I.T. Regulatory Compliance- Answer Key

1.) Which of the following is a scam that claims your machine is infected with a virus and offers a software solution?

Select One:

A.) Corporate Account Takeover

B.) Search Engine Poisoning

C.) Fake Anti-Virus Pop-Ups- CORRECT

2.) In a tactic known as _____, cyber criminals are embedding malicious software code in what seems to be an ordinary social media content.

Select One:

A.) Clickjacking- CORRECT

B.) Drive-by downloading

C.) Fake Anti-Virus Pop-Ups

3.) Be cautious when using _____ internet services. There may be criminals looking at your online activity hoping to gain information about you.

Select One:

A.) private

B.) business

C.) public - CORRECT

4.) Smishing fraud occurs via _____.

Select One:

A.) email

B.) texting- CORRECT

C.) online banking

5.) Avoiding use of the Internet and email on the same computer you conduct online banking will _____ your risks of online account fraud.

Select One:

A.) increase

B.) decrease- CORRECT

C.) maintain

6.) The FDIC insures and covers commercial customers for any financial losses due to online account fraud.

Select One:

A.) True

B.) False- CORRECT

7.) You will be able to tell immediately if you have experienced a drive-by download attack.

A.) True

B.) False- CORRECT

8.) Cyber criminals commonly use a scheme referred to as _____ in order to commit online account fraud.

Select One:

A.) Search Engine Poisoning

B.) Corporate Account Takeover- CORRECT

C.) Drive-by-downloads

9.) _____ is an event where cyber criminals use search engines such as Google or Bing to direct victims to phony websites so that they can launch an attack to obtain your non-public information.

Select One:

A.) Search Engine Poisoning - CORRECT

B.) Drive-by download

C.) Corporate Account Takeover

10.) After logging into an online banking session, you notice a message that states your financial institution's online banking site is experiencing technical issues. Which of the following would be the best next step?

Select One:

A.) Close out of the session and try again in about two hours.

B.) Check your financial institutions website to see if there is more detail regarding this issue.

C.) Call your financial institution immediately to see if this is a legitimate message. - CORRECT