

Real-World Scenario 17-1: Identifying Social Engineering Attacks

Scenario: As an IT professional, you realize that your job spans much more than just computers; for example, it deals with the intangible world of social engineering. You have recently taken over the position of security administrator for a company with 200 users, but prior to your new appointment there was little, if any, security. You are concerned about people who were previously allowed access to the building and how those people might try to infiltrate your company in the future through social engineering techniques.

Conduct research on the Internet and give one example each of pre-texting, hoaxes, and malicious insiders. Then, define ways in which you would protect your company, data, and employees from these social engineering methods.

Real-World Scenario 17-1 Solution

You can read all kinds of stories about social engineering experts and the cons they have pulled off. They might be true, they might not. What matters is this: Does it sound feasible? And if so, how would you protect against it? For example, Kevin Mitnick is one of the most well-known masters of social engineering (as well as a top-notch hacker). Supposedly, in his early days he learned from a bus driver where he could get his own ticket punch, and therefore ride the city bus for free. How did he do this? Probably through the grooming of trust, or because the bus driver simply liked him, but effectively there was some kind of pre-texting going on somewhere along the way.

People who are good at employing social engineering techniques are usually very knowledgeable of psychology in one way or another. They can relate to the person they are attempting to con. So, in the case study scenario, can you think of anyone who used to work for the company who fits this image? Could your company withstand a sweet-talking impersonator? To protect against this, identification and authorization become your best friends.

One common example of a hoax is the virus hoax. These come in many shapes and sizes but usually are either received through e-mail or show up on a website that a user has been redirected to. The hoax might state that the user's computer will catch fire in 10 minutes, or perhaps that the computer's files have all been encrypted. (Be careful here, though, because there is actual ransomware attacks that will do just this.) The real problem with virus hoaxes is not that they cause computers to fail, but that they decrease productivity: people discuss the hoax, and they forward it (as requested) to friends and co-workers. To defend against this from a technical standpoint, implementing e-mail filters, updating firewalls, IDS/IPS, and updating AV software are all recommended.

To protect from a user standpoint, you should train your users on what to be on the lookout for. Give actual examples on a computer screen. Explain that it is very unlikely that a computer will catch fire from a

virus. Train users to screen their e-mails carefully and to not open or accept unknown attachments. If they do get a display that says their computer is doomed, or to pay a ransom immediately, the best thing to do is shut off the computer and notify the IT personnel.

Malicious insiders are among the deadliest, because they already have access to a certain extent, and getting full access is just one step away. Examples of victims and their respective malicious insiders include USB PaineWebber and Roger Duronio (logic bomb); the DoD and Bradley Manning (release of classified documents to Wikileaks); and the city of San Francisco and Terry Childs (network tampering)—the examples go on and on. More often than not, these people are disgruntled and perhaps want some kind of revenge. But there are plenty of cases in which the person was simply in it for the money.

The motive doesn't really matter to a security administrator, because the end result is increased chaos, decreased productivity, and loss of money for the company. So it is a matter of protection, but how? Here are some tips. First, remember your *lessons learned*. Learn from past attacks, whether you have read about them or they have happened to your company. Understand how the attack occurred and what security control could have prevented it. Next, protect the most important data first. For example, work on patents, the design schematics for a new computer, the code for an unreleased computer program, the secret ingredient in your latest and greatest barbeque sauce—whatever it is, use all of your security power to protect that all-important data first and foremost.

Watch for suspect behavior. Human Resources will probably keep a file on people with suspect attitudes, so you should interface with HR often. Watch for quick terminations and resignations. It's good manners for an employee to give two weeks' notice so as to gracefully transition work to other employees. Quick resignations are a red flag. But all this is commentary; the real way to protect against these threats is to have strong policies, well-planned permissions, tough physical security, strong authentication, and enforcement of principles such as need-to-know and least privilege.

Simulation: Complete the simulations “17-1: Identifying Social Engineering Attacks” Parts A and B.

Video Solution: Watch the video solution “17-1: Solution to Simulation 17-1B.”