**Social Engineering**

According to research, social engineering makes up a majority of successful data breaches across the world. However, this simple attack vector is often forgotten in cybersecurity for more technical approaches. OSINT and other online tools provide a wealth of information about individuals. However, this information can be used in unethical and immoral ways as we have seen in social engineering attacks performed by various malicious actors.

**Part 1:**

In this assignment, use open-source intelligence tools such as the OSINT framework, Facebook, LinkedIn, Pinterest, and other social media websites to research a family member or friend. Choose and create two attacks from the list below and include examples.

·      Spear phishing attack

·      Phishing attack

·      Whaling attack

·      Vishing attack

·      Smishing attack

**Note: Do NOT send the attacks.**

**Part 2:**

Write a 250- to 500-word reflection discussing the moral and ethical considerations as they relate to cyberstalking from a Christian worldview of human flourishing. What other abusive behaviors can be performed through the tools we have used, and why, as cybersecurity professionals, must we be ever vigilant in our ethical decisions? Examine how the internet is used for cybercrime, cyberstalking, predators, cyberbullying, and other abusive behaviors. Include at least one biblical reference in your response.

While APA style is not required for the body of this assignment, solid academic writing is expected, and documentation of sources should be presented using APA formatting guidelines, which can be found in the APA Style Guide, located in the Student Success Center.

This assignment uses a rubric. Review the rubric prior to beginning the assignment to become familiar with the expectations for successful completion.

You are required to submit this assignment to LopesWrite. A link to the LopesWrite technical support articles is located in Class Resources if you need assistance.