Cyber Security Snapshot

Exploring and Assessing Current Topics | MICHIGAN CYBER COMMAND CENTER (MC3)

February 14, 2019
CS-01-2019

Social Engineering

Social engineering is the act of manipulating someone into revealing information or tricking the user into performing an action. The goal is to take advantage of a victim's emotional reactions and tendencies to get them to do something the malicious actor wants them to do. Malicious actors use social engineering techniques to conceal their motive and identities. They often present themselves as a trusted source asking for assistance, or a person in need whom the victim is trying to help.

Social engineering is a popular tactic used by hackers and criminals because it is usually easier to exploit a victim's natural trust than to attack a system. For example, it is easier for a malicious actor to fool a victim into giving up their password than it is for them to crack their password. There are multiple types of social engineering techniques. Some of these techniques include but are not limited to: phishing, smishing, and vishing.

Vishing is another type of social engineering tactic which uses a phone call instead of written communication to trick the victim into giving up valuable information. With this type of attack, the malicious actor may use software to recreate a legitimate-sounding copy of an organization's message. For example, "There is a problem with your credit card, press 1 to talk to a representative." Following these instructions will lead directly to a malicious actor attempting to steal your personal information. In many cases, malicious actors will just have a phone conversation with the victim to obtain the information or action they desire.

Phishing typically occurs when a malicious actor sends an email to the target. This email may request the receiver click on a link, open a document, or request additional actions be taken. Phishing attacks can target an individual or they can be used to target an organization. They can also be sent out as widely as possible to increase the likelihood someone will fall victim to their attack.

Smishing is like a phishing attack, except it uses SMS text messaging instead of email as its method of delivery. In this type of attack, the attacker usually asks the victim to divulge information or click on a malicious link. This type of attack is intended to lure victims into taking an immediate action. An example of a smishing message may read "Fraudulent activity on your account is suspected. Click 'here' to verify your activity."

The MC3 has seen numerous social engineering attacks recently where the attacker pretended to be someone else. In one instance the attacker requested help with getting "their" direct deposit information changed. In another instance, the attacker requested money be sent via gift cards in order to "use the cards for marketing purposes while out of town." Multiple incidents have occurred when the attacker was able to get the victim to give them money for "services." Attackers may contact an organization more than once to obtain incremental information. After multiple calls, an attacker may have enough information to compromise an account.

To help prevent yourself from falling victim to this type of attack, the MC3 suggests the following steps be considered and taken when possible.

- Confirm who you are speaking with. This can be done by asking the caller for more information which they should already know or have if they truly are the person or organization they are pretending to be.
- Think before you click. Prior to clicking on a link or attachment in an email, ask yourself if it makes sense for this person to have sent you this email.
- Take a breath before taking any actions. The goal of this type of attack is to get the victim to take hasty actions without realizing what they are doing.
- Give general responses vs providing any leading information. Use caution not to correct or answer any question for the possible attacker.

Any additional questions or concerns can be sent to the Michigan Cyber Command Center (MC3) at mc3@michigan.gov or at 1-877-MI-CYBER