Cyber Security: Threats of Social Engineering

On the continuation of the cyber security webinar series of Website Advice held on September 5, 2021 to give insightful information about the dangers of social engineering. The examples of scams today like messages about prizes or unknown links and emails are some examples of social engineering. And social engineering should be something that everyone is aware of given that along with the advent of technology, cybercrimes increase.

According to the webinar, social engineering by definition refers to using psychological manipulation to someone, or to get sensitive or confidential information usually through digital communication to use for fraudulent purposes. And about 80% of social engineering attacks are successful. In social engineering, the social engineer gathers information about their victims, then poses as a legitimate person and builds trust with their victims. After building trust, the social engineer gathers information about the victim, and then the social engineer disengages to their victims. Social engineering could work in a form of baiting wherein it lures an unsuspecting victim with a highly attractive offer like unknown emails saying you won, this triggers the greedy and curious nature of humans. Another is catfishing, a form of online deception that involves using fake identity to lure the victims into a relationship with the intent of exploiting them, and catfishing triggers the emotion called desire. Another is phishing, wherein it steals user data, login credentials, and credit card numbers. An example of this is a message with a link saying the victim did a transaction which triggers anxiety, so the victim will click on that link. There's also smishing which is a form of phishing, but instead of email they target victims through messages by clicking the link. Another type is pretexting wherein the criminal will invent a scenario to convince the victim to give information they should not because they find it helpful. This social engineering as said on the webinar works because it triggers the emotion, and when emotions are triggered, our judgment and logic are being impaired.

After introducing social engineering and its types, the speaker shared the red flags a user can look for to avoid these scams. First, when a friend's message is strange because hackers can use their name. Second, when your emotion is heightened because of an email or message, one should not click on a link right away. Third is when the request is urgent. Fourth, when the offer is so good to be true. Fifth, when you're receiving help you didn't even ask for. Lastly, if the sender cannot prove their identity, then receiver should think thrice before doing an action. To avoid being victims of these scams, we should be aware/recognize that this social engineering exists. Slowing down also would help, because hackers know people nowadays like one click away. Slowing down will allow us to don't act or judge immediately and evaluate the messages we received. Third is not to give a password. Lastly, is to ask questions when it seems suspicious.

To conclude, social engineering is really effective and harmful, but as a user of cyberspace, it is important to be aware and be disciplined to avoid falling for these social engineering schemes, and to protect our data.