Social Engineering: Don’t Fall for the Hook!

Help and Support

Help Desk

Homepage

The age old saying “*if it seems too good to be true, it is*”, holds true in a lot of aspects of life, even in the cybersecurity realm. In the following article we will go over some of the big scams to look for, and how to avoid yourself some major headaches.

Phishing

Phishing is one of the oldest scams in the books, and the most common. Usually the scammer will try and get personal info from you such as login information, birthdays, social security numbers, anything that could be identifiable information. The transport for these messages is usually a messenger service (like Facebook), or could be the more common method of email. Usually they will imitate a person of trust, such as a family member, IT professional, or an executive. They will use threats (such as locking away your data), or a sense of urgency (such as a great deal that will expire) to convince you into their scam and increase the chance someone will fall for the trap. There are variations of phishing such as spear phishing (going for specific targets), and whaling (going for high executives), but most of these attacks are geared towards regular users.

Physical Attacks

Some phishing attacks involve doing something physical rather than digitally. Tailgating is a tactic of following an authorized user into a locked or restricted area (sometimes even pretending to be a pizza man with a box of pizzas) and having them open the door for them out of kindness. It might seem cold-hearted, but if you don’t recognize someone who is following behind you, don’t let them in (or at least verify they work there).Leaving a PC unlocked could be another form of tailgating. Make sure when you leave your work station, you lock your computer. An unauthorized user could use a unlocked computer to malicious acts such as look for personal information, or use a program they are not authorized to use. Another tactic is dumpster diving. This is exactly what you think it sounds like. It involves a malicious user going through the garbage, looking for sensitive or personal letters or mail that someone threw out. The best defense against dumpster diving is to make sure sensitive or personal info is shredded up or destroyed before going to the garbage.

How Do I Tell If It’s a Scam?

Your next question maybe something to the line of “how do I tell a scam from a real request”? Most scammers generally aren’t from the United states, so the spelling and punctuation might be off. Be sure to check the senders email address. If the email address is something unfamiliar or odd, it is most likely a scammer. If they are a family member or close friend, are they addressing you the way they normally do? My sister in law recently encountered a scammer who was posting jobs in my area and insisted on getting her birthday and her current residential address. When she asked this person (who by the way was masquerading as someone from the east coast, with identical profile picture and personal info) why she needed this info, the scammer persisted in asking for the info claiming it was for “employment purposes”. With all the facts lining up, my sister in law decided this person was a scammer and cut off ties with her. She recently tried to look this person up now, but the scammer had already deleted their account. Once someone has discovered their identity, these scammers generally delete the profile and move onto the next scam.

What's the Takeaway?

The main point to take from this article would be this: lean towards the side of caution on emails or notifications. If you have any doubts on whether you should click on the email, call your It professional, or ask a co-worker. Asking a co-worker a simple question is a lot better than exposing yourself (or your entire computer network) to a potentially debilitating virus or malware.

If you have any questions about the Phishing, please give us a call at 509.433.7606 or submit a service request online at http://support.simplepowerit.com/

Last update: 05/24/2019