**Topic- Cyber Security Awareness (Gyan Kasouti)**

**MTDT015**

1. **Which of the below is not a role and Responsibility of Group Chief Information Security Officer?**
    a. To oversee the overall cyber security risk management throughout the Bank and its group entities
    b. To act as an advisor to the top management of group entity for their cyber security related functions.
    c. To take part in the Technology Committee/IT Steering Committee/Risk Management Committee meetings whichever is applicable in the group entities as special permanent invitee
    d. To ensure group entities meet the minimum requirements with respect to group cyber security management
    e. All are role and Responsibility of Group Chief Information Security Officer

    **Answer:- All are role and Responsibility of Group Chief Information Security Officer**
2. **All types of phishing URLs/Emails received in Bank's official email ids to be reported to which email ID of CISO office?**
    a. phishing@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. **Which among the following method you will use to report a Cyber Fraud?**
    a. Report in local Cyber Crime police station
    b. Report in www.cybercrime.gov.in
    c. Dial 1930 and Report the incident
    d. Report to the Bank's Customer Care
    e. All of the above

    **Answer:- All of the above**
4. **What is Spear Phishing?**
    a. Phishing mail targeted to different people who are not related professionally
    b. A tool used to detect technical issues in a system
    c. A phishing mail targeted to employees of a specific organization
    d. A type of Denial of Service Attacks
    e. A Phishing attempt to a targeted employee

    **Answer:- A phishing mail targeted to employees of a specific organization**
5. **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**

6. **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**

7. **What is a Ransomware?**
   a. Accessing information that was not intended for the specific user
   b. A type of malicious software designed to block access to a computer system until a sum of money is paid
   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 type of malicious software designed to block access to a computer system until a sum of money is paid**

8. **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 with the intention of fulfilling a social or political agenda
   d. A hacker having political background
   e. All of the above

   **Answer:- A socially or politically motivated hacker with the intention of fulfilling a social or political agenda**

9. **Who is a Cyber Warriors?**
   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 governments to serve their military/economic objectives via Cyberspace
e. None of the above

**Answer:- A hacker that works for specific governments to serve their military/economic objectives via Cyberspace**

10. **Information 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**

11. **Sensitive Personal Information are Data elements which may pose heightened risks to the individual if disclosed or compromised. Which of the below is not considered a sensitive personal information?**
    a. PAN Card/Aadhar card
    b. Bank account information
    c. Passport
    d. Mobile Handset Make & Model
    e. Driver's license number

**Answer:- Mobile Handset Make & Model**

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

**Answer:- Classified**

13. **Which of the below mentioned points are governed by Information security policy?**
    a. Use of Mobile Devices issued to Bank staff & also the use of personal mobiles within Bank offices/ premises
    b. Computer Operations, Network & Communications
    c. Email Security
    d. Internet Usage & Access Policy
    e. All of the above

**Answer:- All of the above**

14. **Which of the following doesn't comes under employees responsibility in Cyber Security?**
    a. Not to install their personally owned software on Bank equipment.
    b. Only to use licensed software acquired by Bank
    c. Only softwares authorized by the bank should be installed in office systems
    d. Use of unlicensed software in Banks computer
    e. To ensure that bank provided electronic mail facility is not misused

    **Answer:- Use of unlicensed software in Banks computer**

15. **As per Banks policy, which of the below minimum credentials should be recorded in audit trail and activity logs maintenance?**
    a. User ID's
    b. Dates and times for logon and logoff
    c. Terminal identity or location if possible
    d. Only A & B
    e. All A,B & C

    **Answer:- All A,B & C**

16. **Which of the below statement(s) is/are true as per Banks ICD policy IC 04459 dt.28.11.2023 for Access Control ?**
    a. The Bank monitors system usage to ensure that the systems are used in a secure manner and only by authorised users
    b. The Bank ensures that there are strong access controls and monitoring procedures for powerful system utilities
    c. The Bank will provide mobile computing facilities to a restricted set of individuals based on business requirements.
    d. The Bank shall give access to electronic information including applications and databases, computing facilities and network services to all users
    e. Only A,B & C

    **Answer:- Only A,B & C**

17. **What are the benefits of the Business Continuity Plan?**
    a. Identify & Reduce Risk of any cyber incident
    b. It helps to carry business in the normal manner with least interruption
    c. It helps to restore critical processes within acceptable time scale
    d. It helps to reduce the damage caused by disasters and security failures to an acceptable level
    e. All of the above

**Answer:- All of the above**

18. **Which of the below type of hackers are hired by organizations to infiltrate their competitors and harm them?**
    a. Crackers
    b. Spy Hackers
    c. Spammers
    d. Adware spreaders
    e. All of the above

**Answer:- Spy Hackers**

19. **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**

20. **Bank shall assess and evaluate the Cyber Risk of Vendors. What is the objective of IT outsourcing policy of Bank?**
    a. Visualize the risk involved with vendor onboarding
    b. Annual Information/Cyber Security Risk Assessment to maintain the
    c. risk level
    d. Classify the vendor's based on criticality of risk assessment
    e. To assess the business dependency on the vendors
    f. All A, B & C

**Answer:- All A, B & C**

21. **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**

22. **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**

**23. 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**

**24. What are included in the information assets?**

a. Servers
b. Laptop/Desktops
c. Hardware Devices/Softwares
d. Customer Data/Transaction Data
e. All of the above

**Answer:- All of the above**

**25. 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**

**26. 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. All of the above
e. None of the above

**Answer:- Access to camera only**

27. **Which of the following could pose a threat to your identity and information?**
    a. Handing over your credit/debit card to a waiter in hotel
    b. Online purchase on a SSL website
    c. Throwing your old tax information in trash bin without destroying properly
    d. Shopping in the shopping mall
    e. Both A & C

    **Answer:- Both A & C**

28. **Which among the following can be Symptoms of a Virus/Worm/Trojans/Bot nets/Spyware attack/infection in a system?**
    a. Poor system performance
    b. Presence of suspicious files on system
    c. Connections to suspicious remote systems
    d. Computer reboots on its own
    e. All of the above

    **Answer:- All of the above**

29. **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 unknown to the vendor/developer
    d. A cyber attack which happens on the last day of the month
    e. Attack in which the system files are locked

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

30. **Who is an Insider Hacker ?**
    a. A hacker who does not possess technical expertise and relies on pre-developed tools to perform attack
    b. A hacker who breaks into system/network for entertainment
    c. An employee/Consultant who performs security exploits within firms system/network
    d. A Socially motivated hacker with intention of fulfilling social agenda
    e. None of the above

    **Answer:- An employee/Consultant who performs security exploits within firms system/network**

31. **Who is a White Hat hacker**
    a. Individuals who are hired by a company to break into their system/network to discover potential security Weaknesses

b. Malicious hacker who exploits security vulnerabilities for personal gain
c. A Hacker who breaks into system/network without the owners consent/knowledge and publicly discloses security flaws
d. Hackers who work for profit and are hired to engage in electronic corporate espionage
e. Hackers who are hired by corporations to infiltrate their competitors systems/network

**Answer:- Individuals who are hired by a company to break into their system/network to discover potential security Weaknesses**

**32. Who is a Black Hat hacker**

a. Individuals who are hired by a company to break into their system/network to discover potential security Weaknesses
b. Malicious hacker who exploits security vulnerabilities for personal gain
c. A Hacker who breaks into system/network without the owners consent/knowledge and publicly discloses security flaws
d. Hackers who work for profit and are hired to engage in electronic corporate espionage
e. Hackers who are hired by corporations to infiltrate their competitors systems/network

**Answer:- Malicious hacker who exploits security vulnerabilities for personal gain**

**33. What is Spoofing ?**

a. Sending indiscriminately unsolicited bulk messages
b. Attack on Update mechanism of softwares/apps to distribute malware
c. It is a new kind of cyber attack started this year
d. Attack in which the system files are locked
e. Attack in which the hacker impersonates as another user by falsifying data to gain advantage

**Answer:- Attack in which the hacker impersonates as another user by falsifying data to gain advantage**

**34. What precautions are advisable for safe use of bank's e-mail ID?**

a. Use bank's e-mail ID only for official purpose
b. Don't Click on link in unknown E-mail
c. Don’t download attachment from unknown e-mails
d. Always use a strong password
e. All of the above

**Answer:- All of the above**

35. **What is the best prescribed practice to report a phishing email to CISO department among the given option?**
    a. Send a screen shot of the phishing email
    b. Forward the entire email
    c. Write a new email mentioning all the details
    d. click on the link and copy the URL & send
    e. Any of the above

    **Answer:- Send a screen shot of the phishing email**

36. **Information ,Cyber & Digital Payment Security policy provides guidelines for which among the following ?**
    a. To ensure Confidentiality, Integrity, Availability of all Information assets of Bank
    b. To ensure that all Information is protected from Unauthorised Physical and Logical access whether by Staff, Contractors, Visitors or Outsiders
    c. To ensure user Awareness about legislation related to maintenance, protection, retention and withholding of information.
    d. To ensure Information is protected from Fraud, corruption or loss during input, processing, transmission and storage
    e. All of the above

    **Answer:- All of the above**

37. **Which of the below mentioned points are governed by Information ,Cyber & Digital Payment 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**

38. **What are the main responsibilities of Information Security Committee (ISC)?**
    a. Review Information Security Policy
    b. Initiate Information Security Awareness Programs
    c. Decide on future security solutions to be implemented in Bank
    d. Approval security policy
    e. All of the above

    **Answer:- All of the above**

39. **Mr. Shyam is a highly skilled individual who has taken written permission from organization to identify vulnerabilities and gained access to a critical system of the organization. He falls under**
    a. Black hat hacker
    b. White hat hacker
    c. Grey hat hacker
    d. Incident Responder
    e. Red hat Hacker

    **Answer:- White hat hacker**
40. **Consider a situation when you are unable to log in to the server due to system compromise and change of password by the attacker. The probable root cause may NOT be:**
    a. Ransomware attack
    b. Phishing attack
    c. Malware infection
    d. DDOS attack
    e. Man-in-the-middle attack

    **Answer:- DDOS attack**
41. **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**
42. **To report suspected fraud communications (Call, SMS, WhatsApp) Department of Telecommunications, Ministry of Communications, GoI has launched a portal in the sancharsaathi.gov.in website. What is the name of the portal ?**
    a. Aakshu
    b. Chakshu
    c. Aankhee
    d. Sakshi
    e. None of the above

    **Answer:- Chakshu**
43. **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**

**44. What is the objective of Cyber Fraud Prevention Chapter under ICD policy of Bank?**

a. Prevent Cyber-attacks
b. Reduce
c. vulnerabilities in critical infrastructure
d. Minimize damage and recovery in reasonable time
e. Reporting to Monitoring authorities
f. All of the above

**Answer:- All of the above**

**45. Identify the fraud which is not considered as a Cyber Fraud.**

a. Social Engineering Scams
b. Hacking of Devices
c. Identity Theft
d. Selling of Old Mobile Phones
e. Selling of unlicensed/copyright products

**Answer:- Selling of Old Mobile Phones**

**46. Bank has formulated a Fraud review councils by the fraud risk management group within various business groups in the bank. Who are the members of the council?**

a. Head of the business
b. Head of the fraud risk management department
c. Head of operations supporting that particular business function
d. Head of information technology supporting that business function
e. All of the above

**Answer:- All of the above**

**47. Bank will ensure the security, privacy and confidentiality of any sensitive personal data or information that it collects, receives, possess, stores or deals with. Which of the following is a method via which Bank collects personal information?**

a. Open an account or perform online transactions
b. For the Government purpose, like tax collection
c. Via cookies when the customer visits the bank's web site
d. Apply for a loan or use his/her credit or debit card

e. All of the above

**Answer:- All of the above**

**48. Which of the below statement(s) is/are true as per Banks ICD policy?**

a. Bank shall obtain consent in letter or Fax or email from the customers/end users who provides personal information and informs them regarding the purpose of usage before collecting the information

b. Bank shall ensure that the provider of the personal information has the knowledge of intended recipients of the information & Bank should not keep any sensitive personal data of information for longer than required

c. Bank shall provide an option to the provider of the information to not to provide the data or information sought to be collected also provide an option to withdraw its consent given earlier to the Bank

d. Bank shall ensure that the provider of the information can review the information anytime to ensure that it is correct & information can be corrected /amended whenever required

e. All of the above

**Answer:- All of the above**

**49. What is a software patch ?**

a. Optional Fix

b. Emergency Fix

c. Daily or routine Fix

d. All of the above

e. None of the above.

**Answer:- Emergency Fix**

**50. Which is not a 2 factor authentication methodology?**

a. One Time Password

b. Biometric Authentication

c. Hardware tokens

d. Getting Green PIN through post

e. All of the above

**Answer:- Getting Green PIN through post**