
Attack methods

There are five methods that could be beneficial for understanding, recognizing, socializing, and preparing the target for your final operation. These methods have been categorized and described according to their unique representation in the social engineering field. We have also included some examples to present a real-world scenario under which you can apply each of the selected methods. Remember that psychological factors form the basis of these attack methods, and to make these methods more efficient, they should be regularly drilled and exercised by social engineers.

Impersonation

Attackers will pretend to be someone else in order to gain trust. For instance, to acquire the target's bank information, phishing would be the perfect solution unless the target has no e-mail account. Hence, the attacker first collects or harvests the e-mail addresses from the target and then prepares the scam page that looks and functions exactly like the original bank web interface.

After completing all the necessary tasks, the attacker then prepares and sends a formal e-mail (for example, the accounts' update issue), which appears to be from the original bank's website, asking the target to visit a link in order to provide the attacker with up-to-date bank information. By holding qualitative skills on web technologies and using an advanced set of tools (for example, SSLstrip), a social engineer can easily automate this task in an effective manner. While thinking of human-assisted scamming, this could be accomplished by physically appearing and impersonating the target's banker identity.

Reciprocation

The act of exchanging a favor in terms of gaining mutual advantage is known as reciprocation. This type of social engineering engagement may involve a casual and long-term business relationship. By exploiting the trust between business entities, someone could easily map their target to acquire any necessary information. For example, Bob is a professional hacker and wants to know about the physical security policy of the ABC company at its office building. After careful examination, he decides to develop a website, drawing keen interest of two of their employees by selling antique pieces at cheap rates. We assume that Bob already knows their personal information including the e-mail addresses through social networks, Internet forums, and so on. Out of the two employees, Alice comes out to purchase her stuff regularly and becomes the main target for Bob. Bob is now in a position where he could offer a special antique piece in exchange for the information he needs. Taking advantage of human psychological factors, he writes an e-mail to Alice and asks her to get the ABC company's physical security policy details, for which she would be entitled to a unique antique piece. Without noticing the business liability, she reveals this information to Bob. This proves that creating a fake situation while strengthening the relationship by trading values can be advantageous for a social engineering engagement.

Influential authority

An attack method by which one manipulates the target's business responsibilities is known as an **influential authority attack** . This kind of social engineering attack is sometimes part of an impersonation method. Humans, by nature, act in an automated fashion to accept instructions from their authority or senior management even if their instincts suggest that certain instructions should not be pursued. This nature makes us vulnerable to certain threats. For example, if someone wanted to target the XYZ company's network administrator to acquire their authentication details, they would have observed and noted the phone numbers of the administrator and the CEO of the company through a reciprocation method. Now, using a call-spoofing service (for example, www.spoofcard.com) to call the network administrator, they would notice that the call is coming from the CEO and should be prioritized. This method influences the target to reveal information to an impersonated authority; as such, the target has to comply with the company's senior management instructions.