

[A Definition from Whatis.com:](#)

DEFINITION- In computer security, social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. A social engineer runs what used to be called a "con game". For example, a person using social engineering to break into a computer network would try to gain the confidence of someone who is authorized to access the network in order to get them to reveal information that compromises the network's security. They might call the authorized employee with some kind of urgent problem; social engineers often rely on the natural helpfulness of people as well as on their weaknesses. Appeal to vanity, appeal to authority, and old-fashioned eavesdropping are typical social engineering techniques.

Another aspect of social engineering relies on people's inability to keep up with a culture that relies heavily on information technology. Social engineers rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it. Frequently, social engineers will search dumpsters for valuable information, memorize access codes by looking over someone's shoulder (shoulder surfing), or take advantage of people's natural inclination to choose passwords that are meaningful to them but can be easily guessed. Security experts propose that as our culture becomes more dependent on information, social engineering will remain the greatest threat to any security system. Prevention includes educating people about the value of information, training them to protect it, and increasing people's awareness of how social engineers operate.