Social Engineering: You are at Risk!

The term "social engineering" refers to an attempt to gain access to information, primarily through misrepresentation, and often relies on the trusting nature of most individuals. Most users should be familiar with email 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.

However, there are other ways that a perpetrator might try 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 manager from your organization or someone from your Help Desk. The impersonation may occur over the telephone, in person, or via email. 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.

Follow your organization's 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."

SYSTEMS AND PHYSICAL ACCESS
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. Do not allow unauthorized individuals to follow you through secured access doors, and report this to appropriate officials.

SHOULDER SURFING
This scenario refers to the ability of a perpetrator 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 that are utilized for sensitive information should not have the monitors facing outward.

BAITING
This scenario involves a perpetrator asking a variety of seemingly innocuous questions designed to probe for information. The attack is often done over the telephone but can also be done in person.   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 the perpetrator--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 security 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. Then check with your supervisor or appropriate individual, such as your privacy or security officer to determine if it is ok to respond to the survey. If you do respond, make sure you are not sharing sensitive or confidential information with unauthorized individuals or organizations.

DUMPSTER DIVING
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 policy.

SOCIAL MEDIA & NETWORKING WEBSITES
Use discretion when posting information online or commenting about anything on social networking sites. Once information is posted, it can potentially be viewed by anyone and may not be retracted afterwards. The more information you post, the more information is available for a perpetrator to use in an attempt to conduct a social engineering attack.

RECOMMENDATIONS
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
    * 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. 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.
4. 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.

For More Information:
DHS Blog - Protect Yourself Against Social Engineering Attacks
http://blog.dhs.gov/2011/07/protect-yourself-against-social.html

CSO Magazine - Social Engineering: the Basics
http://www.csoonline.com/article/514063/social-engineering-the-basics

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Brought to you by: