

Date: _____ Name _____ Last 4 SSN# _____

Cyber Security Quiz

1. If you saw someone using a VA computer to commit fraud, you would call:
 - a. Your friend down the hall.
 - b. Nobody, because it is not your business.
 - c. Your Service Chief
 - d. Your Information Security Officer (ISO)
 - e. All of the above.

2. In the VA, passwords must:
 - a. Have a minimum of eight characters
 - b. Be changed every 120 days.
 - c. Include your middle initial
 - d. Have all letters capitalized.

3. Which statement best represents the definition of confidentiality in the VA?
 - a. Confidentiality is the condition in which VA's information is available to only those people who need it to do their jobs.
 - b. Confidentiality is the condition in which information whose unauthorized disclosure could be detrimental to the national interest.
 - c. Confidentiality is a feeling or consciousness of one's powers or of reliance on one's circumstances.

4. What is one of the major purposes of HIPPA?
 - a. Provides information about privacy to the veteran audience.
 - b. Outlines privacy policies and procedures for VA employees.
 - c. Clarifies and standardizes responsibilities government employees have regarding providing information about veterans.
 - d. Clarifies the privacy guidelines mandated by all health insurance companies.

5. Which of the following items is NOT recommended when backing up your files?
 - a. Store files in a single location.
 - b. Identify the work on the storage medium.
 - c. Verify access to your storage medium
 - d. Backing up software programs such as WORD on your storage medium

6. What should you do if you receive an email attachment from someone you don't know?
 - a. Do not open the attachment
 - b. Open the attachment if the subject line seems appropriate.
 - c. Reply to the email and request more information.

- d. Open the attachment if your virus software doesn't alert you not to.
7. Software specifically designed to damage, corrupt, and disrupt a computer or network system is collectively known as:
- a. Computer destroyer
 - b. Malicious software, or "malware"
 - c. Junk mail
 - d. Spam
8. When you think a computer security incident may have occurred, you should:
- a. Gather details of the incident so you can communicate specific information to your ISO.
 - b. Collect the date, time, location, and involved computer systems.
 - c. Describe what you believe happened.
 - d. Write down any error messages displayed on your computer screen.
 - e. Write down any involved web address, server names, or IP addresses
 - f. None of the above
 - g. All of the above.

Answers:

- | | | | | |
|------|------|------|------|------|
| 1. D | 2. A | 3. A | 4. C | 5. D |
| 6. A | 7. B | 8. G | | |