**Cyber Social Engineering**

**Social engineering**, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

The term "social engineering" as an act of psychological manipulation of a human, is also associated with the social sciences, but its usage has caught-on among computer and information security professionals.

All social engineering techniques are based on specific attributes of human decision-making known as cognitive biases. These biases, sometimes called "bugs in the human hardware", are exploited in various combinations to create attack techniques, some of which are listed below. The attacks used in social engineering can be used to steal employees' confidential information. The most common type of social engineering happens over the phone. Other examples of social engineering attacks are criminals posing as exterminators, fire marshals and technicians to go unnoticed as they steal company secrets.

One example of social engineering is an individual who walks into a building and posts an official-looking announcement to the company bulletin that says the number for the help desk has changed. So, when employees call for help the individual asks them for their passwords and IDs thereby gaining the ability to access the company's private information.

Another example of social engineering would be that the hacker contacts the target on a social networking site and starts a conversation with the target. Gradually the hacker gains the trust of the target and then uses that trust to get access to sensitive information like password or bank account details.

*Source: https://en.wikipedia.org/wiki/Social\_engineering\_(security)*