



Enterprise Security Office Monthly Security Tips

NEWSLETTER

APRIL 2008

Volume 3, Issue 4

Social Engineering – Are You at Risk?

The term “social engineering” can be defined in various ways, relating to both physical and cyber aspects of that activity. For the purposes of the discussion in this newsletter, social engineering is referred to as an approach to gain access to information, primarily through misrepresentation, and often relies on the trusting nature of most individuals. It involves the conscious manipulation of people to obtain information without the individual realizing that a security breach is occurring. Most users are familiar with e-mail phishing scams (a form of social engineering) and have been taught not to open attachments from unknown or untrusted sources or to visit untrusted Web sites. There are other ways that a perpetrator may prey on the trusting human nature to gain access to information or systems.

Below are several examples of social engineering methods, many of which rely on direct contact with an individual, along with suggestions to minimize the likelihood that such methods will be successful.

Impersonation

In this situation, the perpetrator pretends to be someone else – for example, impersonating a senior official from your organization or someone from your Help Desk. The impersonation may occur over the telephone, in person, or via e-mail. The perpetrator may try to make you feel obligated to assist or under pressure to follow their directions. They may use intimidation or a false sense of urgency to seek your cooperation – prompting you to react before you’ve fully thought through the consequences.

Remember to follow your internal procedures when responding to requests for sensitive or confidential information. Never give out your password to anyone, even if they claim to be from “technical support.”

Piggybacking or Tailgating

All too often, people will hold the door open for someone entering into a secure area or building without even knowing who the individual is or asking where they are going. The unauthorized individual may pretend to be a delivery person, a visitor, or even a fellow employee. Be cautious if an unknown or unauthorized individual is trying to follow you through access doors.

Shoulder Surfing

This scenario refers to the ability of an attacker to gain access to information by simply watching what you are typing or seeing what is on your computer screen. This is known as “shoulder surfing,” and can also be done by looking through a window, doorway, or simply listening in on conversations. Be aware of your work environment and who is around you when you are working with confidential information, or even when you are typing in your password. Do not let others see you type your password, and protect your computer screen from unauthorized viewing. Computers in public areas should not have the monitors facing outward.

Baiting

This scenario involves an attacker asking a variety of seemingly innocuous questions designed to “catch” the right answers. The attack is often done over the telephone but can also be done in person. Items of conversation can also be introduced based upon replies received. Small amounts of facts are interjected at the right time into the conversation to make requests for information sound legitimate. Information you know could be valuable to an attacker – whether that information is about your work environment, fellow employees, projects, or personal information – must be handled with extreme care. Be mindful of what you say to whom.

Surveys

Many of us have no doubt been recipients of requests to participate in surveys – whether online, via telephone or otherwise. The surveys may be for legitimate purposes or might be a scam. In either case, be aware of unwittingly disclosing information that may be used inappropriately. For example, disclosure of details about your organization, its network or infrastructure could prove extremely useful to someone with malicious intent. If you receive a survey request, you should contact the sponsoring organization to ensure the survey is legitimate, and make sure you are not sharing sensitive or confidential information with unauthorized individuals or organizations.

Dumpster Diving

Do you shred all unneeded confidential or sensitive documents? Searching through trash (“dumpster diving”) is a method used by perpetrators to obtain sensitive information. When confidential and sensitive documents are no longer needed, be sure to shred or properly destroy them in accordance with your organization’s records retention policy.

Putting It All Together

The scenarios above represent just a few types of social engineering attempts you may encounter. By following some common sense rules and using your best judgment, you can defend against these attacks and better protect yourself and your information:

1. Before releasing any information to anyone, it is essential to at least establish:
 - the sensitivity of the information
 - your authority to exchange or release the information
 - the real identity of the third party (positive identification)
 - the purpose of the exchange
2. Be aware of your surroundings. Make sure you know who is in range of hearing your conversation or seeing your work. Computer privacy screens are a great way to deter shoulder surfing in public places.
3. Before you throw something in the trash, ask yourself, “Is this something I would give to an unauthorized person or want to become publicly available?” If you are not certain, always err on the side of caution and shred the document or deposit it in a secure disposal container.
4. If you don’t know someone who is in a restricted area, look for a badge or a visitor pass. If you are unsure about their authorization or access permission, report the situation to the appropriate staff.

Brought to you by:



<http://www.msisac.org>