Roll. No. .....

O.M.R. Serial No. | | | | | | | |

Question Booklet Number

B.Com. (FYUP) (SEM.-II) EXAMINATION, 2025-26
VOCATIONAL COURSE
CYBER SECURITY
[CODE : VOC-160]

Paper Code							
A	9	0	1	0	1	2	T

Question Booklet Series

A

Time : 1 : 00 Hours **Max. Marks : 60**

Instructions to the Examinee :

1. Do not open the booklet unless you are asked to do so.
2. The booklet contains 60 questions. Examinee is required to answer all 60 questions in the OMR Answer-Sheet provided and not in the question booklet. All questions carry equal marks.
3. Examine the Booklet and the OMR Answer-Sheet very carefully before you proceed. Faulty question booklet due to missing or duplicate pages/questions or having any other discrepancy should be got immediately replaced.
4. Four alternative answers are mentioned for each question as - A, B, C & D in the booklet. The candidate has to choose the correct / answer and mark the same in the OMR Answer-Sheet as per the direction :

(Remaining instructions on last page)

परीक्षार्थियों के लिए निर्देश :

1. प्रश्न-पुस्तिका को तब तक न खोलें जब तक आपसे कहा न जाए।
2. प्रश्न-पुस्तिका में 60 प्रश्न हैं। परीक्षार्थी को सभी 60 प्रश्नों को केवल दी गई OMR आन्सर-शीट पर ही हल करना है, प्रश्न-पुस्तिका पर नहीं। सभी प्रश्नों के अंक समान हैं।
3. प्रश्नों के उत्तर अंकित करने से पूर्व प्रश्न-पुस्तिका तथा OMR आन्सर-शीट को सावधानीपूर्वक देख लें। दोषपूर्ण प्रश्न-पुस्तिका जिसमें कुछ भाग छपने से छूट गए हों या प्रश्न एक से अधिक बार छप गए हों या उसमें किसी अन्य प्रकार की कमी हो, उसे तुरन्त बदल लें।
4. प्रश्न-पुस्तिका में प्रत्येक प्रश्न के चार सम्भावित उत्तर- A, B, C एवं D हैं। परीक्षार्थी को उन चारों विकल्पों में से सही उत्तर छाँटना है। उत्तर को OMR उत्तर-पत्रक में सम्बन्धित प्रश्न संख्या में निम्न प्रकार भरना है :

(शेष निर्देश अन्तिम पृष्ठ पर)

1. Which cyber-crime involves cloning ATM or credit card information?
   (A) Cryptojacking
   (B) Skimming
   (C) Cyber bullying
   (D) Doxxing

2. Interpol's "Purple Notice" is issued to:
   (A) Arrest criminals without warrants
   (B) Monitor missing children
   (C) Issue travel restrictions
   (D) Share information on new cyber-crime techniques

3. One of the major tools used by scammers in digital arrest fraud is:
   (A) Online news channels
   (B) VPN discount coupons
   (C) Remote desktop apps and video calls pretending to be police
   (D) Photo editing filters

4. According to FBI IC3 reports, which attack causes the highest financial loss worldwide?
   (A) Cryptocurrency mining
   (B) Social media hacks
   (C) Game account hacking
   (D) Business Email Compromise (BEC)

5. Which IPC section is frequently used in online harassment and defamation cases?
   (A) IPC 509 / 499
   (B) IPC 302
   (C) IPC 144
   (D) IPC 118

1. किस साइबर-क्राइम में ATM या क्रेडिट कार्ड की जानकारी क्लोन करना शामिल है?
   (A) क्रिप्टोजैकिंग
   (B) स्किमिंग
   (C) साइबर बुलिंग
   (D) डॉक्सिंग

2. इंटरपोल का ''पर्पल नोटिस'' इसलिए जारी किया जाता है :
   (A) बिना वारंट के क्रिमिनल्स को अरेस्ट करना
   (B) लापता बच्चों पर नज़र रखना
   (C) ट्रैवल पर रोक लगाना
   (D) नई साइबर-क्राइम टेक्नीक के बारे में जानकारी शेयर करना

3. डिजिटल अरेस्ट फ्रॉड में स्कैमर्स द्वारा इस्तेमाल किए जाने वाले मुख्य टूल्स में से एक है :
   (A) ऑनलाइन न्यूज़ चैनल
   (B) VPN डिस्काउंट कूपन
   (C) पुलिस बनकर रिमोट डेस्कटॉप ऐप और वीडियो कॉल
   (D) फोटो एडिटिंग फिल्टर

4. FBI IC3 रिपोर्ट के अनुसार, दुनिया भर में किस अटैक से सबसे ज़्यादा फ़ाइनेंशियल नुकसान होता है?
   (A) क्रिप्टोकरेंसी माइनिंग
   (B) शोसल मीडिया हैक्स
   (C) गेम अकाउंट हैकिंग
   (D) बिज़नेस ईमेल कॉम्प्रोमाइज़ (BEC)

5. ऑनलाइन हैरेसमेंट और मानहानि के मामलों में IPC की कौन-सी धारा अक्सर इस्तेमाल होती है?
   (A) IPC 509 / 499
   (B) IPC 302
   (C) IPC 144
   (D) IPC 118

6. Identity theft occurs when:

(A) A person steals hardware from an office

(B) A user deletes their own email

(C) Hackers attack only government websites

(D) Someone steals another's personal information for misuse

7. What is the main goal of a romance scammer?

(A) To make friends

(B) To steal money or personal information

(C) To play online games

(D) To promote movies

8. Which sign often indicates online grooming?

(A) Asking about hobbies

(B) Asking for private photos or secrets

(C) Sending memes

(D) Talking about school

9. Fake giveaway scammers usually ask victims to:

(A) Pay a "processing fee"

(B) Take free gifts

(C) Visit a park

(D) Join a study group

6. आइडेंटिटी थेफ़्ट तब होती है जब :

(A) कोई व्यक्ति किसी ऑफ़िस से हार्डवेयर चुराता है

(B) कोई यूज़र अपना ईमेल डिलीट कर देता है

(C) हैकर्स सिर्फ़ सरकारी वेबसाइट पर अटैक करते हैं

(D) कोई व्यक्ति किसी दूसरे की पर्सनल जानकारी गलत इस्तेमाल के लिए चुराता है

7. रोमांस स्कैमर का मुख्य लक्ष्य क्या है?

(A) दोस्त बनाना

(B) पैसे या पर्सनल जानकारी चुराना

(C) ऑनलाइन गेम खेलना

(D) मूवीज़ को प्रमोट करना

8. कौन-सा संकेत अक्सर ऑनलाइन ग्रूमिंग की ओर इशारा करता है?

(A) हॉबी के बारे में पूछना

(B) प्राइवेट फ़ोटो या सीक्रेट पूछना

(C) मीम भेजना

(D) स्कूल के बारे में बात करना

9. नकली गिवअवे स्कैमर आमतौर पर पीड़ितों से कहते हैं :

(A) ''प्रोसेसिंग फ़ीस'' दें

(B) मुफ़्त गिफ़्ट लें

(C) पार्क में जाएँ

(D) स्टडी ग्रुप में शामिल हों

10. Crypto scam promotions often promise:
(A) Low returns
(B) Guaranteed high profits
(C) Normal market growth
(D) Slow investment

11. Metadata can reveal:
(A) Weather details
(B) Hidden information like date/time an image was created
(C) Movie files
(D) Shopping history

12. A behavioral red flag for a fake profile is:
(A) Posting daily life photos
(B) Messaging many people the same lines
(C) Having old posts
(D) Having friends and family tagged

13. Reviewing recent login history helps you:
(A) Learn time management
(B) Check if someone logged in from unknown devices
(C) Increase followers
(D) Find new friends

14. If a hacker changed your password, you should:
(A) Give up
(B) Use "Forgot Password" recovery steps
(C) Create a new email
(D) Logout from all devices

10. क्रिप्टो स्कैम प्रमोशन अक्सर ये वादे करते हैं :
(A) कम रिटर्न
(B) ज़्यादा मुनाफ़े की गारंटी
(C) नॉर्मल मार्केट ग्रोथ
(D) धीमा इन्वेस्टमेंट

11. मेटाडेटा से ये पता चल सकता है :
(A) मौसम की जानकारी
(B) छिपी हुई जानकारी जैसे इमेज बनाने की तारीख/समय
(C) मूवी फ़ाइलें
(D) शॉपिंग हिस्ट्री

12. एक नकली प्रोफ़ाइल के लिए एक बिहेवियरल रेड फ़्लैग है :
(A) रोज़मर्रा की जिंदगी की फोटो पोस्ट करना
(B) कई लोगों को एक ही लाइन में मैसेज करना
(C) पुरानी पोस्ट रखना
(D) दोस्तों और परिवार को टैग करना

13. हाल की लॉगिन हिस्ट्री देखने से आपको मदद मिलती है :
(A) टाइम मैनेजमेंट सीखें
(B) चेक करें कि किसी ने अनजान डिवाइस से लॉग इन तो नहीं किया
(C) फॉलोअर्स बढाएं
(D) नए दोस्त बनाएं

14. अगर किसी हैकर ने आपका पासवर्ड बदल दिया है, तो आपको ये करना चाहिए :
(A) हार मान लें
(B) ''पासवर्ड भूल गए'' रिकवरी स्टेप्स का इस्तेमाल करें
(C) नया ईमेल बनाएं
(D) सभी डिवाइस से लॉगआउट करें

15. To stay safe, users should:

(A) Reuse old passwords

(B) Use strong & unique passwords

(C) Share passwords with friends

(D) Remove 2FA

16. Hackers get leaked passwords from:

(A) Movies

(B) Data breaches on other websites

(C) YouTube

(D) Weather apps

17. Spoofed calls are dangerous because:

(A) They are long calls

(B) They look like genuine bank numbers

(C) They have jokes

(D) They use loud music

18. A data leak happens when:

(A) Data is safely backed up

(B) User information is exposed without permission

(C) Apps update themselves

(D) Users change passwords

19. Malicious QR codes can:

(A) Improve phone speed

(B) Steal personal data

(C) Clean your phone screen

(D) Charge your battery

20. A dangerous QR code often:

(A) Opens unknown suspicious links

(B) Shows a wallpaper

(C) Opens camera

(D) Plays music

15. सुरक्षित रहने के लिए, यूज़र्स को ये करना चाहिए :

(A) पुराने पासवर्ड दोबारा इस्तेमाल करना

(B) मज़बूत और यूनिक पासवर्ड का इस्तेमाल करना

(C) दोस्तों के साथ पासवर्ड शेयर करना

(D) 2FA हटाना

16. हैकर्स को पासवर्ड लीक इन चीज़ों से होते हैं :

(A) मूवीज़

(B) दूसरी वेबसाइट्स पर डेटा ब्रीच

(C) यूट्यूब

(D) वेदर ऐप्स

17. नकली कॉल खतरनाक होती हैं क्योंकि :

(A) ये लंबी कॉल होती हैं

(B) ये असली बैंक नंबर जैसी दिखती है

(C) इनमें मज़ाक होता है

(D) इनमें तेज़ म्यूज़िक का इस्तेमाल होता है

18. डेटा लीक तब होता है जब :

(A) डेटा का सुरक्षित बैकअप लिया जाता है

(B) यूज़र की जानकारी बिना इजाज़त के सामने आ जाती है

(C) ऐप्स खुद को अपडेट करते हैं

(D) यूज़र पासवर्ड बदलते हैं

19. गलत QR कोड ये कर सकते हैं :

(A) फ़ोन की स्पीड बढ़ा सकते हैं

(B) पर्सनल डेटा चुरा सकते हैं

(C) आपके फ़ोन की स्क्रीन साफ़ कर सकते हैं

(D) आपकी बैटरी चार्ज कर सकते हैं

20. एक खतरनाक QR कोड अक्सर :

(A) अनजान संदिग्ध लिंक खोलता है

(B) वॉलपेपर दिखाता है

(C) कैमरा खोलता है

(D) म्यूज़िक चलाता है

21. Which of the following is a common online financial fraud?

(A) Phishing

(B) Gardening

(C) Online gaming

(D) Grocery shopping

22. A fake call pretending to be from a bank asking for OTP is known as:

(A) Farming

(B) Vishing

(C) Surfing

(D) DDoS

23. If someone sends you a payment request on UPI:

(A) Accept without thinking

(B) Decline and verify the person

(C) Enter random PIN

(D) Call the number in the request

24. Fake shopping websites mainly aim to:

(A) Sell original products

(B) Steal money and personal information

(C) Improve customer service

(D) Provide cashback

25. CERT-IN regularly issues early alerts to which of the following sectors?

(A) Insurance only

(B) Only mobile companies

(C) Government, banks, and corporates

(D) Travel and hotel industry

21. इनमें से कौन-सा एक आम ऑनलाइन फ़ाइनेंशियल फ्रांड है?

(A) फ़िशिंग

(B) बागवानी

(C) ऑनलाइन गेमिंग

(D) किराने का सामान खरीदना

22. बैंक से OTP मांगने का नाटक करने वाली नकली कॉल को क्या कहते हैं?

(A) फार्मिंग

(B) विशिंग

(C) सर्फिंग

(D) DDoS

23. अगर कोई आपको UPI पर पेमेंट रिक्वेस्ट भेजता है :

(A) बिना सोचे-समझे एक्सेप्ट करना

(B) डिक्लाइन करना और व्यक्ति को वेरिफाई करना

(C) रैंडम PIN डालना

(D) रिक्वेस्ट में दिए गए नंबर पर कॉल करना

24. नकली शॉपिंग वेबसाइट का मुख्य मकसद होता है :

(A) ओरिजिनल प्रोडक्ट बेचना

(B) पैसे और पर्सनल जानकारी चुराना

(C) कस्टमर सर्विस को बेहतर बनाना

(D) कैशबैक देना

25. CERT-IN रेगुलर तौर पर इनमें से किन सेक्टर्स को अर्ली अलर्ट जारी करता है?

(A) केवल इंश्योरेंस

(B) केवल मोबाइल कंपनियाँ

(C) सरकार, बैंक और कॉर्पोरेट्स

(D) ट्रैवल और होटल इंडस्ट्री

26. What's the core reason UPI frauds happen when users click unknown payment links?

(A) Server error

(B) App crash

(C) Phishing and social engineering

(D) Network delay

27. Who can complain to the RBI Ombudsman?

(A) Only businessmen

(B) Anyone having a banking issue

(C) Only NRIs

(D) Only RBI staff

28. How can you protect your mobile from SIM swapping?

(A) Use basic phone

(B) Share number online

(C) Set SIM lock or telecom PIN

(D) Never charge phone

29. What is the danger of oversharing on social media?

(A) It may lead to data misuse, stalking, or financial fraud

(B) It helps you gain more followers

(C) It makes your posts more popular

(D) It improves internet connectivity

26. जब यूज़र अनजान पेमेंट लिंक पर क्लिक करते हैं तो UPI फ्रॉड होने का मुख्य कारण क्या है?

(A) सर्वर एरर

(B) ऐप क्रैश

(C) फ़िशिंग और सोशल इंजीनियरिंग

(D) नेटवर्क में देरी

27. RBI ओम्बड्समैन से कौन शिकायत कर सकता है?

(A) केवल बिज़नेसमैन

(B) कोई भी जिसे बैंकिंग से जुड़ी कोई समस्या हो

(C) केवल NRI

(D) केवल (RBI) स्टाफ़

28. आप अपने मोबाइल को SIM स्वैपिंग से कैसे बचा सकते हैं?

(A) बेसिक फ़ोन इस्तेमाल करें

(B) ऑनलाइन नंबर शेयर करें

(C) SIM लॉक या टेलीकॉम PIN सेट करें

(D) फ़ोन कभी चार्ज न करें

29. सोशल मीडिया पर ज़्यादा शेयर करने का क्या खतरा है?

(A) इससे डेटा का गलत इस्तेमाल, स्टॉकिंग या फ़ाइनेंशियल फ्रॉड हो सकता है

(B) इससे आपको ज़्यादा फ़ॉलोअर्स पाने में मदद मिलती है

(C) इससे आपकी पोस्ट ज़्यादा पॉपुलर होती है

(D) इससे इंटरनेट कनेक्टिविटी बेहतर होती है

30. What should you do first if you or someone you know is cyberbullied?

(A) Retaliate with mean comments

(B) Ignore it completely

(C) Delete your account immediately

(D) Save evidence and report to a trusted adult or authority

31. Which is a sign that a website is secure for transactions?

(A) It has colorful ads

(B) It opens on full screen

(C) It has a lock icon and 'https' in the address bar

(D) The URL starts with 'http'

32. Which of the following is an example of cyberstalking?

(A) Writing online blogs

(B) Sending a job offer

(C) Repeatedly messaging someone despite them asking to stop

(D) Playing games together

33. Why is personal information valuable in the digital world?

(A) It can be sold or misused for fraud, identity theft, or scams

(B) It helps in watching movies

(C) It increases internet speed

(D) It gives access to free shopping

30. अगर आपको या आपके किसी जानने वाले को साइबरबुलिंग होती है, तो आपको सबसे पहले क्या करना चाहिए?

(A) बुरे कमेंट्स करके जवाब दें

(B) इसे पूरी तरह से इग्नोर करें

(C) अपना अकाउंट तुरंत डिलीट करें

(D) सबूत सेव करें और किसी भरोसेमंद एडल्ट या अथॉरिटी को रिपोर्ट करें

31. कौन-सी निशानी है कि कोई वेबसाइट ट्रांज़ैक्शन के लिए सिक्योर है?

(A) इसमें कलरफुल ऐड होते हैं

(B) यह फुल स्क्रीन पर खुलती है

(C) इसमें एक लॉक आइकन होता है और एड्रेस बार में 'https' होता है

(D) URL 'http' से शुरू होता है

32. इनमें से कौन-सा साइबरस्टॉकिंग का उदाहरण है?

(A) ऑनलाइन ब्लॉग लिखना

(B) जॉब ऑफ़र भेजना

(C) किसी के रोकने के कहने के बावजूद उसे बार-बार मैसेज करना

(D) साथ में गेम खेलना

33. डिजिटल दुनिया में पर्सनल जानकारी कीमती क्यों है?

(A) इसे फ्रॉड, आइडेंटिटी थेफ्ट या स्कैम के लिए बेचा या गलत इस्तेमाल किया जा सकता है

(B) यह मूवी देखने में मदद करता है

(C) यह इंटरनेट स्पीड बढ़ाता है

(D) यह फ्री शॉपिंग का एक्सेस देता है

34. Which of these actions is a safe response to cyberbullying?

(A) Create a fake account to fight back

(B) Block and report the bully on the platform

(C) Keep it a secret

(D) Share bullying post with others

35. What does 'Digital Underground' refer to?

(A) A video game

(B) Hidden digital communities and markets beyond the surface web

(C) Metro train system

(D) Secret tunnels in a city

36. Who are often the actors behind cyber terrorism?

(A) State-sponsored hackers or extremist groups

(B) Shopkeepers

(C) College students doing homework

(D) Digital artists

37. Which of the following is a cybercrime often initiated through dark web services?

(A) Online banking

(B) Social networking

(C) Online shopping

(D) Phishing kits and hacking tools distribution

34. इनमें से कौन-सा काम साइबरबुलिंग का सुरक्षित जवाब है?

(A) जवाब देने के लिए एक नकली अकाउंट बनाएं

(B) प्लेटफॉर्म पर बुली करने वाले को ब्लॉक करें और रिपोर्ट करें

(C) इसे सीक्रेट रखें

(D) दूसरों के साथ बुलिंग पोस्ट शेयर करें

35. 'डिजिटल अंडरग्राउंड' का मतलब क्या है?

(A) एक वीडियो गेम

(B) वेब के बाहर छिपे हुए डिजिटल कम्युनिटी और मार्केट

(C) मेट्रो ट्रेन सिस्टम

(D) शहर में सीक्रेट टनल

36. साइबर टेररिज्म के पीछे अक्सर कौन लोग होते हैं?

(A) सरकार द्वारा स्पॉन्सर्ड हैकर या एक्सट्रीमिस्ट ग्रुप

(B) दुकानदार

(C) होमवर्क करते कॉलेज स्टूडेंट

(D) डिजिटल आर्टिस्ट

37. इनमें से कौन-सा साइबर क्राइम अक्सर डार्क वेब सर्विस के जरिए शुरू होता है?

(A) ऑनलाइन बैंकिंग

(B) सोशल नेटवर्किंग

(C) ऑनलाइन शॉपिंग

(D) फ़िशिंग किट और हैकिंग टूल का डिस्ट्रीब्यूशन

38. Which critical sectors are often targeted in cyber terrorism?
(A) Movie theatres
(B) Power grids, airports, banks, and government websites
(C) Schools only
(D) Cafes

39. What is one major risk of visiting dark web sites?
(A) Free gaming
(B) Better education
(C) Improved Wi-Fi speed
(D) Exposure to scams, illegal content, and surveillance

40. What is the 'Dark Web'?
(A) The part of the internet is not indexed by regular search engines
(B) A secret part of space
(C) A type of computer virus
(D) A website for kids

41. Which of the following is an effective preventive measure against cyber terrorism?
(A) Ignoring updates
(B) Clicking unknown ads
(C) Regularly updating software and practicing digital hygiene
(D) Using outdated antivirus

42. What type of human-related crimes are often reported on the dark web?
(A) Lost-and-found websites
(B) Food delivery scams
(C) Job interviews
(D) Human trafficking, child exploitation, and illegal pornographic content

38. साइबर टेररिज़्म में अक्सर कौन-से ज़रूरी सेक्टर टारगेट किए जाते हैं?
(A) मूवी थिएटर
(B) पावर ग्रिड, एयरपोर्ट, बैंक और सरकारी वेबसाइट
(C) केवल स्कूल
(D) कैफ़े

39. डार्क वेब साइट पर जाने का एक बड़ा रिस्क क्या है?
(A) फ़्री गेमिंग
(B) बेहतर एजुकेशन
(C) बेहतर Wi-Fi स्पीड
(D) स्कैम, गैर-कानूनी कंटेंट और सर्विलांस का सामना करना

40. 'डार्क वेब' क्या है?
(A) इंटरनेट का वह हिस्सा जिसे रेगुलर सर्च इंजन इंडेक्स नहीं करते हैं
(B) स्पेस का एक सीक्रेट हिस्सा
(C) एक तरह का कम्प्यूटर वायरस
(D) बच्चों के लिए एक वेबसाइट

41. इनमें से कौन-सा साइबर टेररिज़्म से बचने का एक असरदार तरीका है?
(A) अपडेट्स को इग्नोर करना
(B) अनजान ऐड्स पर क्लिक करना
(C) रेगुलर सॉफ्टवेयर अपडेट करना और डिजिटल हाइजीन रखना
(D) पुराने एंटीवायरस का इस्तेमाल करना

42. डार्क वेब पर अक्सर किस तरह के इंसानों से जुड़े क्राइम रिपोर्ट किए जाते हैं?
(A) खोई-पाई वेबसाइट
(B) फूड डिलीवरी स्कैम
(C) जॉब इंटरव्यू
(D) ह्यूमन ट्रैफिकिंग, बच्चों का शोषण, और गैर-कानूनी पोर्नोग्राफिक कंटेंट

43. Backing up important data helps to:

(A) Prevent power failures

(B) Recover data after attacks

(C) Avoid internet usage

(D) Increase device speed

44. Which of the following habits should be avoided?

(A) Regular scanning for viruses

(B) Using outdated software

(C) Updating passwords

(D) Taking backups

45. Good cyber hygiene protects you from:

(A) Only physical theft

(B) Online threats and cyberattacks

(C) Weather changes

(D) Hardware manufacturing defects

46. Before clicking a link, you should:

(A) Click instantly

(B) Check the sender

(C) Forward it to friends

(D) Ignore warnings

47. Which activity is unsafe?

(A) Using official apps

(B) Downloading from trusted stores

(C) Installing apps from unknown sources

(D) Enabling screen lock

48. Screens locks such as PIN or pattern help:

(A) Slow down phone

(B) Protect device access

(C) Delete photos

(D) Increase RAM

43. ज़रूरी डेटा का बैकअप लेने से इन चीज़ों में मदद मिलती है :

(A) पावर जाने से बचें

(B) अटैक के बाद डेटा रिकवर करें

(C) इंटरनेट का इस्तेमाल न करें

(D) डिवाइस की स्पीड बढ़ाएँ

44. नीचे दी गई आदतों में से किनसे बचना चाहिए?

(A) वायरस के लिए रेगुलर स्कैनिंग

(B) पुराने सॉफ्टवेयर का इस्तेमाल करना

(C) पासवर्ड अपडेट करना

(D) बैकअप लेना

45. अच्छी साइबर हाइजीन आपको इनसे बचाती है :

(A) सिर्फ फिजिकल चोरी

(B) ऑनलाइन खतरे और साइबर अटैक

(C) मौसम में बदलाव

(D) हार्डवेयर मैन्युफैक्चरिंग डिफेक्ट

46. किसी लिंक पर क्लिक करने से पहले, आपको ये करना चाहिए :

(A) तुरंत क्लिक करें

(B) भेजने वाले को चेक करें

(C) इसे दोस्तों को फॉरवर्ड करें

(D) चेतावनियों को इग्नोर करें

47. कौन-सी एक्टिविटी असुरक्षित है?

(A) ऑफिशियल ऐप्स का इस्तेमान करना

(B) भरोसेमंद स्टोर से डाउनलोड करना

(C) अनजान सोर्स से ऐप्स इंस्टॉल करना

(D) स्क्रीन लॉक चालू करना

48. PIN या पैटर्न जैसे स्क्रीन लॉक मदद करते हैं :

(A) फोन को स्लो करें

(B) डिवाइस एक्सेस को प्रोटेक्ट करें

(C) फोटो डिलीट करें

(D) RAM बढ़ाएं

49. Which malware displays unwanted advertisements on a system?
(A) Spyware (B) Adware
(C) Worm (D) Rootkit

50. Scareware usually tricks users by:
(A) Showing fake threat warnings
(B) Silently monitoring keystrokes
(C) Stealing credentials
(D) Encrypting all files

51. A collection of compromised machines controlled remotely is called a:
(A) Worm network (B) Botnet
(C) Trojan group (D) Spy cluster

52. A computer virus can spread only when:
(A) There is user action
(B) The system is encrypted
(C) The firewall is disabled
(D) Data backup is removed

53. RDP compromise generally happens due to:
(A) Strong passwords
(B) Default or weak credentials
(C) Two-factor authentication
(D) Firewall monitoring

54. Which of the following is most commonly used by attackers to deliver initial malware?
(A) Corporate intranet
(B) Malicious email attachment
(C) Google search results
(D) Printer drivers

55. Who must be informed during an incident as per best practice?
(A) Neighbours
(B) Relevant internal teams
(C) Social media followers
(D) Cab drivers

49. कौन-सा मैलवेयर सिस्टम पर अनचाहे विज्ञापन दिखाता है?
(A) स्पाइवेयर (B) एडवेयर
(C) वर्म (D) रूटकिट

50. स्केयरवेयर आमतौर पर यूज़र्स को इस तरह धोखा देता है :
(A) नकली खतरे की चेतावनी दिखाकर
(B) चुपचाप कीस्ट्रोक्स पर नज़र रखकर
(C) क्रेडेंशियल चुराकर
(D) सभी फ़ाइलों को एन्क्रिप्ट करके

51. दूर से कंट्रोल की जाने वाली खराब मशीनों के कलेक्शन को क्या कहते हैं?
(A) वर्म नेटवर्क (B) बॉटनेट
(C) ट्रोजन ग्रुप (D) स्पाई क्लस्टर

52. कम्प्यूटर वायरस तभी फैल सकता है जब :
(A) यूज़र एक्शन हो
(B) सिस्टम एन्क्रिप्टेड हो
(C) फ़ायरवॉल डिसेबल हो
(D) डेटा बैकअप हटा दिया गया हो

53. RDP कॉम्प्रोमाइज़ आमतौर पर इन वजहों से होता है :
(A) स्ट्रॉन्ग पासवर्ड
(B) डिफॉल्ट या कमज़ोर क्रेडेंशियल
(C) टू-फैक्टर ऑथेंटिकेशन
(D) फ़ायरवॉल मॉनिटरिंग

54. इनमें से किसका इस्तेमाल अटैकर शुरुआती मैलवेयर डिलीवर करने के लिए सबसे ज़्यादा करते हैं?
(A) कॉर्पोरेट इंट्रानेट
(B) मैलिशियस ईमेल अटैचमेंट
(C) गूगल सर्च रिज़ल्ट
(D) प्रिंटर ड्राइवर

55. किसी घटना के दौरान बेस्ट प्रैक्टिस के हिसाब से किसे इन्फॉर्म किया जाना चाहिए?
(A) पड़ोसी
(B) रिलेवेंट इंटरनल टीम
(C) सोशल मीडिया फॉलोअर्स
(D) कैब ड्राइवर

56. Recovery from ransomware should start only after:

(A) Attackers send a friendly message

(B) Infection is fully contained

(C) Antivirus is uninstalled

(D) Users run random scripts

57. Online grooming often begins with:

(A) Slow friendship-building

(B) Asking for bank passwords

(C) Meeting parents

(D) Sending official documents

58. Digital extortion on social media usually begins when attackers:

(A) Ask for game recommendations

(B) Gain access to private photos, chats, or accounts

(C) Request to join online study groups

(D) Offer emojis and filters for free

59. Why is covering the keypad while entering ATM PIN still important on chip-enabled ATMs?

(A) Prevents network hacking

(B) Avoids shoulder surfing or hidden camera capture

(C) Speeds up transaction

(D) Bypasses OTP

60. Which malware hides deep inside the operating system to avoid detection?

(A) Rootkit

(B) Adware

(C) Scareware

(D) Virus

56. रैंसमवेयर से रिकवरी तभी शुरू होनी चाहिए जब :

(A) अटैकर्स कए फ्रेंडली मैसेज भेजें

(B) इन्फेक्शन पूरी तरह से कंट्रोल हो जाए

(C) एंटीवायरस अनइंस्टॉल हो जाए

(D) यूज़र्स रैंडम स्क्रिप्ट चलाएं

57. ऑनलाइन ग्रूमिंग अक्सर ऐसे शुरू होती है :

(A) धीरे-धीरे दोस्ती बनाना

(B) बैंक पासवर्ड पूछना

(C) माता-पिता से मिलना

(D) ऑफिशियल डॉक्यूमेंट भेजना

58. सोशल मीडिया पर डिजिटल एक्सटॉर्शन आमतौर पर तब शुरू होता है जब अटैकर :

(A) गेम के सुझाव मांगते हैं

(B) प्राइवेट फ़ोटो, चैट या अकाउंट का एक्सेस पाते हैं

(C) ऑनलाइन स्टडी ग्रुप में शामिल होने का अनुरोध करते हैं

(D) मुफ़्त में इमोजी और फ़िल्टर ऑफ़र करते हैं

59. चिप वाले ATM में ATM PIN डालते समय कीपैड को ढकना अभी भी क्यों ज़रूरी है?

(A) नेटवर्क हैकिंग से बचाता है

(B) शोल्डर सर्फिंग या हिडन कैमरा कैप्चर से बचाता है

(C) ट्रांज़ैक्शन तेज़ करता है

(D) OTP को बायपास करता है

60. कौन-सा मैलवेयर पता लगने से बचने के लिए ऑपरेटिंग सिस्टम के अंदर छिपा रहता है?

(A) रूटकिट

(B) एडवेयर

(C) स्केयरवेयर

(D) वायरस

Rough Work / रफ कार्य

Example :

Question :

Q.1 Ⓐ ● Ⓒ Ⓓ

Q.2 Ⓐ Ⓑ ● Ⓓ

Q.3 Ⓐ ● Ⓒ Ⓓ

5. Each question carries equal marks. Marks will be awarded according to the number of correct answers you have.

6. All answers are to be given on OMR Answer Sheet only. Answers given anywhere other than the place specified in the answer sheet will not be considered valid.

7. Before writing anything on the OMR Answer Sheet, all the instructions given in it should be read carefully.

8. After the completion of the examination, candidates should leave the examination hall only after providing their OMR Answer Sheet to the invigilator. Candidate can carry their Question Booklet.

9. There will be no negative marking.

10. Rough work, if any, should be done on the blank pages provided for the purpose in the booklet.

11. To bring and use of log-book, calculator, pager & cellular phone in examination hall is prohibited.

12. In case of any difference found in English and Hindi version of the question, the English version of the question will be held authentic.

Impt. On opening the question booklet, first check that all the pages of the question booklet are printed properly. If there is any discrepancy in the question Booklet, then after showing it to the invigilator, get another question Booklet of the same series.

उदाहरण :

प्रश्न :

प्रश्न 1 Ⓐ ● Ⓒ Ⓓ

प्रश्न 2 Ⓐ Ⓑ ● Ⓓ

प्रश्न 3 Ⓐ ● Ⓒ Ⓓ

5. प्रत्येक प्रश्न के अंक समान हैं। आपके जितने उत्तर सही होंगे, उन्हीं के अनुसार अंक प्रदान किये जायेंगे।

6. सभी उत्तर केवल ओ०एम०आर० उत्तर-पत्रक (OMR Answer Sheet) पर ही दिये जाने हैं। उत्तर-पत्रक में निर्धारित स्थान के अलावा अन्यत्र कहीं पर दिया गया उत्तर मान्य नहीं होगा।

7. ओ०एम०आर० उत्तर-पत्रक (OMR Answer Sheet) पर कुछ भी लिखने से पूर्व उसमें दिये गये सभी अनुदेशों को सावधानीपूर्वक पढ़ लिया जाये।

8. परीक्षा समाप्ति के उपरान्त परीक्षार्थी कक्ष निरीक्षक को अपनी OMR Answer Sheet उपलब्ध कराने के बाद ही परीक्षा कक्ष से प्रस्थान करें। परीक्षार्थी अपने साथ प्रश्न-पुस्तिका ले जा सकते हैं।

9. निगेटिव मार्किंग नहीं है।

10. कोई भी रफ कार्य, प्रश्न-पुस्तिका में, रफ-कार्य के लिए दिए खाली पेज पर ही किया जाना चाहिए।

11. परीक्षा-कक्ष में लॉग-बुक, कैल्कुलेटर, पेजर तथा सेल्युलर फोन ले जाना तथा उसका उपयोग करना वर्जित है।

12. प्रश्न के हिन्दी एवं अंग्रेजी रूपान्तरण में भिन्नता होने की दशा में प्रश्न का अंग्रेजी रूपान्तरण ही मान्य होगा।

महत्वपूर्णः प्रश्नपुस्तिका खोलने पर प्रथमतः जाँच कर देख लें कि प्रश्नपुस्तिका के सभी पृष्ठ भलीभाँति छपे हुए हैं। यदि प्रश्नपुस्तिका में कोई कमी हो, तो कक्षनिरीक्षक को दिखाकर उसी सिरीज की दूसरी प्रश्नपुस्तिका प्राप्त कर लें।