2018 Information Security Module 4 – Post Test Questions

1. Some ways to recognize a phishing email include:

   a) Unusual file attachments
   b) Unknown sender
   c) Suspicious website links
   d) All of the above

---

2. Unintentional disclosures include:

   a) Sending the sensitive information unencrypted to the wrong email recipient
   b) Sending sensitive information without knowing it was included in a file (e.g. hidden rows or columns in spreadsheets)
   c) Allowing your computer screen or mobile device to be seen by unauthorized individuals while you have sensitive information displayed
   d) All of the above

---

3. What are some ways to secure your mobile device?

   a) Keep your mobile device software up to date
   b) Password-protect your personal device with a PIN
   c) Configure the lock screen feature to come on after a short period of inactivity
   d) All of the above

4. The best way to ensure your screen is not viewed by unauthorized individuals is to:

   a) Hang a towel over your screen
   b) Lock your screen when you walk away
   c) Turn your screen towards a wall when you take a break
   d) All of the above

---

5. If you receive a suspicious email with an attachment:

   a) You should open the attachment to verify the email
   b) Do not open the attachment and report the email
   c) Respond to the sender and ask for more information
   d) All of the above

6. How can you avoid becoming a victim of phishing?

a) By learning how to recognize the clues of a phishing scam
b) Avoid using email
c) Ask the criminals to be taken off their email list
d) None of the above

7. If purchasing new technology for use in the Sharp HealthCare network, you should:

a) Have your project manager request a TRC (Technology Committee Review) of the systems to ensure it is compatible with the Sharp HealthCare environment and meets minimum-security standards
b) Negotiate the best deal and get it installed as fast as possible
c) Involve the IT department only if you think the technology is not safe
d) Try the technology in a clinical setting for 90 days, then decide if you want to keep

8. Who has the responsibility of keeping Sharp secure?

a) A dedicated security team
b) All of Information Systems Department
c) The entire Sharp workforce
d) No staff, only technical tools are used