.). All questions are compulsory and carry 01 mark each. There is not negative marking.
   इस प्रश्न पत्र में 40 बहुविकल्पीय प्रश्न हैं। सभी प्रश्न अनिवार्य हैं व प्रत्येक प्रश्न 01 अंक का है। गलत उत्तर के लिए अंक नहीं काटे जायेंगे।
2. Each question has four alternative responses marked (A), (B), (C) and (D). You have to choose an appropriate answer option and mark it on the OMR sheet.
   प्रत्येक प्रश्न के चार उत्तर विकल्प (A), (B), (C) एवं (D) दिए गए हैं। आपको उपयुक्त उत्तर विकल्प का चुनाव कर ओ एम आर प्रपत्र पर अंकित करना है।
3. For marking answers on OMR sheet, follow the detailed instructions given on the OMR Sheet.
   ओ0एम0आर0 प्रपत्र पर अपने सही उत्तर को चिन्हित करने के लिए प्रपत्र पर अंकित निर्देशों का पालन कीजिए।
4. Use only Blue or Black ball point pen for marking on OMR.
   ओ0एम0आर0 पर चिन्ह लगाने के लिए केवल नीली या काली बॉल प्वाइन्ट पैन का ही इस्तेमाल कीजिए।

1. What is the first line of defense against hackers when accessing online accounts?
   (A) Weak passwords
   (B) Multi-factor authentication
   (C) Sharing login details openly
   (D) Ignoring account security settings

2. What is the practice of keeping software and systems up-to-date to protect against known vulnerabilities called?
   (A) Outdated software
   (B) System negligence
   (C) Software stagnation
   (D) Patching

3. How can individuals enhance the security of their Wi-Fi network?
   (A) Use default router passwords
   (B) Disable encryption
   (C) Enable WPA3 encryption and change default passwords
   (D) Share Wi-Fi passwords neighbors

4. What is a recommended practice to create a strong and secure password?
   (A) Use your name and birthdate
   (B) Include a mix of uppercase, lowercase, numbers, and symbols
   (C) Keep it short for easy remembrance
   (D) Share it with trusted friends

5. What is the purpose of two-factor authentication (2FA)?
   (A) To make login difficult
   (B) To provide an extra layer of security by verifying the user's identity through two different methods
   (C) To simplify the login process
   (D) To increase the risk of unauthorized access

1. ऑनलाइन खातों तक पहुँचते समय हैक्से के खिलाफ पहली रक्षा क्या है?
   (A) कमजोर पासवर्ड
   (B) मल्टी-फैक्टर प्रमाणीकरण
   (C) लॉगिन विवरणों को खुलकर साझा करना
   (D) खाता सुरक्षा सेटिंग्स को नजरअंदाज करना

2. सॉफ्टवेयर और सिस्टम को ज्ञात सुरक्षा कमी के खिलाफ अपडेट रखने का अभ्यास किसे कहा जाता है?
   (A) पुराने सॉफ्टवेयर
   (B) सिस्टम की लापरवाही
   (C) सॉफ्टवेयर स्थिरता
   (D) पैंचिंग

3. Wi-Fi नेटवर्क की सुरक्षा कैसे बढाई जा सकती है?
   (A) डिफॉल्ट राउटर पासवर्ड का उपयोग करना
   (B) एन्क्रिप्शन को अक्षम करना
   (C) एन्क्रिप्शन सक्षम करें और डिफॉल्ट पासवर्ड बदलें
   (D) पड़ोसी के साथ वाईफाई पासवर्ड साझा करना

4. एक मजबूत और सुरक्षित पासवर्ड बनाने के लिए एक सुझाए गए अभ्यास क्या है?
   (A) अपना नाम और जन्मतिथि उपयोग करें
   (B) अपरकेस, लोअरकेस, संख्या, और चिन्हों का मिश्रण शामिल करें
   (C) इसे आसान स्मरण के लिए छोटा रखें
   (D) इसे विश्वसनीय दोस्तों के साथ साझा करें

5. टू-फैक्टर प्रमाणीकरण (2FA) का उद्देश्य क्या है?
   (A) लॉगिन को कठिन बनाने के लिए
   (B) उपयोगकर्ता की पहचान को दो विभिन्न तरीकों से सत्यापित करके एक अतिरिक्त सुरक्षा स्तर प्रदान करने के लिए
   (C) लॉगिन प्रक्रिया को सरल बनाने के लिए
   (D) अनधिकृत पहुंच के जोखिम को बढ़ाने के लिए

6. What is the primary purposes of enabling a screen lock on your mobile device?
   (A) Enhance battery life
   (B) Personalize the device
   (C) Protect sensitive data and unauthorized access
   (D) Improve network connectivity

7. What is the recommended action if your mobile device is lost or stolen?
   (A) Ignore it, as it's just a device
   (B) Report the loss to the device manufacturer
   (C) Inform the local police immediately
   (D) Share the incident on social media for help

8. What is the purpose of mobile antivirus software?
   (A) Improve battery performance
   (B) Enhance call quality
   (C) Increase storage capacity
   (D) Protect against malicious software and threats

9. What is the significance of keeping your mobile operating system updated?
   (A) To change the device's appearance
   (B) To receive the latest features and security patches
   (C) To decrease device speed
   (D) To reduce battery life

6. अपने मोबाइल डिवाइस पर स्क्रीन लॉक सक्षम करने का मुख्य उद्देश्य क्या है?
   (A) बैटरी लाइफ को बढ़ावा देना
   (B) डिवाइस को व्यक्तिगत करना
   (C) संवेदनशील डेटा और अनधिकृत पहुंच से बचाना
   (D) नेटवर्क कनेक्टिविटी को सुधारना

7. यदि आपका मोबाइल डिवाइस खो जाता है या चोरी हो जाता है, तो सुझाव क्या है?
   (A) इसे नजरअंदाज करें, क्योंकि यह केवल एक डिवाइस है
   (B) डिवाइस निर्माता को हानि की सूचना दें
   (C) स्थानीय पुलिस को तुरंत सूचित करें
   (D) सोशल मीडिया पर मदद के लिए घटना साझा करें

8. मोबाइल एंटीवायरस सॉफ्टवेयर का उद्देश्य क्या है?
   (A) बैटरी प्रदर्शन में सुधार करना
   (B) कॉल क्वालिटी में सुधार करना
   (C) स्टोरेज क्षमता बढ़ाना
   (D) हानिकारक सॉफ्टवेयर और खतरों से बचाना

9. अपने मोबाइल ऑपरेटिंग सिस्टम को अपडेट रखने का क्या महत्व है?
   (A) डिवाइस का स्वरूप बदलने के लिए
   (B) नवीनतम सुविधाएँ और सुरक्षा पैच प्राप्त करने के लिए
   (C) डिवाइस की गति को कम करने के लिए
   (D) बैटरी लाइफ को कम करने के लिए

10. What should you avoid while using your credit/debit card online?
(A) Share your card details on social media
(B) Use public computers for online transactions
(C) Keep the PIN written on the card
(D) All of the above

11. If you lose your card, what should you do?
(A) Inform the bank immediately
(B) Contemplate the bank's phone number
(C) Slowly attempt to find the card
(D) Any of the above

12. What is the purpose of the three-digit CVV on the back of your card?
(A) Access the cardholder's account
(B) Verify online transactions
(C) Unlock the card
(D) All of the above

13. What may happen if you use a credit/debit card insecurely?
(A) Unauthorized transactions
(B) Increased credit limit
(C) Enhanced security features
(D) None of the above

14. What does SSID stand for in the context of Wi-Fi networks?
(A) Secure System Identifier
(B) Service Set Identifier
(C) Signal Strength Identifier
(D) System Security Identifier

10. अपने क्रेडिट/डेबिट कार्ड का ऑनलाइन उपयोग करते समय आपको किस चीज से बचना चाहिए?
(A) सोशल मीडिया पर अपनी कार्ड विवरण साझा करें
(B) ऑनलाइन लेन-देन के लिए सार्वजनिक कंप्यूटर का उपयोग करें
(C) पिन को कार्ड पर लिखा रखें
(D) उपर्युक्त सभी

11. अगर आप अपना कार्ड खो देते हैं, तो आपको क्या करना चाहिए?
(A) तुरंत बैंक को सूचित करें
(B) बैंक के फोन नंबर पर विचार करें
(C) धीरे-धीरे कार्ड खोजने का प्रयास करें
(D) उपर्युक्त में से कोई भी

12. आपके कार्ड के पीछे तीन-अंकीय सीवीवी का क्या उद्देश्य है?
(A) कार्डधारक के खाते तक पहुँचना
(B) ऑनलाइन लेन-देन की पुष्टि करना
(C) कार्ड को अनलॉक करना
(D) उपर्युक्त सभी

13. यदि आप क्रेडिट/डेबिट कार्ड का असुरक्षित इस्तेमाल करते हैं, तो क्या हो सकता है?
(A) अनधिकृत लेन-देन
(B) क्रेडिट सीमा में वृद्धि
(C) बढ़ाई गई सुरक्षा सुविधाएँ
(D) उपर्युक्त में से कोई भी नहीं

14. Wi-Fi नेटवर्क के संदर्भ में SSID का क्या अर्थ है?
(A) Secure System Identifier
(B) Service Set Identifier
(C) Signal Strength Identifier
(D) System Security Identifier

15. What is the purpose of MAC filtering in Wi-Fi security?
(A) Managing network speed
(B) Filtering internet content
(C) Restricting device access
(D) Enhancing signal strength

16. What is a common step to enhance Wi-Fi security?
(A) Broadcasting SSID
(B) Using default passwords
(C) Disabling encryption
(D) Regularly updating firmware

17. What does HTML stand for?
(A) Hyper Text and Multimedia Language
(B) Hyperlink and Text Markup Language
(C) High-Level Text Markup Language
(D) HyperText Markup Language

18. Which protocol is used for sending emails?
(A) HTTP
(B) SMTP
(C) FTP
(D) TCP

19. What is the full form of ISP in the context of the Internet?
(A) Internet Service Provider
(B) International Service Provider
(C) Intranet Service Provider
(D) Integrated Service Provider

15. Wi-Fi सुरक्षा में MAC फिल्टरिंग का उद्देश्य क्या है?
(A) नेटवर्क स्पीड प्रबंधन
(B) इंटरनेट सामग्री छाँटना
(C) डिवाइस पहुँच प्रतिबंधित करना
(D) सिग्नल ताकत बढ़ाना

16. Wi-Fi सुरक्षा को बढ़ाने के लिए सामान्य कदम क्या है?
(A) SSID प्रसारण
(B) डिफॉल्ट पासवर्ड का उपयोग
(C) एन्क्रिप्शन को अक्षम करना
(D) नियमित रूप से फर्मवेयर अपडेट करना

17. HTML का मतलब क्या है?
(A) Hyper Text and Multimedia Language
(B) Hyperlink and Text Markup Language
(C) High-Level Text Markup Language
(D) HyperText Markup Language

18. ईमेल भेजने के लिए कौन-कौन सा प्रोटोकॉल उपयोग होता है?
(A) HTTP
(B) SMTP
(C) FTP
(D) TCP

19. इंटरनेट के संदर्भ में ISP का पूरा नाम में क्या है?
(A) Internet Service Provider
(B) International Service Provider
(C) Intranet Service Provider
(D) Integrated Service Provider

20. What is the purpose of a firewall in network security?
(A) To enhance internet speed
(B) To filter network traffic
(C) To create a secure tunnel
(D) To increase device compatibility

21. Which protocol is used for secure data transfer between the browser and the web server?
(A) HTTP
(B) FTP
(C) SSH
(D) HTTPS

22. How can you identify a phishing email?
(A) It asks for personal information
(B) It comes from a known contact
(C) It contains only text
(D) It has a catchy subject line

23. What should you avoid in instant messaging to ensure security?
(A) Use strong, unique passwords
(B) Share personal details freely
(C) Accept messages from unknown contacts
(D) Use public computers for messaging

24. What is a common security measure for social networking accounts?
(A) Sharing passwords openly
(B) Using the same password for multiple accounts
(C) Enabling two-factor authentication
(D) Ignoring privacy settings

20. नेटवर्क सुरक्षा में फायरवॉल का क्या उद्देश्य है?
(A) इंटरनेट स्पीड को बढ़ाने के लिए
(B) नेटवर्क ट्रैफिक को छाँटने के लिए
(C) एक सुरक्षित टनल बनाने के लिए
(D) डिवाइस संगतता बढ़ाने के लिए

21. ब्राउजर और वेब सर्वर के बीच सुरक्षित डेटा स्थानांतरण के लिए कौन-कौन सा प्रोटोकॉल उपयोग होता है?
(A) HTTP
(B) FTP
(C) SSH
(D) HTTPS

22. आप कैसे पता लगा सकते हैं कि एक फिशिंग ईमेल है?
(A) यह व्यक्तिगत जानकारी के लिए पूछता है
(B) यह एक जाने-माने संपर्क से आता है
(C) यह केवल पाठ होता है
(D) इसमें एक आकर्षक विषय लाइन होती है

23. सुरक्षा सुनिश्चित करने के लिए तत्काल संदेशिका में क्या बचना चाहिए?
(A) मजबूत, अद्वितीय पासवर्ड का उपयोग करें
(B) व्यक्तिगत विवरणों को स्वतंत्रता से साझा करें
(C) अज्ञात संपर्कों से संदेश स्वीकार करें
(D) संदेशिका के लिए सार्वजनिक कंप्यूटर का उपयोग करें

24. सोशल नेटवर्किंग खातों के लिए एक सामान्य सुरक्षा उपाय क्या है?
(A) पासवर्डों को स्वतंत्रता से साझा करना
(B) कई खातों के लिए एक ही पासवर्ड का उपयोग करना
(C) टू-फैक्टर ऑथेंटिकेशन सक्षम करना
(D) गोपनीयता सेटिंग्स को नजरअंदाज करना

25. How often should you review and update your privacy settings on social media platforms?
(A) Never
(B) Once a year
(C) Only when prompted
(D) Regularly

26. What should you do if you come across suspicious or inappropriate content on social media?
(A) Like and share the content
(B) Report the content to the platform
(C) Ignore it
(D) Engage in negative comments

27. What is a recommended practice when downloading files from the internet?
(A) Download files from untrusted sources
(B) Use a reliable antivirus program
(C) Disable firewall protection
(D) Ignore file extensions

28. How can you verify the authenticity of a downloaded file?
(A) Ignore digital signatures
(B) Check the file size
(C) Use checksums or hashes
(D) Download file from any source

25. सोशल मीडिया प्लेटफॉर्म्स पर अपनी गोपनीयता सेटिंग्स को कितनी बार समीक्षा और अपडेट करना चाहिए?
(A) कभी नहीं
(B) एक बार साल में
(C) केवल जब कहा जाए
(D) नियमित रूप से

26. यदि आप सोशल मीडिया पर संदिग्ध या अनुचित सामग्री के साथ सामना करते हैं, तो आपको क्या करना चाहिए?
(A) सामग्री को लाइक और साझा करें
(B) प्लेटफॉर्म को सामग्री की सूचना दें
(C) इसे नजरअंदाज करें
(D) नकारात्मक टिप्पणियों में व्यस्त रहें

27. इंटरनेट से फाइलें डाउनलोड करते समय का सुझाव क्या है?
(A) अविश्वसनीय स्रोतों से फाइलें डाउनलोड करें
(B) एक विश्वसनीय एंटीवायरस प्रोग्राम का उपयोग करें
(C) फायरवॉल सुरक्षा को अक्षम करें
(D) फाइल एक्सटेंशन को नजरअंदाज करें

28. डाउनलोड की गई फाइल की सत्यापन कैसे कर सकते है?
(A) डिजिटल साइनेचर्स को नजरअंदाज करें
(B) फाइल का आकार जाँचें
(C) चेकसम या हैश का उपयोग करें
(D) किसी भी स्रोत से फाइलें डाउनलोड करें

29. What is a potential risk when uploading files to online platforms?
(A) Loss of internet connection
(B) Unauthorized access to your files
(C) Improved file accessibility
(D) Enhanced file security

30. What should you avoid when uploading files to cloud storage?
(A) Regularly update file permissions
(B) Share files publicly by default
(C) Encrypt sensitive files before uploading
(D) Use the same password for all files

31. What is a recommended practice for ensuring the security of instant messaging?
(A) Share sensitive information freely
(B) Use end-to-end encryption when available
(C) Accept messages from unknown contacts
(D) Disable notifications

32. Why is it important to log out of instant messaging apps when not in use?
(A) To save battery life
(B) To prevent unauthorized access
(C) To receive notifications
(D) To reset chat history

29. ऑनलाइन प्लेटफॉर्म पर फाइलें अपलोड करते समय क्या संभावित जोखिम है?
(A) इंटरनेट कनेक्शन का नुकसान
(B) आपकी फाइलों का अनधिकृत पहुँच
(C) फाइल पहुँचने योग्यता में सुधार
(D) फाइल सुरक्षा में सुधार

30. क्लाउड स्टोरेज पर फाइलें अपलोड करते समय आपको किन चीज़ों से बचना चाहिए?
(A) फाइल अनुमतियों को नियमित रूप से अपडेट करें
(B) डिफॉल्ट रूप से फाइलें सार्वजनिक रूप से साझा करें
(C) अपलोड करने से पहले संवेदनशील फाइलें एन्क्रिप्ट करें
(D) सभी फाइलों के लिए एक ही पासवर्ड का उपयोग करें

31. इंस्टेंट मैसेजिंग की सुरक्षा सुनिश्चित करने के लिए किस सुझाव का पालन करना चाहिए?
(A) संवेदनशील जानकारी को स्वतंत्रता से साझा करें
(B) जब उपलब्ध हो, तो एंड-टू-एंड एन्क्रिप्शन का उपयोग करें
(C) अज्ञात संपर्कों से संदेश स्वीकार करें
(D) नोटीफिकेशन निष्क्रिय करें

32. जब उपयोग में नहीं है, तो इंस्टेंट मैसेजिंग एप्स से लॉग आउट करना क्यों महत्वपूर्ण है?
(A) बैटरी जीवन बचाने के लिए
(B) अनधिकृत पहुँच को रोकने के लिए
(C) सूचनाएँ प्राप्त करने के लिए
(D) चैट हिस्ट्री को रीसेट करने के लिए

33. What is a crucial step to enhance security while playing online games?
(A) Share your gaming account details
(B) Use a weak password for easy recall
(C) Install and update antivirus software
(D) Accept friend requests from unknown players

34. What is a potential risk of downloading games from unofficial sources?
(A) Enhanced gaming experience
(B) Malware and viruses
(C) Faster download speed
(D) Access to exclusive content

35. How can you protect your gaming account from unauthorized access?
(A) Use a public computer for logins
(B) Share your password with trusted friends
(C) Enable two-factor authentification
(D) Use a common password for multiple accounts

36. What is a recommended practice to enhance the security of your blog?
(A) Share your login credentials openly
(B) Use a simple and easily guessable password
(C) Regularly update your blogging platform and plugins
(D) Keep all blog content private

33. ऑनलाइन गेमिंग करते समय सुरक्षा बढ़ाने के लिए क्या महत्वपूर्ण कदम है?
(A) अपने गेमिंग खाते की विवरण साझा करें
(B) आसान स्मरण के लिए कमजोर पासवर्ड का उपयोग करें
(C) एंटीवायरस सॉफ्टवेयर स्थापित और अपडेट करें
(D) अज्ञात खिलाड़ियों से आने वाले फ्रेंड रिक्वेस्ट स्वीकार करें

34. अनधिकृत स्रोतों से गेम्स डाउनलोड करने का क्या संभावित खतरा है?
(A) सुधारित गेमिंग अनुभव
(B) मैलवेयर और वायरस
(C) तेज डाउनलोड स्पीड
(D) विशेष सामग्री तक पहुँच

35. अनधिकृत पहुँच से अपने गेमिंग खाते की सुरक्षा कैसे कर सकते है?
(A) लॉगिन के लिए सार्वजनिक कंप्यूटर का उपयोग करें
(B) विश्वसनीय दोस्तों के साथ अपना पासवर्ड साझा करे
(C) दो-पैर यौगिक प्राधिकृत को सक्षम करें
(D) कई खातों के लिए एक सामान्य पासवर्ड का उपयोग करें

36. अपने ब्लॉग की सुरक्षा बढ़ाने के लिए क्या सुझावित अभ्यास है?
(A) अपनी लॉगिन सामग्री खुलकर साझा करें
(B) एक सरल और आसानी से अनुमान लगाया जा सकने वाला पासवर्ड का उपयोग करें
(C) नियमित रूप से अपने ब्लॉगिंग प्लेटफॉर्म और प्लगइन्स को अपडेट करें
(D) सभी ब्लॉग सामग्री को निजी रखें

37. What should bloggers consider to protect their intellectual property in the content they create?
(A) Allow free use without attribution
(B) Use watermarks on all blog images
(C) Avoid copyright notices
(D) License their content and enforce it

38. Why is it crucial to use secure and reputable hosting services for your blog?
(A) To save money on hosting fees
(B) To compromise on security for better performance
(C) To ensure website speed is not affected
(D) To protect against security threats and downtime

39. What is the potential risk associated with cyberbullying?
(A) Increased online collaboration
(B) Enhanced self-esteem of the victim
(C) Emotional and psychological harm
(D) Improved social relationships

40. How can one respond to a situation of cyberbullying?
(A) Retaliate with similar behavior
(B) Ignore the bullying and hope it stops
(C) Report the incident to a trusted adult or authority
(D) Share the experience openly on social media

37. ब्लॉगर्स को अपने द्वारा बनाई गई सामग्री में अपने बौद्धिक संपत्ति की सुरक्षा के लिए क्या विचार करना चाहिए?
(A) बिना श्रेय दिए मुक्ति दे
(B) सभी ब्लॉग छवियों पर वॉटरमार्क का उपयोग करें
(C) कॉपीराइट सूचनाओं से बचें
(D) अपनी सामग्री को लाइसेंस दें और इसे प्रवर्तित करें

38. अपने ब्लॉग के लिए सुरक्षित और मान्यता प्राप्त होस्टिंग सेवाओं का उपयोग करना क्यों अत्यंत महत्वपूर्ण है?
(A) होस्टिंग शुल्क पर पैसे बचाने के लिए
(B) बेहतर प्रदर्शन के लिए सुरक्षा पर कमी करने के लिए
(C) वेबसाइट की गति पर असर नहीं होने की सुनिश्चित करने के लिए
(D) सुरक्षा खतरों और डाउनटाइम के खिलाफ सुरक्षित रखने के लिए

39. साइबरबुलीइंग के साथ जुड़े जोखिम क्या है?
(A) ऑनलाइन सहयोग बढ़ा
(B) पीड़िता का आत्म-सम्मान में सुधार
(C) भावनात्मक और मानसिक क्षति
(D) सुधारे गए सामाजिक रिश्ते

40. साइबरबुलीइंग की स्थिति का कैसे प्रतिसाद दिया जा सकता है?
(A) इसी प्रकार के व्यवहार के साथ प्रतिक्रिया करें
(B) बुलींग को नजरअंदाज करें और यह रोकने की आशा करें
(C) घटना को एक विश्वसनीय वयस्क या प्राधिकृति को सूचित करें
(D) अनुभव को सामाजिक मीडिया पर खुलकर साझा करें

[SPACE FOR ROUGH WORK / कच्चे काम के लिए पत्रक]