

West Virginia Executive Branch Privacy Tip of the Week

Social Engineering

Question:

Last week a co-worker in my office asked me to look up some information on her neighbor's application for services with the program I work for. I understand she probably just wanted to help her neighbor, but I told her I couldn't even confirm that her neighbor had applied for services. Did I do the right thing?

Answer:

Social engineering is the act of tricking people into doing things, like providing access to personally identifiable information (PII), which they should not do. For example, a person may call you and pretend to be someone else, in order to get you to divulge PII or sensitive PII. Or, a person may pretend to be looking for a lost access card, hoping that you will let him/her into a restricted facility.

Identity thieves often use social engineering as a way to obtain sensitive PII for criminal purposes. Journalists sometimes use social engineering to obtain information for news stories, such as information about accident victims or people who are involved in scandals. Sometimes people with good motives also use social engineering, to try to obtain PII about a family member or friend. **Regardless of the person's motives, it is very important to prevent inappropriate access.**

Your confidentiality agreement requires you to protect all of the PII and other information that is entrusted to you by your Department. You must be certain that a use or disclosure of PII is appropriate before it can happen. To this end, it is very important that you take the following steps for *every* request for PII that you receive:

- ✓ Unless the information is a matter of public record or being disclosed through a FOIA process, confirm the identity of the person asking for the PII. If you do not personally know the individual making the request, take steps to verify the person's identity and authority to receive the PII. Carefully follow your Department's established procedures for identity verification and authorization.
- ✓ Consider the sensitivity of the PII. If the PII is sensitive, such as Social Security number, home address or medical information, extra steps may be needed to ensure that the information is only being provided to an authorized person. If you have any questions at all about a person's identity or authority, contact your manager or Privacy Officer *before* you disclose the PII.

- ✓ Be especially careful if you are entrusted with PII belonging to someone famous or notorious. Even a trusted co-worker may be tempted to satisfy his or her curiosity about someone important. If this risk exists, even internal requests for PII must be carefully validated to make sure they are appropriate.
- ✓ Also be cautious about providing access to restricted areas to people you don't know. While it seems like good manners to hold a door for someone, you should confirm that the person has a badge that would actually allow access.

Social engineering works because we all want to be helpful and polite. However, we need to balance those good instincts with a clear understanding of the rules imposed upon us by our confidentiality agreements!