

Social Engineering

What is Social Engineering?

Social Engineering is a term originally connected to social sciences, but it has now found applications in the field of computer and information security. It is a type of non-technical attacks, where it is not necessary to compromise a system or software. Unlike with other technical attacks, social engineers rely on human interactions to fool users. They can reach their goals by infecting their victim's computer with malware, manipulating them into disclosing their confidential data, or tricking them to open infected sites using a URL link. As a result, legitimate and authorized access to confidential information can be given to the attacker.

Social Engineering attacks are much easier to implement than you think

Social engineering criminals use many ways to launch an attack, be it on a building or a computer system. Either way, they rely primarily on the human tendency to trust. For example, an attacker may get access to a secure building just by asking someone to let him in. On the other hand, he can pretend to be a co-worker and have an urgent need to gain access to network resources to solve it, or just fool a victim to give him the password rather than try to hack his machine. These two examples show clearly that the human element is the weakest link in the security chain.

Types of Social Engineering Attacks

Social engineering attacks can take many forms, depending on the medium used such as email, web, phone, or portable drives. The most common types of social engineering techniques are:

Social engineering attacks can take many forms, depending on the medium used such as email, web, phone, or portable drives. The most common types of social engineering techniques are:

