**WEEK 7 ASSIGNMENT**

1. What is phishing and how would you define it?
2. Name types of phishing and how phishing email gets on your network.
3. How do you analyze phishing email?
4. How do you prevent phishing email?
5. What is DMARC, DKIM and SPF?
6. What are some protocols for email?
7. An email from your boss asks for the name, addresses, and credit card information of the company’s top clients. The email says it’s urgent and to please reply right away. You should reply right away. True or False?
   1. True
   2. False
8. You get a text message from a vendor who asks you to click on a link to renew your password so that you can log in to its website. You should:
   1. Reply to the text to confirm that you really need to renew your password.
   2. Pick up the phone and call the vendor, using a phone number you know to be correct, to confirm that the request is real.
   3. Click on the link. If it takes you to the vendor’s website, then you’ll know it’s not a scam.
9. Email authentication can help protect against phishing attacks. True or False?
   1. True
   2. False
10. If you fall for a phishing scam, what should you do to limit the damage?
    1. Delete the phishing email.
    2. Unplug the computer. This will get rid of any malware.
    3. Change any compromised passwords.