PROTECT Your Company

Social Engineering & Your Employees

by Rod Scher

KEY POINTS

▲ People tend to want to be helpful; this puts your company at risk.

▲ Social engineers are excellent researchers and actors: They troll the Web and social networks to get information about your company, and then they "pretext" to get information from you.

▲ Even seemingly unimportant information can be used to compromise your company.

▲ Key defensive strategies include training your staff and running regular security audits.

That new all-in-one printer/copier your company just bought cost a small fortune, but it sure does a great job—worth every penny, no doubt. The vendor even sent out some slick little 4GB flash drives to everyone involved in the purchase: you, the IT director, the head tech; even the purchasing agent got one. Heck, you have to smile about it: At $10 or so apiece for the USB drives, you probably just made back $50 of your purchase.

Except that you didn't. Those flash drives didn't come from the vendor; they were sent by a social engineer who called last week under the pretext of selling you some equipment and found out that you recently purchased a copier from XYZ company. Printing some dummy letterhead and putting logos on a few cheap flash drives took him maybe an hour or two. Loading malware onto the drives took another few minutes. Then he just dropped them into a mailbox and let the U.S. government do his dirty work for him. You've just been scammed: As soon as you insert one of those drives into a company computer (and one or more of the recipients will do that), your company network will have been compromised.

Your Staff Only Wants To Help, But . . .

You just found the weakest link in your security chain: people. People are fallible. They want to do the right thing, but their desire to be helpful often leads them astray because social engineers—"hackers" who use various pretexts to convince employees to give away seemingly innocuous information—can use that desire to please against them. And it happens more often than you realize.

"It seems to me that almost every time we see a report of a company being compromised, we find that some part of the attack involved social engineering," says security expert Chris Hadnagy. "Whether it's a malicious email, a USB [flash drive] drop, or a Web site loaded with malware, we hear about it more and more. Social engineering is a very real threat that is harming people and companies every day."

Hadnagy, author of Social Engineering: The Art of Human Hacking, spends much of his time running social engineering-oriented security audits, and he finds that he can use social engineering skills to break into almost any company—even if the company managers believe they have everything locked down.

"One attack that we might commonly use in an audit is to mail a 'free gift' of an iPhone or other great new device to an executive. The device is hacked, and it gives us access as soon as they get on the Web with it on their network. Executives tend to not focus on the risks; more than a few times I've heard, 'Oh we would never fall for that,' only to use a very similar attack that they do fall for."

More Information, More Risk

The very technologies that help us do our jobs—the Web, the telephone, email—can be (and often are) used against us by hackers. Social engineers, seeking to influence the behavior of anyone from the receptionist to the custodial staff to the head of IT, use those tools to build profiles of companies that they intend to target. Then they pretext, taking on the role of salesman, repair tech, magazine reporter, or any of countless others, to convince us to part with information that can range from email addresses to contact names to the names and versions of the software tools we use in our jobs.

"Profiling is used very heavily today", notes Hadnagy, "and it's gotten much easier with the proliferation of social media. Some people and companies use social media to outline their company's personnel, job offers, departments, internal news, the whereabouts of employees, and more. This makes it easy to get enough information to get a very clear picture of the best attack vector into a company."

Most of the information sought by social engineers seems innocuous; after all, no one is going to respond positively to, "So, what's the company checking account number, anyway?" (Or so we hope, at any rate.) But seemingly innocuous information can be (and is) used against you: "During last year's DEFCON [hacker convention] CTF [Capture The Flag competition]," says Hadnagy, "we saw companies give up things like who handles their dumpster removal, their cafeteria food, paper shredding, and antivirus, as well as what PDF software and browsers they use, and more."

Details like that can give a good social engineer all the information he needs to compromise your company.

Hadnagy paints a typical scenario: "Let's say a malicious social engineer calls a company, pretending to be a supplier of some kind. During the call he's able to determine that the target uses Internet Explorer 7 and Adobe Reader 8. Armed with that information, he closes the call by requesting an email address, saying that he'll send the contact a proposal in PDF format for the contact's approval. A day later a PDF is in the contact's inbox, but it's not a real document. Instead, it's a maliciously encoded PDF that gives the social engineer a reverse shell [a tool that allows a remote connection] on the target's computer. And all because he gave out seemingly innocent information."

Protect Your Company

Given the obvious danger, the question becomes: What should you do to protect yourself and your company?

As always, knowledge is power. Hadnagy recommends several things you can do to defend your company from a social engineering attack: First, learn to identify attacks such as we've noted previously. Then, create a personal security awareness program. Create awareness of the value of the information that is being sought by social engineers. Be sure to keep your software updated. Finally, run regular security audits, and make sure that they include a social engineering component.

You're Not Immune

A skilled social engineer can talk his way into your building and convince your staff to give him information he can then use to compromise your network and your company. This is a fact, and it does you no good—and potentially much harm—to pretend that it can't happen to you. Instead, educate your employees, run audits, and stay aware. Admitting that you're at risk is half the battle.

And finally, as Hadnagy says in his book, "Don't let life get in the way of security. Conversely, don't let too much fear of the bad guys keep you from enjoying life." ▲

"Training employees about how these attacks are carried out can help them be more aware of the danger," says author and security expert Chris Hadnagy.