Your Security: Understanding Social Engineering

By Sam Horowitz, Chief Information Security Officer

Social engineering is one of the greatest threats to UCSB’s cybersecurity. In all likelihood, you have already been targeted.

- Have you received an email or Facebook message from a friend who claims to have been mugged and beaten while overseas and now needs you to send money to help them return home?
- Has your bank emailed you about a problem with your account and asked you to click a link to log in?
- How about a phone call from the IRS threatening arrest if you do not transfer money immediately?

These are all examples of social engineering. EDUCAUSE, a nonprofit association dedicated to advancing higher education through the use of information technology, defines social engineering as “a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.” Approximately 80 percent of all cyber breaches begin with some form of social engineering.

Popular types of social engineering attacks include:

**Phishing**

Phishing is the practice of using email, text, chat or social media messages to collect information such as passwords. The good news is many people have learned to identify and ignore phishing attacks. As a result, blanket email phishing is going the way of the dinosaur. The bad news is these attacks are getting more sophisticated.

*Spear phishing* is the new normal. This type of attack leverages information the attacker has on a victim. Email messages are carefully crafted using personal information to compel a victim to act on a request.

There are two main types of phishing requests:

- **Click a Link.** A link in an email takes the victim to a hostile webpage where the victim’s PC is infected or where information is sought. The target webpage usually looks legitimate, prompting the victim to enter personal data. For example, the user thinks they are logging into their bank account when they are really giving their username and password to an attacker.

- **Make a Call.** A message asks a victim to call a “customer support” phone number that really goes to the attacker. In highly targeted attacks, bad actors may ask the victim to wire transfer money to a third party. We have seen this type of attack at UCSB; fortunately, no money was lost.

**Whaling** refers to spear phishing against a high value victim, like a senior executive. These highly targeted attacks appear as executive-level business emails, like legal subpoenas or complaints. The higher someone is in the organization, the greater the potential gain from a successful attack.

Social engineering is not limited to phishing via email, text, chat or social media. A simple telephone call is frequently used to launch attacks. One common scenario is for an attacker to call a victim posing as IT support asking for their password. To intimidate the victim, the attacker will make dire claims about the grave consequences if the victim doesn’t share their password. Do not fall for this scam. Sharing passwords is against UC policy, and your IT support person should never ask you for yours, especially over the phone.
**Pretexting**
Pretexting is when the attacker pretends to be the victim and asks a third party, like a bank or a health care provider, to do something. Pretexting can happen over the phone or via email. In either case, the third party is tricked into thinking that the victim is making a request. If the request deals with creating a new credit card account, then the victim's credit report may suffer.

**Baiting**
When attackers leave a malware-infected physical device in a place where it will be found, this is called a baiting attack. Even though lost USB thumb drives are common throughout campus, never use one that you find laying around. Some of the most successful attacks in recent history started with thumb drives left in parking lots for victims to find.

Social engineering attacks are becoming increasingly sophisticated. Protect yourself and the UCSB community by remembering these defenses:

- Look at the link before you click.
- Don’t give away your username and password.
- If you’re asked to do something out of the ordinary, call or send a separate email to someone to verify the legitimacy of a request.