Social Engineering: The Ultimate Con

Social engineering is the ultimate con – the bag of tricks employed by fraudsters who lie, cheat and steal their way past your organization’s security controls. Their goals: theft, fraud or espionage. Social engineering bypasses all technologies, including firewalls. It appeals to hackers because there is a general lack of awareness of the problem and it’s nearly 100% effective.

What is an organization’s best line of defense?

Their people. Properly trained staff, not technology, is the best protection against social engineering attacks. Learn how to protect yourself and your organization against social engineering attacks by understanding social engineering tactics and knowing how to recognize scams. People are the weakest link and as a result, organizations must build a human firewall by training their people.

What is social engineering?

Social engineering is the human side of breaking into a corporate network. Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.

Social engineers manipulate people into speaking/acting contrary to their normal manner. The goal of a social engineer is to fool someone into providing valuable information or access to that information. In most cases the attacker never comes face-to-face with the victim, but they get the information or the access they need to commit fraud nearly 100% of the time.

Why are social engineers so successful?

Experienced social engineers relate well with others. They are consistently quick to establish a personal connection with the target and use that connection as the basis of building rapport. The simplest way to get information is to ask for it directly, and this forms the basis for the various techniques used by hackers.

Common social engineering techniques include:

1. Pretexting is when a social engineer develops a storyline that he or she is able to portray to the target. It provides the justification for the questions being asked.

2. Impersonation, such as posing as an employee, is arguably the best technique used by social engineers to deceive people because most people are basically helpful toward coworkers without question.
3. **Phishing** is a way of attempting to acquire information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

4. **Dumpster Diving** – Improperly discarded memos, organizational charts, or policy manuals could be used for footprinting (the art of gathering information or pre-hacking). Social engineers commonly research a predetermined target and determine the best opportunities for exploitation. Dumpsters provide a huge amount of information, including the information a hacker needs to impersonate an employee.

**How do you protect yourself and your company?**

Social engineering attacks may be inevitable in the world today for the simple reason that humans are easy targets; nevertheless, that does not mean that attacks are unpreventable.

The single most important key to avoiding social engineering attacks is to not give sensitive information to anyone unless you can verify that they are who they claim to be and that they have a legitimate need for access to the information. Organizations and individuals can protect themselves through training and awareness as well as security-related policies and procedures.

By staying alert to potential security threats and keeping in mind the suggestions listed above, you will be much more prepared to enjoy the conveniences of online services with peace of mind!

*These helpful tips are provided by InfoSight Inc., an information security consultancy working to help ensure the privacy and security of your corporate, personal and financial information.*