

Thwarting Social Engineering Attacks

By

Tom DeSot, IAM
Chief Compliance Officer
Digital Defense, Inc.

AT AN OFFICE...CLOSE TO YOU...VERY RECENTLY...

It was a normal day at the office for Margaret, not much had happened that morning, a few phone calls from clients, and of course a ton of e-mails that needed a response, as always. Margaret was just getting up to get another cup of coffee when a technician walked into her office. “Hi, my name is Ed and I’m here to work on your Internet circuit. We had a ticket open from your headquarters stating that you were having some intermittent problems.” Though Margaret did not recall any particular issues, she also did not know if someone else had called it in, or if perhaps headquarters had some type of monitoring equipment that told them there had been issues. “Besides,” thought Margaret, “he does look official with his uniform, name badge, and toolkit.” “Follow me,” said Margaret, “I will take you to the telco room in the hall.” With that, Margaret led Ed to the telco closet, a small poorly lit room that housed all the office’s telecommunications equipment as well as the office switch and router. She unlocked the door for him and went back to her office to continue responding to those pesky e-mails. “Geez,” thought Margaret, “I really do hate technology sometimes.” Fifteen minutes later, Ed came by Margaret’s office and indicated to her that he did not see any problems and that he was finished. Margaret shook Ed’s hand and Ed left the office for the parking garage off the street. Margaret never saw Ed drive away though, but she was far too busy with her e-mail woes to think about it twice.

Two hours later, Margaret got an urgent call from the IT department at the headquarters office. “Margaret, we are seeing a lot of strange traffic from your office, is anything going on?” “No,” responded Margaret, “We are not doing anything different today than other days, and the telco repair man that you sent out earlier said things looked good to him.” “What telco repairman?” asked the caller from headquarters, “We didn’t send anyone out.” With those few words from a person hundreds of miles away, Margaret’s day just went from good to horrible. She was a victim of social engineering, and now the office network, and potentially that of the entire company, had been compromised.

A COMMON ATTACK

So what happened? Did Margaret really do anything wrong? Would you have done the same? Margaret trusted someone (Ed) and tried to be helpful. She did a quick analysis of the situation, found that everything looked legitimate, and decided to help “Ed” so that he could get his job done. Is this a rare situation? Hardly. Every company that has employees who interface with the public educates these same employees to do what Margaret did, that is, to be helpful. Sadly,

the people that are looking to exploit a situation and gain access to computing systems and/or networks are hoping that you have trained them the same way that Margaret's company did. In fact, these attackers are depending on it.

Every day perpetrators attack organizations using methods similar to those experienced by Margaret. Financial institutions, military bases, oil and gas firms, and many other industries; none are immune to being targeted by an attacker looking to take advantage of trust and thereby gain access to sensitive areas of the organization. How these same organizations respond to these attacks has a direct bearing on whether or not the attack is successful, and whether or not subsequent attacks can be thwarted as well.

RESPONDING TO SOCIAL ENGINEERING

More than with any other type of attack, social engineering is directly tied to the information security training that an organization's staff members receive. Properly structured and delivered, a strong information security program ensures that staff members have the information they need to monitor for, detect, and prevent social engineering attacks.

When training staff members about social engineering, great care should be taken to ensure that no assumptions are made regarding attire and credentials. As Margaret found out, it is incredibly easy to create badges that look professional and authentic. Many times a badge is nothing more than a corporate logo with the person's name and sometimes their role in the organization. As this same logo is often available on the company's website, it is trivial to download the logo and utilize simple software tools to construct and print out a very realistic looking badge. Authentic looking attire, as well, is no guarantee that the individual is who they profess to be. Many organizations do not have formalized policies regarding the return of company shirts and as such, the shirts many times will end up in a donation bin for the local Goodwill or Salvation Army. Attackers know this and frequent thrift shops looking for corporate shirts discarded by employees who have long since left the company. Combine these shirts with the easily developed badge, and you have the recipe for a successful attack.

So if you cannot trust attire or credentials, how is a staff member supposed to know whether a visitor is legitimate, or is someone looking to do the organization harm, even if they are trained? The answer is quite simple. Along with the training program, the organization should have clearly defined practices that all employees are aware of, and that clearly define how to handle non-employees when requesting access to secure areas.

FORMALIZED PROCESSES ARE KEY

Every organization should have a formalized process that defines how staff members should respond when presented with a situation similar to what Margaret encountered. The process should be communicated in not only written form, but also re-enforced in training sessions that involve role-play, where the staff members can see how to actually put the process into effect. As with any training topic, the more "real world" the experience can be made to seem, the better.

As far as the process itself, there are some key components that need to be included to ensure that it is successful in thwarting potential social engineering attacks. Some of these components are:

- Require that all visitors present at least two forms of identification. The likelihood that an attacker has forged a driver's license to match his shiny new badge is slim. He is betting that you will take the company badge as enough ID to get past the front door.
- Require all vendors to arrange their visits through a central contact point. This contact point will be responsible for documenting who will be completing the work, what the purpose of their visit will be, and what areas they should need access to in order to complete their work.
- Require staff members to call into the central contact point and validate the visitor prior to allowing them to gain entrance to any sensitive work areas. Note that e-mail should never be used as form of authorization as they are too easy to forge. The central contact point should inform the staff member if any new equipment will be installed or any old equipment removed.
- Require the visitor to sign into a visitor log and be assigned a clearly marked "Visitor" badge to ensure that all other staff members are aware that the visitor is not a member of the staff.
- Require staff members to escort the visitor and monitor their activities while onsite. Once the work is completed the visitor should turn in their badge, sign out, and leave the premises.
- Once the visitor has departed, the staff member should notify the central contact point that the visit is complete so that it can be properly logged.

MOVING FORWARD

Once the formalized process and training program are in place, the key to their success will be ensuring that staff members are re-trained on a recurring basis so that the information stays fresh. Additionally, measures should be taken to ensure new staff members are properly trained in thwarting social engineering attacks before being placed into a production role. Remember, attackers will many times look for new faces or someone that seems unsure since they will be eager to help and prove that they can do the job. Obviously, make sure that all training efforts are documented and kept on file so that you are aware of when the staff members were last trained and when a refresher course is needed.

With a strong authentication process and training program in place, what happened to Margaret will not happen to you, or a member of your staff.

Digital Defense, Inc. Tel: 888.273.1412
www.digitaldefense.net Fax: 210.822.9216