

1st Semester Examination December, 2024

Practical Guide on Cyber Security

Time : 2:00 Hrs.

Max. Marks : 40

समय : 2:00 घण्टा

अधिकतम अंक : 40

Roll No. (in Figures) :

अनुक्रमांक अंकों में :

Roll No. (in Words) :

अनुक्रमांक शब्दों में :

Examination Centre :

परीक्षा केन्द्र :

Invigilator's Signature / पर्यवेक्षक के हस्ताक्षर

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।

Importance Instructions :

1. This paper consists of **40** Multiple Choice Questions (M.C.Q.). All questions are compulsory and carry **1** mark each. There is not negative marking.
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.
3. For marking answers on OMR sheet, follow the detailed instructions given on the OMR Sheet.
4. Use only Blue or Black ball point pen for marking on OMR.

महत्वपूर्ण निर्देश :

1. इस प्रश्न-पत्र में **40** बहुविकल्पीय प्रश्न हैं। सभी प्रश्न अनिवार्य हैं व प्रत्येक प्रश्न **1** अंक का है। गलत उत्तर के लिए अंक नहीं काटे जायेंगे।
2. प्रत्येक प्रश्न के चार विकल्प (A), (B), (C) एवं (D) दिए गए हैं। आपको उपयुक्त उत्तर विकल्प का चुनाव कर उत्तर ओ.एम. आर. प्रपत्र पर अंकित करना है।
3. ओ.एम.आर. प्रपत्र पर अपने सही उत्तर को चिह्नित करने के लिए प्रपत्र पर अंकित निर्देशों का पालन कीजिए।
4. ओ.एम.आर. पर चिह्न लगाने के लिए केवल नीली या काली बॉल प्वाइन्ट पेन का ही इस्तेमाल कीजिए।

1. What is the primary purpose of hyperlinks on a website ?

- (A) To display images
- (B) To connect different web pages and help with navigation
- (C) To play videos
- (D) To store data

2. What is digital plagiarism ?

- (A) Using licensed software
- (B) Writing original content
- (C) Copying academic work from the internet or fellow students without proper citation
- (D) Using a computer for research

3. How can cookies affect privacy ?

- (A) They can slow down internet browsing
- (B) They prevent access to personal data
- (C) They help in downloading files faster
- (D) They are used to track user preferences and can expose personal information

1. वेबसाइट पर हाइपरलिंक का मुख्य उद्देश्य क्या है ?

- (A) चित्र दिखाना
- (B) अलग-अलग वेब पेजों को जेड़ना और नेविगेट करने में मदद करना
- (C) वीडियो चलाना
- (D) डेटा स्टोर करना

2. डिजिटल साहित्यिक चोरी क्या है ?

- (A) लाइसेंस प्राप्त साफ्टवेयर का उपयोग करना
- (B) मूल सामग्री लिखना
- (C) उचित उद्धरण के बिना इंटरनेट या साथी छात्रों से शैक्षणिक कार्य की नकल करना
- (D) अनुसंधान के लिए कम्प्यूटर का उपयोग करना

3. कुकीज गोपनीयता को कैसे प्रभावित कर सकती हैं ?

- (A) वे इंटरनेट ब्राउजिंग को धीमा कर सकते हैं
- (B) वे व्यक्तिगत डेटा तक पहुँच को रोकते हैं
- (C) वे फ़ाइलों को तेजी से डाउनलोड करने में मदद करते हैं
- (D) इनका उपयोग उपयोगकर्ता की प्राथमिकताओं को ट्रैक करने के लिए किया जाता है और व्यक्तिगत जानकारी को उजागर किया जा सकता है

4. What does Cyber Safety focus on ?

- (A) Protection of hardware from viruses
- (B) Physical protection of technology resources
- (C) Safe and responsible behavior online, protecting personal information
- (D) Monitoring internet usage through security systems

5. Difference between Cyber Safety and Cyber Security :

- (A) Cyber Safety focuses on software security, while Cyber Security focuses on human behavior
- (B) Cyber Safety covers the protection of data and Cyber Security focuses on physical protection of technology
- (C) Cyber Safety involves using the internet, while Cyber Security is about device maintenance
- (D) There is no difference; both terms are used interchangeably

4. साइबर सुरक्षा किस पर केंद्रित है ?

- (A) वायरस से हार्डवेयर की सुरक्षा
- (B) प्रौद्योगिकी संसाधनों की भौतिक सुरक्षा
- (C) व्यक्तिगत जानकारी की सुरक्षा करते हुए ऑनलाइन सुरक्षित और जिम्मेदार व्यवहार
- (D) सुरक्षा प्रणालियों के माध्यम से इंटरनेट उपयोग की निगरानी करना

5. साइबर सेफ्टी और साइबर सिक्योरिटी के बीच अंतर :

- (A) साइबर सुरक्षा सॉफ्टवेयर सुरक्षा पर केंद्रित है जबकि साइबर सुरक्षा मानव व्यवहार पर केंद्रित है
- (B) साइबर सुरक्षा डेटा की सुरक्षा को कवर करती है और साइबर सुरक्षा प्रौद्योगिकी की भौतिक सुरक्षा पर केंद्रित है
- (C) साइबर सुरक्षा में इंटरनेट का उपयोग शामिल है, जबकि साइबर सुरक्षा डिवाइस रखरखाव के बारे में है
- (D) कोई अंतर नहीं है; दोनों शब्दों का प्रयोग परस्पर उपयोग किया जाता है

6. What is Cyberbullying ?

- (A) The use of the internet for personal entertainment
- (B) Sharing educational content online
- (C) Promoting positive online behaviors
- (D) Using the internet to repeatedly harm or harass others intentionally

7. What is a zero-day vulnerability ?

- (A) A known vulnerability with an available fix
- (B) A hardware issue
- (C) An unknown vulnerability exploited by hackers before a fix is available
- (D) A firewall misconfiguration

8. Primary purpose of a web browser :

- (A) To store and organize files
- (B) To access information and resources on the World Wide Web
- (C) To edit and create documents
- (D) To play multimedia files

6. साइबरबुलिंग क्या है ?

- (A) व्यक्तिगत मनोरंजन के लिए इंटरनेट का उपयोग
- (B) शैक्षिक सामग्री ऑनलाइन साझा करना
- (C) सकारात्मक ऑनलाइन व्यवहार को बढ़ावा देना
- (D) जानबूझकर दूसरों को नुकसान पहुँचाने या परेशान करने के लिए इंटरनेट का उपयोग करना

7. शून्य-दिन की भेद्यता क्या है ?

- (A) उपलब्ध समाधान के साथ एक ज्ञात भेद्यता
- (B) एक हार्डवेयर समस्या
- (C) एक अज्ञात भेद्यता जिसका समाधान उपलब्ध होने से पहले हैकर्स द्वारा शोषण किया जाता है
- (D) फ़ायरवॉल ग़लत कॉन्फ़िगरेशन

8. वेब ब्राउजर का प्राथमिक उद्देश्य :

- (A) फाइलों को संग्रहीत और व्यवस्थित करने के लिए
- (B) वर्ल्ड वाइड वेब पर जानकारी और संसाधनों तक पहुँचने के लिए
- (C) दस्तावेजों को संपादित करने और बनाने के लिए
- (D) मल्टीमीडिया फ़ाइलें चलाने के लिए

-
9. What does SMTP stand for ?
- (A) Simple Mail Transfer Protocol
 - (B) Secure Mail Transfer Protocol
 - (C) Standard Mail Transfer Protocol
 - (D) Simple Message Transmission Protocol
-

10. What is one potential consequence of fake profiles on social networking sites ?
- (A) Increased user engagement
 - (B) Identity theft and loss of confidentiality
 - (C) Greater access to educational content
 - (D) Increased exposure to legitimate content
-

11. 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
-

-
9. SMTP का क्या अर्थ है ?
- (A) सरल मेल ट्रांसफर प्रोटोकॉल
 - (B) सुरक्षित मेल ट्रांसफर प्रोटोकॉल
 - (C) मानक मेल स्थानांतरण प्रोटोकॉल
 - (D) सरल संदेश ट्रांसमिशन प्रोटोकॉल
-

10. सोशल नेटवर्किंग साइटों पर नकली प्रोफाइल का एक संभावित परिणाम क्या है ?
- (A) उपयोक्ता सहभागिता में वृद्धि
 - (B) पहचान की चोरी और गोपनीयता की हानि
 - (C) शैक्षिक सामग्री तक अधिक पहुँच
 - (D) वैध सामग्री के संपर्क में वृद्धि
-

11. दो-कारक प्रमाणीकरण (2FA) का उद्देश्य क्या है ?
- (A) लॉगिन को कठिन बनाने के लिए
 - (B) दो अलग-अलग तरीकों से उपयोक्ता की पहचान सत्यापित करके सुरक्षा की एक अतिरिक्त परत प्रदान करना
 - (C) लॉगिन प्रक्रिया को सरल बनाने के लिए
 - (D) अनधिकृत पहुँच के जोखिम को बढ़ाने के लिए
-

12. What is a legal issue that can arise from downloading certain files, such as movies, music, or software ?

- (A) Increased data storage usage
- (B) Faster access to content
- (C) Legal issues related to copyright infringement
- (D) Increased antivirus protection

13. What mistakes should you avoid when using your credit or 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

14. What is a primary risk of sharing personal information on blogging sites ?

- (A) Improved website security
- (B) Increased online visibility
- (C) Identity theft
- (D) Better search engine rankings

15. Which of the following methods are commonly used in cyber stalking ?

- (A) Physical surveillance
- (B) Anonymous letters
- (C) E-mail and instant messaging (IM)
- (D) Phone calls only

12. वह कानूनी समस्या क्या है जो कुछ फाइलें, जैसे फिल्में, संगीत या सॉफ्टवेयर डाउनलोड करने से उत्पन्न हो सकती है ?

- (A) डेटा भण्डारण उपयोग में वृद्धि
- (B) सामग्री तक तेज पहुँच
- (C) कॉपीराइट उल्लंघन से सम्बन्धित कानूनी मुद्दे
- (D) एंटीवायरस सुरक्षा में वृद्धि

13. अपने क्रेडिट या डेबिट कार्ड का ऑनलाइन उपयोग करते समय आपको किन गलतियों से बचना चाहिए ?

- (A) अपने कार्ड का विवरण सोशल मीडिया पर साझा करें
- (B) ऑनलाइन लेनदेन के लिए सार्वजनिक कम्प्यूटर का उपयोग करें
- (C) कार्ड पर पिन लिखकर रखें
- (D) उपरोक्त सभी

14. ब्लॉगिंग साइटों पर व्यक्तिगत जानकारी साझा करने का प्राथमिक जोखिम क्या है ?

- (A) बेहतर वेबसाइट सुरक्षा
- (B) ऑनलाइन दृश्यता में वृद्धि
- (C) पहचान की चोरी
- (D) बेहतर खोज इंजन रैंकिंग

15. साइबर स्टॉकिंग में आमतौर पर निम्नलिखित में से कौन सी विधि का उपयोग किया जाता है ?

- (A) शारीरिक निगरानी
- (B) गुमनाम पत्र
- (C) ई-मेल और त्वरित संदेश (आईएम)
- (D) केवल फोन कॉल

16. What do predators typically ask children to share during grooming ?

- (A) Favorite cartoons
- (B) Personal information and photographs
- (C) Book recommendations
- (D) School projects

17. A common method hackers use to observe passwords from a distance :

- (A) Using binoculars or vision-enhancing tools
- (B) Using encryption software
- (C) Changing passwords frequently
- (D) Creating complex passwords

18. What is one method of protecting mobile phones from connectivity-related security threats ?

- (A) Using public Wi-Fi networks
- (B) Connecting to unknown Bluetooth devices
- (C) Ensuring the mobile phone is not connected to unauthorized networks
- (D) Ignoring app permissions

16. शिकारी आमतौर पर बच्चों को ग्रूमिंग के दौरान क्या साझा करने के लिए कहते हैं ?

- (A) पसंदीदा कार्टून
- (B) व्यक्तिगत जानकारी और तस्वीरें
- (C) पुस्तक अनुशंसाएँ
- (D) स्कूल परियोजनाएँ

17. हैकर्स दूर से पासवर्ड देखने के लिए एक सामान्य तरीका अपनते हैं :

- (A) दूरबीन या दृष्टि बढ़ाने वाले उपकरणों का उपयोग करना
- (B) एन्क्रिप्शन सॉफ्टवेयर का उपयोग करना
- (C) बार-बार पासवर्ड बदलना
- (D) जटिल पासवर्ड बनाना

18. मोबाइल फोन को कनेक्टिविटी-सम्बन्धी सुरक्षा खतरों से बचाने का एक तरीका क्या है ?

- (A) सार्वजनिक वाई-फाई नेटवर्क का उपयोग करना
- (B) अज्ञात ब्लूटूथ डिवाइस से कनेक्ट करना
- (C) यह सुनिश्चित करना कि मोबाइल फोन अनधिकृत नेटवर्क से जुड़ा नहीं है
- (D) ऐप अनुमतियों को अनदेखा करना

19. What is the primary function of Wi-Fi technology ?

- (A) To increase internet speed
- (B) To enhance mobile signal strength
- (C) To transmit data over cellular networks
- (D) To provide a wireless signal for communication between devices

20. What is a recommended practice when downloading files from the internet ?

- (A) Use a reliable antivirus program
- (B) Download files from untrusted sources
- (C) Disable firewall protection
- (D) Ignore file extensions

21. 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

19. वाई-फाई तकनीक का प्राथमिक कार्य क्या है ?

- (A) इंटरनेट स्पीड बढ़ाने के लिए
- (B) मोबाइल सिग्नल की शक्ति बढ़ाने के लिए
- (C) सेलुलर नेटवर्क पर डेटा संचारित करने के लिए
- (D) उपकरणों के बीच संचार के लिए वायरलेस सिग्नल प्रदान करना

20. इंटरनेट से फाइलें डाउनलोड करते समय अनुशंसित अभ्यास क्या है ?

- (A) एक विश्वसनीय एंटीवायरस प्रोग्राम का उपयोग करें
- (B) अविश्वसनीय स्रोतों से फाइलें डाउनलोड करें
- (C) फ़ायरवॉल सुरक्षा अक्षम करें
- (D) फ़ाइल एक्सटेंशन पर ध्यान न दें

21. ऑनलाइन गेम खेलते समय सुरक्षा बढ़ाने के लिए एक महत्वपूर्ण कदम क्या है ?

- (A) अपने गेमिंग खाते का विवरण साझा करें
- (B) आसानी से याद रखने के लिए कमजोर पासवर्ड का उपयोग करें
- (C) एंटीवायरस सॉफ्टवेयर इंस्टॉल और अपडेट करें
- (D) अज्ञात खिलाड़ियों से मित्र अनुरोध स्वीकार करें

22. What type of information is typically stolen in credit card fraud ?

- (A) Only the credit card number
- (B) Only the password
- (C) Credit card number, PIN, and password
- (D) Only the cardholder's name

23. Which of the following is a sign of a phishing attempt on social media ?

- (A) A message from a verified account
- (B) An e-mail asking for your password and login details
- (C) A friend tagging you in a photo
- (D) Receiving a birthday greeting from a friend

24. What is the safest way to store your social media passwords ?

- (A) Write them down on paper
- (B) Save them in your browser without a master password
- (C) Share them with a trusted friend
- (D) Use a secure password manager

22. क्रेडिट कार्ड धोखाधड़ी में आम तौर पर किस प्रकार की जानकारी चुराई जाती है ?

- (A) केवल क्रेडिट कार्ड नंबर
- (B) केवल पासवर्ड
- (C) क्रेडिट कार्ड नम्बर, पिन और पासवर्ड
- (D) केवल कार्डधारक का नाम

23. निम्नलिखित में से कौन सोशल मीडिया पर फिशिंग प्रयास का संकेत है ?

- (A) एक सत्यापित खाते से एक संदेश
- (B) आपका पासवर्ड और लॉगिन विवरण मांगने वाला एक ई-मेल
- (C) एक मित्र आपको फोटो में टैग कर रहा है
- (D) किसी मित्र से जन्मदिन की बधाई प्राप्त करना

24. आपके सोशल मीडिया पासवर्ड को स्टोर करने का सबसे सुरक्षित तरीका क्या है ?

- (A) उन्हें कागज पर लिख लें
- (B) उन्हें बिना मास्टर पासवर्ड के अपने ब्राउजर में सहेजें
- (C) उन्हें किसी विश्वसनीय मित्र के साथ साझा करें
- (D) एक सुरक्षित पासवर्ड मैनेजर का उपयोग करें

-
25. What is the most effective way to secure your mobile phone ?
- (A) Enable biometric authentication (e.g., fingerprint or face ID)
 - (B) Use a simple 4-digit PIN
 - (C) Keep your phone unlocked for convenience
 - (D) Use the same password for all apps
-

26. What is a key indicator of a phishing attack via SMS (Smishing) ?
- (A) SMS from known contacts
 - (B) Messages with urgent language and suspicious links
 - (C) SMS confirming bank transactions
 - (D) Texts from customer service with proper identification
-

27. What does CVV on a credit card stand for ?
- (A) Card Verification Value
 - (B) Credit Validation Vault
 - (C) Card Virtual Verification
 - (D) Cash Value Verification
-

28. What is phishing in the context of credit card security ?
- (A) A secure payment gateway
 - (B) An email scam designed to steal credit card details
 - (C) A credit card verification process
 - (D) A transaction approval system
-

-
25. अपने मोबाइल फोन को सुरक्षित करने का सबसे प्रभावी तरीका क्या है ?
- (A) बायोमेट्रिक प्रमाणीकरण सक्षम करें (उदाहरण के लिए, फिंगरप्रिंट या फेस आईडी)
 - (B) एक साधारण 4-अंकीय पिन का उपयोग करें
 - (C) सुविधा के लिए अपने फोन को अनलॉक रखें
 - (D) सभी ऐप्स के लिए एक ही पासवर्ड का उपयोग करें
-

26. एसएमएस (स्मिशिंग) के माध्यम से फिशिंग हमले का प्रमुख संकेतक क्या है ?
- (A) ज्ञात संपर्कों से एसएमएस
 - (B) अत्यावश्यक भाषा और संदिग्ध लिंक वाले संदेश
 - (C) बैंक लेनदेन की पुष्टि करने वाला एसएमएस
 - (D) उचित पहचान के साथ ग्राहक सेवा से संदेश
-

27. क्रेडिट कार्ड पर CVV का क्या मतलब है ?
- (A) कार्ड सत्यापन मूल्य
 - (B) क्रेडिट वैलिडेशन वॉल्ट
 - (C) कार्ड वर्चुअल सत्यापन
 - (D) नकद मूल्य सत्यापन
-

28. क्रेडिट कार्ड सुरक्षा के संदर्भ में फिशिंग क्या है ?
- (A) एक सुरक्षित भुगतान गेटवे
 - (B) क्रेडिट कार्ड विवरण चुराने के लिए बनाया गया एक ई-मेल घोटाला
 - (C) एक क्रेडिट कार्ड सत्यापन प्रक्रिया
 - (D) एक लेनदेन अनुमोदन प्रणाली
-

29. Which of the following can be a target of a DoS attack ?

- (A) Servers
- (B) Websites
- (C) Networks
- (D) All of the above

30. Which of the following is NOT a cyber security threat ?

- (A) Malware
- (B) Phishing
- (C) Firewall
- (D) Ransomware

31. What should you avoid while browsing online ?

- (A) Clicking on unknown links or pop-ups
- (B) Using a VPN for public Wi-Fi
- (C) Keeping your browser updated
- (D) Using HTTPS websites

32. Which of the following is a common cyber safety practice ?

- (A) Sharing passwords with friends
- (B) Using public Wi-Fi for financial transactions
- (C) Regularly updating software and systems
- (D) Ignoring security warnings

29. निम्नलिखित में से कौन DoS हमले का लक्ष्य हो सकता है ?

- (A) सर्वर
- (B) वेबसाइटें
- (C) नेटवर्क
- (D) उपरोक्त सभी

30. निम्नलिखित में से कौन सा साइबर सुरक्षा खतरा नहीं है ?

- (A) मैलवेयर
- (B) फिशिंग
- (C) फायरवॉल
- (D) रैंसमवेयर

31. ऑनलाइन ब्राउज करते समय आपको किन चीजों से बचना चाहिए ?

- (A) अज्ञात लिंक या पॉप-अप पर क्लिक करना
- (B) सार्वजनिक वाई-फाई के लिए वीपीएन का उपयोग करना
- (C) अपने ब्राउजर को अपडेट रखना
- (D) HTTPS वेबसाइटों का उपयोग करना

32. निम्नलिखित में से कौन सा एक सामान्य साइबर सुरक्षा अभ्यास है ?

- (A) दोस्तों के साथ पासवर्ड साझा करना
- (B) वित्तीय लेनदेन के लिए सार्वजनिक वाई-फाई का उपयोग करना
- (C) सॉफ्टवेयर और सिस्टम को नियमित रूप से अपडेट करना
- (D) सुरक्षा चेतावनियों को नजर अंदाज करना

33. What does “https://” in a URL indicate ?

- (A) The website is under maintenance
- (B) The website is secure and encrypted
- (C) The website is for high-traffic users only
- (D) The website is outdated

34. What is ransomware ?

- (A) A type of antivirus software
- (B) Malicious software that encrypts files and demands payment
- (C) A secure communication protocol
- (D) A software update

35. What is the purpose of encryption in cyber security ?

- (A) To speed up internet connections
- (B) To simplify login processes
- (C) To track user activity
- (D) To make data unreadable to unauthorized users

36. What is the role of an antivirus program ?

- (A) Speed up your device
- (B) Prevent hardware failures
- (C) Detect, prevent, and remove malware
- (D) Manage internet connections

33. URL में “https://” क्या दर्शाता है ?

- (A) वेबसाइट रखरखाव के अधीन है
- (B) वेबसाइट सुरक्षित और एन्क्रिप्टेड है
- (C) वेबसाइट केवल उच्च-ट्रैफिक उपयोगकर्ताओं के लिए है
- (D) वेबसाइट पुरानी हो चुकी है

34. रैनसमवेयर क्या है ?

- (A) एक प्रकार का एंटीवायरस सॉफ्टवेयर
- (B) दुर्भावनापूर्ण सॉफ्टवेयर जो फाइलों को एन्क्रिप्ट करता है और भुगतान की मांग करता है
- (C) एक सुरक्षित संचार प्रोटोकॉल
- (D) एक सॉफ्टवेयर अद्यतन

35. साइबर सुरक्षा में एन्क्रिप्शन का उद्देश्य क्या है ?

- (A) इंटरनेट कनेक्शन को तेज करने के लिए
- (B) लॉगिन प्रक्रियाओं को सरल बनाने के लिए
- (C) उपयोगकर्ता गतिविधि को ट्रैक करने के लिए
- (D) अनधिकृत उपयोक्ताओं के लिए डेटा को अपठनीय बनाना

36. एंटीवायरस प्रोग्राम की क्या भूमिका है ?

- (A) अपने डिवाइस की गति बढ़ाएं
- (B) हार्डवेयर विफलताओं को रोकें
- (C) मेलवेयर का पता लगाएं, रोकें और हटाएं
- (D) इंटरनेट कनेक्शन प्रबंधित करें

37. What is spyware ?

- (A) Malicious software used to monitor and gather user information
- (B) Software that speeds up your device
- (C) A security firewall
- (D) A password manager

38. What does a Virtual Private Network (VPN) do ?

- (A) Slows down internet speed
- (B) Blocks social media websites
- (C) Repairs damaged files
- (D) Provides anonymous and secure internet access

39. What is an example of social engineering ?

- (A) Phishing emails
- (B) Using antivirus software
- (C) Regular software updates
- (D) Enabling two-factor authentication

40. What is the primary purpose of a CAPTCHA ?

- (A) To slow down website performance
- (B) To verify human users and prevent bots
- (C) To block suspicious emails
- (D) To improve website graphics

37. स्पाइवेयर क्या है ?

- (A) दुर्भावनापूर्ण सॉफ्टवेयर का उपयोग उपयोगकर्ता की जानकारी की निगरानी और एकत्र करने के लिए किया जाता है
- (B) सॉफ्टवेयर जो आपके डिवाइस को गति देता है
- (C) एक सुरक्षा फायरवॉल
- (D) एक पासवर्ड मैनेजर

38. वर्चुअल प्राइवेट नेटवर्क (VPN) क्या करता है ?

- (A) इंटरनेट की गति धीमी कर देता है
- (B) सोशल मीडिया वेबसाइटों को ब्लॉक करता है
- (C) क्षतिग्रस्त फाइलों की मरम्मत करता है
- (D) गुमनाम और सुरक्षित इंटरनेट पहुँच प्रदान करता है

39. सोशल इंजीनियरिंग का उदाहरण क्या है ?

- (A) फिशिंग ई-मेल
- (B) एंटीवायरस सॉफ्टवेयर का उपयोग करना
- (C) नियमित सॉफ्टवेयर अपडेट
- (D) दो-कारक प्रमाणीकरण सक्षम करना

40. कैप्चा का प्राथमिक उद्देश्य क्या है ?

- (A) वेबसाइट के प्रदर्शन को धीमा करने के लिए
- (B) मानव उपयोगकर्ताओं को सत्यापित करने और बॉट्स को रोकने के लिए
- (C) संदिग्ध ई-मेल को ब्लॉक करने के लिए
- (D) वेबसाइट ग्राफिक्स को बेहतर बनाने के लिए

Rough Work/रफ़ कार्य

