Social Engineering Attacks

What they are and how to counter them.

"Social engineers" are nothing more than conmen. However, the scope and unorthodoxy of modern social engineering attacks are often not truly realised, even by dedicated information security professionals. Some of these attacks can be quite complex, and involve both human deceit and technical tricks.

General terms

All social engineers want is to get their hands on confidential and valuable data or systems. They will try to reach it by deceiving you or your employees via different channels of communication. Such "avenues of contact" can range from E-mail, social networks and instant messengers to faxes, phone conversations, written letters and personal contact. A social engineering attack might also involve physical intrusion into the company premises.

The most recent attacks against Google involved the assailants first finding online friends of key Google employees, and then hacking them to use their hijacked identities in further attacks against Google staff. One is more likely to click on a link sent by a friend. This example demonstrates a combination of social engineering and technical hacking approaches.

From the social engineering viewpoint, there are only two types of people:

1) Those who have what the social engineer wants
2) Those who are vulnerable to social engineering tricks

If 1 and 2 applies to the same person, you are in trouble. If it does not, a social engineer will find vulnerable persons who are connected with their designated targets, and use them as proxies.

The tricks

Classical "419" (Nigerian) scam mail - low-skilled social engineering tricks designed to exploit naivety and total lack of security awareness. They include E-mails claiming to be from technical support asking to change login credentials or install an "update". Unfortunately, there are still people who fall prey to these.

Higher skill level social engineering attacks usually involve proficient identity forgery combined with good knowledge of human (psychological) weaknesses. Social engineers can pretend to be your current or prospective customers, representatives from partner and third party service companies, authorities or regulatory bodies, salesman offering interesting products and solutions, new employees and so on. There are even a few known cases, in which the assailants managed to get employed by their target companies to get insider access.

Modern technical attack methods can make social engineering attempts infinitely more effective. For example, client-side attacks against browsers can allow accessing target computers if their users click on a malicious URL link, or open a specially constructed E-mail (without the need to click on any attachment). Such attacks casually lead to theft of legitimate user identities, which are further abused to attack their colleagues and friends. Notice, that there are numerous means to obfuscate the URL link and source E-mail address, to make it look less suspicious. These and other technical tricks can also be used to direct victims web browsers and other common applications to phishing or malicious script-hosting sites, in hope that the users would not notice the counterfeit.

Finally, the spread of social networking and instant messengers opens a great channel for attacks, as it is reasonably easy to be an impostor in such a milieu, and their users are accustomed to talking to complete strangers. By posting a malicious link to a popular blog or message board, while supplying it with a well-composed luring promise, a wile attacker can hit thousands of targets simultaneously.

The weaknesses

Social engineers prey on psychological weaknesses and insecurities known for the millennia. While the largest of them is ignorance, there is a great deal of others such as ego that attackers can gain advantage of. For example, the widely reported Twitter attacks included a lucrative promise to provide users with thousands of Twitter followers and fame. All you need is to send valid login credentials to the "helpers". Many have bought into this promise, with their submitted credentials being used by attackers to access on-line banking and personal web mail accounts, if the same username and password applied. There are other ways of exploiting human egos, like asking for an advice while looking humble and indulging in flattery.

Social engineers will also try to gain trust by pretending that they share their victims interests, hobbies, views, opinions, values, are in a similar situation, or have a common enemy. They can offer "help" and cooperation, simulate compassion, express sympathy towards your cause, and claim that they have what you need, or can assist in getting it.

Many social engineering attacks also exploit FUD (Fear, Uncertainty and Doubt). They can play on a fear of being dismissed or held responsible for not fulfilling one's duties, by pretending to be a dissatisfied customer or partner, or resorting to blackmail. So-called "scareware" ("we have found a dangerous virus on your system, please install our free virus removal tool") targets the common fear of being hacked. Social engineers look for targets like disgruntled employees, and will blend with the environment to suppress suspicions and appear as if in a due business course.

How to counter them

There are a few useful steps you can take to prevent social engineering attacks:

- Implement security awareness programs and training. All employees should be aware of the social engineering threats and be familiar with common tricks (many of them already described in this document). This includes staff that do not have access to sensitive information and systems, as they can be used as a beachhead to launch attacks against those who do
- Regularly test the effectiveness of your defences by ordering social engineering tests from an independent information security company. See how far the legitimate social engineers can get, and whether they can gain any access to your sensitive data and systems. If they do - eliminate all security gaps that have allowed it ASAP
- Trust, but monitor. Even the intelligence agencies cannot operate in the atmosphere of total mistrust. However, do monitor all your employees, in order to spot suspicious behaviour and acts that clearly fall out of the routine pattern. Maintain a healthy psychological climate in the company to prevent personnel dissatisfaction and discontent. Deal with any disgruntled employees immediately.
- Do proper background checks of all staff. Employ specialist vetting companies and verify the CIFAS database. If these measures are unaffordable, at least do thorough searches online, verify authenticity and veracity of all the submitted documents, and contact the previous employers of prospective applicants
- Perform thorough identity management and verification. This includes verifying identity online, on the phone, and for all physical trespassers. Two or three factor authentication systems make impostors life far more difficult. Phone calls, E-mails and other requests where the identity is unknown, or cannot be verified, should come under suspicion and, depending on the circumstances, be either reported or ignored
- Ban all unnecessary channels of communication. The use of social networks, instant messengers and other online communication means by employees for business-unrelated purposes while at work or from your company systems does not only reduce productivity, but also provides an excellent avenue for social engineering attacks

Finally, do not forget that numerous effective attacks combine a variety of offensive approaches. By reducing relevant technical vulnerabilities, you can also decrease the risks posed by social engineering attacks that rely on exploiting such security flaws in complex.

Dr. Andrew Vladimirov
Arhont Information Security