**Social Engineering Attack**

**Description 1**

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility. [1]

**Description 2**

Social engineering, in the context of information security, refers to [psychological manipulation](https://en.wikipedia.org/wiki/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. [2]

**Description 3**

Social engineering is the practice of using non-technical means, usually communication via phone or another means, to attack a target. An example of a social engineering attack is when a hacker calls up a company, pretends they’re from the internal IT department and starts asking an employee for sensitive information that will help them gain access to the network. [3]

**Refrences**

**[1]** <https://www.us-cert.gov/ncas/tips/ST04-014>

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

**[3] https://www.wordfence.com/learn/understanding-social-engineering-attacks/**