A-1161 **No. of Pages: 32**

GECS-01

Foundation of Cyber Security

Examination, 2026 (Feb.)

Time: 2 Hours Max Mark: 100

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 100 multiple choice questions (M.C.Q.). All questions are Compulsory and carry 01 mark each. There is no negative marking.
   इस प्रश्न पत्र में 100 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) एव (D) दिए गए हैं। आपको उपयुक्त उत्तर विकल्प का चुनाव कर उत्तर 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 प्वॉइन्ट पैन का ही इस्तेमाल कीजिए।

1. What is the full form of DNS?
A. Domain Naming Scheme
B. Data Network Server
C. Digital Number Service
D. Domain Name System
DNS का पूरा रूप क्या है?
A. डोमेन नेमिंग स्कीम
B. डेटा नेटवर्क सर्वर
C. डिजिटल नंबर सर्विस
D. डोमेन नेम सिस्टम

2. Who developed the World Wide Web?
A. Tim Berners-Lee
B. Bill Gates
C. Steve Jobs
D. Mark Zuckerberg
विश्व व्यापी वेब (World Wide Web) किसने विकसित किया?
A. टिम बर्नर्स-ली
B. बिल गेट्स
C. स्टीव जॉब्स
D. मार्क जुकेरबर्ग

3. What is meant by Cyber Crime?
A. Crimes that occur only in the physical world.
B. Illegal activities carried out using computers or the internet.
C. Theft that happens in shops or markets.
D. Activities related to online shopping.
साइबर अपराध (Cyber Crime) से क्या अभिप्राय है?
A. वे अपराध जो केवल भौतिक दुनिया में होते हैं।
B. वे अवैध गतिविधियाँ जो कंप्यूटर या इंटरनेट का उपयोग करके की जाती हैं।
C. वे चोरी जो दुकानों या बाजारों में होती हैं।
D. ऑनलाइन शॉपिंग से संबंधित गतिविधियाँ।

4. Which of the following is NOT malware?
A. Worm
B. Virus

C. Trojan
D. PDF File
निम्न में से कौन-सा मालवेयर नहीं है?
A. वर्म
B. वायरस
C. ट्रोजन
D. पीडीएफ फ़ाइल

5. What is the main purpose of browser hijacking software?
A. To improve the quality of internet browsing.
B. To redirect users to unwanted or malicious webpages.
C. To increase the processing speed of the computer.
D. To play music automatically.
ब्राउज़र हाईजैकिंग सॉफ़्टवेयर का मुख्य उद्देश्य क्या होता है?
A. इंटरनेट ब्राउज़िंग की गुणवत्ता में सुधार करना
B. उपयोगकर्ताओं को अवांछित या हानिकारक वेबपेजों पर रीडायरेक्ट करना
C. कंप्यूटर की प्रोसेसिंग स्पीड बढ़ाना
D. अपने-आप संगीत चलाना

6. Cyber Stalking is a crime related to-
A. Video editing.
B. Downloading files
C. Online harassment
D. Printing
साइबर स्टॉकिंग किससे संबंधित अपराध है?
A. वीडियो एडिटिंग
B. फाइलें डाउनलोड करना
C. ऑनलाइन उत्पीड़न
D. प्रिंटिंग

7. What is the primary goal of phishing attacks?
A. Charging mobile batteries.
B. Speeding up device performance.
C. Sending deceptive messages to steal sensitive information.
D. Installing system updates.
फ़िशिंग हमलों का मुख्य उद्देश्य क्या होता है?

A. मोबाइल बैटरी चार्ज करना.
B. डिवाइस का प्रदर्शन बढ़ाना
C. संवेदनशील जानकारी चुराने के लिए भ्रामक संदेश भेजना
D. सिस्टम अपडेट इंस्टॉल करना

8. What is a Logic Bomb?
A. A hidden malicious program that activates when specific conditions are met
B. A regular computer utility tool
C. A physical explosive device.
D. A harmless software update.
लॉजिक बॉम्ब क्या होता है?
A. एक छिपा हुआ हानिकारक प्रोग्राम जो किसी विशेष स्थिति में सक्रिय होता है
B. सामान्य कंप्यूटर उपयोगिता उपकरण
C. एक भौतिक विस्फोटक उपकरण
D. एक साधारण सॉफ़्टवेयर अपडेट

9. What happens in Email Spoofing?
A. The inbox storage is increased.
B. The email's background color is modified.
C. The email is automatically printed.
D. A false sender address is used to deceive the recipient.
Email Spoofing में क्या होता है?
A. इनबॉक्स स्टोरेज बढ़ जाता है
B. ईमेल की बैकग्राउंड रंग बदला जाता है
C. ईमेल अपने-आप प्रिंट हो जाता है
D. प्राप्तकर्ता को धोखा देने के लिए नकली प्रेषक पता उपयोग किया जाता है

10. What is the main purpose of a DoS (Denial of Service) attack?
A. Overloading a system or service to make it unavailable.
B. Improving the performance of a server.
C. Cleaning unwanted files from a system.
D. Enhancing network speed.
DoS (सेवा निषेध) हमले का मुख्य उद्देश्य क्या है?
A. किसी सिस्टम या सेवा को ओवरलोड करके उसे अनुपलब्ध बनाना।
B. सर्वर के प्रदर्शन में सुधार करना।
C. सिस्टम से अवांछित फ़ाइलें हटाना।

D. नेटवर्क की गति बढ़ाना।

11. What does "Data Diddling" refer to?
A. Repairing computer hardware
B. Unauthorized alteration of data before or during processing
C. Formatting mobile devices
D. No change to data
"डेटा डिडलिंग" किसे कहते हैं?
A. कंप्यूटर हार्डवेयर की मरम्मत
B. प्रोसेस होने से पहले या दौरान डेटा में अनधिकृत बदलाव करना
C. मोबाइल डिवाइस को फॉर्मेट करना
D. डेटा में कोई बदलाव न करना

12. What is the main purpose of authentication?
A. To run games.
B. To delete files.
C. To verify the user's identity.
D. To change system appearance.
प्रमाणीकरण (Authentication) का मुख्य उद्देश्य क्या होता है?
A. गेम चलाना.
B. फाइलें हटाना
C. उपयोगकर्ता की पहचान की पुष्टि करना
D. सिस्टम की दिखावट बदलना

13. What does "Encryption" mean?
A. Loading files into memory
B. Displaying data on screen
C. Transforming readable data into a secure, unreadable format
D. Printing documents
Encryption का क्या अर्थ है?
A. फ़ाइलों को मेमोरी में लोड करना
B. डेटा को स्क्रीन पर दिखाना
C. पढ़ने योग्य डेटा को सुरक्षित, अपठनीय रूप में बदलना
D. दस्तावेज़ों को प्रिंट करना

14. What does a Digital Signature verify?

A. Data integrity and the authenticity of the sender.
B. Text colour settings
C. Font style of the document
D. Page layout design
डिजिटल सिग्नेचर क्या सत्यापित करता है?
A. डेटा की अखंडता और भेजने वाले की प्रामाणिकता
B. टेक्स्ट के रंग सेटिंग्स
C. दस्तावेज़ के फ़ॉन्ट शैली
D. पेज लेआउट डिज़ाइन

15. What is the primary purpose of an Antivirus?
A. To detect and remove malware
B. To record audio on the computer
C. To increase the computer's RAM
D. To adjust screen brightness
Antivirus का मुख्य उद्देश्य क्या होता है?
A. हानिकारक सॉफ़्टवेयर (Malware) का पता लगाना और उसे हटाना
B. कंप्यूटर में ऑडियो रिकॉर्ड करना
C. कंप्यूटर की RAM क्षमता बढ़ाना
D. सिस्टम की स्क्रीन ब्राइटनेस नियंत्रित करना

16. A Firewall acts as a security barrier between-
A. A computer's fan and CPU
B. An internal network and external/untrusted networks.
C. A keyboard and mouse connection
D. A printer and scanner
फ़ायरवॉल किसके बीच सुरक्षा अवरोध (Security Barrier) के रूप में कार्य करता है?
A. कंप्यूटर के फैन और CPU के बीच
B. आंतरिक नेटवर्क और बाहरी/अविश्वसनीय नेटवर्क के बीच
C. कीबोर्ड और माउस कनेक्शन के बीच
D. प्रिंटर और स्कैनर के बीच

17. What does Steganography hide?
A. Wallpaper designs
B. Secret data concealed inside images, audio, or other media
C. Cooking recipes

D. Computer games
स्टेगनोग्राफी में क्या छिपाया जाता है?
A. वॉलपेपर डिज़ाइन
B. छवियों, ऑडियो या अन्य मीडिया के भीतर छिपाया गया गुप्त डाटा
C. खाना बनाने की रेसिपी
D. कंप्यूटर गेम्स

18. What is the opposite process of Encryption?
A. Code Formatting
B. Data Rotation
C. File Compression
D. Decryption
एन्क्रिप्शन की विपरीत प्रक्रिया क्या होती है?
A. कोड फ़ॉर्मेटिंग
B. डेटा रोटेशन
C. फ़ाइल कम्प्रेशन
D. डिक्रिप्शन

19. What does Two-Factor Authentication (2FA) require for user login?
A. Two different verification steps for confirming identity
B. Two separate computers for accessing the account
C. Two email accounts for registration
D. Two keyboards connected to the device
Two-Factor Authentication (2FA) में उपयोगकर्ता लॉगिन के लिए क्या आवश्यक होता है?
A. पहचान की पुष्टि के लिए दो अलग-अलग सत्यापन चरण
B. खाते तक पहुँचने के लिए दो कंप्यूटर
C. पंजीकरण के लिए दो ईमेल खाते
D. डिवाइस से जुड़े दो कीकीबोर्ड

20. What is the primary purpose of Cyber Forensics?
A. To develop entertainment games
B. To investigate cyber-crimes by collecting and examining digital evidence
C. To produce digital music tracks
D. To design graphical themes
साइबर फॉरेंसिक्स का मुख्य उद्देश्य क्या होता है?
A. मनोरंजन के लिए गेम विकसित करना

B. डिजिटल साक्ष्यों को एकत्रित और जांचकर साइबर अपराधों की जांच करना

C. डिजिटल म्यूज़िक ट्रैक बनाना

D. ग्राफ़िकल थीम्स डिज़ाइन करना

21. Which cyber-crime involves tricking users into revealing personal information through fake websites or emails?

A. Keylogging

B. SQL Injection

C. DDoS Attack

D. Phishing

कौन सा साइबर अपराध नकली वेबसाइट या ईमेल के माध्यम से उपयोगकर्ताओं से व्यक्तिगत जानकारी निकलवाने से संबंधित है?

A. की-लॉगिंग.

B. SQL इंजेक्शन

C. DDoS हमला

D. फ़िशिंग

22. Which cyber-crime focuses on gaining unauthorized access to a system by exploiting software vulnerabilities?

A. Hacking

B. Cyber Bullying

C. Social Engineering

D. Data Backup

कौन सा साइबर अपराध सॉफ़्टवेयर की कमजोरियों का फायदा उठाकर सिस्टम में अनधिकृत प्रवेश करने पर केंद्रित है?

A. हैकिंग

B. साइबर बुलिंग

C. सोशल इंजीनियरिंग

D. डेटा बैकअप

23. What is the primary goal of a Distributed Denial-of-Service (DDoS) attack?

A. To modify system logs secretly.

B. To steal personal banking information

C. To overwhelm a server and make services unavailable

D. To encrypt data for ransom

Distributed Denial-of-Service (DDoS) हमले का मुख्य उद्देश्य क्या होता है?

A. सिस्टम लॉग को गुप्त रूप से बदलना.

B. बैंकिंग जानकारी चुराना
C. सर्वर को ओवरलोड करके सेवाओं को अनुपलब्ध करना
D. डेटा को फिरौती के लिए एन्क्लिप्ट करना

24. What is the most important rule in digital evidence collection?
A. Rearranging folders for convenience
B. Editing images to enhance clarity
C. Compressing files to reduce size
D. Preserving the integrity of the evidence
डिजिटल साक्ष्य एकत्रित करने का सबसे महत्वपूर्ण नियम क्या है?
A. सुविधा के लिए फोल्डरों को पुनः व्यवस्थित करना.
B. तस्वीरों को संपादित करना
C. फ़ाइलों का आकार कम करने के लिए उन्हें कम्प्रेस करना
D. साक्ष्य की अखंडता (Integrity) को सुरक्षित रखना

25. Why is digital evidence considered volatile?
A. It is physically heavy
B. It can be easily altered or lost
C. It is very costly to store
D. It is stored in printed form
डिजिटल साक्ष्य को अस्थिर (volatile) क्यों माना जाता है?
A. यह भौतिक रूप से भारी होता है
B. इसे आसानी से बदला या मिटाया जा सकता है
C. इसे संग्रहीत करना बहुत महंगा होता है
D. यह मुद्रित रूप में संग्रहीत होता है

26. Recent cyber-attacks generally target-
A. Manual records.
B. Internet data.
C. Household documents.
D. Critical information infrastructure.
हाल के साइबर हमले सामान्यतः किसे निशाना बनाते हैं?
A. मैनुअल रिकॉर्ड
B. इंटरनेट डेटा
C. घरेलू दस्तावेज़
D. क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर

27. A cyber-attack that steals user data is known as

A. Data Breach

B. Data Cleaning

C. Data Compression

D. Data Formatting

जिस साइबर हमले में उपयोगकर्ता का डेटा चुराया जाता है, उसे क्या कहा जाता है?

A. डेटा ब्रीच (Data Breach)

B. डेटा क्लीनिंग

C. डेटा कम्प्रेशन

D. डेटा फॉर्मेटिंग

28. The primary objective of a ransomware attack is to

A. Enhance graphics quality

B. Increase system performance

C. Lock data and demand payment

D. Slows down the internet connection

रैनसमवेयर हमले का मुख्य उद्देश्य क्या होता है?

A. ग्राफ़िक्स गुणवत्ता बढ़ाना

B. सिस्टम प्रदर्शन बढ़ाना

C. डेटा को लॉक करना और पैसे की मांग करना

D. इंटरनेट कनेक्शन को धीमा करना

29. "WannaCry" is an example of-

A. Ransomware

B. Spyware

C. Adware

D. Keylogger

"WannaCry" किसका उदाहरण है?

A. रैनसमवेयर

B. स्पायवेयर

C. ऐडवेयर

D. कीलॉगर

30. Recent cyber-attacks are rising mainly due to-

A. Growing interest in travelling

B. Reduced newspaper reading habits
C. Increased dependency on digital services
D. Increased outdoor activities
हाल के साइबर हमलों में वृद्धि मुख्य रूप से किस कारण हो रही है?
A. यात्रा में बढ़ती रुचि
B. अख़बार पढ़ने की आदत में कमी
C. डिजिटल सेवाओं पर बढ़ती निर्भरता
D. बाहरी गतिविधियों में वृद्धि

31. Cyber-crime incidents are reported to the-
A. Local Police station.
B. Cybercrime Cell / Cyber Police
C. Interpole
D. General Government office.
साइबर अपराध की घटनाएँ किसे रिपोर्ट की जाती हैं?
A. स्थानीय पुलिस स्टेशन
B. साइबरक्राइम सेल / साइबर पुलिस
C. इंटरपोल
D. सामान्य सरकारी कार्यालय

32. The primary aim of India's Cyber Security Policy is to-
A. Conduct internet awareness programmes
B. Promote usage of digital services
C. Boost agricultural production
D. Secure and protect cyberspace
भारत की साइबर सुरक्षा नीति का मुख्य उद्देश्य क्या है?
A. इंटरनेट जागरूकता कार्यक्रम चलाना
B. डिजिटल सेवाओं के उपयोग को बढ़ावा देना
C. कृषि उत्पादन बढ़ाना
D. साइबर स्पेस को सुरक्षित और संरक्षित करना

33. CERT-In stands for-
A. Computer Emergency Response Team-India
B. Central Emergency Rescue Taskforce
C. Cyber Expert Research Team
D. Computer Education Resource Team

CERT-In का पूर्ण रूप क्या है?
A. कम्प्यूटर इमरजेंसी रिस्पॉन्स टीम - इंडिया
B. सेंट्रल इमरजेंसी रेस्क्यू टास्कफोर्स
C. साइबर एक्सपर्ट रिसर्च टीम
D. कम्प्यूटर एजुकेशन रिसोर्स टीम

34. The Cyber Surakshit Bharat Mission focuses on-
A. Improving sports performance
B. Promoting cyber hygiene and awareness
C. Enhancing culinary skills
D. Increasing tourist activities
Cyber Surakshit Bharat Mission का मुख्य उद्देश्य है
A. खेल प्रदर्शन में सुधार करना
B. साइबर हाइजीन और जागरूकता को बढ़ावा देना
C. पाक-कौशल में सुधार करना
D. पर्यटन गतिविधियों को बढ़ाना

35. The National Cyber Coordination Centre (NCCC) monitors-
A. Roadways traffic.
B. Railway Traffic
C. Weather forecasting systems
D. Internet traffic and cyber threats
नेशनल साइबर कोऑर्डिनेशन सेंटर (NCCC) किसकी निगरानी करता है?
A. सड़क यातायात
B. रेलवे यातायात
C. मौसम पूर्वानुमान प्रणाली
D. इंटरनेट ट्रैफिक और साइबर खतरों की

36. What is the primary purpose of clearing the browser cache?
A. Increase internet bill
B. Remove stored temporary files and improve browser performance
C. Install new extensions
D. Slow down the browser
ब्राउज़र कैश को साफ़ करने का मुख्य उद्देश्य क्या है?
A. इंटरनेट बिल बढ़ाना
B. अस्थायी संग्रहीत फ़ाइलों को हटाना और ब्राउज़र का प्रदर्शन बेहतर करना

C. नए एक्सटेंशन इंस्टॉल करना
D. ब्राउज़र को धीमा करना

37. When shopping online, which practice increases your safety?
A. Using public Wi-Fi for payments
B. Sharing OTP with trusted friends
C. Purchasing only from reputed and verified websites
D. Saving debit card details on all websites
ऑनलाइन खरीदारी करते समय, कौन-सा अभ्यास आपकी सुरक्षा बढ़ाता है?
A. भुगतान के लिए पब्लिक वाई-फाई का उपयोग करना
B. भरोसेमंद दोस्तों के साथ ओटीपी साझा करना
C. केवल विश्वसनीय और सत्यापित वेबसाइटों से ही खरीदारी करना
D. सभी वेबसाइटों पर डेबिट कार्ड विवरण सहेजना

38. In Chrome browser versions 10 and above, how do you generally clear the cache?
A. Settings → Clean Disk
B. Settings → Privacy and Security → Clear browsing data
C. File → Save Page As → Delete
D. Tools → Exit
क्रोम ब्राउज़र (संस्करण 10 और उससे ऊपर) में कैश कैसे साफ़ किया जाता है?
A. सेटिंग्स → क्लीन डिस्क
B. सेटिंग्स → प्राइवेसी एंड सिक्योरिटी → क्लियर ब्राउज़िंग डेटा
C. फ़ाइल → सेव पेज ऐज़ → डिलीट
D. टूल्स → एग्ज़िट

39. In early Chrome versions (1 to 9), cache clearing was mainly done through:
A. Preferences → Security → Remove Password
B. Settings → Under the Hood → Clear browsing data
C. Tools → Find → Delete
D. Chrome Store → Cache Cleaner
शुरुआती क्रोम संस्करणों (1 से 9) में, कैश साफ़ करना मुख्य रूप से इन तरीकों से किया जाता था:
A. प्राथमिकताएँ → सुरक्षा → पासवर्ड हटाएँ
B. सेटिंग्स → अंदरूनी जानकारी → ब्राउज़िंग डेटा साफ़ करें
C. टूल्स → ढूँढें → हटाएँ
D. क्रोम स्टोर → कैश क्लीनर

40. On Safari for iOS (iPhone/iPad), cache is cleared using:

A. Settings → General → Reset iPhone

B. iCloud → Delete Device

C. Safari → File → Clear All

D. Settings → Safari → Clear History and Website Data

iOS (iPhone/iPad) के लिए Safari पर, कैशे साफ़ करने का तरीका इस प्रकार है:

A. सेटिंग्स → सामान्य → iPhone रीसेट करें

B. iCloud → डिवाइस हटाएँ

C. Safari → फ़ाइल → सभी साफ़ करें

D. सेटिंग्स → Safari → इतिहास और वेबसाइट डेटा साफ़ करें

41. Cache clearing in Safari on macOS is commonly done by first enabling:

A. Developer menu

B. Spotlight Search

C. Siri Search

D. FileVault Disk Encryption

macOS पर Safari में कैश साफ़ करने के लिए आमतौर पर सबसे पहले इन चीज़ों को सक्षम किया जाता है:

A. डेवलपर मेनू

B. स्पॉटलाइट सर्च

C. सिरी सर्च

D. फ़ाइलवॉल्ट डिस्क एन्क्रिप्शन

42. Internet Explorer 9, 10, and 11 allow cache clearing from:

A. Safety menu → Delete browsing history

B. Task Manager → End Task

C. Control Panel → Devices

D. Windows Media Player settings

इंटरनेट एक्सप्लोरर 9, 10 और 11 कैश क्लियरिंग की सुविधा देते हैं:

A. सुरक्षा मेनू → ब्राउज़िंग इतिहास मिटाएँ

B. कार्य प्रबंधक → कार्य समाप्त करें

C. नियंत्रण कक्ष → उपकरण

D. विंडोज़ मीडिया प्लेयर सेटिंग्स

43. In Firefox (including Firefox 33), the cache can be cleared from:

A. File → New Window

B. Options → Privacy → Clear recent history

C. Tools → Bookmark Manager

D. Downloads → Delete

फ़ायरफ़ॉक्स (फ़ायरफ़ॉक्स 33 सहित) में, कैश को इन तरीकों से साफ़ किया जा सकता है:

A. फ़ाइल → नई विंडो

B. विकल्प → गोपनीयता → हाल का इतिहास साफ़ करें

C. उपकरण → बुकमार्क प्रबंधक

D. डाउनलोड → हटाएं

44. CCleaner is primarily used for:

A. Updating operating systems

B. Cleaning temporary files, cache, and optimizing system performance

C. Designing websites

D. Installing antivirus

CCleaner का मुख्य रूप से उपयोग निम्न के लिए किया जाता है:

A. ऑपरेटिंग सिस्टम अपडेट करना

B. अस्थायी फ़ाइलें, कैश साफ़ करना और सिस्टम प्रदर्शन को अनुकूलित करना

C. वेबसाइट डिज़ाइन करना

D. एंटीवायरस इंस्टॉल करना

45. Which of the following is responsible for translating domain names into IP addresses?

A. URL Server

B. DNS

C. SMTP

D. FTP

निम्नलिखित में से कौन डोमेन नामों को आईपी पतों में बदलने के लिए ज़िम्मेदार है?

A. URL सर्वर

B. DNS

C. SMTP

D. FTP

46. An IP address is best described as:

A. A physical machine label

B. A type of digital certificate

C. A browser security code

D. A numerical identifier for devices on a network

IP पते का सबसे अच्छा वर्णन इस प्रकार किया जा सकता है:

A. एक भौतिक मशीन लेबल

B. एक प्रकार का डिजिटल प्रमाणपत्र

C. एक ब्राउज़र सुरक्षा कोड

D. नेटवर्क पर उपकरणों के लिए एक संख्यात्मक पहचानकर्ता

47. Which protocol is most commonly used to transfer web pages on the Internet?

A. FTP

B. SMTP

C. HTTP

D. Telnet

इंटरनेट पर वेब पेजों को स्थानांतरित करने के लिए सबसे अधिक इस्तेमाल किया जाने वाला प्रोटोकॉल कौन सा है?

A. FTP

B. SMTP

C. HTTP

D. टेलनेट

48. The main purpose of Internet Infrastructure is to:

A. Provide printing services

B. Manage screen resolution

C. Display website themes

D. Support global connectivity and data exchange

इंटरनेट इन्फ्रास्ट्रक्चर का मुख्य उद्देश्य है:

A. प्रिंटिंग सेवाएँ प्रदान करना

B. स्क्रीन रिज़ॉल्यूशन प्रबंधित करना

C. वेबसाइट थीम प्रदर्शित करना

D. वैश्विक कनेक्टिविटी और डेटा एक्सचेंज का समर्थन करना

49. Which of the following is NOT a form of malware?

A. Adware

B. Spyware

C. Worm

D. Firewall

निम्नलिखित में से कौन मैलवेयर का एक रूप नहीं है?

A. एडवेयर

B. स्पाइवेयर

C. वर्म

D. फ़ायरवॉल

50. A malware that secretly collects user information and sends it to a remote attacker is called:

A. Adware

B. Spyware

C. Worm

D. Cookie

एक मैलवेयर जो गुप्त रूप से उपयोगकर्ता की जानकारी एकत्र करता है और उसे दूरस्थ हमलावर को भेजता है, उसे कहते हैं:

A. एडवेयर

B. स्पाइवेयर

C. वर्म

D. कुकी

51. A Trojan Horse typically:

A. Replicates itself aggressively

B. Repairs system files

C. Appears legitimate but performs malicious actions

D. Works only offline

एक ट्रोजन हॉर्स आम तौर पर-

A. खुद को तेजी से कॉपी करता है

B. सिस्टम फाइलों की मरम्मत करता है

C. वैध दिखता है लेकिन हानिकारक कार्य करता है

D. केवल ऑफ़लाइन काम करता है

52. Browser Hijacking Software is used to:

A. Increase browser speed

B. Modify browser settings without permission

C. Automatically clear cache

D. Encrypt user data

Browser Hijacking Software का उपयोग किस लिए किया जाता है?

A. ब्राउज़र की गति बढ़ाने के लिए

B. बिना अनुमति ब्राउज़र सेटिंग्स बदलने के लिए

C. स्वचालित रूप से कैश साफ़ करने के लिए
D. उपयोगकर्ता डेटा एन्क्रिप्ट करने के लिए

53. Scareware manipulates users by:
A. Showing fake warnings to force unnecessary actions
B. Encrypting personal files
C. Updating antivirus software
D. Speeding up hardware
Scareware उपयोगकर्ताओं को इस प्रकार प्रभावित करता है-
A. नकली चेतावनियाँ दिखाकर अनावश्यक कार्य करने के लिए मजबूर करना
B. व्यक्तिगत फ़ाइलों को एन्क्रिप्ट करना
C. एंटीवायरस सॉफ़्टवेयर अपडेट करना
D. हार्डवेयर की गति बढ़ाना

54. Software Piracy refers to:
A. Buying licensed software
B. Using or distributing software without authorization
C. Encrypting software
D. Testing trial versions
Software Piracy का अर्थ है-
A. लाइसेंस प्राप्त सॉफ़्टवेयर खरीदना
B. बिना अनुमति सॉफ़्टवेयर का उपयोग या वितरण करना
C. सॉफ़्टवेयर को एन्क्रिप्ट करना
D. ट्रायल वर्ज़न का परीक्षण करना

55. Logic Bombs are malicious programs that:
A. Execute only when triggered by a specific condition
B. Heal infected files
C. Spread only via email
D. Require manual installation
लॉजिक बम दुर्भावनापूर्ण प्रोग्राम होते हैं जो:
A. केवल किसी विशिष्ट स्थिति द्वारा ट्रिगर होने पर ही क्रियान्वित होते हैं
B. संक्रमित फ़ाइलों को ठीक करते हैं
C. केवल ईमेल के माध्यम से फैलते हैं
D. मैन्युअल इंस्टॉलेशन की आवश्यकता होती है

56. Cyber Squatting involves:
A. Hacking wireless signals
B. Registering domain names similar to popular brands
C. Crashing servers
D. Encrypting DNS records
साइबर स्क्वाटिंग में शामिल हैं:
A. वायरलेस सिग्नल हैक करना
B. लोकप्रिय ब्रांडों से मिलते-जुलते डोमेन नाम पंजीकृत करना
C. सर्वर क्रैश करना
D. DNS रिकॉर्ड्स को एन्क्रिप्ट करना

57. Salami Attack refers to:
A. Small, repeated thefts that go unnoticed individually
B. Large-scale financial fraud
C. Physical destruction of servers
D. Encrypting entire databases
सलामी हमले से तात्पर्य है:
A. छोटी, बार-बार होने वाली चोरियाँ जो व्यक्तिगत रूप से ध्यान में नहीं आतीं
B. बड़े पैमाने पर वित्तीय धोखाधड़ी
C. सर्वरों का भौतिक विनाश
D. संपूर्ण डेटाबेस को एन्क्रिप्ट करना

58. Email Spoofing involves:
A. Encrypting emails for protection
B. Faking the sender's email identity
C. Blocking incoming messages
D. Deleting inbox folders
ईमेल स्पूफिंग में शामिल हैं:
A. सुरक्षा के लिए ईमेल एन्क्रिप्ट करना
B. प्रेषक की ईमेल पहचान को फर्जी बनाना
C. आने वाले संदेशों को ब्लॉक करना
D. इनबॉक्स फ़ोल्डर्स को हटाना

59. Which of the following is the first step in ensuring smartphone security?
A. Installing games
B. Using public Wi-Fi

C. Changing wallpaper
D. Setting a strong screen lock (PIN/Pattern/Password)
स्मार्टफोन सुरक्षा सुनिश्चित करने के लिए निम्नलिखित में से कौन सा पहला कदम है?
A. गेम इंस्टॉल करना
B. सार्वजनिक वाई-फाई का उपयोग करना
C. वॉलपेपर बदलना
D. एक मजबूत स्क्रीन लॉक (पिन/पैटर्न/पासवर्ड) सेट करना

60. A "locked smartphone" generally refers to:
A. A phone that cannot be carried outside
B. A device tied to a specific telecom operator
C. A phone without a battery
D. An encrypted device
एक "लॉक्ड स्मार्टफोन" आमतौर पर निम्न को संदर्भित करता है:
A. एक ऐसा फोन जिसे बाहर नहीं ले जाया जा सकता
B. एक विशिष्ट दूरसंचार ऑपरेटर से जुड़ा उपकरण
C. बिना बैटरी वाला फोन
D. एक एन्क्रिप्टेड डिवाइस

61. Which mobile OS is known for its open-source architecture?
A. iOS
B. Windows Phone
C. Android
D. Symbian
कौन सा मोबाइल ऑपरेटिंग सिस्टम अपने ओपन-सोर्स आर्किटेक्चर के लिए जाना जाता है?
A. iOS
B. विंडोज फोन
C. एंड्रॉइड
D. सिम्बियन

62. Feature phones differ from smartphones mainly because they:
A. Have better cameras
B. Use only iOS
C. Provide unlimited storage
D. Do not support advanced apps and Internet browsing
फ़ीचर फ़ोन स्मार्टफ़ोन से मुख्यतः इसलिए भिन्न होते हैं क्योंकिः

A. बेहतर कैमरे होते हैं
B. केवल iOS इस्तेमाल करते हैं
C. असीमित स्टोरेज प्रदान करते हैं
D. उन्नत ऐप्स और इंटरनेट ब्राउज़िंग का समर्थन नहीं करते

63. During initial setup of a smartphone, it is recommended to:
A. Disable automatic updates
B. Avoid setting a backup email
C. Install apps from unknown websites
D. Connect to a secure Wi-Fi network
स्मार्टफोन के शुरुआती सेटअप के दौरान, यह सलाह दी जाती है:
A. स्वचालित अपडेट अक्षम करें
B. बैकअप ईमेल सेट करने से बचें
C. अज्ञात वेबसाइटों से ऐप्स इंस्टॉल करें
D. सुरक्षित वाई-फाई नेटवर्क से कनेक्ट करें

64. Installing applications should ideally be done through:
A. Third-party APK sites
B. Trusted app stores (Google Play Store / Apple App Store)
C. Unknown links shared via SMS
D. Browser pop-ups
एप्लिकेशन इंस्टॉल करना आदर्श रूप से निम्नलिखित माध्यमों से किया जाना चाहिए:
A. तृतीय-पक्ष APK साइट्स
B. विश्वसनीय ऐप स्टोर (Google Play Store / Apple App Store)
C. SMS के माध्यम से साझा किए गए अज्ञात लिंक
D. ब्राउज़र पॉप-अप

65. Updating applications regularly helps in:
A. Fixing vulnerabilities and improving security
B. Increasing screen brightness
C. Removing all notifications
D. Deleting media files
नियमित रूप से एप्लिकेशन अपडेट करने से निम्नलिखित में मदद मिलती है:
A. कमज़ोरियों को ठीक करना और सुरक्षा में सुधार करना
B. स्क्रीन की चमक बढ़ाना
C. सभी सूचनाएँ हटाना

D. मीडिया फ़ाइलें हटाना

66. Sending messages securely generally means:
A. Using social media comments
B. Sending plain SMS
C. Using end-to-end encrypted messaging apps
D. Sharing screenshots
सुरक्षित रूप से संदेश भेजने का सामान्यतः अर्थ है:
A. सोशल मीडिया टिप्पणियों का उपयोग करना
B. साधारण एसएमएस भेजना
C. एंड-टू-एंड एन्क्रिप्टेड मैसेजिंग ऐप्स का उपयोग करना
D. स्क्रीनशॉट साझा करना

67. What is the safest place to store sensitive information on a smartphone?
A. Photo gallery
B. Notes without a password
C. Encrypted secure folders/storage
D. Social media drafts
स्मार्टफोन पर संवेदनशील जानकारी संग्रहीत करने के लिए सबसे सुरक्षित स्थान कौन सा है?
A. फोटो गैलरी
B. बिना पासवर्ड वाले नोट्स
C. एन्क्रिप्टेड सुरक्षित फ़ोल्डर/स्टोरेज
D. सोशल मीडिया ड्राफ्ट

68. When sending email from a smartphone, users should:
A. Use secure email apps and strong passwords.
B. Avoid enabling two-factor authentication
C. Save passwords in plain text
D. Share OTPs for verification
स्मार्टफोन से ईमेल भेजते समय, उपयोगकर्ताओं को ये करना चाहिए:
A. सुरक्षित ईमेल ऐप्स और मज़बूत पासवर्ड का उपयोग करें।
B. दो-कारक प्रमाणीकरण सक्षम करने से बचें।
C. पासवर्ड को सादे टेक्स्ट में सेव करें।
D. सत्यापन के लिए OTP साझा करें।

69. Before capturing media that contains sensitive information, a user should:
A. Disable device security
B. Ensure the storage is encrypted
C. Share the photo on social media
D. Turn off file permissions
संवेदनशील जानकारी वाले मीडिया को कैप्चर करने से पहले, उपयोगकर्ता को यह करना चाहिए:
A. डिवाइस सुरक्षा अक्षम करें
B. सुनिश्चित करें कि स्टोरेज एन्क्रिप्टेड है
C. फ़ोटो को सोशल मीडिया पर साझा करें
D. फ़ाइल अनुमतियाँ बंद करें

70. Which feature provides strong protection if the phone is stolen?
A. Full-disk encryption.
B. Airplane mode
C. Silent mode
D. Auto rotate
फोन चोरी होने पर कौन सा फीचर मजबूत सुरक्षा प्रदान करता है?
A. फुल-डिस्क एन्क्रिप्शन
B. एयरप्लेन मोड
C. साइलेंट मोड
D. ऑटो रोटेट

71. A major characteristics of modern cyber-crimes is that they are often:
A. Fully visible to victims
B. Faster, global, and difficult to trace
C. Possible only in offices
D. Performed without internet
आधुनिक साइबर अपराधों की एक प्रमुख विशेषता यह है कि वे अक्सरः
A. पीड़ितों को पूरी तरह दिखाई देते हैं
B. तेज़, वैश्विक और पता लगाना मुश्किल होते हैं
C. केवल कार्यालयों में ही संभव होते हैं
D. बिना इंटरनेट के किए जाते हैं

72. Which of the following is an example of a recent cyber-crime incident?
A. Ransomware attacks on hospitals and corporations
B. ATM withdrawal.

C. Manual filing of data
D. Local electricity repair
निम्नलिखित में से कौन सा हाल ही में हुई साइबर अपराध घटना का उदाहरण है?
A. अस्पतालों और निगमों पर रैनसमवेयर हमले
B. एटीएम से पैसे निकालना
C. डेटा की मैन्युअल फाइलिंग
D. स्थानीय बिजली मरम्मत

73. Data breaches in recent years primarily target:
A. Offline records
B. Manual files
C. Weather stations
D. Digital databases containing personal information
हाल के वर्षों में डेटा उल्लंघनों का मुख्य लक्ष्य हैं:
A. ऑफ़लाइन रिकॉर्ड
B. मैन्युअल फ़ाइलें
C. मौसम केंद्र
D. व्यक्तिगत जानकारी वाले डिजिटल डेटाबेस

74. A common reason for the rise of cyber-crime is:
A. Slow internet speed
B. Increased digital dependence
C. Lack of social media platforms
D. Reduction in device usage
साइबर अपराध में वृद्धि का एक सामान्य कारण है:
A. धीमी इंटरनेट स्पीड
B. डिजिटल निर्भरता में वृद्धि
C. सोशल मीडिया प्लेटफॉर्म का अभाव
D. डिवाइस के उपयोग में कमी

75. In India, which agency acts as the national nodal agency for cyber-security?
A. IRCTC
B. CERT-In
C. UIDAI
D. RBI
भारत में, साइबर सुरक्षा के लिए राष्ट्रीय नोडल एजेंसी के रूप में कौन सी एजेंसी कार्य करती है?

A. IRCTC

B. CERT-In

C. UIDAI

D. RBI

76. Cyber Swachhta Kendra is mainly established for:

A. Cleaning old computers

B. Hosting government websites

C. Providing social media training

D. Botnet cleaning and malware analysis

साइबर स्वच्छता केंद्र मुख्यतः निम्नलिखित के लिए स्थापित किया गया है:

A. पुराने कंप्यूटरों की सफाई

B. सरकारी वेबसाइटों की होस्टिंग

C. सोशल मीडिया प्रशिक्षण प्रदान करना

D. बॉटनेट सफाई और मैलवेयर विश्लेषण

77. Which Indian law amendment strengthened cyber-crime penalties and data protection?

A. IT Act 2000 Amendment 2008

B. Company Act 2013

C. Income Tax Amendment 2020

D. Consumer Protection Act

किस भारतीय कानून संशोधन ने साइबर अपराध दंड और डेटा सुरक्षा को मज़बूत किया?

A. आईटी अधिनियम 2000 संशोधन 2008

B. कंपनी अधिनियम 2013

C. आयकर संशोधन 2020

D. उपभोक्ता संरक्षण अधिनियम

78. "Cyber Forensics Labs" in India are used for:

A. Repairing damaged laptops

B. Photo editing

C. Investigating and preserving digital evidence

D. Teaching computer basics only

भारत में "साइबर फोरेंसिक लैब" का उपयोग निम्नलिखित के लिए किया जाता है:

A. क्षतिग्रस्त लैपटॉप की मरम्मत

B. फोटो संपादन

C. डिजिटल साक्ष्य की जाँच और संरक्षण
D. केवल कंप्यूटर की मूल बातें पढ़ाना

79. A counter-cyber-security initiative that helps report cyber-crime in India is:
A. 100 emergency number
B. National Cybercrime Reporting Portal (www.cybercrime.gov.in)
C. Postal department website
D. School education portal
भारत में साइबर अपराध की रिपोर्ट करने में मदद करने वाली एक साइबर-सुरक्षा पहल है:
A. 100 आपातकालीन नंबर
B. राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (www.cybercrime.gov.in)
C. डाक विभाग की वेबसाइट
D. स्कूल शिक्षा पोर्टल

80. The major challenge in managing cyber-crime incidents is:
A. Rapid evolution of malware and attack methods
B. Low number of devices
C. High-speed internet
D. Strong passwords used everywhere
साइबर अपराध की घटनाओं के प्रबंधन में प्रमुख चुनौतियाँ हैं:
A. मैलवेयर और हमले के तरीकों का तेज़ी से विकास
B. उपकरणों की कम संख्या
C. तेज़ गति वाला इंटरनेट
D. हर जगह इस्तेमाल होने वाले मज़बूत पासवर्ड

81. Password managers are primarily used to:
A. Share passwords publicly
B. Store and manage complex passwords securely
C. Disable device security
D. Delete all login information
पासवर्ड मैनेजर मुख्यतः निम्नलिखित के लिए उपयोग किए जाते हैं:
A. पासवर्ड सार्वजनिक रूप से साझा करना
B. जटिल पासवर्ड को सुरक्षित रूप से संग्रहीत और प्रबंधित करना
C. डिवाइस सुरक्षा अक्षम करना
D. सभी लॉगिन जानकारी हटाना

82. A commonly used second factor in two-step verification is:
A. OTP sent to phone/email
B. Reading a PDF
C. Restarting the device
D. Updating wallpaper
द्वि-चरणीय सत्यापन में आमतौर पर इस्तेमाल किया जाने वाला दूसरा कारक है:
A. फ़ोन/ईमेल पर भेजा गया OTP
B. PDF पढ़ना
C. डिवाइस को पुनः प्रारंभ करना
D. वॉलपेपर अपडेट करना

83. Free antivirus software helps users by:
A. Removing operating systems
B. Increasing spam
C. Detecting and removing basic malware
D. Deleting all documents
मुफ़्त एंटीवायरस सॉफ़्टवेयर उपयोगकर्ताओं की मदद इस प्रकार करता है:
A. ऑपरेटिंग सिस्टम हटाकर
B. स्पैम बढ़ाना
C. बुनियादी मैलवेयर का पता लगाकर उन्हें हटाना
D. सभी दस्तावेज़ों को हटाना

84. Windows Firewall primarily protects a system by:
A. Speeding up system performance
B. Changing keyboard layout.
C. Deleting files automatically
D. Allowing and blocking network traffic based on rules
विंडोज़ फ़ायरवॉल मुख्य रूप से सिस्टम की सुरक्षा इस प्रकार करता है:
A. सिस्टम के प्रदर्शन को तेज़ करके
B. कीबोर्ड लेआउट बदलकर।
C. फ़ाइलों को स्वचालित रूप से हटाकर
D. नियमों के आधार पर नेटवर्क ट्रैफ़िक को अनुमति देकर और ब्लॉक करके

85. "Inbound Rules" in Windows Firewall manage:
A. Traffic going out of the computer
B. Brightness levels

C. Traffic coming into the computer
D. USB device functioning
विंडोज फ़ायरवॉल में "इनबाउंड नियम" निम्नलिखित का प्रबंधन करते हैं:
A. कंप्यूटर से बाहर जाने वाला ट्रैफ़िक
B. ब्राइटनेस लेवल
C. कंप्यूटर में आने वाला ट्रैफ़िक
D. USB डिवाइस की कार्यप्रणाली

86. "Outbound Rules" in Windows Firewall control:
A. Incoming data packets
B. Outgoing data packets
C. Mouse speed
D. Display resolution
विंडोज़ फ़ायरवॉल नियंत्रण में "आउटबाउंड नियम":
A. इनकमिंग डेटा पैकेट
B. आउटगोइंग डेटा पैकेट
C. माउस की गति
D. डिस्प्ले रिज़ॉल्यूशन

87. Windows Firewall with Advanced Security can be opened using:
A. Run → wf.msc
B. Run → calc.exe
C. Run → notepad.exe
D. Run → explorer.exe
उन्नत सुरक्षा के साथ Windows फ़ायरवॉल को निम्न का उपयोग करके खोला जा सकता है:
A. Run → wf.msc
B. Run → calc.exe
C. Run → notepad.exe
D. Run → explorer.exe

88. Connection Security Rules are used to:
A. Secure network connections using authentication or encryption
B. Improve sound quality
C. Change wallpaper
D. Organize files
कनेक्शन सुरक्षा नियमों का उपयोग निम्नलिखित के लिए किया जाता है:

A. प्रमाणीकरण या एन्क्रिप्शन का उपयोग करके नेटवर्क कनेक्शन सुरक्षित करना
B. ध्वनि की गुणवत्ता में सुधार करना
C. वॉलपेपर बदलना
D. फ़ाइलें व्यवस्थित करना

89. The firewall monitor in Windows Firewall with Advanced Security shows:
A. Only system brightness
B. Active firewall rules and current network status
C. List of installed movies
D. Battery usage report
उन्नत सुरक्षा वाले Windows फ़ायरवॉल में फ़ायरवॉल मॉनिटर दिखाता है:
A. केवल सिस्टम ब्राइटनेस
B. सक्रिय फ़ायरवॉल नियम और वर्तमान नेटवर्क स्थिति
C. इंस्टॉल की गई मूवीज़ की सूची
D. बैटरी उपयोग रिपोर्ट

90. When selecting the best browser, the most important factor is:
A. Number of available themes
B. Size of the browser icon
C. User's specific requirements (speed, security, extensions)
D. Colour of the interface
सर्वश्रेष्ठ ब्राउज़र चुनते समय, सबसे महत्वपूर्ण कारक हैं:
A. उपलब्ध थीम की संख्या
B. ब्राउज़र आइकन का आकार
C. उपयोगकर्ता की विशिष्ट आवश्यकताएँ (गति, सुरक्षा, एक्सटेंशन)
D. इंटरफ़ेस का रंग

91. Which browser is known for strong privacy features and tracking protection?
A. Internet Explorer
B. Mozilla Firefox
C. Classic Netscape
D. Opera Mini (Java version)
कौन सा ब्राउज़र मज़बूत गोपनीयता सुविधाओं और ट्रैकिंग सुरक्षा के लिए जाना जाता है?
A. इंटरनेट एक्सप्लोरर
B. मोजिला फ़ायरफ़ॉक्स
C. क्लासिक नेटस्केप

D. ओपेरा मिनी (जावा संस्करण)

92. For users who prefer speed and Google integration, the recommended browser is:

A. Safari (Windows edition)

B. Tor Browser

C. Netscape Navigator

D. Google Chrome

जो उपयोगकर्ता गति और Google एकीकरण पसंद करते हैं, उनके लिए अनुशंसित ब्राउज़र है:

A. सफारी (विंडोज़ संस्करण)

B. टोर ब्राउज़र

C. नेटस्केप नेविगेटर

D. गूगल क्रोम

93. For maximum anonymity and privacy-focused browsing, users often choose:

A. Tor Browser

B. Basic Text Browser

C. Classic Opera

D. Internet Explorer 8

अधिकतम गुमनामी और गोपनीयता-केंद्रित ब्राउज़िंग के लिए, उपयोगकर्ता अक्सर चुनते हैं:

A. टोर ब्राउज़र

B. बेसिक टेक्स्ट ब्राउज़र

C. क्लासिक ओपेरा

D. इंटरनेट एक्सप्लोरर 8

94. Smartphone updates primarily help in---

A. Fixing security vulnerabilities and enhancing overall device protection

B. Increasing promotional advertisements across applications

C. Automatically installing harmful software

D. Reducing built-in safety features of the operating system

स्मार्टफ़ोन अपडेट मुख्य रूप से निम्नलिखित में मदद करते हैं

A. सुरक्षा कमज़ोरियों को ठीक करना और समग्र डिवाइस सुरक्षा को बेहतर बनाना

B. सभी एप्लिकेशन में प्रचार विज्ञापनों को बढ़ाना

C. हानिकारक सॉफ़्टवेयर को स्वचालित रूप से इंस्टॉल करना

D. ऑपरेटिंग सिस्टम की अंतर्निहित सुरक्षा सुविधाओं को कम करना

95. Branded and carrier-locked smartphones typically provide-

A. Operate without requiring any carrier authorization or SIM validation

B. Allow installation of all applications without any limitations

C. Provide completely unrestricted access to all network and device settings

D. Limited installation

ब्रांडेड और कैरियर-लॉक वाले स्मार्टफ़ोन आमतौर पर क्या प्रदान करते हैं-

A. बिना किसी कैरियर प्राधिकरण या सिम सत्यापन की आवश्यकता के संचालित होते हैं

B. बिना किसी सीमा के सभी एप्लिकेशन इंस्टॉल करने की अनुमति देते हैं

C. सभी नेटवर्क और डिवाइस सेटिंग्स तक पूरी तरह से अप्रतिबंधित पहुँच प्रदान करते हैं

D. सीमित इंस्टॉलेशन

96. Which of the following represents commonly used smartphone operating systems?

A. Google Chrome and Microsoft Edge

B. Microsoft Word and Adobe Photoshop

C. Android and iOS

D. ZIP Extractor and Media Player

निम्नलिखित में से कौन सा सामान्यतः प्रयुक्त स्मार्टफोन ऑपरेटिंग सिस्टम को दर्शाता है?

A. गूगल क्रोम और माइक्रोसॉफ्ट एज

B. माइक्रोसॉफ्ट वर्ड और एडोब फोटोशॉप

C. एंड्रॉइड और iOS

D. ज़िप एक्सट्रैक्टर और मीडिया प्लेयर

97. From where should users ideally install mobile applications to ensure security?

A. Trusted official app stores such as Google Play Store or Apple App Store

B. Random websites offering free application downloads

C. Links received through unsolicited emails or messages

D. Pop-up advertisements claiming to provide premium apps

सुरक्षा सुनिश्चित करने के लिए उपयोगकर्ताओं को मोबाइल एप्लिकेशन कहाँ से इंस्टॉल करने चाहिए?

A. विश्वसनीय आधिकारिक ऐप स्टोर जैसे Google Play Store या Apple App Store

B. मुफ़्त एप्लिकेशन डाउनलोड की पेशकश करने वाली यादृच्छिक वेबसाइटें

C. अनचाहे ईमेल या संदेशों के माध्यम से प्राप्त लिंक

D. प्रीमियम ऐप प्रदान करने का दावा करने वाले पॉप-अप विज्ञापन

98. Photo sharing online should be-

A. Uploaded automatically.

B. Shared with everyone
C. Posted without checking privacy
D. Controlled and selective
ऑनलाइन फ़ोटो साझा करना चाहिए-
A. स्वचालित रूप से अपलोड किया जाना चाहिए।
B. सभी के साथ साझा किया जाना चाहिए।
C. गोपनीयता की जाँच किए बिना पोस्ट किया जाना चाहिए।
D. नियंत्रित और चयनात्मक होना चाहिए।

99. Social media groups should be joined-
A. Without checking details
B. After verifying their purpose
C. Just because friends joined
D. Forwards-based groups only
सोशल मीडिया ग्रुप्स में शामिल होना चाहिए-
A. बिना विवरण की जाँच किए
B. उनके उद्देश्य की पुष्टि करने के बाद
C. सिर्फ़ इसलिए कि दोस्त शामिल हुए हैं
D. केवल फ़ॉरवर्ड-आधारित ग्रुप्स

100. Posting live location is-
A. Risky for personal safety
B. Fine to share with everyone
C. Needed for all posts
D. Done without thinking
लाइव लोकेशन पोस्ट करना-
A. व्यक्तिगत सुरक्षा के लिए जोखिम भरा है
B. सभी के साथ साझा करना ठीक है
C. सभी पोस्ट के लिए आवश्यक है
D. बिना सोचे-समझे किया गया है

****