Beware of social engineering attacks!

Information Security & Privacy Office

When people think of a cybercriminal they usually think of a person sitting behind a computer using advanced hacking tools and techniques to try and gain access to people's confidential information. This perception couldn't be further from the truth.

It's much easier for a cybercriminal to hack your account, steal your information, or infect your computer with malicious software by tricking you into making a mistake.

What is social engineering?

Social engineering is a psychological attack used by cyber criminals where they trick you into doing something you shouldn't. Think of a social engineer as a con artist or scammer. Attacks can happen through email, over the phone, or in person.

Examples of social engineering attacks

- **Vishing** (same as phishing, but by telephone): Someone calls claiming to be from Microsoft tech support and says they need to fix a problem on your computer. They may ask you to buy security software from an unknown website or trick you into letting them have access to your computer.

  Note: Microsoft will never reach out to you to provide unsolicited technical support.

- **Tailgating:** An unknown individual attempts to access a secure area by following - or tailgating - an employee entering the building or area. The unknown tailgater may even pretend to be a repair person and ask the employee to hold to door open for him or her.

How to detect and stop social engineering attacks

Stopping a social engineering attack is easier than you think. Common sense is your best defense. If something doesn't feel right, it may be an attack. Here are some indicators:

- Someone creating a sense of urgency and pressuring you to make a quick decision.
- Someone trying to get you to ignore agency policies or processes you are expected to follow.
- Someone asking for your password.

More information on social engineering

- DAS Enterprise Security Office - Tailgating Video
- DAS Enterprise Security Office - Passwords Video

Questions?

Contact ISPO at 503-945-5780 or ISPO.AwarenessEducation@state.or.us.

Letting unidentified people into the office is like allowing a stranger into your house.

Never let anyone into the building without proper identification

Tip Sheet

Information & Resources

- Privacy and security policies
- ISPO website
- Inside DHS|OHA
- Training Resources
- Report an Incident

DHS Oregon Department of Human Services

Oregon Health Authority