

## Recognize and Resist Social Engineering Ploys

### Clever manipulation

Not all computer security problems are technological problems. Some are people problems. Just as talented hackers can use their programming skills to exploit applications, operating systems, and protocols to get inside your company's network, talented social engineers can breach your network by using their people skills and powers of observation to exploit your company's employees, partners, and others who have network access. Let's look at some of the tactics and techniques commonly used by these intruders.

### Impersonating IT staff

**The ploy:** You receive a phone call from someone who claims to be a member of the IT department and asks for your password. He mentions the name of your company's IT director and someone who's handled some of your help desk requests. He tells you there's a problem with your account and it could be disabled, leaving you without e-mail or access to needed network shares, unless you supply the information he needs for troubleshooting.

#### What should you do?

**The reality:** Good social engineers will do their homework and find out the names of real members of the IT department. They'll even find a way to place the call from inside the company or have a plausible excuse for why it's coming from outside (for example, saying that they're troubleshooting the problem from your company's headquarters or its special "central IT center"). The truth is, there's rarely any reason a real IT administrator would need to know your password. If they need to get into your account, they can simply use their administrative privileges to change the password to whatever they want and access the account that way.

***NEVER give out your password to someone claiming to be in your IT department unless you have an explicit policy and procedure to follow (such as a callback process) to verify the person's authenticity.***

### Playing the sympathy card

**The ploy:** Someone arrives and tells you he's from the phone company and needs the key to the server room. He says he's new on the job and is supposed to get back to the office in an hour— he got lost trying to find your office and now he's running way behind. He just needs to check out some wiring to follow up on a recent repair job. He's afraid he'll be in big trouble if he doesn't get back in time and he seems genuinely worried and upset.

#### What should you do?

**The reality:** It's possible that he's really on the up-and-up... but not likely. Throwing himself at your mercy is a textbook example of a sympathy ploy, no matter how good an actor he happens to be.

***NEVER allow anyone to have physical access to equipment or facilities without following your company procedures regarding such access. It may be tempting to help this person out, but that's what policies are for: to give you an ironclad reason to resist such temptation and ensure that no company assets are put at risk.***

### **Wooing you with words**

**The ploy:** For the past couple of months, you've been dating a guy who's just starting his IT career as an entry-level net admin. He has a lot of questions about networking practices in general, and it's been fun showing off your knowledge and helping him learn the ropes. But lately, he's begun asking fairly specific questions about your network infrastructure, and once or twice he's asked you to share some sensitive information. You figure he's just being curious, and you trust him, but it still seems like he should know better than to ask.

#### **What should you do?**

**The reality:** If the stakes are high enough, some social engineers will engage in elaborate, long-term schemes that include slowly becoming your friend or even developing a romantic relationship so that you eventually trust them enough to reveal confidential information they can use to break into your network or defeat security mechanisms. Another example of wooing involves persuading you that you've been wronged by your company or that it's doing something illegal or unethical and deserves to be "taken down" by the social engineer—who just needs your help in the form of passwords or other access to bring about justice.

***NEVER reveal sensitive information to an unauthorized person, even if it's someone you feel close to and think you can trust. If someone shows an interest in such information, it should send up a flag that something could be wrong.***

### **Intimidation tactics**

**The ploy:** You pick up your phone and an angry voice tells you that your top client has been unable to access critical files on your company's network. The person says she's a consultant working with the client and demands that you provide her with information that will allow her to log in and access the necessary files. She tells you that the client is THIS close to ditching its relationship with your company, and that failure to cooperate could result in legal action and most certainly the termination of your job. Although some of this sounds like idle threats, it's hard not to think about what could happen if you don't play along.

#### **What should you do?**

**The reality:** Some social engineers take the intimidation route to try to elicit information from their victims. They may threaten you over the phone or come storming in, identifying themselves as a boss from headquarters, a major client, an inspector from the government—someone with sufficient firepower to make you uneasy or downright scared. It takes a strong person to say "no" to the (supposed) boss, risk alienating an important client, get the company in trouble with the government, or stand up to the threat of being fired—but that's exactly what you should do.

***NEVER reveal sensitive information to an unauthorized person, regardless of how they represent themselves or what consequences they threaten you with. Tell them that company policy prohibits you from divulging the information they're asking for. Nobody can second-guess you for adhering to company procedures.***

### **Shoulder surfing**

**The ploy:** One of the vendors you work with has a habit of walking around behind you when you're at your computer and hanging around to chat while you type. At first it seemed innocent enough, although it's fairly annoying. But you've noticed that sometimes, he appears to be scanning your inbox or studying your screen as he talks. In fact, once or twice he's asked you to bring up a particular document, which would require you to log onto the network or navigate to a company intranet page.

#### **What should you do?**

**The reality:** This situation is a little touchy, since you generally want to be polite to partners, clients, vendors, and coworkers who visit you at your workstation. On the other hand, reading over your shoulder is nosy at best and a possible security risk at worst.

***NEVER allow someone to stand behind you and read your screen or watch what you type, unless it's someone who has the same privileges and permissions as you or there's absolutely nothing sensitive that could display on your screen. A better practice is to always ask anyone who tries to stand behind you to move. If they're innocent, they'll be happy to comply; if they're guilty of snooping, they'll have to comply to look innocent.***

### **Something is just "off"**

Even if you don't think you're a target of a scenario such as those we've looked at here, you should trust your powers of observation and your instincts. When something seems just a little out of kilter, it could be a clue that some social engineering is afoot. Here are some examples:

- Someone you're dealing with won't provide contact information
- Someone is in an extreme rush for something you aren't sure they should have
- Someone seems intent on dropping a lot of names to establish credibility or authority
- Someone leans on you for information, making you feel uncomfortable or intimidated
- Someone seems to make lots of small mistakes, such as misspelling or mispronouncing names or asking weird questions (possibly about things they should know if they're part of your organization)
- Someone requests confidential information