1. ‘Cyber Security’ is the protection of computers from threats and attacks that originate from the Internet.
   A. True
   B. False

2. Do you have a role to play in defending against cyber-attacks?
   A. Yes
   B. No

3. Phishing is a type of fraud that uses deceptive e-mails, websites, and/or text messages to gather personal, financial, and confidential information for fraudulent purposes.
   A. True
   B. False

4. Phishing is a type of cyber-attack.
   A. True
   B. False

5. Which of the following are common examples of cyber-attacks?
   A. Fraudulent e-mails requesting your username and password.
   B. E-mails containing attachments with viruses.
   C. E-mails containing links that direct you to malicious websites.
   D. All of the above.

6. Which of the following will help guard against a cyber-attack?
   A. Never disclose your Government-issued username and password.
   B. Never click on links or attachments in e-mails from unknown sources.
   C. Never use your Government-issued e-mail address for personal use.
   D. All of the above.

7. What should you do if you suspect you have received a suspicious e-mail to your Government e-mail account?
   A. Do not respond to the e-mail.
   B. Do not click on any links or attachments in the e-mail.
   C. Report your suspicion by calling the OCIO Service Desk at 709-729-HELP.
   D. Do not forward the e-mail to anyone else.
   E. All of the above.

8. Usernames and passwords should:
   A. Be treated as confidential and protected from unauthorized access, use, or disclosure.
   B. Not be shared or otherwise disclosed.
   C. Not be written down or stored in a file.
   D. Not be communicated via e-mail.
   E. All of the above.

9. Why shouldn’t you use your Government e-mail account or e-mail address for personal use?
   A. Your Government e-mail account was created for the conduct of Government business.
   B. Personal e-mails increase the potential exposure of Government’s e-mail system to SPAM attacks.
   C. Personal e-mails (jokes) increase the potential transmission of malicious attachments, links, and viruses.
   D. All of the above.

10. Information Protection is:
    A. Protecting information from inappropriate access.
    B. Protecting information from inappropriate use.
    C. The responsibility of everyone.
    D. All of the above.