Social Engineering

"the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes"

We often associate hacking as something that is done on a computer. Social engineering is a skill that hacks human trust and relationships. Social engineering attacks are used to get you to disclose sensitive information (such as log-in information) or behave in a way that you normally would not. Successful social engineering attacks employ a sense of urgency or familiarity because it hijacks your trust for others, especially if you think it is someone you know.

Common "social engineering" tactics include:

- "Seeking your help!" - Attempts to hijack your good will towards strangers
- "I need this fixed immediately!" - Attempts to hijack your willingness to comply with authority
- "... or else something bad will happen!" - Attempts to hijack your fear of causing something bad to happen, even if it is by inaction
- "Hey buddy!" - Attempts to hijack your willingness to help a friend, even one you just met

Signs of Social Engineering

- "Dear Friend" - Creating a sense of familiarity
- "... mutual benefit to the two of us" - Making it sound too good to be true
- "I am … Attorney to the late … " - Creating a sense of authority
- "... involved in a car accident … " - Creating a sense of empathy
- "Unfortunately, they all lost their lives … " - Creating a sense of empathy
- "I can easily convince the bank with my legal practice" - Openly admitting to manipulation
- "... share the money." - Making it sound too good to be true
- "All I require is your honest cooperation …" - Simplifying their request as not a big deal

What to do about social engineering?

Social engineering is hard to detect, especially if the bad actor is experienced. Best way to prepare yourself against these types of attacks is to be skeptical and wary of what they ask for. You can focus on determining if their actions are suspicious and untrustworthy later.

Ask why they need something from you.

Often, social engineering attacks fall apart once you start questioning why they need something; however, it is not always enough to simply question them about it because they may have prepared responses for that.

Ask yourself how they gained your trust.

Once you have become skeptical of what they are asking for, the next step is to re-evaluate how they initially gained your trust. Often, hindsight is enough to determine that what they did to gain your trust is not always trustworthy at all. Use the things you may have overlooked to determine if the person is who they say they are and if their justifications are legitimate.

What do I do about it?

- If it is an email, forward as attachment to itemailreview@health.southalabama.edu
- If it is a text message, take a screenshot and email it to itemailreview@health.southalabama.edu

Content Created by USA Health IT Office of Information Security & the Office of HIPAA Compliance *October 2021*