The Cyber Con Game – Social Engineering

Christopher Paradowski
February 18, 2001

Con men, and or women have been gracing us with their playful games since the beginning of time. According to the Association of Certified Fraud Examiners', fraud and abuse cost U.S. organizations more than $400 billion annually. The average organization loses more than $9 per day per employee to fraud and abuse. The average organization loses about 6% of its total annual revenue to fraud and abuse committed by its own employees. As you can see, fraud is very costly. With the ever-changing way we conduct business, these statistics are sure to rise in the near future. The majority of today's organizations are using the Internet and Intranet computer networks to conduct everyday business. This brings about a whole new ballgame when it comes to fraud. We will call these people the Cyber-Cons. These digital Cyber-Cons employ Social Engineering to get what they want.

Basically, Social Engineering is the art and science of getting people to comply with your wishes. It is not a way of mind control, it will not allow you to get people to perform tasks wildly outside of their normal behavior and it is far from foolproof. Social Engineering is defined by Hacking Exposed, Second Edition as the technique of using persuasion and/or deception to gain access to information systems. Such persuasion and deception is typically implemented through human conversation or other interaction. The type of information Cyber-Cons would try to obtain would be user names, passwords, operating systems, network topology, hardware configurations, and just about any tidbit of information they can get their dirty hands on. The main goals of Social Engineering are fraud, network intrusion, industrial espionage and identity theft. We will concentrate on industrial espionage. Why industrial espionage? The answer is very simple: Information is power, and power equals money! Confidential company information would be very useful to a competing company. Often, millions of dollars are on the line for a new product or technology. The Company who gets to it first will most likely gain financially. Protecting this information could mean the life or death of your organization.

Social Engineering comes in many forms. Most likely it will occur in the form of human intervention. The simplest model would come in the way of a telephone call. For example: Someone calls you and says they are from your companies help desk. They say they are upgrading their current configuration and are verifying all user names and passwords. They ask you what your user name and password are and you tell them. BINGO! The Cyber-Con now has user access to your network! It sounds simple, but it does happen. A more dramatic approach would take some good acting on the behalf of the Cyber-Con. For example: Someone comes to your office acting like a high level consultant. This person will come to your office when he knows the boss is on vacation or out to lunch. He says, "I am here to meet with so and so to conduct some important business" You say, "Mr. So and So is on vacation, How can I help you?" The Cyber-Con now knows he has you and proceeds with the game. You proceed to give this" consultant" a tour of your facilities including your engineer and research and development department. While conducting the tour you tell the Cyber-Con about a new break through technology that will take the computer industry into the next millennium, and will re-write the book on Information Technology. The Cyber-Con starts asking questions like, "Who will be your supplier, how much does this cost, what will it look like? " You say, "Let me show you". You take Mr. So and So to the Finance department to find out the cost. You take him to the accounts payable department to find out who are the major suppliers. You even take him to the research department to see what it looks like. After the tour, the Cyber-Con, knowing you are an easy target, decides to take you to lunch. While at lunch he gets all sorts of information from you. You freely give out this information thinking that if the boss were here he would be so proud of me! I should get a good raise for this! The Cyber-Con has just read your mind. The two of you go back to the office and proceed to say your good-byes. Mr. So and So says thank you to all the people in the various departments. He especially thanks you for giving him your undivided attention. He hands you a fake business card and tells you to have your boss call him when he gets back from vacation. All the while you are thinking I AM AWESOME! What you do not know is that Mr. So and So is going directly back to his company to pass all the information he learned from you. His company will be the one who implements this new technology, his company will be the leading the way into the next millennium and he will be the one who gets the big raise. You in the meantime are looking for work in Siberia because that is the only place you can hide from the fact that you put your company out of business. This seems far-fetched but it has happened and will continue to happen in the future. While most types of Social Engineering take the form of human intervention, there are some that do not. Be weary of unknown e-mails, faxes, Java applications, chat rooms, and snail mail (US postal Service).

While snail mail is the oldest and slowest methods of communication, it is often quite effective. The Cyber-Con can rent a PO Box from a variety of mail stores. The equipment and overall cost of snail mail is relatively inexpensive. It is quite easy to hide and fake a business this way. It is important to remember that snail mail is not tapped. People are more likely to respond to a survey they receive in the mail. The survey could ask tons of information about you and your company. The survey will have a stamped envelope included so you will not pay to have it mailed back. The survey will even promise cash or other prizes for completed and returned surveys. By the time your company notices that this survey was a scam, the Cyber-Con has moved on to a different PO Box, under a different name, targeting a new company.

Regular e-mails or faxes can also prompt you to give away important company information. This type of Social Engineering happens, but not often. E-mails and faxes can be easily traced, so the Cyber-Con usually tries more covert methods. The newest type of Social Engineering is conducted over the World Wide Web, inside chat rooms, and with Java applications. Be cautious when logged on to chat rooms. Cyber-Cons are there looking to find their newest victim. It is not good practice to give personal and organizational information inside a chat room. People often disguise themselves when inside chat rooms, and often are not who they say they are. Java is probably the newest form of Social Engineering. Everyone can remember at one time or another a "pop up" widow when surfing the Internet. Often, these Java windows are asking for personal information, asking for surveys or just trying to force you into giving up information. A good example would be a Java pop up login screen. Dial-Up accounts are susceptible to this easy form of Social Engineering. For instance, while surfing, a pop-up window appears telling you have been logged off your ISP. It prompts you to re-enter your user name and password and then click the "ok" button. Once you do this, the information you typed was just sent to the Cyber-Con. BINGO! He/She now has your user name and password! As you can see, Social Engineering has many forms and techniques. Everyday there is a Cyber-Con person inventing new ways to obtain personal and proprietary information about you or your company. Can this be stopped? Probably not. There are numerous preventative measures companies can take to hopefully put a stop to the Cyber-Con game.

The most important step in helping prevent the Cyber-Con from stealing information is to EDUCATE all your personnel. One cannot overemphasize the importance of educating all personnel on the dangers of Social Engineering. Adding a section on Social Engineering to ones security policy is also a good idea.

The first key to countering Social Engineering is to put a limit on the amount of information available. Use a good encryption package such as PGP or PKI to protect your information from Cyber-Cons and internal employees. Do not advertise your internal network addresses by configuring your firewall to do so and make sure your DNS configuration does not display internal systems to an external query. Make sure all your Websites, public databases, Internet Registries, and Yellow Pages list only generic listings. Only give employee names instead of "DNS Zone Administrator", or "NT 4.0 System Administrator" Have a strict policy for internal and external help desk support. All callers should be required to provide some sort of identification before receiving support. Educate all employees on E-Mail safety, such as Viruses, Trojans, and MS Word macros. Have the system administrator disable Java on web browsers. This will help in stopping the Java pop up window attack to obtain passwords. One should also make sure their system stays current on all vulnerabilities. Upgrade as soon as new patches are released for your operating system and other network software and hardware.

The second key to deterring Social Engineering is to have good physical security. Good physical security to building access cannot be overemphasized. Keep a running log on who enters the facility. Have all employees wear identification badges and limit the number of employee's access to the different areas. There is NO need for finance personnel having access to the main server room and vice versa. Be wary what goes into the dumpster. Cyber-Cons have been known to "Dumpster Dive" to obtain information. Buy a good shredder to destroy important information. Make sure all old hard drives CDs, and floppy disks have been degaussed before putting them in the trash. Have a good surveillance system set up to monitor who goes where inside the building.

While all these examples will aid in the deterrence of Social Engineering, all will be naught if employees are not educated that it can really happen. To aid in education have annual education classes on the security policy and social engineering. Educate the employees everyday by hanging security placards throughout the office, have weekly news letters, log-on banners, and send security tips via e-mail. Punish those employees that purposely give out information. Praise employees that make a good catch in preventing information or security leaks.

Remember, Social Engineering happens everyday and will always continue. Although almost impossible to totally stop, it can be easily deterred. There is nothing wrong about being "over paranoid". Doing so my prevent information theft in the future. EDUCATE, EDUCATE and EDUCATE even more! If your people don't know what is going on, you will loose the battle and the Cyber-Cons will prevail. Deterring Social Engineering is a team effort. If ONE person on the team strays either by accident or on purpose, you will fail. It sounds harsh, but it is true.

Bibliography

Scabbray, Joel; McClure, Stuart; Kurtz, George "Hacking Exposed, Second Edition" Osborne-McGraw-Hill, 2001

Anonymous, Association of Certified Fraud Examiners, "News and Facts", URL: http://www.cfenet.com/newsandfacts/fraudfacts/index.shtml (February 15, 2001)

Fennelly, Carole," The Human Guide to Computer Security", Unix Insider. July 1999 URL: http://www.unixinsider.com/swol-07-1999/swol-07-security.html (February 8, 2001)

Computer Security Institute, "Social Engineering: Examples and Countermeasures from the Real-World", Anonymous. November 1999. URL: http://www.gocsi.com/soceng.htm (February 10, 2001)

CERT Coordination Center, "CERT Advisory CA-1991-04 Social Engineering" Carnegie Mellon University, 1991 URL: http://www.cert.org/advisories/CA-1991-04.html (February 15, 2001)

Unknown, HRSA Security Awareness Course, "Social Engineering" URL: **Learn more about how Java™ applets can be used for social engineering.**
(February 12, 2001)