

Social Engineering

Social Engineering is an attack method where an attacker tries to manipulate people into doing something for them, including but not limited to divulging confidential information. This term usually refers to misleading a victim by persuasion, being aggressive, or using other interpersonal skills to obtain authentication information or access to a computer system. Rarely does the attacker ever come face to face with said victim. There are two categories of social engineering: physical and psychological. The physical category includes areas in the workplace and dumpster diving, while the psychological category includes persuasion by telephone and online communications.

The Workplace

In the workplace, the attacker can simply walk in the door, like in the movies, and masquerade as a maintenance worker, consultant, or contractor who already has access to the organization or who must have immediate access to correct a system performance problem. Once the intruder gains physical access, he will use this access to obtain sensitive information (i.e. passwords written down and not secured, and other documents that will provide information about the organization's set up). The attacker emerges from the building with ample information to exploit the network from home later that night. Another technique to gain authentication information is to just stand there and watch an oblivious employee type in his password or to simply ask the employee for the information under the pretense it is needed to fix the system problem.

Dumpster Diving

Dumpster diving, also known as trashing, is another popular method of social engineering. A huge amount of information can be collected through company dumpsters. The following items are potential security leaks in your trash: company phone books (directories), employee lists, organizational charts, memos, policy manuals, calendars of meetings, events and vacations, system manuals, printouts of sensitive data or login names and passwords, printouts of source code, disks and tapes, company letterhead and memo forms, and outdated hardware.

Telephone

The most prevalent type of social engineering attack is conducted by phone. A hacker will call up and imitate someone in a position of authority or relevance and gradually pull information out of the user. The attacker may also masquerade as a legitimate user who needs a password reset. Call Centers and Help Desks are particularly prone to this type of attack. Hackers are able to pretend they are calling from inside the company by playing tricks on the phone system or operator and asking to be transferred to another extension, so caller-ID is not always the best defense.

Call Centers and Help Desks are particularly vulnerable because they are in place specifically to help, a fact that may be exploited by people who are trying to gain illicit information. Call Center and Help Desk employees are trained to be friendly and give out information, so this is a gold mine for social engineering. Most of these employees are minimally educated in the area of security, so they tend to just answer questions and go on to the next phone call. This can create a huge security hole.

Online

There are many types of online social engineering attacks. We will talk about a few of the most popular here.

Phishing - Phishing applies to emails appearing to come from a legitimate source requesting "verification" of information and warning of some dire consequence if not responded to. The email usually contains a link to a fraudulent web page that looks legitimate - with proper logos and content - and requests that the user enter everything from contact information to usernames and passwords.

Trojan horse - E-mail attachments sent from someone of authority can carry viruses, worms, and Trojan horses. These e-mails often promise a critical antivirus or system upgrade that must be completed, but in actuality deliver

malware up to and including backdoor exploits that open connections to your internal network through the firewall.

Road Apple

The road apple is a newer, up-and-coming variation of the Trojan Horse which uses physical media (CD, USB Flash Drive) and relies on the curiosity of victims. The attacker leaves a malware infected CD ROM or USB flash drive in a location sure to be found (bathroom, elevator, parking lot) and waits for a victim to find it. Once the media has been found, the user usually inserts it into his or her computer and will unknowingly install the malware. This attack has become increasingly successful with the use of USB flash drives, because almost everyone would pick one up if found on the street.

Controls against social engineering attacks involve strong identification policies and employee training. Some of these controls might include:

- Visitor identification policies, including asking for personal identification as well as verifying with management who the visitor is and the nature of the visit, especially if at a branch location.
- Continual escort of visitors to sensitive areas of the company.
- Visitor logs and badges.
- Telephone identity procedures to include call backs to the vendor location using a telephone number not provided by the caller.
- Classifying information (for example as public, confidential, restricted) and then training employees on the rules of use, security, and disposal for each type of information.
- Security awareness training for all employees - not just for new hires, but throughout the year as a constant reminder of what they are up against and how to handle different situations.

No matter how much you spend on security technology and devices, the weakest link in any security system is usually the human factor, and the best way to help prevent attacks is continuous training of your employees. Additionally, regular testing of your employees is

important to help you determine whether your training is adequate and completed regularly enough that it stays fresh in their minds. It is highly recommended that a 3rd party be commissioned to complete this testing to ensure segregation of duties. Testing times should not be communicated to employees as this may invalidate the results. Before selecting a company to provide this testing, you should verify a couple things: First, ensure they are willing to sign a confidentiality agreement; after all, they may end up accessing confidential company information. Second, ensure the company is properly bonded and insured. Third, verify references and qualifications. Finally, ensure that the company can test via Phone, E-mail and Physical attack methods to get a full picture of your company's security.