RISK INSIGHTS

Social Engineering

Reliable security systems can prevent losses for your business. While many businesses invest large sums of money into building sound physical structures and robust IT systems or even hiring on-site security guards, they often overlook the biggest security vulnerability—people.

No matter how dependable security systems might be, people with authorized access to those systems will always be a vulnerability. That's why criminals have begun employing a series of tactics called "social engineering" to convince people to give them access—something that costs companies billions each year, and is completely preventable.

What is social engineering?

Social engineering is the art of accessing information, physical places, systems, data, property or money by using psychological methods, rather than technical methods or brute force. In order to do so, social engineering relies upon a set of tactics that exploit psychological weaknesses and blind spots in order to convince victims to give social engineers what they want.

That's what can be so dangerous about social engineering—criminals can use psychological blind spots to have employees willingly give unauthorized parties access, information or property. These attacks can occur in a number of different forms, including a well-crafted spear-phishing campaign, a plausible-sounding phone call from a criminal posing as a vendor, or even an on-site visit from a "fire inspector" who demands access to the company's server room.

Psychological Weaknesses

There are a number of different types of attacks, but social engineers almost always prey upon the following psychological weaknesses in order to get what they want:

- **Fear of conflict.** People dislike conflict and confrontation and will use almost any excuse to avoid them. Social engineers exploit this by exuding confidence when they ask for information or physical access that they have no right to. When social engineers display confidence, most people prefer to comply with requests rather than challenge them.

Social engineering is the art of accessing information, physical places, systems, data, property or money by using psychological methods, rather than technical methods or brute force.

- **Getting a deal.** Confidence artists have always relied upon the greed of their victims; social engineers exploit a similar principle. These criminals have often been known to use gifts and giveaways to get victims to let down their guard. Sometimes, the giveaway itself will be used to masquerade a piece of malicious code that the unsuspecting victim then uploads to his

or her computer.

- **Sympathy.** Sometimes, social engineers employ a softer tactic, using charisma and humor to gain sympathy or to ingratiate themselves to an individual or group. By establishing rapport and breeding positive feelings, victims are too distracted to realize that they're being scammed.

- **Need for closure.** The need for closure is a well-documented psychological need, and one which social engineers exploit. In the event that they are ever questioned or confronted, social engineers who've done their homework will have an answer to any challenge or question likely to come their way. In most cases, any answer—even if it's undocumented, unsubstantiated or blatantly untrue—offers people psychological closure, giving them the sense that they've done their due diligence.

Preventing Social Engineering Attacks

Educating your employees is essential to minimizing the risk of social engineering. Even the best security system will fail if employees willingly allow unauthorized use of their workstations or email their system credentials to a criminal. In order to make your educational efforts stick, consider employing the following strategies:

- **Encourage your employees to "Stop. Think. Connect."** The "Stop. Think. Connect." campaign is a global initiative that encourages people to be smarter about online privacy and security. The motto is an easy-to-remember way to approach divulging sensitive information, both in person and online.

- **Make a personal connection.** The same principles that make your company vulnerable can make your employees vulnerable in their personal lives. Show employees how the same practices for security at work will make them more secure in their personal lives as well.

- **Use "social proof" to your advantage.** Social engineers will often deploy social proof—evidence of a large number of people or select important people engaging in a behavior as proof of its validity—in order to gain compliance. Use that to your organization's advantage by making sure executives and managers make security a top priority as an example for the rest of the company.

- **Train.** Getting the information out there is important, but most adult learners retain more information when they receive interactive training. Consider specific social engineering training that encourages questions and incorporates interactive examples that relate directly to your employees' work activities.

- **Test.** Make sure your educational and training efforts work by conducting regular tests. Despite growing awareness of social engineering tactics like phishing, large numbers of people still open emails and click on links that they shouldn't. Consider conducting an in-house phishing audit to find out just how many employees have taken their security training to heart.

Remain Vigilant

Your employees will always represent a possible vector of attack for criminals, which is why you should always remember the human factor when considering security. Just as your company upgrades systems and installs software patches, so too should you periodically remind your employees of best practices and determine what new tactics social engineers are using to exploit people.

You can trust your partners at EHD to help identify and communicate security threats to your organization, and to keep you up to date on new threats as they emerge.