# Social Engineering

Chris Werner

March 3, 2006

Computer security, privacy and information integrity have never been harder to maintain. Today there are millions of viruses, Trojans, spyware programs, phishing schemes, and the original computer threat, the computer hacker. Computer security has been able to keep up with these new types of threats as they emerge pretty effectively. But as fast as these new types of threats come out, and the speedy response from the security field, they are still unable to completely fortify themselves from one of the oldest threats in the book; the social engineer.

Social engineering is a tool that some computer hackers use to get into computer systems, networks, or databases. It is an attack against the weakest-link in security; the human user. Social engineering is the use of manipulative ways to persuade a user of a system to give out sensitive data, such as passwords, usernames, and IP addresses, which allows the social engineer to gain access to the system. . The attackers get the data by pretending to be legitimate administrators and preying on unknowing users of the system. Kevin Mitnick describes a social engineer in his book The Art of Deception as “an unscrupulous magician who has you watching his left hand while with his right he steals your secrets. This character is often so friendly, glib, and obliging that you're grateful for having encountered him” (13). This attack usually starts off with a few phone calls to get the information, then they proceed to simply log into the system. Why bother breaking in if a user is willing to open the door for you?

Social engineering has the same goals as conventional hacking; gaining access to a computer system that one is not authorized to access, but social engineering can be done without the traditional technical hacking methods. Social engineering can be done over the phone, through dumpster diving, online, or through email.

Social engineering targets major weaknesses in human character, from a security standpoint: the desire to be helpful, the tendency to trust people, the fear of getting in trouble from the boss, naivety, and the fear of questioning supervisors. And where do you find people with these characteristics and the lack of knowledge to realize the damage they could be causing? The help desk. That is where many social engineers start their search. It's unbelievable the amount of information some people are willing to give up over the phone.

One of history's biggest bank robberies was committed without a gun; the weapon of choice was a payphone. It was done by Stanly Rifkin in 1978. He successfully stole $10 million from Security Pacific National Bank in Los Angeles, which has since closed its doors. He worked for a company that was hired to install a backup system in the wire-transfer room just in case their system went down. While working in the wire-transfer room he learned all the information needed to make an authorized wire-transfer along with all the people allowed to make them. All he did was use a payphone in the bank lobby to con the staff in the wire-transfer room to transfer $10 million into a Swiss bank account. A few days later he flew to Switzerland to pick up the cash, then flew to Russia and exchanged $8 million for diamonds and flew back to the U.S.

What sunk him was the fact that he needed to brag about his success, and the police got tipped off. When the police contacted the bank, they didn't even realize the money was missing. Stanly Rifkin made the Guinness Book of World Records where he remained until 1999 when he was replaced by, the "World's Most Notorious Hacker", Kevin Mitnick.

Social Engineers don't only use the phone; there are many security leaks in a company's trash. As illustrated in an article "Social Engineering Fundamentals, Part 1: Hacker Tactics" by Sarah Granger, found at SecurityFocus.com

> "company phone books, organizational charts, memos, company policy manuals, calendars of meetings, events and vacations, system manuals, printouts of sensitive data or login names and passwords, printouts of source code, disks and tapes, company letterhead and memo forms, and outdated hardware"

are all security leaks. The company phone books give the hacker a place to start learning names of possible victims, or people to impersonate, and their numbers. It might also reveal company authority positions and rankings. Policy manuals and memos can give insight of the company's security, and small pieces of the hacker's puzzle. The company calendars can show when certain people might be out of the office or out of town. And outdated hardware such as hard drives or tape drives can be restored to reveal the information that was previously on them if they weren't disposed of correctly.

A newer form of social engineering is the online form. The most common method is a spoofed website that looks just like the legitimate one. The user will put in a username and password, but instead of just signing into the real website, they just sent their username and password to the hackers. Throw this method in with an official looking email and you now have what is called phishing. This is currently the hot security topic of the year, and is costing companies billions of dollars. A common example of this attack is the eBay/PayPal emails that everyone gets everyday. Click the links in these emails and attempt to sign in, and you might be seeing a few strange charges on your credit card in a few weeks. With these three items: email address, username and password to a given site, hackers can most likely get into other accounts that you might have, because most people use the same username and password at more than one site.

Another form of social engineering is reverse social engineering. The hacker creates a character, and eventually gets in the position where people turn to him for help. This in turn gives him better chances of getting confidential information. A paper by Rick Nelson, “Methods of Hacking: Social Engineering” tells us that

> “the three parts of reverse social engineering attacks are sabotage, advertising, and assisting. The hacker sabotages a network, causing a problem to arise. That hacker then advertises that he is the appropriate contact to fix the problem, and then, when he comes to fix the network problem, he requests certain bits of

> information from the employees and gets what he really came for. They never know it was a hacker, because their network problem goes away and everyone is happy."

Along with these many ways to carry out the attack, there are also different ways of delivering the attack as well. There is intimidation, where the attacker will introduce negative consequences for not following directions. They might drop names of upper management to add to this effect. There is the impersonation technique where they will impersonate someone usually in a position of power and authority. This is where getting a company calendar can come in handy. There is simple flattery or befriending. People will give out more information to someone they have talked to in the past than to a stranger. Another technique used is pressure. Victims tend to make bad decisions when they're under pressure. Also some attackers can act like they are in a great hurry and request information, not giving the victim time to think about the information they are giving out. Another tool in the social engineer toolbox is getting sympathy, make the victim feel that if they don't give you the information you are asking for, they are responsible for getting you in trouble.

Hardware and software devices only prevent physical attacks, the employees of a company must be trained and be made aware of social engineering tactics and the psychological side of computer hacking. Policies should be put in place and enforced. Building security is also important. IDs should be checked at all times. Documents should be shredded before thrown

away or incinerated. And all storage devices should be destroyed before being disposed of.

Another point to make is that employees should know that a system administrator will never call an employee and ask for their username and password. They don't need it, they have administrative access. Another important aspect is to tell employees about email phishing prevention. Help desk personnel should have a call-back policy where they call the supposed employee back using the company directory when a password request is made. The idea here is that employee education is just as important as hardware. The first level of security is coming up with a good security policy; the next level would be education and enforcement. Occasional emails about real life social engineering attacks would also be a good idea; it keeps the topic in the back of employees' minds.

There are companies in business to help in securing computer systems, both physical and psychological.

> "In computer attacks, the weaknesses are in design, implementation, configuration, procedure, and proper use of technology. Risk analysis is a process by which to identify those weaknesses and mitigate them in a cost-effective way. It is rarely possible to cancel out all risks. In social engineering, it is never possible. The weakest link is the human psyche." (Peikari, 209)

But the idea is to cut all risks down as much as possible, including social engineering attacks, and one such company that can help in this area is Trace

Security Inc, www.TraceSecurity.com. They are security consultants that specialize in social engineering attacks. They have people call up and see what kind of information they can get out of the employees. They send phishing emails with links to one-off websites. For example, if they are doing consulting work for a nationalbank.com they might register the domain name nationa1bank.com, and with the font the browser uses, the ‘1’ will look like an ‘l’, that’s assuming the user will even look to see where the link is taking them.

Another trick Trace Security pulls is sending an email with a spoofed header to say that it came from the vice-president, informing employees that exterminators will be coming. Then the team moves in and installs data stealing devices, since people rarely follow maintenance people around. They get very creative and teach the employees an important lesson.

The only real technical way to detect a possible social engineering attack in a company’s future is to catch them in their preparation process. If hackers are going to set up a spoofed website, they will be downloading a company’s logos or whole webpages, which is detectable. Another thing to look for is to see what external people have been looking at public information that usually only company people would look at. Again, the cost issue comes into place here. This takes time and money to look back at logs and look for small things like this.

With all of today’s computer security advancements, they still can’t protect against social engineering without educating employees. The social engineer is today’s con man, and they will continue to be successful until people learn to

stop giving out sensitive data. Many employers are not willing to pay for this education, sometimes the employee education ends up being a simple company memo explaining not to give your password to anyone.

Kevin Mitnick once said “You could spend a fortune purchasing technology and services… and your network infrastructure could still remain vulnerable to old-fashioned manipulation” (Mitnick, SecurityFocus). So technology cannot single-handedly solve computer security problems. As previously shown, the weakest-link in security is the human user. Software and hardware, firewalls, intrusion detection and intrusion prevention systems are all great, but if you have employees that are sweet talked into giving away sensitive data, they are all worthless.

# Works Cited

Granger, Sarah. "Social Engineering Fundamentals, Part I: Hacker Tactics." SecurityFocus. 18 Dec. 2001. 3 Mar. 2006. <http://www.securityfocus.com/infocus/1527>.

Peikari, Cyrus, and Anton Chuvakin. Security Warrior. Sebastopol, CA: O'Reilly, 2004.

Mitnick, Kevin. "My first RSA Conference." SecurityFocus. 30 Apr. 2001. 3 Mar. 2006. <http://www.securityfocus.com/news/199>.

Mitnick, Kevin and William L. Simon. The Art of Deception. Indianapolis, IN: Wiley, 2002.

Nelson, Rick. "Methods of Hacking: Social Engineering." 3 Mar. 2006. <http://vvv.snugg.net/security/dokumentation/dokumentation/soceng/socialeng.html>