Que.1 : Cyber Security policy of the bank protects:

a) Confidentiality of data
b) Integrity of data
c) Availability of data
d) Originality of data
e) All A,B,C

Ans.: All A,B,C

Que.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

Ans.: antiphishing.ciso@unionbankofindia.bank

Que.3 : Which 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

Ans.: Confidentiality

Que.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

Ans.: A phishing mail targeted to employees of a specific organization

Que.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

Ans.: Phishing attack through an SMS with a malicious link

Que.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

Ans.: Man in the middle Attack

Que.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

Ans.: A type of malicious software designed to block access to a computer system until a sum of money is paid

Que.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

Ans.: A socially or politically motivated hacker with the intention of fulfilling a social or political agenda

Que.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

Ans.: A hacker that works for specific governments to serve their military/economic objectives via Cyberspace

Que.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

Ans.: Customers

Que.11 : Which of the below is not a category of classification of Information based on the IS policy of the bank?

a) Classified
b) Confidential
c) Internal
d) Public
e) Secret

Ans.: Classified

Que.12 : Which of the below mentioned points are governed by Information security policy?

a) Use of Mobile Devices issued by the Bank
b) Computer Operations, Network & Communications of Bank
c) Email Security
d) Internet Usage & Access Policy
e) All of the above

Ans.: All of the above

Que.13 : The objective of the Cyber Security (CS) Policy is:

a) To achieve Cyber Resiliency by the implemented IT infrastructure
b) For RBI & SEBI compliance only
c) Timely response to potential Cyber attacks
d) To Digitize banks products

e) Both A & C

Ans.: Both A & C

Que.14 : What is the correct order of different Stages for Cyber Security Strategies Used in Bank ?

a) Identify, Protect, Detect, Respond, Recover, Learn
b) Identify, Detect, Protect, Respond, Recover, Learn
c) Identify, Detect, Protect, Recover, Respond, Learn
d) Identify, Protect, Detect, Recover, Respond, Learn
e) Identify, Detect, Protect, Respond, Learn, Recover

Ans.: Identify, Protect, Detect, Respond, Recover, Learn

Que.15 : What are the key objectives of multi-factor authentication?

a) Protect the Confidentiality
b) Avoid Cyber Attack
c) Enhance confidence in digital payment
d) Only a&b
e) All a,b&c

Ans.: All a,b&c

Que.16 : 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

Ans.: Spy Hackers

Que.17 : Who among the following is not a member in the Cyber Crisis Management Team

a) CISO
b) CTO
c) CGM - HR Operations
d) CRO
e) CFO

Ans.: CFO

Que.18 : In order to secure banks network what controls have not been implemented for Removable Media in our cyber security policy?

a) scan removable media using up-to-date anti-virus
b) Centralised policies shall be implemented via Active directory/Endpoint Management system to whitelist/blacklist/restrict the use of removable media
c) Registration and management of personally owned devices
d) Seizing of removable media for forensic examination, if required
e) Delete all data from the removable device as soon as it is connected to the bank's computer

Ans.: Delete all data from the removable device as soon as it is connected to the bank's computer

Que.19 : 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

Ans.: A vulnerability in software that is unknown to the vendor

Que.20 : 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

Ans.: Access to camera only

Que.21 : Which if the below is/are not a evidence handling guideline during a cyber crisis?

a) Remove the network cable if plugged in
b) If the computer is on do not turn it off
c) Format the Entire System Completely
d) If the computer is off do not turn it on
e) Do not connect infected systems to any network

Ans.: Format the Entire System Completely

Que.22 : What is a supply chain attack ?

a) Sending indiscriminately unsolicited bulk messages
b) Attack on Update mechanism of software's/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

Ans.: Attack on Update mechanism of software's/apps to distribute malware

Que.23 : Who is a 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

Ans.: An employee/Consultant who performs security exploits within firms system/network

Que.24 : What is Spoofing ?

a) Sending indiscriminately unsolicited bulk messages
b) Attack on Update mechanism of software's/apps to distribute malware
c) It is a new kind of cyber attack started after Covid
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

Ans.: Attack in which the hacker impersonates as another user by falsifying data to gain advantage

Que.25 : 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

Ans.: White hat hacker

Que.26 : 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

Ans.: DDOS attack

Que.27 : 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

Ans.: Black hat hacker

Que.28 : When Personally Identifiable Information (PII) is transmitted across networks, there must be adequate controls over:

a) Consent to data transfer
b) Privacy protection
c) Change management
d) Encryption devices
e) All of the above

Ans.: Privacy protection

Que.29 : What is a Red Team?

a) trained professionals authorized to emulate a potential adversary's attack on an enterprise's security
b) A team of security professionals with hackers certificate
c) A team of cyber security experts wearing red t-shirts
d) Professionals from Red Security company
e) None of the above.

Ans.: trained professionals authorized to emulate a potential adversary's attack on an enterprise's security

Que.30 : _____ 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

Ans.: Remote Access Trojan