



Beware the *Social* Engineers

Spending a lot of money and resources on protecting your company's network security from computer hackers? Good idea. But maybe your greatest threat is from smooth talking telephone callers and seemingly innocent visitors.

“WHEN WE FIRST started doing this I thought we'd get people's user names and passwords, sensitive information like that, maybe 5% of the time,” says Todd Snapp, president of RocketReady, a Tampa-based security firm that specializes in finding human security weaknesses. “In fact, our success rate is about 30% to 35%, which I find amazing.” When Snapp expands his definition of success to include a wider range of information, even down to obtaining the names and titles of a company's key personnel, the success rate is far higher, almost 90%.

How does his company acquire information that would allow it to gain access to a company's network and most valuable information? The old-fashioned way—by asking people for it, usually over the telephone. The methodology has

a modern buzz phrase—social engineering.

Social engineering has been defined by a U.S. Senate Subcommittee on Investigations as “the gaining of privileged information about a computer system by an unauthorized person masquerading as a legitimate user. The high tech version of the old ‘confidence game.’” Rich Mogull, research director for information security and risk at global research firm Gartner Inc., predicted to *Hemispheres* magazine that such old-fashioned swindles will be “the single greatest security risk in the decade ahead.” Well-meaning employees, he says, often inadvertently help hackers pilfer company secrets, including information about customers, products in development, pricing, and other data.

The most common way social

engineers work is by telephoning users or company operators and pretending to be an authorized user in hope of gaining illicit access to systems. The most successful social engineers are blessed with the gift of the gab, and an innate or learned set of people skills.

As RocketReady's results illustrate, social engineering can be very effective.

It's a weapon few companies are aware even exists, or realize is being used against them. “I believe there is not a company of any size right now that is not being attacked by social engineers trying to obtain some kind of information,” Snapp says. To back up his claim, he refers to a website called privacyrights.org, which chronicles security breaches.

“Since February 15, 2005, more than 88 million personal records have been reported lost due to

security breaches in 214 separate personal data loss instances,” he says, in a late July 2006 interview. “Those are the ones *reported*. Only 24% were caused by computer hacking, which means that 76% were because of another method, including social engineering.”

A good talker himself, Snapp says companies need to educate and train their employees about social engineering. Before that happens, however, the companies need to accept that sophisticated security technology is not enough to protect access to their network, not when he can show them how easy it is for his staff to breach that security.

GET THEM TALKING

Most of RocketReady’s clients are Fortune 500 companies and government departments, which retain his firm to test their vulnerability to social engineering attacks. He began offering this service about two years ago when a large telecom client noticed the negative publicity suffered by a competitor when its customer data was stolen due to a social engineering incident. The client asked RocketReady, which was conducting other work for it at the time, to see how much information it could extract from the telecom’s employees. Since then, this type of work has become RocketReady’s mainstay.

“We usually start with a zero knowledge attack,” he says, meaning that his clients provide RocketReady with no inside information. “We have them sign a get-out-of-jail free card to protect us [from any legal action that could arise from what they have to do to conduct their intrusions].” In some cases,

“When people talk, listen completely.

Most people never listen.”

—Ernest Hemingway

the client provides direct information about its policies and procedures and has RocketReady test those specifically.

In its zero knowledge assignments, RocketReady’s staff start out by educating themselves as much as possible on the company, its organizational structure, number of locations, its language (such as particular terms or acronyms it uses), the names of key personnel, the user name configurations, and any other information they believe will help them sound like an insider when they begin to call specific individuals in the company as part of their direct attacks.

This preliminary stage usually involves such benign approaches as mining the Internet, researching public databases, pretending to be an interested customer or client, showing up at a facility, and calling the communications department. “We need to know, for example, what they call the IT department, who the IT managers are, the buzz words they use, that sort of thing,” says Snapp.

Once educated about the target company, Snapp’s team begin to call the company’s staff, going after individuals for whom they know their user name. “Obviously, for us to succeed, the company needs to be fairly large,” he says. “If you call a small company like ours everyone knows everyone, their voices. But in a large firm, that’s not usually a problem.”

Nor is caller ID (see sidebar). “We can use spoof caller ID to

make it look as if we’re calling from within the company,” he says, “although sometimes we make the calls deliberately from an outside location, like a hotel or from a client’s, somewhere out of the office and where we need their help right away.”

Snapp rarely has his team take an aggressive tone when they call. “Some people who do this type of work will be chewing the person out and cussing and trying to intimidate the person,” he says. “We find this rarely works. We also find that this kind of call typically gets reported internally as a suspicious call. Our calls are reported only about 5% of the time.”

TYPICAL RUSES

A typical call begins with a request for help, which Snapp says is highly effective:

“Oh hi, I’m so-and-so and I’m really sorry to bother you but I’m having a real problem with [for example, something to do with gaining access to the network] and I’m really hoping you can help me.”

Sometimes, he agrees, it can be beneficial to up the tone a degree:

“Listen, I’m calling you because this thing is all messed up and I’m under the gun here, I’m in real trouble, and we have to get this thing going right now!”

These opening gambits begin a dialogue with the target person that has one ultimate objective: the target person will inadvertently share a user name, password or

continued...

other information that will allow Snapp's caller to gain access to the network.

One strategy, he says, is to pose as a member of the IT group:

"We're having trouble with the system and we just need you to log in so we can check out the status because we think there's been a breach."

If the person is reluctant to reveal his password, Snapp's caller then tries another approach:

"Good, you're not supposed to do that because we didn't want you to share your password. Instead, can you just reset it—" Snapp explains that almost all companies have a default password, such as 12345 or just the word "password." Most people agree to do this. "Once they do, we can then access the network (using the already obtained user name and now the default password). There's usually a short period of time before they select a new password and during that window of time we can get in to the network," he says.

Another approach is the already mentioned call for help. "Some people just give us their password over the phone," he says, but if they don't, his team try various ploys. "We often start with the internal help desk, which we find tends to be...very helpful." They usually ask for an employee ID and location, which RocketReady has previously obtained. "We'll say we're trying to get on to our VPN but it's not working, and then they start to ask us questions, which in themselves are very helpful," he says. "All the

while we're emphasizing over the phone that we urgently need to get on the network. Maybe they'll ask what client are you using and we'll know the answer from our research. They tell us to open it up and we tell them we can't. So then we ask, 'is there another way I can log in?'"

How successful is that question? "We've had them fax us or email a prefigured VPN client to our personal email account, because of course we can't access our company email," he says. That still requires a password, which takes another call, such as the one in which an employee is asked to reset her password.



If the password ruse doesn't work, Snapp's caller often starts to make up an incredibly confusing process the company person has to go through to help the caller. Snapp's caller keeps urging the person not to do anything that he finds uncomfortable—an old

trick—while continuing to make the solution as difficult to understand as possible. Many people then surrender and offer their own password and other secure information just to get the "urgent" work completed.

"The key," says Snapp, "is to get them to a point where they believe we are who we say we are. Once that occurs, they'll do just about anything we ask."

One of his favorite stories involved a person who was called under the pretext that it was the IT department, which believed the person's staff wasn't logging in to the network properly. "Just as he was about to provide an IP address for logging into the network, he stopped and said, 'Hold on a second, I'm just not really feeling good about this. Are you really from [his company]?' " Snapp says. "And our person answers 'Yes, I am,' and he said 'Okay, I just wanted to be sure,' and proceeded to give it to us."

Snapp says most of his engagements take about three or four weeks and, upon completion, he hands his client a thick binder of information obtained by the various social engineering methods. How do the clients react? "Jaws drop, heads wag," he says.

From what he understands, companies don't tend to reprimand or fire employees who have divulged the sensitive information. "Typically, they are shocked and blame themselves for not having educated their staff on how vulnerable they are to social engineering," he says. "They had no idea we could obtain this information without having to hack into their computers. Sometimes, I say, it's so easy it's like shooting fish in a barrel." ■

*"The telephone is a good way to talk to people without having to offer them a drink."
—Fran Lebowitz*

If You Can't *Trust* Caller ID...



Just when you thought it was safe to answer the phone, a new scam emerges.

THE FOLLOWING warning appears on the website of the U.S. District Court in Washington: “If you are contacted by a person claiming to be from our jury office, with caller ID showing a courthouse number, requesting that you pay a fine because you missed jury duty, do not give that person any information.”

As RocketReady’s Todd Snapp reveals, we can no longer trust caller ID to let us know who or what organization is calling. Thanks to new technology “that enables con artists to manipulate the phone number and even the name that shows up on the unsuspecting recipient’s caller ID,” reports the *Chicago Tribune*, caller ID can now be faked. As a result, one level of seeming protection — information about the person contacting us by phone — has been taken away.

Known as spoofing, this new technology has obvious appeal to fraudsters of all stripes, but especially those involved in identity theft or scams designed to con

people into spending money on what they believe are legitimate causes, such as donations to charities.

The typical way the technology works is through companies such as SpoofCard, a U.S. firm that has a dedicated toll-free number where users enter a PIN, their desired caller ID and the number they’d like to call, reports the *Tribune*. “SpoofCard users also have the ability to select a male or female voice. The caller speaks normally, but the person on the other end hears the altered voice.”

In June, the U.S. House of Representatives passed the bipartisan Truth in Caller ID Act of 2006, which makes it a crime to transmit misleading caller ID information with the intent to defraud or harm. There’s also a bill before the House Judiciary Committee, The Preventing Harassment through Outbound Number Enforcement (PHONE) Act, that calls for strict penalties for those who commit caller ID fraud.

It’s unlikely fraudsters will be deterred by such legislation, but publicity about them should help to educate the public on yet another way the telephone can be used to separate them from their money. ■

Protect Yourself From Social Engineering

Ira Winkler, author of *Spies Among Us*, recently shared some tips with *United Airlines’ Hemispheres Magazine*:

- Don’t be afraid to say “no” or to ask why a person needs information.
- Never give out sensitive information to an unknown party.
- If someone unknown to you contacts you and needs sensitive information, call him or her back at a number in a company telephone directory.
- Nobody will ever legitimately ask for your password; never give it out. If someone asks, report the incident to security.
- Don’t rely on common corporate identifiers, including employee numbers on identification badges, as a way to verify identity.
- Be aware that social engineering is generally accomplished through several inconsequential attacks, so be aware of unusual calls.
- Always look for your own company’s badges on people when they “tailgate” you through a door.
- Shred all sensitive documents.
- If a credit card company calls you, call back at the number on your card before discussing any details about your account. ■