SECCS- 01

Practical Guide on Cyber Security

Examination, 2025 (June)

Time: 2 Hours Max Mark: 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 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 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।

P.T.O.

1. What does the World Wide Web primarily consist of?

A. Email servers

B. HTML pages and resources

C. Hardware infrastructure

D. Operating systems

वर्ल्ड वाइड वेब मुख्य रूप से किसका संग्रह है?

A. ईमेल सर्वर

B. HTML पेज और संसाधन

C. हार्डवेयर संरचना

D. ऑपरेटिंग सिस्टम

2. How are pages in a website typically connected?

A. Through email links

B. Through software downloads

C. Through cloud storage

D. Through hyperlinks

किसी वेबसाइट के पेज आम तौर पर कैसे जुड़ें होते हैं?

A. ईमेल लिंक के माध्यम से

B. सॉफ़्टवेयर डाउनलोड के माध्यम से

C. क्लाउड स्टोरेज के माध्यम से

D. हाइपरलिंक्स के माध्यम से

3. What is the unique address of a website called?

A. Web Protocol

B. IP Address

C. Uniform Resource Locator (URL)

D. Hyperlink

किसी वेबसाइट के अद्वितीय पते को क्या कहा जाता है?

A. वेब प्रोटोकॉल

B. IP एड्रेस

C. यूनिफॉर्म रिसोर्स लोकेटर (URL)

D. हाइपरलिंक

4. What risk can arise when children share personal information online?

A. A set of laws for using the internet

B. A set of moral principles governing computer usage

C. Rules for writing code

D. Guidelines for social media interaction

जब बच्चे व्यक्तिगत जानकारी ऑनलाइन साझा करते हैं तो क्या जोखिम उत्पन्न हो सकता है?

A. बेहतर ऑनलाइन अनुभव

B. कंप्यूटर के प्रदर्शन में सुधार

C. स्पैम, विज्ञापन और वायरस प्राप्त करना

D. तेज़ डाउनलोड

5. What are computer ethics?

A. Better online experience

B. Improved computer performance

C. Recieving spam, advertisements, and viruses

D. Faster downloads

कंप्यूटर नैतिकता क्या हैं?

A. इंटरनेट के उपयोग के लिए कानूनों का सेट

B. कंप्यूटर के उपयोग को नियंत्रित करने वाले नैतिक सिद्धांतों का सेट

C. कोड लिखने के लिए नियम

D. सोशल मीडिया इंटरएक्शन के लिए दिशा–निर्देश

P.T.O.

6. What is a risk of using publicly accessible computers?

A. Loss of internet connection

B. Faster browsing

C. Leaving personal information like cached web pages and cookies

D. Enhanced security

सार्वजनिक रूप से सुलभ कंप्यूटर का उपयोग करने का जोखिम क्या है?

A. इंटरनेट कनेक्शन का नुकसान

B. तेज़ ब्राउज़िंग

C. कैश्ड वेब पेज और कुकीज़ जैसी व्यक्तिगत जानकारी छोड़ना

D. बढ़ी हुई सुरक्षा

7. What is the primary goal of Cyber Safety?

A. To prevent cyberbullying

B. To protect personal information and reputation

C. To promote the use of social media

D. To enhance the speed of internet browsing

साइबर सुरक्षा का प्राथमिक लक्ष्य क्या है?

A. साइबरबुलिंग को रोकने के लिए

B. व्यक्तिगत जानकारी और प्रतिष्ठा की रक्षा के लिए

C. सोशल मीडिया के उपयोग को बढ़ावा देना

D. इंटरनेट ब्राउजिंग की गति बढ़ाने के लिए

8. What is the 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

साइबर सेफ्टी और साइबर सिक्योरिटी में क्या अंतर है?

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

9. What does "Piggy-backing" refer to in the context of Cyberbullying?

A. Publishing personal materials in someone else's name

B. Spreading false information to harm someone's reputation

C. Using someone's account to carry out unauthorized activities

D. Sending threats through anonymous emails

साइबरबुलिंग के संदर्भ में "पिग्गी–बैकिंग" का तात्पर्य क्या है?

A. किसी और के नाम पर व्यक्तिगत सामग्री प्रकाशित करना

B. किसी की प्रतिष्ठा को नुकसान पहुंचाने के लिए झूठी जानकारी फैलाना

C. अनधिकृत गतिविधियों को अंजाम देने के लिए किसी के खाते का उपयोग करना

D. गुमनाम ईमेल के माध्यम से धमकी भेजना

10. What does the ".co.in" suffix indicate in the URL "www.infosecawareness.co.in"?

A. The website is a commercial organization

B. The website is based in the United States

C. The website is registered in India

D. The website is a global domain

URL "www.infosecawareness.co.in" में ".co.in" प्रत्यय क्या दर्शाता है?

A. वेबसाइट एक वाणिज्यिक संगठन है

B. वेबसाइट संयुक्त राज्य अमेरिका में स्थित है

C. वेबसाइट भारत में पंजीकृत है

D. वेबसाइट एक वैश्विक डोमेन है

P.T.O.

11. What is the primary security reason for updating your web browser regularly?

A. To improve speed and performance

B. To prevent the browser from crashing

C. To fix security vulnerabilities

D. To reduce the amount of advertisements

आपके वेब ब्राउज़र को नियमित रूप से अपडेट करने का प्राथमिक सुरक्षा कारण क्या है?

A. गति और प्रदर्शन में सुधार करने के लिए

B. ब्राउज़र को क्रैश होने से बचाने के लिए

C. सुरक्षा कमजोरियों को ठीक करने के लिए

D. विज्ञापनों की मात्रा कम करना

12. Which of the following is NOT part of an e-mail's structure?

A. Message header

B. Message body

C. Message encryption

D. Attachment

निम्नलिखित में से कौन सा ई–मेल की संरचना का हिस्सा नहीं है?

A. संदेश शीर्षलेख

B. संदेश का मुख्य भाग

C. संदेश एन्क्रिप्शन

D. संलग्रक

13. What is the primary purpose of SMTP?

A. To receive emails from the server

B. To send emails across the Internet

C. To store email messages

D. To secure email communications

SMTP का प्राथमिक उद्देश्य क्या है?

A. सर्वर से ईमेल प्राप्त करने के लिए

B. इंटरनेट पर ईमेल भेजने के लिए

C. ईमेल संदेशों को संग्रहीत करने के लिए

D. ईमेल संचार सुरक्षित करने के लिए

14. What type of email attachment is often associated with malicious software in fake emails?

A. .pdf

B. .zip and .exe

C. .jpg

D. .docx

नकली ईमेल में किस प्रकार का ईमेल अटैचमेंट अक्सर malicious सॉफ्टवेयर से जुडा होता है?

A. .pdf

B. .zip और .exe

C. .jpg

D. .docx

15. WhatsApp messaging potential risks-

A. Messages can only be sent in plain text without encryption

B. Messages sent over public channels like WiFi may be decrypted

C. WhatsApp messages cannot be sent to multiple people at once

D. Messages are automatically encrypted with an unbreakable method

व्हाट्सएप मैसेजिंग के संभावित जोखिम–

A. संदेश केवल एन्क्रिप्शन के बिना सादे पाठ में भेजे जा सकते हैं।

B. वाईफाई जैसे सार्वजनिक चैनलों पर भेजे गए संदेशों को डिक्रिप्ट किया जा सकता है।

C. व्हाट्सएप संदेश एक साथ कई लोगों को नही भेजा जा सकता है।

D. संदेश स्वचालित रूप से एक अटूट विधि से एन्क्रिप्ट किए जाते हैं।

P.T.O.

16. What is one important solution to protect your privacy on Facebook?

A. Always post personal information to get more followers

B. Be cautious about what you publish, as once it's online, you lose control over it

C. Use Facebook without any privacy settings to reach more people

D. Ignore privacy settings and trust Facebook to keep your data secure

फेसबुक पर आपकी गोपनीयता की सुरक्षा के लिए एक महत्वपूर्ण समाधान क्या है?

A. अधिक फॉलोअर्स पाने के लिए हमेशा व्यक्तिगत जानकारी पोस्ट करें

B. आप जो प्रकाशित करते हैं उसके बारे में सावधान रहें, क्योंकि एक बार यह ऑनलाइन हो जाने पर आप उस पर नियंत्रण खो देते हैं

C. अधिक लोगों तक पहुंचने के लिए बिना किसी गोपनीयता सेटिंग के फेसबुक का उपयोग करें

D. गोपनीयता सेटिंग्स पर ध्यान न दें और अपने डेटा को सुरक्षित रखने के लिए फेसबुक पर भरोसा करें

17. What can happen when a user clicks on a malicious link?

A. They can be directed to a harmless webpage

B. Nothing happens; it is safe to click

C. They may receive a message about new updates

D. They may unknowingly download malware or be taken to a phishing site

जब कोई उपयोगकर्ता किसी malicious लिंक पर क्लिक करता है तो क्या हो सकता है?

A. उन्हें हानिरहित वेबपेज पर निर्देशित किया जा सकता है।

B. कुछ नहीं होता; क्लिक करना सुरक्षित है

C. उन्हें नए अपडेट के बारे में एक संदेश प्राप्त हो सकता है।

D. वे अनजाने में मैलवेयर डाउनलोड कर सकते हैं या फ़िशिंग साइट पर ले जाए जा सकते हैं

18. What is the main goal of a social networking phishing attack?

A. To provide free security updates to users

B. To steal user account credentials by redirecting them to a fake login page

C. To promote legitimate themes and applications

D. To help users update their profiles and settings

सोशल नेटवर्किंग फ़िशिंग हमले का मुख्य लक्ष्य क्या है?

A. उपयोगकर्ताओं को मुफ्त सुरक्षा अपडेट प्रदान करना

B. उपयोगकर्ता खाता क्रेडेंशियल को नकली लॉगिन पृष्ठ पर पुनर्निर्देशित करके चुराना

C. वैध विषयों और अनुप्रयोगों को बढ़ावा देने के लिए

D. उपयोगकर्ताओं को उनकी प्रोफाइल और सेटिंग्स अपडेट करने में मदद करने के लिए

19. What can happen if you disable or alter your firewall settings for file sharing programs?

A. Your firewall becomes more secure

B. It allows your antivirus software to block malicious files

C. You will be able to download files faster

D. Your computer becomes more vulnerable to attacks and unauthorized access

यदि आप फ़ाइल साझाकरण प्रोग्राम के लिए अपनी फ़ायरवॉल सेटिंग्स को अक्षम या परिवर्तित करते हैं तो क्या हो सकता है?

A. आपका फ़ायरवॉल अधिक सुरक्षित हो जाता है

B. यह आपके एंटीवायरस सॉफ़्टवेयर को दुर्भावनापूर्ण फ़ाइलों को ब्लॉक करने की अनुमति देता है

C. आप तेजी से फ़ाइलें डाउनलोड करने में सक्षम होंगे

D. आपका कंप्यूटर हमलों और अनधिकृत पहुंच के प्रति अधिक संवेदनशील हो जाता है

20. Key characteristics of firewall tunneling-

A. It allows IM clients to encrypt messages securely.

B. It ensures only authorized users can bypass firewalls

C. It allows IM clients to exploit any open port to bypass firewall controls.

D. It blocks all incoming connections from peer-to-peer networks

फ़ायरवॉल टनलिंग की प्रमुख विशेषता–

A. यह आईएम क्लाइंट के संदेशों को सुरक्षित रूप से एन्क्रिप्ट करने की अनुमति देता है।

B. यह सुनिश्चित करता है कि केवल अधिकृत उपयोगकर्ता ही फ़ायरवॉल को बायपास कर सकते हैं।

C. यह आईएम क्लाइंट को फ़ायरवॉल नियंत्रण को बायपास करने के लिए किसी भी खुले पोर्ट का फायदा उठाने की अनुमति देता है।

D. यह पीयर–टू–पीयर नेटवर्क से आने वाली सभी कनेक्शनों को ब्लॉक कर देता है।

P.T.O.

21. Cyber stalking is-

A. Creating websites for public use

B. Using electronic communication to harass someone

C. Learning how to hack into systems

D. Downloading illegal software

साइबर स्टॉकिंग है–

A. सार्वजनिक उपयोग के लिए वेबसाइट बनाना

B. किसी को परेशान करने के लिए इलेक्ट्रॉनिक संचार का उपयोग करना

C. सिस्टम को हैक करना सीखना

D. अवैध सॉफ्टवेयर डाउनलोड करना

22. One common tactic used by online predators to approach children-

A. Offering help with homework

B. Promoting educational websites

C. Pretending to be a child

D. Sharing informative content

बच्चों से संपर्क करने के लिए ऑनलाइन शिकारियों द्वारा उपयोग की जाने वाली एक सामान्य रणनीति–

A. होमवर्क में मदद की पेशकश करना

B. शैक्षिक वेबसाइटों को बढ़ावा देना

C. बच्चा होने का नाटक करना

D. सूचनात्मक सामग्री साझा करना

23. A weakness associated with passwords-

A. Sharing passwords with others

B. Using passwords with a mix of characters

C. Changing passwords regularly

D. Using encryption software

पासवर्ड से जुड़ी एक कमजोरी–

A. दूसरों के साथ पासवर्ड साझा करना

B. वर्णों के मिश्रण के साथ पासवर्ड का उपयोग करना

C. पासवर्ड नियमित रूप से बदलना

D. एन्क्रिप्शन सॉफ्टवेयर का उपयोग करना

24. A brute force attack is-

A. Stealing passwords by looking over someone's shoulder

B. Trying all possible password combinations until the correct one is found

C. Sending fake emails to steal credentials

D. Cracking passwords by decrypting them directly

एक brute force का आक्रमण है–

A. किसी के कंधे की ओर देखकर पासवर्ड चुराना

B. सही पासवर्ड मिलने तक सभी संभावित पासवर्ड संयोजनों को आज़माना

C. क्रेडेंशियल्स चुराने के लिए फर्जी ईमेल भेजना

D. पासवर्ड को सीधे डिक्रिप्ट करके क्रैक करना

25. A threat related to mobile phone connectivity using technologies like Bluetooth, Wifi, and USB-

A. Theft of SIM cards

B. Unauthorized physical access

C. Exposure of battery life

D. Connectivity security threats

ब्लूटूथ, वाईफाई और यूएसबी जैसी तकनीकों का उपयोग करके मोबाइल फोन कनेक्टिविटी से संबंधित खतरा–

A. सिम कार्ड की चोरी

B. अनधिकृत भौतिक पहुंच

C. बैटरी जीवन का एक्सपोजर

D. कनेक्टिविटी सुरक्षा खतरे

P.T.O.

26. What should you do in case your mobile phone is lost or stolen?

A. Ignore it and continue using the phone

B. Keep the IMEI code of your phone in a safe place to block it with the operator

C. Change your phone number immediately

D. Report the theft to your friends on social media

यदि आपका मोबाइल फोन खो जाए या चोरी हो जाए तो आपको क्या करना चाहिए?

A. इसे नजर अंदाज करें और फोन का इस्तेमाल जारी रखें

B. अपने फोन के आईएमईआई कोड को ऑपरेटर के पास ब्लॉक करने के लिए सुरक्षित स्थान पर रखें

C. अपना फ़ोन नंबर तुरंत बदलें

D. सोशल मीडिया पर अपने दोस्तों की चोरी की रिपोर्ट करें

27. What is credit card fraud?

A. Using a stolen or unauthorized credit card to obtain goods or services

B. Using one's own credit card for purchasing goods

C. Paying credit card bills online

D. Sharing your credit card details with friends

क्रेडिट कार्ड धोखाधड़ी क्या है?

A. सामान या सेवाएं प्राप्त करने के लिए चोरी या अनधिकृत क्रेडिट कार्ड का उपयोग करना

B. सामान खरीदने के लिए स्वयं के क्रेडिट कार्ड का उपयोग करना

C. क्रेडिट कार्ड बिल का ऑनलाइन भुगतान करना

D. दोस्तों के साथ अपने क्रेडिट कार्ड का विवरण साझा करना

28. The primary function of the Microsoft Malicious Software Removal Tool-

A. To block malicious software from running on a computer

B. To detect vulnerabilities in a computer system

C. To remove specific prevalent malicious software from an already-infected computer

D. To provide real-time protection against malware

Microsoft Malicious Software रिमूवल टूल का प्राथमिक कार्य–

A. दुर्भावनापूर्ण सॉफ़्टवेयर को कंप्यूटर पर चलने से रोकने के लिए

B. कंप्यूटर सिस्टम में कमजोरियों का पता लगाने के लिए

C. पहले से ही संक्रमित कंप्यूटर से विशिष्ट प्रचलित दुर्भावनापूर्ण सॉफ़्टवेयर को हटाने के लिए

D. मैलवेयर के खिलाफ वास्तविक समय सुरक्षा प्रदान करने के लिए

29. The primary function of the Microsoft Security Assessment Tool (MSAT)-

A. To scan for viruses and malware

B. To provide risk-assessment and best practices for IT infrastructure security

C. To manage network traffic

D. To enforce security policies and regulations

Microsoft Security Assessment Tool (MSAT) का प्राथमिक कार्य–

A. वायरस और मैलवेयर को स्कैन करने के लिए

B. आईटी बुनियादी ढांचे की सुरक्षा के लिए जोखिम–मूल्यांकन और सर्वोत्तम अभ्यास प्रदान करना

C. नेटवर्क यातायात का प्रबंधन करने के लिए

D. सुरक्षा नीतियों और विनियमों को लागू करना

30. What is the primary feature of X-Scan?

A. It is a firewall management tool

B. It is used to scan for malware in emails

C. It is a basic network vulnerability scanner using multi-threading

D. It is an antivirus program

एक्स–स्कैन की प्राथमिक विशेषता क्या है?

A. यह एक फ़ायरवॉल प्रबंधन उपकरण है

B. इसका उपयोग ईमेल में मैलवेयर को स्कैन करने के लिए किया जाता है

C. यह मल्टी–थ्रेडिंग का उपयोग करने वाला एक बुनियादी नेटवर्क भेद्यता स्कैनर है

D. यह एक एंटीवायरस प्रोग्राम है

P.T.O.

31. Which tool is commonly used to protect data on public Wi-Fi?
   A. Antivirus
   B. VPN (Virtual Private Network)
   C. Firewall
   D. Ad Blocker

सार्वजनिक वाई–फाई पर डेटा की सुरक्षा के लिए आमतौर पर किस उपकरण का उपयोग किया जाता है?
   A. एंटीवायरस
   B. वीपीएन (वर्चुअल प्राइवेट नेटवर्क)
   C. फ़ायरवॉल
   D. विज्ञापन अवरोधक

32. What is a common sign of a phishing email?
   A. Personalized greeting
   B. Official company logo
   C. Detailed contact information
   D. Spelling errors and urgent language

फ़िशिंग ईमेल का सामान्य लक्षण क्या है?
   A. वैयक्तिकृत अभिवादन
   B. आधिकारिक कंपनी का लोगो
   C. विस्तृत संपर्क जानकारी
   D. वर्तनी की त्रुटियां और अत्यावश्यक भाषा

33. Which of these is a secure browsing practice?
   A. Clicking on random pop-up ads
   B. Using public Wi-Fi without a VPN
   C. Checking for 'http://'in the website URL
   D. Ignoring browser security warnings

इनमें से कौन सा सुरक्षित ब्राउज़िंग अभ्यास है?
   A. रैंडप पॉप–अप विज्ञापनों पर क्लिक करना
   B. वीपीएन के बिना सार्वजनिक वाई–फाई का उपयोग करना
   C. वेबसाइट युआरएल में 'http://' की जांच करना
   D. ब्राउज़र सुरक्षा चेतावनियों को अनदेखा करना

34. What is the purpose of encryption in cybersecurity?
   A. To make data easier to access
   B. To hide files from users
   C. To protect data from unauthorized access
   D. To speed up data transfer

साइबर सुरक्षा में एन्क्रिप्शन का उद्देश्य क्या है?
A. डेटा तक पहुंच को आसान बनाने के लिए
B. उपयोगकर्ताओं से फ़ाइलें छिपाने के लिए
C. डेटा को अनधिकृत पहुंच से बचाने के लिए
D. डेटा ट्रांसफर को तेज करने के लिए

35. Which of these is a sign of malware infection?
A. Faster device performance
B. Unwanted pop-ups and ads
C. Reduced internet bills
D. Increased storage space

इनमें से कौन सा मैलवेयर संक्रमण का संकेत है?
A. तेज़ डिवाइस प्रदर्शन
B. अवांछित पॉप–अप और विज्ञापन
C. इंटरनेट बिल कम हो गया
D. भंडारण स्थान में वृद्धि

36. What is the primary purpose of a CAPTCHA?
A. To prevent automated bots from accessing websites
B. To improve website speed
C. To encrypt user data
D. To track user activity

कैप्चा का प्राथमिक उद्देश्य क्या है?
A. स्वचालित बॉट्स को वेबसाइटों तक पहुंचने से रोकने के लिए
B. वेबसाइट की गति में सुधार करने के लिए
C. उपयोगकर्ता डेटा एन्क्रिप्ट करने के लिए
D. उपयोगकर्ता गतिविधि को ट्रैक करने के लिए

37. What should you do if your online account is hacked?
A. Ignore it and hope it resolves itself
B. Immediately change your password and enable 2FA
C. Delete your account permanently
D. Share your password with a friend for help

यदि आपका ऑनलाइन अकाउंट हैक हो जाए तो आपको क्या करना चाहिए?
A. इसे अनदेखा करें और आशा करें कि यह स्वयं हल हो जाएगा
B. तुरंत अपना पासवर्ड बदलें और 2एफए सक्षम करें
C. अपना खाता स्थायी रूप से हटा दें
D. मदद के लिए किसी मित्र के साथ अपना पासवर्ड साझा करें

38. Which of the following is an example of Two-Factor Authentication (2FA)?
   A. Password only
   B. Security question only
   C. Password + OTP on mobile
   D. Username only

निम्नलिखित में से कौन सा टू–फैक्टर ऑथेंटिकेशन (2FA) का उदाहरण है?
   A. केवल पासवर्ड
   B. केवल सुरक्षा प्रश्न
   C. मोबाइल पर पासवर्ड + ओटीपी
   D. केवल उपयोगकर्ता नाम

39. Which of the following is a key indicator of spyware?
   A. Pop-up ads
   B. Unauthorised access to personal files
   C. Unusually slow device performance
   D. All of the above

निम्नलिखित में से कौन सा स्पाइवेयर का प्रमुख संकेतक है?
   A. पॉप–अप विज्ञापन
   B. व्यक्तिगत फ़ाइलों तक अनधिकृत पहुंच
   C. असामान्य रूप से धीमा डिवाइस प्रदर्शन
   D. उपरोक्त सभी

40. What is a common cybersecurity mistake people make?
   A. Using antivirus software
   B. Enabling 2FA
   C. Clicking on unknown links
   D. Regular software updates

लोगों द्वारा की जाने वाली सामान्य साइबर सुरक्षा गलती क्या है?
   A. एंटीवायरस सॉफ़्टवेयर का उपयोग करना
   B. 2एफए सक्षम करना
   C. अज्ञात लिंक पर क्लिक करना
   D. नियमित सॉफ्टवेयर अपडेट

****