COMPUTER SECURITY

SAMPLE QUESTIONS

SECTION A

1. The most common Internet investment fraud is known as what?
a. The Nigerian fraud
b. The Manhattan fraud
c. The pump and dump
d. The bait and switch

2. What is the most likely problem with unsolicited investment advice?
a. You might not earn as much as claimed.
b. The advice might not be truly unbiased.
c. The advice might not be from a legitimate firm.
d. You might lose money.

3. Artificially inflating a stock in order to sell it at a higher value is referred to as what?
a. Bait and switch
b. The Nigerian fraud
c. Pump and dump
d. The Wall Street fraud

4. What is the top rule for avoiding Internet fraud?
A. If it seems too good to be true, it probably is.
B. Never use your bank account numbers.
C. Only work with people who have verifiable email addresses.
D. Don’t invest in foreign deals.

5. Submitting a fake but very high bid to deter other bidders is referred to as what?
a. Bid siphoning
b. Bid shielding
c. Shill bidding
d. Ghost bidding

6. Identity theft is most often attempted in order to accomplish what goal?
a. To make illicit purchases
b. To discredit the victim
c. To avoid criminal prosecution
d. To invade privacy

7. According to the U.S. Department of Justice, identity theft is generally motivated by what?
a. Malicious intent
b. Personal hostility towards the victim
c. Economic gain
d. Thrill seeking

8. What can you do on your local computer to protect your privacy?
a. Install a virus scanner.
b. Install a firewall.
c. Set your browser's security settings.
d. Set your computer's filter settings.

9. A company needs to digitally sign all of the data sent to its customers. What should the administrator use to digitally sing the data?
a. Asymmetric Keys
b. Standard Keys
c. Symmetric Keys
d. Quantitative Keys

10 If an intrusion detection system wanted to only monitor web traffic, what would the rules filter on?
a. IP Address
b. Port
c. User Name
d. Destination Name

11. What security technique can be used to identify malicious HTTPS (Secure Hyper Text Transport Protocol) tunnels?
a. Detection inspection
b. Context inspection
c. Plain HTTP inspection
d. SSL inspection

12. The triad of computing security includes which of the following?

a. Detection, response, and monitoring
b. Vulnerability assessment, detection, and monitoring
c. Vulnerability assessment, intrusion response, and investigation
d. Vulnerability assessment, intrusion response, and monitoring

13. The top rule for chat room safety is what?
A. Make certain you have antivirus software installed.
B. Never use your real name or any real personally identifying characteristics.
C. Only use chat rooms that encrypt transmissions.
D. Use chat rooms that are sponsored by well-known websites or companies.

14. If a suspect computer is running Windows 2000, which of the following can you perform safely?
a. Browsing open applications
b. Disconnecting power
c. Either of the above
d. None of the above

15.In the broadest sense security can be defined as the protection of assets. There are three main aspects to security:

(i) Prevention
(ii) Detection
(iii) Reaction

Do you agree to the above?
a. Yes b. No C. Not sure

16. ……..is the prevention of unauthorized disclosure of information/

a. Confidentiality b .Privacy c. Integrity d. Authentication

17. When a computer system has to verify a user's identity, there are two basic questions that have to be asked and answered appropriately. The first is:

a. Where are you?

b. Who are you?

c. How do you do?

d. What is your address?

18. ……is a process used to ensure that all passwords in a system are unique.

A .Cyber stalking

b. Phishing

c. Password salting

d. Password management

19. Which of the following is not a cardinal computer security element?

a. Availability
b. Utility
c. Integrity
d. Phishing

20. Basically there are ---------- types of computer interrupts.

a.3
b.5
c.7
d.4

SECTION B

1. (a) You receive an email from your bank telling you there is a problem with your account. The email provides instructions and a link so you can log in to your account and fix the problem. What should you do?

(b) The mouse on your computer screen starts to move around on its own and click on things on your desktop. What do you do? Select all that apply

a) Call your co-workers over so they can see

b) Disconnect your computer from the network

c) Unplug your mouse

d) Tell your supervisor

e) Turn your computer off

f) Run anti-virus

g) All of the above

2. The following are seven features that may be provided by a security system. For each write a sentence describing what is meant by the feature:

i. Confidentiality
ii. Integrity
iii. Availability
iv. Non-repudiation
v. Authentication
vi. Access control
vii. Accountability.

b) A University department has a file called exam marks which contains a list of examination marks indexed by student names in alphabetical order. A student manages to access the exam marks file. The student cannot read the file since it is encrypted. However they can work out the position of their own mark making use of the fact that the students are listed in alphabetical order. The student swaps their mark with that of the student who is always 'top of the class'. Explain which of the security features listed in part a) have been breached.

3. Two different offices on campus are working to straighten out an error in an employee's bank account due to a direct deposit mistake. Office #1 emails the correct account and deposit information to office #2, which promptly fixes the problem. The employee confirms with the bank that everything has, indeed, been straightened out. What's wrong here?

4. (a) Write short notes on each of the following topics.
(i) Web application penetration testing

(ii) ISO 27001 Information Security Management System

(b) In what way is the encryption scheme known as DES considered weak?