Global Information Assurance Certification Paper

Security's Biggest Threats: Social Engineering and Your Employees

Thomas Houchins (v.1.4)

August 1, 2002

Introduction:

If you asked a Network administrator to define social engineering and give an example of it, chances are you'll get a blank look in return. When we think of network security, we think "inside the box" so to speak. Meaning administrators are focused only on the security of their physical networks.

With today's computer networks and desktops protected from the growing number of vulnerabilities, scans, and other security weaknesses, social engineering has become the biggest threat to network security professionals. As more attacks are blocked at the server, hackers have turned to social engineering as a way to extract information from employees to complete their attack.

"In order to counteract the increasing amount of computer software and hardware to prevent hackers from gaining entry into unauthorized systems, hackers have employed methods to bypass the technical systems altogether. Instead they attack the system at a possible weak point: the human operators."

Rick Nelson, Methods of Hacking: Social Engineering

This paper will discuss the following topics:

1. Definition of Social Engineering.
2. Reasons for using Social Engineering.
3. Social Engineering techniques used and explained.
4. Reverse Engineering used and explained.
5. Protection against Social Engineering.

Definition:

Social engineering can be defined simply as the process of gathering information through character weaknesses manipulation methods by a hacker without the targets awareness. Jonathan Yarden called social engineering, "The gaining of unauthorized access to a computer system without exploiting a software defect or weakness." (Yarden, 2002) Social hackers take advantage of a person's character weaknesses. "One thing that everyone seems to agree upon is that Social Engineering is generally a hacker's clever manipulation of the natural tendency to trust." (Granger, 2001)

How is this done? The process of social engineering involves taking advantage of a person's ability to trust, their laziness or their lack of attention to detail. "The ability to manipulate others is both a natural personality trait as well as a learnable skill." (Steward, 2002)

Hackers prey on the target's inability to protect the information they process. Many employees do not realize the importance of this information and unwittingly give up this information without much thought. Hackers will also take advantage of a person's natural tendencies to "help" others. This type of attack is prevalent with Help Desks. (Discussed later)

Reasons for using Social Engineering:

I mentioned briefly in the Introduction that today's networks are better protected than ever before. The reason for this is the heightened security awareness caused by the recent high profile attacks such as NIMDA and Code Red. As administrators were burned by these events, servers were made much stronger. As a result of these actions, hackers have a much more difficult time today breaking into servers. John McCormick states in his article Does your social plan neglect social engineering threats?, "Security consciousness is increasing and systems are being hardened, which makes standard hacking over the Internet more difficult." Experienced hacker Susan Thunder adds a message for all LAN managers, "Increased security measures make psychological attacks easier because users think data is safe." (Berg, 1995)

Another reason social engineering is popular today is its much easier and less time consuming than typical hacking methods. It's easier to pick up the phone and "play act" as a company security officer and ask a person working the Help Desk for information such as passwords. The turnover rate in today's corporate society is also part of the blame. With so many workers and temp employees moving around from job to job, security policies can fall through the cracks. This means a new employee may not know what is considered "common" operating procedure. The new employee that is not given the proper training will more likely than not provide the hacker some amount of "unauthorized" information. As you can see, a hacker's ability to exploit this vulnerability is very possible.

As a security professional, this can be very scary. Even if the whole network is patched and firewall protected a hacker can still trick a company employee into giving up the information you are trying to protect. McCormick adds, "The current business environment involves many new employees. From a more paranoid standpoint some of these new hires or temps may be hackers themselves."

An interesting point to add here is that social engineering can be learned. There are websites that "teach" social hacking. These websites give hackers advice on how to attack, what questions to ask, and how much information they need of the target's network to pull off this type of attack. One such site even states that the best way to attack the target is through a chat program or email.

Basically what all this means is people are the weakest link and hackers know it!

Who are the targets? Well no one is really safe but hackers usually are picky about their targets. They usually go after government or military agencies, the bigger more popular corporations, phone companies, and hospitals. I should mention again NO ONE is really safe. Just because you work at a small Internet start up doesn't mean your company will not be targeted. Keep your eyes open. I'll explain some things to look for later in this paper.

What is the social hacker's motivation? Very simply, a hacker can be motivated by political issues, environmental issues, or simply be mad over a large phone bill. Many hackers are in it for their own personal reasons. These reasons mostly center on money. "Hackers are usually involved when fraud scams, company bidding wars, and industrial espionage." (Anonymous, 1999)

Social Engineering techniques used:

Any experienced hacker will take steps to improve his chances of getting the information he seeks. Preparation starts with the hacker doing research and perfecting his skills. He learns his skills by reading books on computers, books on influence (manipulation) techniques, Psychology books, and television shows. All these techniques teach the hacker how to think fast on his feet and how to communicate with the purpose of getting information out of their target or to gain access to their target. "Interpersonal communication predicts trends in the way people speak. It's amazing to see what kinds of things we do and how much pattern there is." (Bernz)

Attacks using the telephone are the most popular. The process is quite simple. The attacker will call up and pretend to be someone else. The person that is imitated can be anyone; an employee on vacation, a high level executive's secretary, or a person from the IT department.

An example of this technique would be the following:

Hacker: "Hi, this is Joe from the IT department. I'm in charge of doing a security audit of all usernames and passwords in our system. Can you tell me your username and password so I can compare it to my list?"

Seems a bit far fetched but it will work if the attacker gets the right person at the right time. A perfect time to call with this attack would be late in the afternoon one Friday right before the target is about to leave. The last thing the target wants to do is sit there and be kept from their weekend. So instead of taking a moment and thinking about what was just asked they will give this information away because they are officially off work for the week.

Another popular attack is to use a company's PBX (internal phone system) to call long distance around the world. The attack happens when the hacker calls in and does his best imitation of a company user and then requests to be transferred to an outside line. Once they have been given an outside line they can make phone calls all over the world and the calls will be charged to the target company.

Perhaps the weakest and most vulnerable phone target is a company's help desk. The reason this is the most vulnerable to a phone attack is that the help desk employee is there to "help". They are there to give as much support as possible for a variety of computer issues. Along with this support, they have a lot of valuable information at their fingertips. To expand on this, John McCormick states, "These employees hear the same problems day after day and offer help based on some reference." He adds that in all likelihood the help desk technician has all possible trouble shooting information in some sort of book, on-line database or other form (procedures).

Looking back on my career as a help desk technician, I realize now how simple it would have been for someone to take advantage of my willingness to help or "right a wrong." Now as a security analyst I see how weak and vulnerable the helpdesk is even with procedures in place.

The phone can be used many other ways to get the hacker the information he needs. Another way is to call the help desk with an "urgent" request. The request would be something like this:

Hacker:"Where's Mary? She promised me so and so information to be given to me last night. Is it possible for you to fax that information right now? I've got to hand in this information to my boss in the next 5 minutes."

This attack is another example of a hacker taking advantage of the help desk employee's willingness to help. One of the most important parts of an employee's job is to offer the "customer" a satisfactory experience. Most of the time this attack would not work if the employee were at work that day. This takes us back to the beginning of this segment when I spoke about all hackers doing their homework. They know when to call and who to pretend that they spoke too. It could be that the hacker knew yesterday was Mary's last day before her vacation to Las Vegas. How would the hacker know that information? Simple the hacker placed a "setup" call the day before and happened to get Mary.

Based on my research there are many other examples of using the phone for social hacking. Posing as an employee of another department and calling to get an executive's phone number. Calling the HR department and requesting a list of all new employees hired in the last month. Using the information that was given to him by HR, the hacker was able to contact these new employees and offer security assistance. Information gained such as type of operating systems platforms the employees were using can be very valuable to any hacker. Then by using a war dialer along with placing a call to the help desk, the hacker can gain access to the phone numbers assigned to the company's modems. With the modem information, the hacker can then gain backdoor access to the target's computer network.

Other ways to use the phone for social engineering is by pretending to be a new employee and calling other users for help, pretending to be an executive of a company and demanding certain information from a system administrator, or posing as an IT technician and asking a user to type dos commands over the phone.

To sum up, the phone is a hacker's best friend when trying to elicit information from an unsuspecting employee or help desk technician. Because its human nature to "help", many an employee has been taken advantage of before they realized what had happened.

Another type of social engineering attack that a network administrator should be aware of is email. This type of attack isn't that popular but when lucky, the unsuspecting target will either give up valuable personal information or allow a hacker a backdoor into their network. When you have unsuspecting employees who have a habit of clicking and opening everything in their email inbox, your job becomes a viscous cycle. Once a computer is infected with a backdoor virus, unless the employee knows the symptoms, which most don't, the hacker can have access for an unknown amount of time before you even catch on. The sad part is a lot of the time it's usually too late. By the time you have gotten this malicious activity halted the employee has clicked another email of a similar type.

Gaining credit card information doesn't happen as much on the business front as it does on the home front, but it's not unlikely that it could happen. A hacker sends a fake email from a known supplier of the target company stating that they have lost the accounting information for the company and would like a call to verify the information. Once the unsuspecting person calls, a hacker can manipulate the employee to giving them phone numbers, addresses, email account information, and possibly the company credit card information.

A less often used attack is when hackers cause a company's email server to become backed up by sending out chain mail or hoax emails. The hacker simply writes in the email that there is a new virus out in the wild and to have your employees forward the email to all their friends and co-workers. As you can imagine, this will create quite a log jam with the amount of email passing though the company's exchange server.

The Internet is no safer. It is also more geared towards the home user as opposed to the business employee. Basically this type of attack is run against your internet service provider's like AOL, CompuServe, or MSN. The hacker will send a message stating there has been a problem with an internal system on the ISP network and some user account information has been lost. The message will prompt the target to a website where the "validation" of the information will take place. According to Richard and Claudia Lowe, this type of attack is very common. "This is a very common way to fraudulently gain credit card, passwords and account numbers." (Lowe, 1999)

Another very popular social engineering attack is called "dumpster diving." It's hard to believe how much valuable information a hacker can obtain just by looking through one employee's trash. Items such as company letterhead, internal phone books, calendars, and post-it notes can give a social hacker all the information he needs to begin the real attack. Think about it: A company's letterhead can easily be forged. Internal company phonebooks not only give the full name of employee's but more importantly their titles. Now with just the company letterhead and the phonebook a hacker has all the information he needs to place that phone call to the help desk or forge a letter requesting network information. Calendars give the hacker clues on when an employee is on vacation, information on company holidays, and employee holiday schedules. Post-it notes can give the hacker a system administrator's login information, the IP addresses of company internal Internet websites, company file locations and names, and unpublished customer names or contact information.

I've just mentioned a few. Al Berg has listed some other material a hacker can find and use when dumpster diving, "Organizational charts, company policy manuals, system manuals, printouts of source code, disks and tapes, and outdated hardware (especially hard drives)."

Organizational charts can give the hacker information on the target company's management hierarchy. This information is very similar to internal phonebooks. Policy manuals provide the hacker with a company's Standard Operating Procedures. With this information the hacker can gain information on how to proceed with his social hacking either via the phone or email. System manuals provide technical information of your network devices and layout. This information can be used on an unsuspecting help desk employee because it gives the hacker "validity". Source code gives the hacker an easy way to find security weaknesses in your code. It can also provide another name for the hacker to use when calling: the web developer. Computer hardware disks and tapes can provide copies of the network settings and software being used. Information from old disk and tapes can be restored which makes them very dangerous if care isn't taken when these items are thrown out.

Another physical attack social hacker's use is disguises to gain access into buildings. Hackers can also make fake badges, which can fool company personnel into allowing them access to restricted areas. What's to stop a hacker from dressing up as a UPS delivery man or a nightly cleaning worker, or dressing up as a SUN technician and conning his way into a data center? The point of this is hackers can find new ingenious ways of getting onto your company's premises. In an article written by Sharon Gaudin called Social Engineering: The Human Side

of Hacking, TruSecure director of risk assessment Paul Robertson states this eloquently, "If you (hackers) dress in brown and stack a whole bunch of boxes in a cart, people will hold the door open for you because they think you're the delivery guy." Robertson adds, "Sometimes you grab a pack of cigarettes and stand in the smoking area listening to their conversations. Then you just follow them right into the building."

One of my favorite eye opening recounts of a physical attack appears in an article by Jason Hiner. In Hiner's article, Change your company's culture to combat social engineering attacks, a consultant was hired to try and bypass a company's defenses against an outside intruder. The consultant created a fake ID and was able to gain access into the building. The consultant continued his unadulterated trek through the building until he came to the company's data center. Upon many failed swipes of his fake ID badge, another employee swiped his card and allowed the consultant into the data center. Once inside the data center, the consultant asked all the employees to leave because he was doing a surprise security audit. Guess what, they all left!

I stated the story because it really brings home how easy a hacker can gain access to unauthorized areas with a little help from "friends". Way back at the beginning off this paper, I mentioned that the human factor is the weakest link in security. In all the examples I have mentioned regarding social engineering attacks, the one constant security weakness exploited has been the employee. The alarming part of this story is that there were many interpersonal events with employees that could have stopped the consultant's advance.

Still more physical social engineering techniques are: looking over the shoulder of an unsuspecting employee to retrieve passwords or other important data. Another is watching the behavior of office employees and their reactions to certain stimulus like a fire drill.

We can't talk about social engineering's impact on your security defenses without mentioning reverse social engineering.

Reverse Social Engineering:

According to Rick Nelson, reverse social engineering is a superior form of social engineering. He describes reverse social engineering as, "a legitimate user of a system asking the hacker questions for information." As you can see the hacker has been placed in a position of authority to help the target. These types of attacks are very hard to pull off and usually require previous access to the target's systems and networks and great amounts of research and planning. Nelson adds, "In order to pull off an RSE attack, the hacker must be knowledgeable of the system and usually must also have previous access granted to him." This is usually accomplished by normal social engineering methods.

A typical RSE attack would consist of three steps: sabotage, advertising and assisting. Sabotage occurs after the hacker has gained access to the target's network and machine. What usually occurs is the hacker will corrupt the settings to give the look of a machine that is not functioning properly. Once the target discovers their workstation is corrupted, they seek help. The next step of this type of attack is marketing. Since the hacker knows the system is corrupt, he wants to ensure that the target contacts him for the resolution of the problem. A hacker can advertise by leaving his calling card on the bulletin board or front desk. Basically the hacker will place the card anywhere that the target will look for information. Another way to

advertise is for the hacker to place their contact information in the actual error the target's corrupt machine displays. Nelson gives a great example of such an error message: "**ERROR 03 – Restricted Access Denied ** - File access not allowed by user. Consult with Mr. Downs at (301) 555-1414 for file permission information." The final step of a RSE attack is assisting. Once the target contacts the hacker for assistance to the problem, the social engineer's goal is to ensure that the target is "clueless" to their information seeking while the assistance is taking place.

Here are some differences between a social engineering attack and a reverse engineering attack: Social Engineering requires the hacker to place a phone call and the attack is carried out with the assistance of the target. With reverse social engineering, the target actually calls the hacker for assistance. In social engineering attacks, the target is left with many unanswered questions. With reverse social engineering, the target assumes that everything is ok because all questions were answered and the problem is fixed. As Nelson puts it, no "lose ends" were left behind. Finally the most important difference between the two attacks is control over the flow of information. When social engineering is used the target has control of the flow of information. With reverse engineering the hacker has total control over the flow of information.

Again the most important thing to remember about reverse engineering is the target depends on the hacker for a solution to the problem at hand. The hacker controls the flow of information causing communication to occur more freely and not appear as suspicious.

Protection against Social Engineering Attacks:

The first step in protecting your company is to test you defenses. The best way to accomplish this is to test the ability of employees to work together. John McCormick states, "The biggest problem is balancing security with the need to have employees cooperate and work well together. " The employees of every company are the first and only line of defense against social engineering attacks. Inter-department communication should be a high priority.

As a Network Administrator, it is important to think about where you're company's most important information is stored. What are the threats to this information? Who is your company's biggest threat? Remember the social hacker has many motivations for hacking. Involve management to help decide what would be the best course of action that should be taken. After this has been determined, arrange tests of your current defenses protecting the information. Involvement of management will ensure that they are aware of any breakdowns in your company's defensive strategies. Listed below are a few of the many ways to test your defenses:

Social engineering phone test: Have an employee with an unfamiliar voice call in and try to extract information. E-mail attacks: Try to get an employee to open a new account with a new password using email with the internet. Recycling data: Try dumpster diving for information. See for yourself what is in your garbage.

In Sarah Gaudin's article, Social Engineering: The Human Side of Hacking, Eddie Rabinovitch, vise president of global networks and infrastructure operations at Cervalis LLS, states about security training, "People are looking for information, They're always looking for new ways to get at that information. In many cases, you can deal with it with tools, but it always comes down to procedures and your people."

If any of the above defense tests reveal unauthorized company information, the next step is to train your employees on social engineering and the social hacker's tactics. One excellent way is through the implementation of classes for new employees as well as "refresher" classes for current employees. The training should include the proper methods of notification to groups being targeted during social engineering attempts, also employee recognition of social engineering methods, and proper employee response as well as proper escalation procedures for combating social engineering attempts. One of the least thought about aspects in today's corporate business environment is how good company communication along with proper training can be effective in preventing further social engineering attacks.

Security policies are another way to test your defenses. If your company already has a written security policy (which it should), then test the written policy. Find weaknesses by testing against all known social engineering methods (both physiological and physical) over and over. Sarah Granger brings up another very important reason for a well-written security policy. "One of the advantages of policies is that they remove the responsibility of employees to make judgment calls regarding a hacker's request." The goal is to create clear and detailed instructions for help identifying an attack and escalation procedures for who should be contacted if an attack has been spotted. A good security policy should include instructions on user network access control and approval, setting up new user accounts, as well as account password changes. Others include intranet security procedures, locks, ID's, shredding of important company documents, storage of important company documents, and most importantly after-hours or weekend company policies. Make sure your company is protected during all shifts. Think about this last statement for a minute. Most cleaning crews come into your office late in the evening when most or all employees have gone home.

Defensive tactics implemented by your security policy should consist of the following items to ensure proper protection of your network. Employees should be using a paper shredder to prevent a hacker from using the trash as a source of information. All discarded computer hardware should be erased to protect data from being retrieved. The physical location of company dumpsters should be securely located and protected by security cameras. All new employees need to have vigorous background checks done on them. All temporary employees should be screened before they are allowed access to computers on your network. A clear reporting process should be in place for documenting security problems. Employee behavior should be monitored for suspicious activity and access violations. Former employees should be prevented from entering the company premises without a company escort. This also should be the case for any contractor visiting the company.

Additional Security recommendations to be aware of include keeping all server rooms, telephone closets and other locations containing important information locked. Inventory all equipment in these locations. Occasionally check and make sure all are there and no additional machines were added. Another way to improve security is to pay your help desk and security personnel well to lower the turnover rate. The use of biometrics will add additional security by limiting access to locations. Biometrics is a very hard technology to falsify currently and is recommended.

We have talked so far about protecting mostly the physical premises from social engineering now we need to talk about protecting your company and employees from social hackers over the phone and email as well. A good security policy should have guidelines on what company business can and can not be discussed over the phone or e-mail. Information about your network should never be given out over the phone, via e-mail, instant messenger, or news

groups. Security policies should address the discussion of company information outside of work also. Employees have a tendency to "run" their mouths about certain happenings at work. It's very important to remind employees of company disclosure agreements. An example would be a group of network engineers going out on a Friday night. After a few drinks they start talking about the weaknesses of your company's network. Social hackers will certainly know where to go to eavesdrop on company employees with "loose lips".

Company passwords should never be given out over the phone or email. Train and test employees to make sure they are aware of company procedures regarding passwords. A good password policy would be to have employees never discuss their passwords over the phone. They should be aware that under no circumstances, should another employee contact them regarding their password. In other words have employees be suspicious regarding all passwords. They should be considered private to each user and not shared with anyone. Training should also include which department company employees should turn to for these requests. Employee awareness also plays a role in password protection. Lee Schlesinger states in his article, Your biggest threat, "The only option for preventing social engineering intrusions is awareness. Learn the perpetrators' secrets." Schlesinger adds training employees to recognize the warning sign's is vital. Train employees to trust their "hunches" regarding any requests from callers. If any employee feels uncomfortable regarding any request, chances are their instincts will be proven right more often than wrong.

Other important phone security procedures to consider are to train employees to never give any company information to the caller if the employee cannot personally identify the caller. This is also a good policy to use if the caller begins to ask personal questions regarding the company's network or personnel. The best bet is to take a name and number then call the person back. What will happen quite often is the employee will be given a false name and call back number.

Help Desk employees need to be trained on social engineering tactics the most. Personnel should be aware of calls coming from the "outside" where the caller has identified themselves as company employees and requests an outside line. Most PBX systems have a different ring or tone that differentiates internal calls from an outside call. Make the help desk employees aware of the different rings and what they represent. Another safeguard is to verify all valid employees before any information is given out. A great way of doing this is to make sure the help desk employees have an up to date roster of all company employees. Once the name of the employee has been found, the help desk personnel will call the employee back on their internal extension. Another security recommendation is giving all employees a PIN number to be used when calling the help desk. Don't allow employees to leave voice mail or email stating they are on vacation or out of the office. Have the employees notify the help desk regarding time out of the office. Reinforce security training by providing employee newsletters, e-mail reminders, and training games.

A major security concern for administrators and security personnel are those pesky instant messenger programs. Not only do most of them search and find open ports on the firewall but they can allow Trojan like programs to invade your network. Get your development team to create an internal instant message program. This will prevent those outside influences that endanger your network on a daily basis.

Email is another concern. Protect your network by teaching employees the signs of possible bad email attachments (.vbs or .exe). Another way to protect your network is to prevent

attachments all together by blocking them at the firewall. If this is not possible then you are going to have to rely on your company employee's instincts. I mentioned earlier that your worst nightmare is a computer illiterate user who just clicks any inbox email without a clue. This is how the Melissa virus and the great Happy99.exe file affected a lot of companies. Train company employees to not open email attachments from anyone without scanning the attachment for a worm or virus with anti-virus software. This doesn't matter if the email sender is internal or external because internal email accounts could be affected also.

Summary:

Social engineering has become one of the most popular attack methods hacker's use today. Because of heightened security awareness, social engineering in many cases is easier and less time consuming than typical computer hacking. Social engineering doesn't just focus on your company's physical weaknesses; it focuses on your employee's character weaknesses also. Make employees aware that social engineering is an everyday occurrence. Train them to recognize signs of any suspicious activity. Educate them on any new security policies or social engineering attacks that may be used. Provide them with positive feedback and company literature to reinforce their security training.

Test your company's defenses. Make sure your company is equipped to handle all types of attacks. Make the necessary security policy changes once an infraction has occurred. Create a concise security model that allows for constant revision because the social hacker will find new ways to penetrate your network. Finally remind all employees that together and only together can your company defeat the social hacker.

Bibliography:

Anonymous. “Social Engineering: examples and countermeasures from the real world”. Computer Security Alert, CSI’s monthly newsletter. November, 1999
URL: http://www.gocsi.com/soceng.htm.

Berg, Al. “Cracking a Social Engineer”. November 6, 1995
URL: http://packetstorm.decepticons.org/docs/social-engineering/soc_eng2.html.

Bernz. “Bernz’s Social Engineering Intro and stuff”.
URL: http://packetstorm.decepticons.org/docs/social-engineering/socintro.html .

Gaudin, Sharon. “How to Thwart the Social Engineers”. May 10, 2002.
URL: http://itmanagement.earthweb.com/secu/print/0,,11953_1041161,00.html.

Gaudin, Sharon. “Social Engineering: The Human Side of Hacking”. May 10, 2002.
URL: http://esecurityplanet.com/trends/print/0,,10751_1040881,00.html.

Granger, Sarah. “Social Engineering Fundamentals, Part I: Hacker Tactics”. December 18, 2001.
URL: http://online.securityfocus.com/infocus/1527 .

Granger, Sarah. “Social Engineering Fundamentals, Part II: Combat Strategies”. January 9, 2002.
URL: http://online.securityfocus.com/infocus/1553 .

Hiner, James. “Change your company’s culture to combat social engineering attacks”. May 30, 2002.
URL: http://www.techrepublic.com/article.jhtml?id=r00220020530hin01.htm&src=search.

Lowe, Richard & Arevalo-Lowe, Claudia. “Social Engineering: More about Social Engineering”. 1999
URL: http://internet-tips.net/Security/social01.htm.

McCormick, John. “Does your security plan neglect social engineering threats?”. April 8, 2002.
URL:
http://www.techrepublic.com/printerfriendly.jhtml?id=r00220020408mco01.htm&rcode=

Nelson, Rick, “Methods of Hacking: Social Engineering
URL: http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html.

Schesinger, Lee. “Your biggest threat”. April 1, 2002.
URL: http://zdnet.com/filters/printerfriendly/0,6061,2859492-92,00.html.

Steward, James Michael. “Thwarting social engineering attacks”. March 5, 2002.
URL: http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci805450,00.html.

Yarden, Jonathan, “Don’t tolerate social hacking”. July 15, 2002.
Internet Security Focus @Builder.com. Online Security Newsletter.