SECCS-01

1st Semester Examination, 2023 (Dec.)

Practical Guide on Cyber Security

Time : 2 Hours] **[Max. Marks : 40**

Roll. No. (in figures) : .....

अनुक्रमांक अंकों में

Roll No. (in words) : .....

अनुक्रमांक शब्दों में

Examination Centre : .....

परीक्षा केन्द्र

Invigilator's Signature

First Read All The Instructions / पहले सभी निर्देशों को पढ़ लें

Important Instructions / महत्वूपर्ण निर्देश

---

1. This paper consists of 40 Multiple Choice Questions (M.C.Q.). All questions are compulsory and carry 01 mark each. There is no 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.
   ओ.एम.आर. 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.
   ओ.एम.आर. पर चिन्ह लगाने के लिए केवल नीली या काली बॉल प्वॉइन्ट पैन का ही इस्तेमाल कीजिए।

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

जब तक कहा न जाये, पुस्तिका न खोलें

1. To ensure secure usage of credit/debit cards or ATM, what should you do?
   (A) Keep your PIN secure
   (B) Share your PIN with acquintances
   (C) Use outdated software
   (D) All of the above

2. 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

3. 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

4. What is the primary purpose of a WPA key in Wi-Fi security?
   (A) Signal strength
   (B) Network speed
   (C) Data encryption
   (D) Device compatibility

5. 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

1. क्रेडिट/डेबिट कार्ड और एटीएम का सुरक्षित उपयोग सुनिश्चित करने के लिए आपको क्या करना चाहिए?
   (A) अपने पिन को सुरक्षित रखें
   (B) जानकारों के साथ पिन साझा करें
   (C) पुराने सॉफ़्टवेयर का उपयोग करें
   (D) उपर्युक्त सभी

2. अगर आप अपना कार्ड खो देते हैं, तो आपको क्या करना चाहिए?
   (A) तुरंत बैंक को सूचित करें
   (B) बैंक का फ़ोन नंबर सोचें
   (C) धीरे-धीरे कार्ड खोजने का प्रयोग करें
   (D) उपर्युक्त में से कोई भी

3. 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

4. Wi-Fi सुरक्षा में WPA कुंजी का मुख्य उद्देश्य क्या है?
   (A) सिग्नल ताकत
   (B) नेटवर्क स्पीड
   (C) डेटा एन्क्रिप्शन
   (D) डिवाइस अनुकूलता

5. Wi-Fi नेटवर्क के संदर्भ में SSID का क्या अर्थ है?
   (A) सिक्योर सिस्टम आइडेंटिफायर
   (B) सर्विस सेट आइडेन्टिफायर
   (C) सिग्नल स्ट्रैन्थ आइडेन्टिफायर
   (D) सिस्टम सिक्योरिटी आइडेनिटफायर

6. Which encryption protocol is considered the most secure for Wi-Fi networks?
(A) WEP
(B) WPA
(C) TKIP
(D) WPA2

7. What does URL stand for?
(A) Universal Resource Link
(B) Unified Rersource Locator
(C) Unique Resource Link
(D) Uniform Resource Locator

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

9. What does SSL/TLS stand for in the context of browser security?
(A) Secure Socket Layer/Transport Layer Security
(B) Safe Surfing Link/Technical Layer Security
(C) Secure Surfing Layer/Transport Link Security
(D) Systematic Security Layer/Technical Link Security

10. Which of the following is a secure way to store passwords in browsers?
(A) Saving in plain text
(B) Using a password manager
(C) Sharing with friends
(D) Emailing passwords to yourself

6. Wi-Fi नेटवर्क के लिए कौन-कौन सा एन्क्रिप्शन प्रोटोकॉल सबसे सुरक्षित माना जाता है?
(A) WEP
(B) WPA
(C) TKIP
(D) WPA2

7. URL का अर्थ क्या है?
(A) यूनिवर्सल रिसोर्स लिंक
(B) यूनिफाइड रिसोर्स लोकेटर
(C) यूनिक रिसोर्स लिंक
(D) यूनिफोर्म रिसोर्स लोकेटर

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

9. ब्राउज़र सुरक्षा के संदर्भ में SSL/TLS का अर्थ क्या है?
(A) Secure Socket Layer/Transport Layer Security
(B) Safe Surfing Link/Technical Layer Security
(C) Secure Surfing Layer/Transport Link Security
(D) Systematic Security Layer/Technical Link Security

10. निम्नलिखित में से कौन-कौन सा एक सुरक्षित तरीका है जिससे ब्राउज़र में पासवर्ड सहेजा जा सकता है?
(A) सादा टैक्स्ट में सहेजना
(B) पासवर्ड मैनेजर का उपयोग करना
(C) दोस्तों के साथ साझा करना
(D) खुद को पासवर्ड ईमेल करना

11. What is the purpose of the "Do Not Track" (DNT) feature in browsers?
(A) To speed up browsing
(B) To disable images
(C) To prevent tracking of user activity
(D) To block JavaScript

12. What is a phishing website?
(A) A website with a lot of fish images
(B) A website that steals sensitive information
(C) A website for fishing enthusiasts
(D) A website that sells fish online

13. What is a common threat associated with email communication?
(A) Phishing attacks
(B) Online gaming risks
(C) Social media likes
(D) Browser security

14. 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

15. What is a recommended practice for handling emails securely?
(A) Click on all links in the email
(B) Open email attachments from unknown sources
(C) Verify the sender's email address
(D) Share sensitive information in emails

11. ब्राउज़र में "डू नॉट ट्रैक" (DNT) फीचर का क्या उद्देश्य है?
(A) ब्राउजिंग को तेज करने के लिए
(B) छवियों को अक्षम करने के लिए
(C) उपयोगकर्ता गतिविधि का ट्रैकिंग रोकने के लिए
(D) जावास्क्रिप्ट को ब्लॉक करने के लिए

12. फिशिंग वेबसाइट क्या है?
(A) एक वेबसाइट जिसमें कई मछलियों की फोटो हैं
(B) एक वेबसाइट जो संवेदनशील जानकारी चुरा लेती है
(C) एक वेबसाइट जो मछली प्रेमियों के लिए हैं
(D) एक वेबसाइट जो ऑनलाइन मछली बेचती है

13. ईमेल संवाद के साथ संबंधित एक सामान्य खतरा क्या है?
(A) फिशिंग हमले
(B) ऑनलाइन गेमिंग की चुनौतियाँ
(C) सोशल मीडिया लाइक्स
(D) ब्राउज़र सुरक्षा

14. 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 टेक्स्ट होता है
(D) इसमें एक आकर्षक विषय लाइन होती है

15. ईमेल को सुरक्षित रूप से संभालने के लिए अनुशंसित अभ्यास क्या है?
(A) ईमेल में सभी लिंक पर क्लिक करें
(B) अज्ञात स्रोतों से ईमेल के अटैचमेंट्स खोलें
(C) भेजने वाले के ईमेल पते को सत्यापित करें
(D) ईमेल में संवेदनशील जानकारी साझा करें

16. 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

17. 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

18. What information should you avoid sharing publicly on social media?
(A) Birthday
(B) Hobbies and interests
(C) Work accomplishments
(D) All of the above

19. 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

16. सुरक्षा सुनिश्चित करने के लिए आपको इंस्टेंट मेस्सेंजिंग में क्या करने से 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 (मेस्सेंजिंग) के लिए सार्वजनिक कंप्यूटर का उपयोग करें

17. सोशल नेटवर्किंग एकाउंट्स 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

18. आपको कौन सी जानकारी सोशल मीडिया पर सार्वजनिक रूप से साझा करने से बचना चाहिए?
(A) जन्मदिन
(B) शौक और रुचियां
(C) काम की प्रशंसाएँ
(D) उपर्युक्त सभी

19. इंटरनेट से फ़ाइलें डाउनलोड करते समय का सुझाव क्या है?
(A) अविश्वसनीय स्रोतों से फ़ाइलें डाउनलोड करें
(B) एक विश्वसनीय एंटीवायरस प्रोग्राम का उपयोग करें
(C) फ़ायरवॉल सुरक्षा को अक्षम करें
(D) फ़ाइल एक्सटेंशन को नजरअंदाज करें

20. 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 files from any source

21. What precaution should be taken when downloading email attachments?

(A) Open attachments from unknown sources

(B) Use a separate email account for attachments

(C) Download all attachments without scanning

(D) Disable antivirus software while downloading attachments

22. 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

23. What should you avoid in instant messaging to enhance security?

(A) Use strong and unique passwords

(B) Click on links from unknown senders

(C) Keep conversations private

(D) Share personal details in group chats

20. डाउनलोड की गई फ़ाइल की सत्यापन कैसे कर सकते हैं?

(A) डिजिटल साइनेचर्स को नजरअंदाज करें

(B) फ़ाइल का आकार जाँचें

(C) चेकसम या हैश का उपयोग करें

(D) किसी भी स्रोत से फ़ाइलें डाउनलोड करें

21. ईमेल अटैचमेंट्स डाउनलोड करते समय कौन सी सावधानी बरतनी चाहिए?

(A) अज्ञात स्रोतों से अटैचमेंट्स खोलें

(B) अटैचमेंट्स के लिए एक अलग ईमेल खाता उपयोग करें

(C) स्कैनिंग के बिना सभी अटैचमेंट्स डाउनलोड करें

(D) अटैचमेंट्स डाउनलोड करते समय एंटीवायरस सॉफ़्टवेयर को अक्षम करें

22. 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) सूचनाएँ अक्षम करें

23. सुरक्षा को बढ़ाने के लिए इंस्टेंट मैसेजिंग में आपको क्या नहीं करना चाहिए?

(A) मजबूत और अद्वितीय पासवर्ड का उपयोग करें

(B) अज्ञात भेजने वालों के लिए लिंक पर क्लिक करें

(C) बातचीत को निजी रखें

(D) समूह चैट में व्यक्तिगत विवरण साझा करें

24. What precaution should you take when receiving links in instant messages?

(A) Click on all links without hesitation

(B) Verify the sender before clicking

(C) Share the links with others immediately

(D) Disable link previews

25. 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

26. Why is it essential to use strong and unique passwords for gaming accounts?

(A) To impress other gamers

(B) To prevent unauthorized access and hacking

(C) For easy sharing with friends

(D) To comply with gaming regulations

27. Why should you be cautious about sharing personal information in online gaming communities?

(A) To make new friends easily

(B) To receive in-game rewards

(C) To avoid potential threats like doxing

(D) To gain popularity among gamers

24. इंस्टेंट मैसेजिंग में लिंक प्राप्त करते समय आपको कौन सी सावधानी बरतनी चाहिए?

(A) बिना संदेह के सभी लिंक पर क्लिक करें

(B) क्लिक करने से पहले भेजने वाले की पहचान सत्यापित करें

(C) तुरंत अन्यों के साथ लिंक साझा करें

(D) लिंक पूर्वावलोकन को अक्षम करें

25. 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

26. गेमिंग खातों के लिए मजबूत और अद्वितीय पासवर्ड का उपयोग करना क्यों आवश्यक है?

(A) अन्य गेमर्स को प्रभावित करने के लिए

(B) अनधिकृत पहुँच और हैकिंग को रोकने के लिए

(C) दोस्तों के साथ साझा करने के लिए

(D) गेमिंग विनियमों का पालन करने के लिए

27. ऑनलाइन गेमिंग समुदायों में व्यक्तिगत जानकारी साझा करने के बारे में आपको सतर्क रहने की क्यों आवश्यकता है?

(A) आसानी से नए दोस्त बनाने के लिए

(B) गेम के भीतर पुरस्कार प्राप्त करने के लिए

(C) डॉक्सिंग जैसे संभावित खतरों से बचने के लिए

(D) गेमर्स के बीच पॉपुलैरिटी प्राप्त करने के लिए

28. 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) Use a common password for multiple accounts
(D) Enable two-factor authentication

29. 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

30. Why is it important to monitor and moderate comments on your blog?
(A) To discourage interaction with readers
(B) To prevent spam and inappropriate content
(C) To limit the engagement on your blog
(D) To avoid positive feedback

31. 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

28. अनधिकृत पहुँच से अपने गेमिंग खाते की सुरक्षा कैसे कर सकते हैं?
(A) लॉगिन के लिए सार्वजनिक कंप्यूटर का उपयोग करें
(B) विश्वसनीय दोस्तों के साथ अपना पासवर्ड साझा करें
(C) कई खातों के लिए एक सामान्य पासवर्ड का उपयोग करें
(D) टू-फैक्टर ऑथेंटिकेशन को समक्षम करें

29. 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

30. अपने ब्लॉग पर टिप्पणियों को मॉनिटर और मॉडरेट करना क्यों महत्वपूर्ण है?
(A) पाठकों के साथ बातचीत को निराश करने के लिए
(B) स्पैम और अनुचित सामग्री को रोकने के लिए
(C) अपने ब्लॉग पर बातचीत को सीमित करने के लिए
(D) सकारात्मक प्रतिपुष्टि से बचने के लिए

31. 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

32. How can bloggers enhance the security of their login credentials?

(A) Use easily guessable passwords

(B) Store passwords in plain text

(C) Enable two-factor authentication

(D) Share passwords with fellow bloggers

33. What is the potential risk associated with cyberbullying?

(A) Increased online collaboration

(B) Enhanced self-esteem of the victim

(C) Improved social relationships

(D) Emotional and psychological harm

34. What can be a potential sign of online predator grooming behavior?

(A) Open communication about online activities

(B) Overly protective behavior from parents

(C) Frequent sharing of personal information

(D) Active participation in online communities

35. 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

32. ब्लॉगर्स अपनी लॉगिन सामग्री की सुरक्षा कैसे बढ़ा सकती हैं?

(A) आसानी से अनुमान लगाए जाने वाले पासवर्ड का उपयोग करें

(B) पासवर्डों को सादा टेक्स्ट में स्टोर करें

(C) टू-फैक्टर ऑथेंटिकेशन को सक्षम करें

(D) फेलो ब्लॉगर्स के साथ पासवर्ड साझा करें

33. साइबरबुलीइंग के साथ जुड़े जोखिम क्या है?

(A) ऑनलाइन सहयोग बढ़ा

(B) पीड़िता का आत्म-सम्मान में सुधार

(C) सुधारी गई सामाजिक रिश्तों

(D) भावनात्मक और मानसिक क्षति

34. ऑनलाइन प्रेडेटर ग्रूमिंग व्यवहार का संभावित संकेत क्या हो सकता है?

(A) ऑनलाइन गतिविधियों के बारे में खुली संवाद

(B) माता-पिता से अत्यधिक सुरक्षा व्यवहार

(C) व्यक्तिगत जानकारी का अक्सर साझा करना

(D) ऑनलाइन समुदायों में सक्रिय भागीदारी

35. साइबरबुलिंग की स्थिति पर कोई कैसे प्रतिक्रिया दे सकता है?

(A) इसी प्रकार के व्यवहार के साथ प्रतिक्रिया करें

(B) बुलिंग 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

36. 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) None of these

37. 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

38. 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 with neighbours

39. What is the significance of avoiding easily guessable passwords?
(A) They are easier to remember
(B) They provide better security
(C) They are required by law
(D) They help hackers

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

36. ऑनलाइन खातों तक पहुँचते समय हैकर्स के खिलाफ पहली रक्षा क्या है?
(A) कमजोर पासवर्ड
(B) मल्टी-फैक्टर प्रमाणीकरण
(C) लॉगिन विवरणों को खुलकर साझा करना
(D) इनमें से कोई नहीं

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

38. Wi-Fi नेटवर्क की सुरक्षा कैसे बढ़ाई जा सकती है?
(A) डिफ़ॉल्ट राउटर पासवर्ड का उपयोग करना
(B) एन्क्रिप्शन को अक्षम करना
(C) WPA3 एनिक्रप्शन सक्षम करें और डिफ़ॉल्ट पासवर्ड बदलें
(D) पड़ोसी के साथ वाईफाई पासवर्ड साझा करना

39. आसानी से अनुमान लगाए जाने वाले पासवर्डों से बचने की अहमियत क्या है?
(A) उन्हें आसानी से याद रखा जा सकता है
(B) वे बेहतर सुरक्षा प्रदान करते हैं
(C) उन्हें कानून द्वारा आवश्यकता है
(D) वे हैकर्स की मदद करते हैं

40. आपके 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

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