1. Viruses are always caught by modern antivirus software.
   1. True b. False
2. Phishing is:
   1. An on-line sport similar to bass fishing, except you do not get a sunburn.
   2. A social engineering method involving sending a link to a bogus website in e-mail.
   3. Sending an e-mail to a friend or business associate with a return request on it.
   4. A sensor used to monitor your on-line activities.
3. I should have NO expectation of privacy with e-mail.

a. True b. False

1. E-mail attachments CAN be opened in the following situation:
   1. The e-mail is from someone you know who always forwards you jokes.
   2. The e-mail attachment is from somebody you do not know, but is a word processing document.
   3. The e-mail attachment has “.doc, .exe, or .pdf” in the file name extension.
   4. None of the above.
2. When someone from the phone company says they need access to your server room, you should:
   1. Verify the person with a photo ID.
   2. Ask the person lots of questions about telephony to make sure they know what they are doing.
   3. Contact your supervisor, who will contact information technology or the appropriate department.
   4. None of the above
3. The Network Administrator is the only one that needs to be concerned about Information Security.
   1. True b. False
4. Passwords should contain which of the following “configuration”:
   1. Part of your username or user ID, numbers, letters, and special characters.
   2. A word from the dictionary followed by numbers so that it is easy to remember.
   3. Numbers, special characters, and upper and lower case text.
   4. Anything you want, as long as it is easy to remember or guess if you forget it.
5. You can surf anywhere on the Internet at work as long as no one can see your computer monitor.
   1. True b. False
6. Which of the following is true about e-mail **(circle the letter for all that apply)**:
   1. As e-mail travels to the recipient, it is copied onto many different servers and thus is not secure.
   2. Forwarding e-mail jokes or stories increases the risk my bank faces from viruses and phishing.
   3. E-mail should not contain any confidential information.
   4. E-mail that I send today can still be around somewhere in twenty years.
7. It is ok to use my favorite login password for all accounts.
   1. True b. False
8. When I write down my password, I am accepting risk on behalf of the bank, and violating policy.
   1. True b. False
9. When I leave my computer, I do not need to lock it AS LONG AS I have automatic lock enabled.
   1. True b. False
10. Though the policy prohibits the use of chat rooms, AOL is okay because it’s an instant messenger.
11. True b. False
12. It’s okay to plug my iPod into my workstation as long as I don’t play country music too loud.

a. True b. False

1. To “authenticate” telephone callers, I should ask “out of pocket questions.” The ***best*** example of this is:
   1. Amount of last deposit
   2. Phone Number
   3. Address
   4. Account Number
2. Our Acceptable Use Policy **(circle the letter for all that apply)**:
   1. Is updated each year to address new technologies as well as changing vulnerabilities and likelihoods.
   2. Addresses issues that all persons logging into the network should understand.
   3. Governs the way I handle information that the bank possesses.
   4. Includes a signature page that I sign, meaning I agree to learn and follow all policies.
3. Passwords are used as:
   1. A first line of defense against hackers.
   2. As a means to frustrate users.
   3. There is no real purpose for passwords.
   4. As a means of testing creativity.
4. To confirm the identity of a person calling me and asking me for information, I should:
   1. Be polite and explain that I am required to follow procedures in order to protect identities.
   2. Ask “out of pocket questions.”
   3. Consider calling the caller back at a number in the computer system.
   4. All of the above.
5. Which of the following is the best password for Larry T. Employee?
   1. Grrrrr8t!
   2. a9b8!
   3. Joe\_Smith
   4. G0\_u$@!s
6. The first thing you should do if you think you just got “phished” is make sure everybody is aware of the e-mail.

a. True b. False

1. Spam is the Internet version of junk e-mail. You should:
   1. Use the “opt-out” feature, if one is available.
   2. Forward it to other employees, as they may be interested in the product/service being offered.
   3. Reply to the sender, requesting they remove you from future mailings.
   4. Delete it from your mailbox.
2. All network activity may be monitored.

a. True b. False

Employee Name (Printed):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Score:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of Trainer: Dan Hadaway, CISA, CISM Infotex Certification: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_