Topic- Information and Cyber Security (UGK)

MTDT016

1. **What is the best and prescribed usage of Bank's official email id as per bank's policy?**
   a. For official communications
   b. To register on social media platforms
   c. On e-commerce websites
   d. To register on UPI platforms for sending money
   e. To use for personal communication

   Answer:- For official communications

2. **All types of phishing URLs/Emails to be reported to which email ID of CISO office?**
   a. antiphishing@unionbankofindia.bank
   b. antiphishing.ciso@unionbankofindia.bank
   c. phishing-report@unionbankofindia.bank
   d. antiphishing@unionbankofindia.in
   e. ciso.phishing@unionbankofindia.co.in

   Answer:- antiphishing.ciso@unionbankofindia.bank

3. **Domain name disguise & Domain name Spoofing techniques are used in which type of cyber attack?**
   a. DDoS
   b. Ransomware
   c. Man-in-the-middle
   d. Phishing
   e. All of the above

   Answer:- Phishing

4. **Which is not a 2 factor authentication methodology?**
   a. One Time Password
   b. Biometric Authentication
   c. Hardware tokens
   d. Getting PIN through post
   e. All of the above

   Answer:- Getting PIN through post

5. **What are the key objectives of multi-factor authentication?**
   a. Protect the Confidentiality
   b. Avoid Cyber Attack
   c. Enhance user confidence
   d. Only a&b
   e. All a,b&c

   Answer:- All a,b&c

6. **Which one is not a tell-tale sign to identify a phishing email?**
    a. Unknown email with attachment
    b. Unknown email with suspicious link
    c. Email with spelling and grammatical errors
    d. Any email from outside of the organization
    e. Urgent and threatening language in email

    Answer:- Any email from outside of the organization

7. **What is the best way to check the original URL address of an embedded link in an unknown email?**
    a. Click on the link and see
    b. Copy the link and paste on the note pad
    c. Hover the mouse pointer on the link
    d. Forward the email to a friend and check in his/her computer
    e. Any of the above

    Answer:- Hover the mouse pointer on the link

8. **What is Whaling?**
    a. A phishing attack targeted to top management of an organization
    b. A phishing attack targeted to network/system administrators of an organization
    c. A phishing attack targeted to all ex-employees of an organization
    d. A phishing attack targeted to all employees of an organization
    e. All of the above

    Answer:- A phishing attack targeted to top management of an organization

9. **Which of the following will cause cyber-security risks?**
    a. Using unpatched and outdated software
    b. Rolling out the software without proper testing
    c. Lack of policies related to usage of external media
    d. Lack of Awareness to staff members
    e. All of the above

    Answer:- All of the above

10. **A scenario where an employee discloses sensitive information to a third party, is a type of:**
    a. Man-in-the-middle attack
    b. Phishing Attack
    c. Insider Threat
    d. Ransomware Attack
    e. All of the above

Answer:- Insider Threat

11. **What pillar of information security ensures that sensitive information is not disclosed without authorization?**
    a. Availability
    b. Non-repudiation
    c. Integrity
    d. Confidentiality
    e. None of the above

Answer:- Confidentiality

12. **What is Smishing?**
    a. Phishing attack through mail
    b. Phishing attack through a QR
    c. Phishing attack through a voice call
    d. Phishing attack through an SMS with a malicious link
    e. Phishing through fake websites

Answer:- Phishing attack through an SMS with a malicious link

13. **What is a full form of MITM attack?**
    a. Man in the middle Attack
    b. Memory input tracking Merge Attack
    c. Malicious in to Memory Attack
    d. Memory in trouble mode Attack
    e. Memory input output Malfunction Attack

Answer:- Man in the middle Attack

14. **What is a Ransomware?**
    a. Accessing information that was not intended for the specific user
    b. A malicious program impacts the availability of the data and demands ransom in return to release the data
    c. A software used to forward phishing mails
    d. A malicious program for gaining access to information for the sake of fun
    e. Any computer virus is a Ransomware

Answer:- A malicious program impacts the availability of the data and demands ransom in return to release the data

15. **Who is a Hacktivist?**
    a. A hacker having history of activism
    b. A activist who is computer literate
    c. A socially or politically motivated hacker

   d. A hacker having political background
   e. All of the above

Answer:- A socially or politically motivated hacker

16. **Who is a Cyber Warrior?**
   a. Hackers Promoting political or social beliefs
   b. Hackers who work for thrill of the Challenge
   c. All hackers are cyber warriors
   d. A hacker that works for specific government
   e. None of the above

Answer:- A hacker that works for specific government

17. **What is a Software Key logger?**
   a. A malicious program which encrypts the data
   b. A malicious program which counts the total number of characters and words a person types
   c. A malicious program which grabs the key strokes and also identifies the mouse activity
   d. A software used to block offensive words
   e. A pdf converter software

Answer:- A malicious program which grabs the key strokes and also identifies the mouse activity

18. **Software that displays advertising banners or pop-ups on your computer when you use an application**
   a. Malware
   b. Spyware
   c. Adware
   d. Ransomware
   e. Freeware

Answer:- Adware

19. **What are the objectives of Information Security Policy of ICD Security Policy?**
   a. Confidentiality, Integrity, Availability of all Information assets of Bank
   b. All Information is protected from Unauthorised Physical and Logical access whether by Staff,Contractors, Visitors or Outsiders
   c. User Awareness about legislation related to maintenance, protection, retention and withholding of information.
   d. Information is protected from Fraud, corruption or loss during input, processing, transmission and storage

e. All of the above

Answer:- All of the above

20. **Information Security policy under ICD Security Policy is not applicable to which among the following groups**
    a. Customers
    b. All Departments and Functions
    c. Overseas Branches
    d. All third party service providers
    e. All information Technology Systems Used

Answer:- Customers

21. **________ is a malware program that includes a back door for administrative control over the target computer?**
    a. Remote Access Trojan
    b. Virus
    c. Worm
    d. Spyware
    e. All of the above

Answer:- Remote Access Trojan

22. **Which of the below doesn't comes under Information security principles?**
    a. Authenticity
    b. Non-repudiation
    c. Authorization
    d. Accountability
    e. Media Handling

Answer:- Media Handling

23. **Which of the below is not a category of classification of Information based on the IS policy of ICD Security Policy of the bank?**
    a. Classified
    b. Confidential
    c. Internal
    d. Public
    e. Secret

Answer:- Classified

24. **A user wants to use a Freeware/software on the banks computer for any specific purpose. What is the best suggested procedure to install it?**
    a. Obtain prior approval from CTO and CISO for the usage of freeware software

   b. Connect the USB drive and install it on own
   c. Inform the Staff members in the branch and install
   d. Ask for prior approval of MD
   e. One time installation doesn't need permission

Answer:- Obtain prior approval from CTO and CISO for the usage of freeware software

25. **What is the objective of Business Continuity Plan (BCP)of Bank?**
    a. Least business interruption due to disaster
    b. Reduce damage caused by disaster
    c. Restoration of critical processes
    d. Identify & reduce risk
    e. All of the above

    Answer:- All of the above

26. **Which of the below mentioned points are governed by Information security policy of ICD Security Policy?**
    a. Use of Mobile Devices
    b. Computer Operations, Network & Communications
    c. Email Security
    d. Internet Usage & Access Policy
    e. All of the above

    Answer:- All of the above

27. **Information Security Committee doesn't include which of the following?**
    a. MD & CEO, EDs, CISO, CRO, CTO
    b. CGM-IT
    c. Chief Law Officer
    d. Branch Manager
    e. GM-TMFM

    Answer:- Branch Manager

28. **What are the characteristics of a strong password?**
    a. Long
    b. Long, random and unique
    c. Long, unique
    d. Long, random
    e. Any password is secured

    Answer:- Long, random and unique

29. **Which of the below is a responsibility of the end user?**
    a. Maitaining confidentiality of the login password

b. Using bank business assets for approved purpose only
c. Adhering to all information security policies
d. Promptly report security incidents to management
e. All of the above

Answer:- All of the above

30. IT controls are divided into 4 categories. Which of the below is not a IT control?

a. Preventive Controls
b. Report Controls
c. Recovery Controls
d. Directive Controls
e. Detective Controls

Answer:- Report Controls

31. What is a Zero Day Attack?

a. A hole in the system in the shape of a circle
b. An attack that happens on the last day of the month
c. A vulnerability in software that is unknown to the vendor
d. The attack that happens on the first day of application launch
e. Device Security

Answer:- A vulnerability in software that is unknown to the vendor

32. A QR code scanning app installed in your mobile phone is asking for permissions while installation. What permission you should give?

a. Access to your files/Folders
b. Access to location service
c. Access to camera only
d. Access to Microphone
e.
f. None of the above

Answer:- Access to camera only

33. A situation in which an unauthorized person can view another user's display or keyboard to learn their password or other confidential information is referred to as

a. Tailgating
b. Spear Phishing
c. Man-in-the-middle
d. Spoofing
e. Shoulder Surfing

Answer:- Shoulder Surfing

34. **Mr. Sam is a highly skilled individual who has gained access to server of an organization by exploiting vulnerability in the system, illegally for monetary benefit. He falls under**
    a. Black hat hacker
    b. White hat hacker
    c. Responsible Disclosure Program
    d. Incident Responder
    e. Grey hat hacker

    Answer:- Black hat hacker

35. **Identify the right web address of National Cyber Crime Reporting Portal?**
    a. https://www.cybercrime.gov.in/
    b. https://www.cybercomplain.gov.in/
    c. https://www.cybercrimereporting.gov.in/
    d. https://www.cybercrimeincident.gov.in/
    e. There is no such portal

    Answer:- https://www.cybercrime.gov.in/

36. **What is the toll free number to register a cyber crime?**
    a. 911
    b. 1930
    c. 15530
    d. 1503
    e. Any of the above.

    Answer:- 1930

37. **What is a supply chain attack ?**
    a. Sending indiscriminately unsolicited bulk messages
    b. Attack on Update mechanism of softwares/apps to distribute malware
    c. Attack by exploiting a vulnerability in a software that is
    d. unknown to the vendor/developer
    e. A cyber attack which happens on the last day of the month
    f. Attack in which the system files are locked

    Answer:- Attack on Update mechanism of softwares/apps to distribute malware

38. **Identify the statement which correctly represents the role of CISO during crisis:**
    a. To co-ordinate with respective departments via mail, telephone, SMS alerts for Cyber Crisis management plan Invocation
    b. The CISO leads the IT Security team and heads the mitigation and forensic investigation of the crisis

c. Depending on crisis, the CISO should identify and appoint leaders across affected business units

d. CISO shall report, communicate and coordinate with CERT-IN, IDRBT, and RBI during the crisis

e. All of the above

Answer:- All of the above

39. **In the computer networks, the encryption techniques are primarily used for improving the ________**

a. Security

b. Performance

c. Reliability

d. Longevity

e. All of the above

Answer:- Security

40. **What is the purpose of a Cyber Crisis Management Plan (CCMP)?**

a. To effectively respond to a crisis

b. To recover and restore the affected systems within the expected time duration

c. To minimize the business impact due to a crisis

d. To establish a response structure with representation from key stakeholders across the Bank

e. All of the above

Answer:- All of the above

41. **Who among the following is not a representative of the Cyber crisis management team (CCMT)?**

a. CISO

b. Network Admin

c. Public relations officer

d. MD & CEO

e. Compliance / Financial Risk Management

Answer:- MD & CEO

42. **Which of the following does NOT come under Social Engineering?**

a. Phishing

b. Tailgating

c. Pretexting

d. Spamming

e. All of the above

Answer:- Spamming

43. **What does the term "Malware" stand for?**
    a. Malfunctioning Software
    b. Malicious systems
    c. Malfunctioning Hardware
    d. Multiple softwares
    e. Malicious Software

Answer:- Malicious Software

44. **Social engineering is ______ ?**
    a. A cybersecurity principle that focuses on data confidentiality
    b. A method used to protect data from modification by unauthorized users
    c. A type of cyber-attack that manipulates human psychology to deceive individuals and gain unauthorized access.
    d. A software technique used to prevent unauthorized access to a system.
    e. None of the above

Answer:- A type of cyber-attack that manipulates human psychology to deceive individuals and gain unauthorized access.

45. **Which of these methods is used to check the validity of a message ?**
    a. Digital signature
    b. Message Digest
    c. Protocol
    d. Decryption
    e. All the above

Answer:- Message Digest

46. **Which of the following does not clone or replicate itself through infection?**
    a. Trojans
    b. Worms
    c. Rootkits
    d. Viruses
    e. None of the above

Answer:- Trojans

47. **Methods used for hiding information inside a picture ?**
    a. Image rendering
    b. Rootkits
    c. Steganography
    d. Bitmapping

e. All the above

Answer:- Steganography

48. Which of the following is not a security threat ?

a. Hackers
b. Spam
c. Virus
d. Trojan
e. Worm

Answer:- Spam

49. Network failure is primarily a __________ issue ?

a. Reliability
b. Performance
c. Security
d. All the above
e. None of the above

Answer:- Reliability

50. Encryption of text means ____ ?

a. Expanding the text
b. Compressing text
c. Hashing text
d. Scrambling it to preserve its security
e. All the above

Answer:- Scrambling it to preserve its security