Ramatu Hallie

3/28/24

Journal Entry 10

A cybersecurity analyst monitors the network and identify flaws in a company's security systems. This so relates back to social behaviors. Similar to a cybersecurity analyst, attackers look into and track a company's network with the objective of identifying weak points or flaws that can be abused. This relationship between the two is better understand the way social engineering is, which involves tricking people into violating standard security protocols, has become an important part of cyberattacks. Cybersecurity is more than just a technical problem; it also requires having an understanding of social structures and how people think. Cybersecurity is a discipline that spans the gap between technology and human behavior since analysts have to think like hackers to anticipate their activities. Improving security involves an understanding of how human behavior can be manipulated by cyberattacks. It's not only about troubleshooting technical problems; it's also about understanding how security can be damaged by misleading people. Cybersecurity professionals are better able to prepare for and prevent assaults by knowing about social engineering, or the method of manipulating others. This involves informing employees about typical hacking strategies and teaching them to identify suspicious activity. These two have a lot in common and they could be either used for good or bad. Analyst may use the skills as an advantage and harm their company, some may use their skills for good and protect their company. People have good skills and they choice whether they want to do good or bad with that skill