

**SECURITY - Now ...more than ever!**

Cyber Security - Disaster Recovery - Continuity of Government

**DTI eSecurity News - Social Engineering****What is Social Engineering?**

Social engineering is 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.

**Putting It All Together**

You may encounter social engineering attempts, many of which might rely on direct contact with an individual. By following some common sense guidance, and using your best judgment, you can defend against these attacks and better protect yourself.

1. Before releasing information to anyone, 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. Know who is in range of hearing conversations or seeing your work.
3. Before you throw something in the trash or recycle bin, ask "Is this something I would give to an unauthorized person or want to become publicly available?". If not certain, always err on the side of caution by shredding the document, or deposit it in a secure disposal container.
4. At your office, if you see someone in a restricted area who you don't know, and they don't have a visitor badge, ask them who they are. If you are unsure about their authorization or access permission, report the situation to the appropriate staff.

For more information, visit the Delaware Cyber Security website:  
<http://dti.delaware.gov/cybersecurity>.

Questions or comments?  
 E-mail us at [eSecurity@state.de.us](mailto:eSecurity@state.de.us)

**Social Engineering Methods**

**Impersonation:** The perpetrator pretends to be someone else, such as someone from a Help Desk. The impersonation may occur over the phone, in person, or by email. This person may try to make you feel obligated to assist, pressure you to follow their directions, or use intimidation or a false sense of urgency to seek your cooperation. You may 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:** Often, people will hold the door open for someone entering a secure area or building, without knowing who the individual is or asking where they are going. This unauthorized person may pretend to be a delivery person, a visitor, or fellow employee. *Be cautious if an unknown or unauthorized individual is trying to follow you through access doors.*



**Shoulder Surfing:** An attacker has the ability to gain access to information by simply watching what you are typing or seeing what is on your computer screen. Shoulder surfing can also be done by looking through a window or doorway, or simply listening in on conversations. *Be aware of who is around you when working with non-public information or when typing your password. Protect your computer screen from unauthorized viewing.*



**Baiting:** An attacker asks a variety of seemingly innocuous questions designed to 'catch' the right answers. This attack is usually done over the phone but can also be done in person. *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 may have been recipients of requests to participate in surveys, whether online, via telephone, or otherwise. Surveys may be for legitimate purposes or might be a scam. If you receive a survey request, you should contact the sponsoring organization to ensure the survey is legitimate. *Make sure you are not sharing sensitive or confidential information with unauthorized individuals or organizations.*



**Dumpster Diving:** Searching through trash 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. *Do you shred all unneeded confidential or sensitive documents?*