



Active Blog Managing

www.active-technologies.com
info@active-technologies.com

Protect Yourself from Social Engineering

By Debra Littlejohn Shinder, MCSE, MVP

Not all computer security problems are technological problems. Some are people problems. Just as talented hackers can use their programming skills to exploit applications, operating systems, and protocols to get inside your company's network, talented social engineers can breach your network by using their "people skills" and powers of observation to exploit your company's employees, partners, and others who have legitimate network access. They are adept at psychologically manipulating people into giving them access or the information necessary to get access using a variety of schemes. Here's a look at some of the tactics and techniques commonly used by these intruders and what you can do to thwart them.

1. Impersonating IT staff

A favorite ploy of social engineers is to pretend to be someone from inside the company—often a member of the IT department. Many users who would never give their passwords to a "stranger" don't think twice before supplying whatever information is requested by a phone call from a member of the IT staff. This is especially true if the caller implies that their account may be disabled and that they might not be able to get important e-mail or access needed network shares if they don't cooperate. It's not enough to warn users to be careful; good social engineers will do their homework and find out the names of real members of the IT department. They'll even find a way to place the call from inside the company or have a plausible excuse for why it's coming from outside (for example, saying that they're troubleshooting the problem from the company's headquarters or its special "central IT center").

So how are employees to know whether the person asking for their passwords is legit? In fact, there's rarely any reason a real IT administrator would need to know a user's password. If administrators need to get into a user's account, they can simply use their administrative privileges to change the password to whatever they want and access the account that way. Asking users for their passwords usually indicates either an administrator who doesn't know the job or a social engineering attempt.

2. Playing on users' sympathy

Another favorite tactic of social engineers is to elicit sympathy from a user to get him or her to reveal password information or allow physical access to sensitive servers. For example, the social engineer may pretend to be a worker from outside, perhaps from the phone company or the company's Internet service provider. He tells the secretary who has the key to the server room that he's new on the job and supposed to be back to the office in an hour, and he just needs to check out some wiring very quickly. Or he pretends to be with the ISP and tells the user he calls that he has messed up her account and if he doesn't get it fixed right away, he'll lose his job—and of course, he needs her password to do it. Whatever the story, the social engineer appears to be upset, worried, and afraid of some dire consequence that will befall him if the target victim doesn't help. This exploits the natural people of most people to want to help a person who's in trouble.

3. Wooing them with words

Some social engineers will go to great lengths to pry information out of a user, especially if the stakes are high (e.g., in cases of corporate espionage where the social engineer stands to gain a big financial reward for getting into the network). They'll engage in elaborate, long-term schemes

Active Blog
Managing

www.active-technologies.com
info@active-technologies.com

that include slowly becoming close friends with their target victims or even initiating and developing a romantic relationship to get to the point where the victim trusts the social engineer enough to reveal confidential information, including network passwords and other information needed to break in. This may also make it possible for the social engineer to gain access to keys, smart cards, etc., that can be used to defeat security mechanisms.

Another example of wooing involves gradually persuading the victim that he or she has been wronged by the company or that the company is doing something illegal or unethical and thus deserves to be “taken down” by the social engineer—who just needs the victim’s help in the form of passwords or other access to bring about justice.

4. Intimidation tactics

Some victims don’t respond well to the sympathy tactic or romantic overtures. In that case, social engineers may need to turn to stronger stuff: intimidation. In this case, the social engineer pretends to be someone important—a big boss from headquarters, a top client of the company, an inspector from the government, or someone else who can strike fear into the heart of regular employees. He or she comes storming in, or calls the victim up, already yelling and angry. They may threaten to fire the employee they don’t get the information they want—even if the employee protests that company policy says not to divulge that information to anyone. It takes a very strong person to say “no” to the (supposed) boss or risk losing the company a big contract or getting the company in trouble with the government.

5. The greed factor

Many con games rely on people’s greed, and social engineers take advantage of it, too. Sometimes they just come out and offer money or goods in exchange for passwords or access, but they’re usually more subtle than that. Regardless of the approach, the bottom line is that the social engineer promises the employee some benefit (for example, a better paying job with a competing company) if he or she divulges the requested information.

6. Creating confusion

Another ploy involves first creating a problem and then taking advantage of it. It can be as simple as setting off a fire alarm so that everyone will vacate the area quickly, without locking down their computers. Social engineers can then use a logged-on session to do their dirty work.

7. Shoulder surfing

Shoulder surfing is a form of “passive” social engineering in which social engineers put themselves in a position to observe when the victim is typing in passwords or other confidential information. They may do this without the victim’s knowledge that they’re there or they may use their people skills to win the victim’s trust so they don’t mind their being there.

8. Dumpster diving

Dumpster diving is a form of social engineering that predates computers. The social engineer goes through the victim’s trash can or the company’s dumpster, in this case looking for hard copies of information that can be used to break into the network. The social engineer may pose as a janitor to get access to discarded papers, diskettes, discs, etc., that are supposed to be taken to a central shredding or incineration facility.

9. Gone phishing

Active Blog
Managing

www.active-technologies.com
info@active-technologies.com

The well-publicized Internet scam called “phishing” is a type of social engineering, often done via e-mail rather than in person. (However, phishing scams can also be conducted by snail mail or telephone.) Traditional phishers pretend to represent a company with which the victim does business, often requesting that the victim go to a Web site that looks like the site of the company they claim to represent. (In reality, the site belongs to the phisher.) The victim enters password and other information on the site, and it goes directly to the phisher, who then uses it for nefarious purposes. A clever social engineer who wants to break into your network might create a site that purports to be set up by the IT department for the purpose of confirming or changing the user’s network password. The information is redirected to the phisher, providing a “free pass” to log onto your network.

10. Reverse (social) engineering

An even sneakier method of social engineering occurs when a social engineer gets others to ask him or her questions instead of questioning them. These social engineers usually have to do a lot of planning to pull it off, placing themselves in a position of seeming authority or expertise. This often involves creating a problem with the network hardware or software (or the appearance of a problem) and then showing up as the expert who can fix it (and who gets full access to the systems to make the repairs).

Protecting against social engineering

Although all of these methods differ, some solutions are common to all of them. User education is the number one line of defense against social engineering, backed up by strong, clear (written) policies that define when and to whom (if ever) users are permitted to give their passwords, open up the server room, etc. Strict procedures should be laid down. For example, if you want to enable users to give their password information to the IT department in some cases when administrators call and ask for it, you should direct that they first hang up and call the department back (using the number in the company directory, not one left by the caller) and that administrators supply a prearranged verbal password to verify their identity.

Social engineering itself is not a technological problem, but it does have a technological solution. In most cases, social engineering is aimed at getting a user to reveal network logon passwords. By implementing multifactor authentication (smart cards/tokens or, even better, biometrics), you can thwart a high percentage of social engineering attempts. Even if the social engineer manages to learn the password, it will be useless without the second authentication factor.

If you require additional information or assistance with this item, please give us a call.