

1) Phishing is when someone sends an e-mail pretending to be a legitimate company and asking for confidential data, such as account numbers.

- a. True
- b. False

Answer: a

Diff: 1

Type: TF

Page Reference: 369

Topic: Q3

Skill: RECALL

2) Spoofing is a technique for intercepting computer communications.

- a. True
- b. False

Answer: b

Diff: 1

Type: TF

Page Reference: 369

Topic: Q3

Skill: RECALL

3) People who intentionally gain unauthorized access to computer systems are called hackers.

- a. True
- b. False

Answer: a

Diff: 1

Type: TF

Page Reference: 370

Topic: Q3

Skill: RECALL

4) Drive-by sniffers take computers with wireless connections through an area and search for unprotected wireless networks.

- a. True
- b. False

Answer: a

Diff: 1

Type: TF

Page Reference: 369

Topic: Q3

Skill: RECALL

5) Denial of service always occurs because of malicious attacks on the system.

a. True

b. False

Answer: b

Diff: 2

Type: TF

Page Reference: 370

Topic: Q3

Skill: RECALL

6) When a hacker floods a web server with millions of bogus service requests so that it cannot service legitimate requests, this is called a denial of service attack.

a. True

b. False

Answer: a

Diff: 2

Type: TF

Page Reference: 370

Topic: Q3

Skill: RECALL

7) Any action, device, procedure, technique, or other measure that reduces a system's vulnerability to a threat is a safeguard.

a. True

b. False

Answer: a

Diff: 1

Type: TF

Page Reference: 371

Topic: Q3

Skill: RECALL

8) Despite warnings, users have a tendency to write their passwords on sticky notes next to the computer.

- a. True
- b. False

Answer: a

Diff: 1

Type: TF

Page Reference: 372

Topic: Q4

Skill: RECALL

9) Smart cards are convenient and easy to use since they don't require any PIN numbers for authentication.

- a. True
- b. False

Answer: b

Diff: 2

Type: TF

Page Reference: 372

Topic: Q4

Skill: RECALL

10) A retinal scan would be considered a biometric authentication technique.

- a. True
- b. False

Answer: a

Diff: 2

Type: TF

Page Reference: 372

Topic: Q4

Skill: RECALL

11) Biometric authentication has been around for some time, and because of weaknesses is not likely to see much usage in the future.

- a. True
- b. False

Answer: b

Diff: 2

Type: TF

Page Reference: 372

Topic: Q4

Skill: RECALL

12) Technical safeguards involve the hardware and software components of an information system.

- a. True
- b. False

Answer: a

Diff: 2

Type: TF

Page Reference: 371

Topic: Q4

Skill: RECALL

13) Malware protection is an example of a technical safeguard.

- a. True
- b. False

Answer: a

Diff: 2

Type: TF

Page Reference: 371

Topic: Q4

Skill: RECALL

14) Encryption is one of several technical safeguards.

- a. True
- b. False

Answer: a

Diff: 2

Type: TF

Page Reference: 371

Topic: Q4

Skill: RECALL

15) Malware is used in denial of service attacks.

- a. True
- b. False

Answer: b

Diff: 2

Type: TF

Page Reference: 371

Topic: Q3

Skill: RECALL

16) Most anti-malware programs check e-mail attachments for malware code.

- a. True
- b. False

Answer: a

Diff: 2

Type: TF

Page Reference: 374

Topic: Q4

Skill: RECALL

17) Data safeguards are designed to protect computer networks.

- a. True
- b. False

Answer: b

Diff: 2

Type: TF

Page Reference: 374

Topic: Q5

Skill: RECALL

18) To protect against lost or sabotaged encryption keys, a trusted party should keep a copy of the key.

- a. True
- b. False

Answer: a

Diff: 2

Type: TF

Page Reference: 374

Topic: Q5

Skill: RECALL

19) Even if a potential new hire will not have access to sensitive data and systems, they should be extensively screened for security purposes.

- a. True
- b. False

Answer: a

Diff: 2

Type: TF

Page Reference: 376

Topic: Q6

Skill: RECALL

20) Care must be taken when terminating employees because they may take harmful and malicious actions.

- a. True
- b. False

Answer: a

Diff: 1

Type: TF

Page Reference: 376

Topic: Q6

Skill: RECALL

21) Hardened web sites use special versions of the operating systems and functions that are not required by the application.

- a. True

b. False

Answer: a

Diff: 3

Type: TF

Page Reference: 378

Topic: Q6

Skill: RECALL

22) Help desks have not been the source of many security problems in the past.

a. True

b. False

Answer: b

Diff: 2

Type: TF

Page Reference: 380

Topic: Q6

Skill: RECALL

23) If you ever receive notification that your password has been reset when you did not request a reset, immediately contact your IS department.

a. True

b. False

Answer: a

Diff: 1

Type: TF

Page Reference: 380

Topic: Q6

Skill: RECALL

24) The best safeguard against a natural disaster is to have a safe location.

a. True

b. False

Answer: a

Diff: 2

Type: TF

Page Reference: 383

Topic: Q7

Skill: RECALL

25) Following a disaster, hot sites provide office space, but customers themselves must come and provide and install the equipment needed to continue operations.

- a. True
- b. False

Answer: b

Diff: 3

Type: TF

Page Reference: 383

Topic: Q7

Skill: RECALL

26) Viruses and worms don't spread very quickly so it is not essential to move cautiously when one is discovered by someone in your organization.

- a. True
- b. False

Answer: b

Diff: 1

Type: TF

Page Reference: 384

Topic: Q8

Skill: RECALL

27) Backup and recovery, passwords, and encryption are human safeguards.

- a. True
- b. False

Answer: b

Diff: 2

Type: TF

Page Reference: 371

Topic: Q3

Skill: RECALL

28) Bloggers have not yet had much of an impact on the main stream media.

- a. True
- b. False

Answer: b

Diff: 2

Type: TF

Page Reference: 391

Topic: Q6

Skill: RECALL

29) About ninety percent of all viruses are spread via

- a. spreadsheets.
- b. AOL.
- c. technology.
- d. network worms.
- e. email.

Answer: e

Diff: 1

Type: MC

Page Reference: 373

Topic: Q4

Skill: RECALL

30) Since most organizations are protected by a(n) _____, it is not surprising that most viruses spread via e-mail.

- a. data dictionary
- b. antivirus program
- c. biometric authentication device
- d. firewall
- e. white-hat hacker

Answer: d

Diff: 3

Type: MC

Page Reference: 374

Topic: Q4

Skill: RECALL

31) Be sure and purchase your antispyware program from a(n) _____ vendor, because some free programs in the past were actually malware programs in disguise.

- a. reasonable
- b. reputable
- c. entrepreneurial
- d. inexpensive
- e. illegitimate

Answer: b

Diff: 2

Type: MC

Page Reference: 373

Topic: Q4

Skill: RECALL

32) Users should scan their computers with anti-malware programs at least

- a. once a year.
- b. biannually.
- c. once a week.
- d. daily.
- e. once a month.

Answer: c

Diff: 2

Type: MC

Page Reference: 373

Topic: Q4

Skill: RECALL

33) _____, which are the patterns that exist in malware code, should be downloaded and updated frequently.

- a. Software updates
- b. Service packs
- c. Malware patterns

- d. Network patches
- e. Malware definitions

Answer: e

Diff: 2

Type: MC

Page Reference: 373

Topic: Q4

Skill: RECALL

34) It is possible for some malware to install itself on your computer by you doing nothing more than opening a(n)

- a. web page.
- b. file.
- c. e-mail
- d. computer.
- e. account.

Answer: a

Diff: 2

Type: MC

Page Reference: 374

Topic: Q4

Skill: RECALL

35) Organizations should protect sensitive data by storing it in _____ form.

- a. compressed
- b. secure
- c. digital
- d. encrypted
- e. standardized

Answer: d

Diff: 2

Type: MC

Page Reference: 374

Topic: Q5

Skill: RECALL

36) Because encryption keys can be lost or destroyed, a copy of the key should be stored with a trusted third party called a(n)

- a. key account.
- b. white-hat hacker.
- c. key escrow.
- d. authentication certifier.
- e. control account.

Answer: c

Diff: 3

Type: MC

Page Reference: 374

Topic: Q5

Skill: RECALL

37) The purpose of a(n) _____ is to protect databases and other organizational data.

- a. data warehouse
- b. data security group
- c. operations group
- d. data safeguard
- e. steering committee

Answer: d

Diff: 2

Type: MC

Page Reference: 374

Topic: Q5

Skill: RECALL

38) Organizations should store at least some of the _____ of the database contents off the premises, possibly in a remote location.

- a. backups
- b. company information

- c. malware definitions
- d. smaller parts

Answer: a

Diff: 2

Type: MC

Page Reference: 375

Topic: Q5

Skill: RECALL

39) _____ to (for) the physical computers that run the DBMS and all devices that store database data should be carefully controlled.

- a. References
- b. Access
- c. Design plans
- d. Connections
- e. Documentation

Answer: b

Diff: 2

Type: MC

Page Reference: 375

Topic: Q5

Skill: RECALL

40) _____ safeguards involve the people and procedure components of information systems.

- a. Human
- b. Data
- c. Technical
- d. Malware
- e. Firewall

Answer: a

Diff: 2

Type: MC

Page Reference: 375

Topic: Q6

Skill: RECALL

41) In order to prioritize their activities and protect an organization from possible risk and loss, security personnel must document the position _____ of all employees.

- a. riskiness
- b. data access
- c. controls
- d. level
- e. sensitivity

Answer: e

Diff: 3

Type: MC

Page Reference: 375

Topic: Q6

Skill: RECALL

42) _____ considerations should be part of the hiring process.

- a. Weight
- b. Position
- c. Gender
- d. Age
- e. Security

Answer: e

Diff: 1

Type: MC

Page Reference: 376

Topic: Q6

Skill: RECALL

43) A company should clearly define the security _____ for each position.

- a. accounts
- b. levels

- c. responsibilities
- d. backups
- e. safeguards

Answer: c

Diff: 2

Type: MC

Page Reference: 376

Topic: Q6

Skill: RECALL

44) When an employee is terminated, system administrators should receive advance notice so they can

- a. plan for security changes.
- b. get the employees computer.
- c. remove accounts and passwords.
- d. fight over the person's office.
- e. plan a termination party.

Answer: c

Diff: 2

Type: MC

Page Reference: 377

Topic: Q6

Skill: RECALL

45) The best way to safeguard a web site from public users is to _____ the web site against an attack.

- a. secure
- b. prepare
- c. defend
- d. harden
- e. update

Answer: d

Diff: 3

Type: MC

Page Reference: 378

Topic: Q6

Skill: RECALL

46) Some of the biggest security threats are from _____ employees.

- a. disinterested
- b. disgruntled
- c. self-motivated
- d. happy
- e. contrarian

Answer: b

Diff: 1

Type: MC

Page Reference: 374

Topic: Q5

Skill: RECALL

47) The existence of _____ user accounts is a serious security threat.

- a. unused
- b. network
- c. meta
- d. employee
- e. modified

Answer: a

Diff: 2

Type: MC

Page Reference: 378

Topic: Q6

Skill: RECALL

48) _____ are the primary means of authentication.

- a. Encrypted keys
- b. Network administrators

- c. Passwords
- d. Single sign-on
- e. Facial scans

Answer: c

Diff: 1

Type: MC

Page Reference: 374

Topic: Q5

Skill: RECALL

49) Because they kept giving out passwords to users who claimed to have forgotten them, _____ were a serious security risk in the organization.

- a. interns
- b. help desks
- c. data administrators
- d. executives
- e. developers

Answer: b

Diff: 2

Type: MC

Page Reference: 380

Topic: Q6

Skill: RECALL

50) Firewalls produce _____ of their activities, which include lists of all dropped packets, and attempts to gain unauthorized access.

- a. programs
- b. logs
- c. graphics
- d. calls
- e. accounts

Answer: b

Diff: 3

Type: MC

Page Reference: 381

Topic: Q6

Skill: RECALL

51) Computing infrastructure should be located in _____ buildings designed to house expensive and critical equipment.

- a. central
- b. air-conditioned
- c. high-tech
- d. fire-resistant
- e. easily accessible

Answer: d

Diff: 2

Type: MC

Page Reference: 383

Topic: Q7

Skill: RECALL

52) A _____ is a remote processing centre run by a commercial disaster-recovery service that provides all the equipment needed to continue operations after a disaster.

- a. web farm
- b. development site
- c. cold site
- d. hot site
- e. server farm

Answer: d

Diff: 2

Type: MC

Page Reference: 383

Topic: Q7

Skill: RECALL

53) When an employee notices a virus on his machine, the _____ plan should specify what to do.

- a. antivirus
- b. security
- c. technology
- d. company
- e. incident response

Answer: e

Diff: 3

Type: MC

Page Reference: 384

Topic: Q7

Skill: RECALL

54) A(n) _____ is someone who pretends to be a legitimate company and sends e-mail requesting confidential data.

- a. hacker
- b. phisher
- c. spoofer
- d. hawker
- e. employee

Answer: b

Diff: 2

Type: MC

Page Reference: 369

Topic: Q3

Skill: RECALL

55) _____ is a technique for intercepting computer communications.

- a. Spoofing
- b. Hacking
- c. Pretexting
- d. Phishing
- e. Sniffing

Answer: e

Diff: 3

Type: MC

Page Reference: 369

Topic: Q3

Skill: RECALL

56) In order to intercept communications on _____ networks, drive-by sniffers simply drive or walk around with computers with wireless connections.

- a. commercial
- b. LAN
- c. wireless
- d. ISP
- e. WAN

Answer: c

Diff: 3

Type: MC

Page Reference: 369

Topic: Q3

Skill: RECALL

57) _____ is one of the fastest-growing crimes in Canada because it is relatively easy to do.

- a. phishing
- b. Hacking
- c. Spoofing
- d. PIPEDA
- e. Identity theft

Answer: e

Diff: 2

Type: MC

Page Reference: 366

Topic: Q1

Skill: RECALL

58) A hacker can launch a denial of service attack against a web server by _____ it with millions of bogus service requests.

- a. programming
- b. flooding
- c. denying
- d. hacking
- e. probing

Answer: b

Diff: 2

Type: MC

Page Reference: 370

Topic: Q3

Skill: RECALL

59) Passwords have weaknesses because users often choose simple passwords, which _____ systems can easily guess.

- a. security
- b. intrusion
- c. antivirus
- d. malware
- e. biometric

Answer: b

Diff: 3

Type: MC

Page Reference: 372

Topic: Q4

Skill: RECALL

60) A(n) _____ card has a microchip on it that is loaded with identifying data.

- a. smart
- b. debit
- c. credit

- d. ATM
- e. identity

Answer: a

Diff: 3

Type: MC

Page Reference: 372

Topic: Q4

Skill: RECALL

61) Users often resist biometric identification because they feel it is

- a. expensive.
- b. ineffective.
- c. too technical.
- d. invasive.
- e. hard to use.

Answer: d

Diff: 2

Type: MC

Page Reference: 372

Topic: Q4

Skill: RECALL

62) The web site _____ lists simple things to do to lower your risk of identity theft.

- a. www.wordpress.com
- b. www.google.ca
- c. www.safecanada.com
- d. www.priv.gc.ca
- e. www.equifax.com

Answer: c

Diff: 2

Type: MC

Page Reference: 367

Topic: Q2

Skill: RECALL

63) PIPEDA stands for

- a. Personal Information Protection and Electronic Disclosure Act.
- b. Personal Information Protection and Effective Disclosures Act.
- c. Personal Information Protection and Electronic Disclosures Act.
- d. Personal Information Protection and Electronic Documents Act.
- e. Personal Information Protection and Electronic Disclosure Actions.

Answer: d

Diff: 2

Type: MC

Page Reference: 369

Topic: Q3

Skill: RECALL

64) PIPEDA gives individuals the right to know why an organization is _____ their personal information.

- a. collecting and disclosing
- b. collecting and changing
- c. collecting, using or disclosing
- d. changing
- e. using and disclosing

Answer: c

Diff: 3

Type: MC

Page Reference: 369

Topic: Q3

Skill: RECALL

65) According to PIPEDA every organization needs to identify anyone in the organization who is responsible for _____ personal information.

- a. using
- b. safeguarding

- c. disclosing
- d. collecting
- e. maintaining

Answer: b

Diff: 3

Type: MC

Page Reference: 369

Topic: Q3

Skill: APPLIED

66) The popularity and efficacy of search engines like Google have created a source of

- a. entertainment.
- b. inadvertent information disclosure.
- c. phishing.
- d. pretexting.
- e. sniffing.

Answer: b

Diff: 2

Type: MC

Page Reference: 369

Topic: Q3

Skill: RECALL

67) If you suspect an organization has inappropriately disclosed your personal information to a 3rd party, you can lodge a complaint with

- a. Industry Canada
- b. RCMP
- c. the local police.
- d. Revenue Canada.
- e. Office of the Privacy Commissioner of Canada.

Answer: e

Diff: 2

Type: MC

Page Reference: 367

Topic: Q2

Skill: RECALL

68) Security policy establishment is the responsibility of

- a. middle managers.
- b. the CEO.
- c. corporate lawyers.
- d. senior management.
- e. the IT department.

Answer: d

Diff: 2

Type: MC

Page Reference: 371

Topic: Q3

Skill: RECALL

69) Adware is _____ than spyware.

- a. more serious
- b. less annoying
- c. more malicious
- d. more benign
- e. harder to get rid of

Answer: d

Diff: 3

Type: MC

Page Reference: 373

Topic: Q4

Skill: RECALL

70) After installing anti-virus and antispyware, what is the best way to avoid malware?

- a. Encrypt your work
- b. Give your friend your passwords.

- c. Shut the computer down at the end of the day.
- d. Open all email by double clicking.
- e. Don't open email attachments from unknown sources.

Answer: e

Diff: 3

Type: MC

Page Reference: 373

Topic: Q4

Skill: APPLIED

71) _____ is an organization-wide function that is in charge of developing data policies and enforcing data standards.

- a. Data contents protection
- b. Data safeguarding
- c. Data integrity
- d. Data administration
- e. Data rights administration

Answer: d

Diff: 2

Type: MC

Page Reference: 374

Topic: Q5

Skill: RECALL

72) User accounts should be given (the) _____ to perform their jobs

- a. least possible privileges needed
- b. most possible privileges needed
- c. administrator privileges
- d. user privileges
- e. company standard privileges

Answer: a

Diff: 2

Type: MC

Page Reference: 375

Topic: Q6

Skill: RECALL

73) Enforcement consists of _____ interdependent factors.

- a. 4
- b. 2
- c. 5
- d. 3
- e. 6

Answer: d

Diff: 2

Type: MC

Page Reference: 378

Topic: Q6

Skill: RECALL

74) Hardening is actually a(n) _____ safeguard.

- a. technical
- b. security
- c. data
- d. human
- e. accountability

Answer: a

Diff: 3

Type: MC

Page Reference: 378

Topic: Q6

Skill: RECALL

75) A company establishes data rights and responsibilities and educates employees on how to backup and recover the database. But, The company still needs to address the _____ safeguards.

- a. inadvertent

- b. security
- c. human
- d. data
- e. technical

Answer: e

Diff: 3

Type: MC

Page Reference: 371

Topic: Q3

Skill: APPLIED

76) A security incident reporting plan should _____ all incident reports.

- a. centralize
- b. generalize
- c. standardize
- d. decentralize
- e. prioritize

Answer: a

Diff: 2

Type: MC

Page Reference: 384

Topic: Q8

Skill: RECALL

77) When an incident is reported, _____ is (are) of the essence.

- a. the response
- b. preparation
- c. speed
- d. a systematic approach
- e. actions

Answer: c

Diff: 2

Type: MC

Page Reference: 384

Topic: Q8

Skill: RECALL

78) The sources of security problems are human error, malicious activity, and disasters.

Diff: 1

Type: FIB

Page Reference: 368

Topic: Q3

Skill: RECALL

79) Pretexting is the same as spoofing in the world of malicious computer activities.

Diff: 1

Type: FIB

Page Reference: 369

Topic: Q3

Skill: RECALL

80) E-mail spoofing, where a hacker uses e-mail to pretend to be someone else, is another name for phishing.

Diff: 1

Type: FIB

Page Reference: 369

Topic: Q3

Skill: RECALL

81) IP spoofing occurs when an intruder uses another site's IP address as if it were their own.

Diff: 2

Type: FIB

Page Reference: 369

Topic: Q3

Skill: RECALL

82) Unauthorized data disclosure can occur by simple human error when someone inadvertently releases data in violation of a policy.

Diff: 1

Type: FIB

Page Reference: 368

Topic: Q3

Skill: RECALL

83) Phishing is an example of unauthorized data disclosure.

Diff: 2

Type: FIB
Page Reference: 369
Topic: Q3
Skill: RECALL

84) A(n) phisher is an operation or person that spoofs legitimate companies in an attempt to illegally capture credit card or bank account numbers.

Diff: 2
Type: FIB
Page Reference: 369
Topic: Q3
Skill: RECALL

85) When someone calls and pretends to be from a credit card company in order to check the validity of your credit card number, they are most likely engaging in pretexting.

Diff: 2
Type: FIB
Page Reference: 369
Topic: Q3
Skill: RECALL

86) Phishing is usually initiated via a(n) e-mail.

Diff: 2
Type: FIB
Page Reference: 369
Topic: Q3
Skill: RECALL

87) Sometimes, just opening a web page can install malware on your computer.

Diff: 2
Type: FIB
Page Reference: 374
Topic: Q4
Skill: RECALL

88) With wired networks, sniffing requires a(n) physical connection to the network.

Diff: 2
Type: FIB
Page Reference: 369
Topic: Q3
Skill: RECALL

89) Sniffing is a technique for intercepting computer communications.

Diff: 2
Type: FIB
Page Reference: 369

Topic: Q3
Skill: RECALL

90) Drive-by sniffers simply take computers with wireless connections through an area and search for unprotected networks.

Diff: 2
Type: FIB
Page Reference: 279
Topic: Q1
Skill: RECALL

91) Hacking occurs when a person gains unauthorized access to a computer system.

Diff: 1
Type: FIB
Page Reference: 370
Topic: Q3
Skill: RECALL

92) By starting a computationally intense application at the wrong time, users can inadvertently shut down a network or web server resulting in a(n) denial of service.

Diff: 3
Type: FIB
Page Reference: 370
Topic: Q3
Skill: RECALL

93) A computer worm is a program that infiltrates networks and generates so much artificial traffic that it virtually shuts down the network for legitimate traffic.

Diff: 2
Type: FIB
Page Reference: 370
Topic: Q3
Skill: RECALL

94) An organization's security program has three components: senior management involvement, safeguards, and an incident response.

Diff: 2
Type: FIB
Page Reference: 370
Topic: Q3
Skill: RECALL

95. A(n) smart card has a microchip, which is loaded with authenticating data.

Diff: 1
Type: FIB
Page Reference: 372

Topic: Q4
Skill: RECALL

96) A(n) PIN must be entered when using a smart card in order to provide authentication.

Diff: 1

Type: FIB

Page Reference: 372

Topic: Q4

Skill: RECALL

97) Fingerprints and facial features are used to provide authentication for biometric security devices.

Diff: 1

Type: FIB

Page Reference: 372

Topic: Q4

Skill: RECALL

98) Operating systems today have the capability to authenticate users to multiple networks and servers.

Diff: 3

Type: FIB

Page Reference: 372

Topic: Q4

Skill: RECALL

99) Some new operating systems offer a feature called single sign-on, which remembers your data once you enter it the first time and authenticates you to other machines in the network.

Diff: 2

Type: FIB

Page Reference: 372

Topic: Q4

Skill: RECALL

100) Spyware programs can be installed on the user's computer without the user's knowledge or permission.

Diff: 2

Type: FIB

Page Reference: 373

Topic: Q4

Skill: RECALL

101) One aspect of security programs is how an organization establishes controls that provide checks and balances for the people in charge of sensitive data and applications.

Diff: 3

Type: FIB

Page Reference: 369

Topic: Q3

Skill: APPLIED

102) Enforcement consists of three interdependent factors: (1) responsibility, (2) accountability and (3) compliance.

Diff: 2

Type: FIB

Page Reference: 376

Topic: Q5

Skill: APPLIED

103) What is an unauthorized data disclosure?

Answer:

Unauthorized data disclosure can occur by human error when someone inadvertently releases data in violation of policy. An example at a university would be a new department administrator who posts student names, numbers, and grades in a public place, when the releasing of names and grades violates provincial law. Another example is employees who unknowingly or carelessly release proprietary data to competitors or to the media.

Diff: 2

Type: ES

Page Reference: 368

Topic: Q3

Skill: RECALL

104) What is pretexting?

Answer:

Pretexting occurs when someone deceives by pretending to be someone else. A common scam involves a telephone caller who pretends to be from a credit card company and claims to be checking the validity of credit card numbers: "I'm checking your MasterCard number; it begins 5181. Can you verify the rest of the number?" All MasterCard numbers start with 5181; the caller is attempting to steal a valid number.

Diff: 2

Type: ES

Page Reference: 369

Topic: Q3

Skill: RECALL

105) What is phishing?

Answer:

Phishing is a technique for obtaining unauthorized data that uses pretexting via email. The phisher pretends to be a legitimate company and sends an email requesting confidential data, such as account numbers, social insurance numbers, account passwords, and so forth. Phishing compromises legitimate brands and trademarks.

Diff: 2

Type: ES

Page Reference: 369

Topic: Q3

Skill: RECALL

106) What is spoofing?

Answer:

Spoofing is another term for someone pretending to be someone else. If you pretend to be your professor, you are spoofing your professor. IP spoofing occurs when an intruder uses another site's IP address as if it were that other site. Email spoofing is a synonym for phishing.

Diff: 2

Type: ES

Page Reference: 369

Topic: Q3

Skill: RECALL

107) What is sniffing?

Answer:

Sniffing is a technique for intercepting computer communications. With wired networks, sniffing requires a physical connection to the network. With wireless networks, no such connection is required: drive-by sniffers simply take computers with wireless connections through an area and search for unprotected wireless networks.

Diff: 2

Type: ES

Page Reference: 369

Topic: Q3

Skill: RECALL

108) What are the three general sources of IS security threats? Which one is the most dangerous? Which one is the easiest to plan for?

Answer:

The three sources of security threats are from human errors, malicious activities, and natural disasters. The most dangerous in terms of losses to corporations is still without a doubt, human error, though the potential cost of hackers can be significantly higher. It is easiest to plan for natural disasters because much of this involves just planning for the right location.

Diff: 3

Type: ES

Page Reference: 368

Topic: Q3

Skill: APPLIED

109) Unauthorized data disclosure is a major type of security problem. How do the different sources of threats exploit this problem?

Answer:

Unauthorized data disclosure can occur through human error, hacker activity, and from natural disasters. There have been a number of cases where companies have mistakenly released customer names on Web sites and through other means. More serious is the growth in the number of phishers who pretend to be someone else and send e-mail messages trying to get access to credit card and bank account data. Some versions of this are called pretexting, spoofing, e-mail spoofing, and IP spoofing. Sniffing is a technique where hackers intercept regular network and wireless network traffic. Sensitive data may also be inadvertently released during a natural disaster crisis.

Diff: 3

Type: ES

Page Reference: 368

Topic: Q3

Skill: APPLIED

110) What is a denial of service security problem? How does this result from actions by the various sources of security threats?

Answer:

For telecommunications applications and especially Web sites, there is a significant risk that servers are so overwhelmed with service requests, that they cannot serve legitimate requests. A denial of service can be the result of human error by inadvertently running applications that are too complicated for the network or by too many users making requests at the same time. Hackers have written programs such as network worms that are designed to exploit this flaw and shut networks down by flooding the networks with traffic. Some crime organizations have been known to try to extort money from firms by threatening to do this. Natural disasters can cause networks to go down, also resulting in a denial of service.

Diff: 3

Type: ES

Page Reference: 370

Topic: Q3

Skill: APPLIED

111) What is a technical safeguard? Describe two of these.

Answer:

Technical safeguards involve the hardware and software components of an information system and how they can be used to prevent security problems. Smart cards are like credit cards but they have chips on them that hold a lot more data than the magnetic strips. This data is used to identify the user who is required to enter a PIN in order to be authenticated. Biometric authentication is similar except that it uses unique personal characteristics such as fingerprints, retinal scans, or facial features that can be scanned by a computer and matched in a database. This technology is still in the early stages of adoption, but holds a lot of promise for the future.

Diff: 3

Type: ES

Page Reference: 371

Topic: Q3

Skill: RECALL

112) What is the idea of a single sign-on for multiple systems? What are the benefits and negatives associated with single-sign on?

Answer:

Some advanced operating systems and applications such as enterprise portals, require users to login once and then have the ability to store this information and login the user into any other servers or applications that are part of the allowed network of servers. Users like this because it reduces the time and annoyance of having to remember a whole

bunch of different passwords for each server and application. It also reduces the amount of time the password is traveling the network and so reduces the probability that it will be intercepted. The only bad thing is when a hacker does get in, the damage can be much more severe since there are no safeguards in place once the hacker is into the system.

Diff: 3

Type: ES

Page Reference: 372

Topic: Q4

Skill: APPLIED

113) What is meant by the term "malware"? How can we safeguard against it?

Answer:

Short for malicious software, malware is software designed specifically to damage or disrupt a system. Malware can be a virus, spyware, adware, or a Trojan horse. Sometimes you don't even know you have it on your machine. If your machine gets really slow and has an inordinate number of pop-ups and suspicious changes to the browser homepage or taskbar, then you probably have some form of malware.

The most obvious safeguard is to install antivirus and anti-spyware programs. Be careful to get one from a reputable vendor, since malware has been disguised as antivirus programs that you can get for free. Once installed you should set it to scan your computer frequently, at least once a week. To keep it current you must frequently update your malware definitions. Be sure that you don't open any e-mail attachments from unknown e-mail addresses, since this is the most common way to get malware on your computer.

Diff: 3

Type: ES

Page Reference: 372

Topic: Q4

Skill: RECALL