Social Engineering

What is Social Engineering?

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

Review the following resources to learn how to protect yourself AND your organization, as well as how to report suspicious communications.

What can I do about it?

If you have given personal information in response to a phone call, phishing email or on a suspicious webpage, **your account may be compromised.**

Change your password and report suspicious communications to the Oakland Schools Service Desk. ServiceDesk@oakland.k12.mi.us

Social Engineering Tips

Identify scams

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Scammers will pressure victims to make immediate decisions to get what they want, which may include:
    - Threats of consequences—such as fines or penalties—if you don't provide money or information.
    - Unprofessional, hostile, or even obscene language.
    - Unsolicited calls offering to help you with debt, unpaid taxes, or previous cases of fraud.
- If you are unsure whether a communication request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information.
- The IRS will never ask you for debit or credit card numbers by phone or demand immediate payments using specific methods, such as prepaid gift cards, debit cards, or wire transfers. The IRS will generally contact you first via U.S. Mail.
- Don't trust caller ID. Phone numbers and caller identities can be faked. There have been reports of forged phone numbers from government offices, and other businesses and institutions.

Protect yourself from scams

- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the internet before checking a website's security.
- Do not pay fees for prizes or rewards offered by phone.
- Do not send money or give out personal information (such as credit card numbers and expiration dates, bank account numbers, dates of birth, or Social Security numbers) in response to unsolicited phone calls from unfamiliar companies or unknown persons.

Additional Resources

If you'd like to get further information on how to avoid bad actors from getting their hands on your data, see the links below.

US Department of Homeland Security:

Preventing and Responding to Identity Theft

Follow this guidance from the Federal Trade Commission (FTC):

Federal Trade Commission (FTC): Phone Scams

How to Handle an Unexpected Sales Call

What To Do About Pre-Recorded Calls