

Social Engineering – Can Organizations Win the Battle?

Terry Turner

East Carolina University

Abstract

According to Gartner Research, the greatest security risk facing large companies over the next ten years will be the increasingly sophisticated use of social engineering to bypass IT security defenses. Social engineering is best used to circumvent internal controls. Social engineering attacks can be behavioral or psychological. Behavioral tactics could be dumpster diving, shoulder surfing or learning about a company by reading public documents. Psychological tactics can be regarded as “people hacking” or the exploitation of the human factor. This paper discusses social engineering attacks using psychological tools to legally gain information about a company that would result in unauthorized access or unauthorized use to an information system, network or data. Recognizing social engineering traps are necessary in defeating the social engineer or people hacker. Techniques are presented that will improve employees abilities to recognize when someone is trying to gain information from them. Lastly, the paper presents measures to promote the awareness of social engineering and methods to employ to secure against human attacks.

What is Social Engineering?

A CEO of a company goes on vacation. The day after he leaves, a consultant, wearing a suit, carrying all the right references, walks in the door of the office and says, Mr. Johnson hired me and asked me to take a look at your engineering plans. Apparently, there was a technical problem. Someone says, Oh, he just went on vacation, he's not here. The consultant responds: Well, you know, I came from out-of-town, I'm only here for basically the one day. This is pretty important, and, frankly, you guys already paid me a lot of money. Is there anyone I could talk to about this? So this person sits down, spends an entire day going over the engineering plan, and walks out with copies because there are some issues that he needs to work on later. Meanwhile, the CEO gets back from vacation and says: What consultant? (D'Agostino, 2003)

People are, by nature, unpredictable and susceptible to persuasion and manipulation. Social engineering is the most difficult security issue to manage and most IT departments do a poor job of combating the threat. (Mogull, 2004). Risk associated with social engineering is extremely high. Insiders tend to divulge valuable information to the social engineers posing as genuine recipients of information. Therefore, security must begin in the user's mind and cannot be embedded in the technology alone. If an employee in possession of a vital resource divulges it unknowingly, the entire security architecture could be ruined.

If you can read this paper, at some time in your life, probably several times, you have been manipulated into unconsciously providing information or changed your behavior and did something you would not normally do. Social engineering is the age-old art of human persuasion. It uses deception to con someone into providing information or access they would not normally have provided. People are manipulated, rather than machines, to successfully breach the security systems of an enterprise. People, by nature, are unpredictable and susceptible

to manipulation and persuasion. Studies show that humans have certain behavioral tendencies that can be exploited with careful manipulation. (Kotadia, 2004).

Exploiting human nature.

From an interview of Kevin Mitnick, an infamous hacker in the 1980s and 1990s, with the BBC News Online 6: The biggest threat to the security of a company is not a computer virus, an unpatched hole in a key program or a badly installed firewall. In fact, the biggest threat could be you. What I found personally to be true was that it's easier to manipulate people rather than technology. Most of the time organizations overlook that human element. (Mitnick, 2002).

Exploiting human behaviors such as trust, helpfulness, or ignorance can lead to security breaches. Humans desire to trust others and can be too trusting of others without good reason. Every honest person assumes that others are similarly well intentioned. A very competent social engineer can make a target trust him or her to such an extent that the worker casually gives out sensitive internal information. It may not be a significant disclosure in and of itself, but the information gleaned by such manipulation can easily be combined with other small bits of information to produce a detailed and dangerous roadmap to our organizational riches. Hackers take advantage of peoples' ignorance because people may be ignorant about the consequences of being careless with information. Employees ignoring correct procedures related to an information system may use it incorrectly, causing integrity problems within the system. Just about everyone likes to be helpful, especially in times of need.

Example: It is 8 pm on Friday evening, and Employee A is working on resolving a critical problem in the Personnel computer system, and is called away by an emergency at home. Employee B, who has been upset with his manager, offers to help out, and work on the problem. However B does not have access to the system, and there is no time to go through the proper channels to request the access for B. So A gives B his ID and password, without realizing that B has an ulterior motive in offering to help. When A is fighting fires at home, B has access to the

network, the database and anything else that A has access to. B can now do what he wishes, and even better, he can do it without having his identity revealed in the process. (Gulati, 2003)

In the example, the helpful employee reveals his password and the intruder posed as being helpful in a deceptive approach to gain access to the network.

Social engineering depends on an understanding of human behavior, and on the ability to persuade others to release information or perform actions on the attacker's behalf. Persuasion itself is an art and a science; studies show that humans have certain behavioral tendencies that are exploitable via careful manipulation. Some individuals possess a natural ability to manipulate, while others develop the skill through practice using positive (and negative) reinforcement. Social engineering attackers play on these tendencies and motivators to elicit certain responses in the target. For example:

- Fear of job loss or personal embarrassment may cause an individual to release proprietary information if he or she thinks it will prevent the unwanted result.
- Desire for prestige can be stimulated to induce bragging, often resulting in information release.
- Overworked and tired employees tend to make mistakes, and it's often possible to predict when people are more likely to be susceptible to manipulation (e.g., end of month, end of quarter or lunch hour).

Consider the well-known quote of Bruce Schneier, CTO, Counterpane Internet Security, Inc., "Always remember: Amateurs hack systems. Professionals hack people." Once experienced hackers decide to commit a social engineering attack, things quickly escalate to alarming levels. It may be worthwhile to note that social engineering is not an impromptu attack, but requires a tremendous amount of preparatory work. (Damie, 2002)

Persuasion tools.

The hackers themselves teach social engineering from a psychological point-of-view, emphasizing how to create the perfect psychological environment for the attack. Basic methods of persuasion include: impersonation, ingratiation, conformity, diffusion of responsibility, and plain old friendliness. Regardless of the method used, the main objective is to convince the person disclosing the information that the social engineer is in fact a person that they can trust with that sensitive information. The other important key is to never ask for too much information at a time, but to ask for a little from each person in order to maintain the appearance of a comfortable relationship.

Impersonation generally means creating some sort of character and playing out the role. The simpler the role, the better. Sometimes this could mean just calling up, saying: “Hi, I’m Joe in MIS and I need your password,” but that doesn’t always work. Other times, the hacker will study a real individual in an organization and wait until that person is out of town to impersonate him over the phone.

Some common roles that may be played in impersonation attacks include: a repairman, IT support, a manager, a trusted third party (for example, the President’s executive assistant who is calling to say that the President okayed her requesting certain information), or a fellow employee. In a huge company, this is not that hard to do. There is no way to know everyone - IDs can be faked. Most of these roles fall under the category of someone with authority, which leads us to ingratiation. Most employees want to impress the boss, so they will bend over backwards to provide required information to anyone in power. Here again, exploiting the human tendency to be helpful.

Conformity is a group-based behavior, but can be used occasionally in the individual setting by convincing the user that everyone else has been giving the hacker the same information now requested, such as if the hacker is impersonating an IT manager. When hackers attack in such a way as to diffuse the responsibility of the employee giving the password away, that alleviates the stress on the employee.

When in doubt, the best way to obtain information in a social engineering attack is just to be friendly. The idea here is that the average user wants to believe the colleague on the phone and wants to help, so the hacker basically only needs to be believable. Beyond that, most employees respond in kind, especially to women. Slight flattery or flirtation might even help soften up the target employee to co-operate further, but the smart hacker knows when to stop pulling out information, just before the employee suspects anything odd. A smile, if in person, or a simple “thank you” clinches the deal. And if that’s not enough, the new user routine often works too: “I’m confused, (batting eyelashes) can you help me?” (Granger, 2001)

Peripheral routes to persuasion.

In any situation where one person seeks to persuade another to do something, social psychology has identified two alternative routes that the persuader can employ. A central route to persuasion marshals systemic and logical arguments to stimulate a favorable response, prompting the listener or reader to think deeply and reach agreement. A peripheral route to persuasion, in contrast, relies on peripheral cues and mental shortcuts to bypass logical argument and counterargument and seek to trigger acceptance without thinking deeply about the matter. As every scheme to defraud necessarily involves the offering of goods or services in ways that misrepresent their objective qualities and features, the principals in the scheme can never afford

to use a direct route to persuasion, and therefore invariably fall back on methods using peripheral routes to persuasion. (Rusch, 2000).

In a recent stock-trading fraud case, the attacker's key task was to persuade the victim to act. Rather than use direct logical arguments, he had to use peripheral routes to persuasion, which aim to gain acceptance without the victim thinking too much about it. The suspect had to disguise and completely misrepresent the functionality of a financial charting tool, while focusing the victim on its potential benefits, without questioning or testing either the tool or person who offered it. The hacker, allegedly employed the following peripheral techniques, which psychologists say are likely to persuade individuals:

- **Authority:** People can be highly responsive to assertions of authority. By representing himself as a software developer, the hacker could assert authority as a purveyor of a valuable and safe tool to download and install. People tend to listen and heed the advice of those in a position of authority.
- **Similarity:** People respond favorably to others with like interests. People generally look to other people similar to themselves when making decisions. The hacker and victim met in a newsgroup and shared similar investment interests. The victim thought the hacker had to be okay because they were interested in similar investments.
- **Reciprocity:** People are strongly inclined to provide something in return. Because the hacker favored the victim and gave him the opportunity to try out a beta-version tool, the victim felt he should return the favor by evaluating the tool.

- **Scarcity:** People can be highly responsive to items that are in limited supply. In this case, the hacker allowed the victim the use and profit from a tool that was not generally available. (Morrison, 2004).

Attacks on the Psyche.

There are four general categories of social engineering attacks. Psychological tools are used in each category and behavioral tools are employed in specific situations.

- **Technical Attack:** There is no direct interpersonal contact with victims. The attacker forges e-mail messages, pop ups, web sites, or some other medium. The attacker pretends to be an authorized support or system administration person attempting to legitimize the request and tries to obtain sensitive account information from users (e.g., passwords, user-ids, CC #s, PINs etc.). This type of attack has been very successful to date.
- **Ego Attack:** The attacker appeals to the vanity, or ego of the victim. Usually targets someone they sense is frustrated with their current job position. The victim wants to prove how smart or knowledgeable they are and provides sensitive information or even access to the systems or data. The attacker may pretend to be law enforcement, the victim feels honored to be helping. The victim usually never realizes what happened.
- **Sympathy Attack:** The attacker pretends to be a fellow employee (new hire), contractor, or a vendor, etc. There is some urgency to complete some task or obtain some information

The attacker pretends to need assistance or they will be in trouble or lose their job etc.

This attack plays on the empathy & sympathy of the victim. The attackers “shop around” until they find someone who will help. This method of attack is usually very successful.

- **Intimidation Attack:** The attacker pretends to be someone influential (e.g., authority figure, law enforcement). The attacker attempts to use their authority to coerce the victim into cooperation. If there is resistance they use intimidation, and threats (e.g., job sanctions, criminal charges etc.). If the attacker pretends to be Law Enforcement, they will claim the investigation is hush hush and not to be discussed etc. (Rogers, 2001).

Spotting a Social Engineering Attack

Obviously, in order to foil an attack, it helps to be able to recognize one. The Computer Security Institute (CSI) notes several signs of social engineering attacks to recognize: refusal to give contact information, rushing, name-dropping, intimidation, small mistakes (misspellings, misnomers, odd questions), and requesting forbidden information. Look for things that don't quite add up. Train employees to think like a hacker. Recommend that employees familiarize themselves with works such as the Sherlock Holmes stories, *How to Make Friends and Influence People*, and other psychology books. To understand the enemy, one must think like him. (Granger, 2001).

Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company. Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information. (McDowell, 2004)

Resistance Techniques.

Dealing with social engineering threats to users is a straightforward matter of establishing administrative controls, policies, and procedures. To obtain acceptable levels of compliance with

these policies and procedures and make them effective, an organization should maintain ongoing programs against social engineering as part of its control environment. Such programs should provide intense and focused training to personnel whose job function is to be cooperative and helpful, such as help-desk staff, customer service representatives, and business and executive assistants. The training curriculum should fight fire with fire against the social engineers by employing resistance-training techniques to:

- Dispel employees' illusion of invulnerability by showing them that they can be easily victimized by social engineers. This will make them more resistant to persuasion.
- Warn employees about and explicitly demonstrate social engineering techniques intended to deceive and manipulate them.
- Give employees a list of common arguments used by social engineers and strong responses employees can employ against them. (Morrison, 2004)

Secure the People

The bulk of your company's IT security budget should be invested in the single biggest and most glaring security hole in your entire organization: your end users. Doing that will be protecting your pricey IT infrastructure and the priceless information it contains better than all the other technology combined.

The Ernst & Young Global Information Security Survey last year revealed that end-user security training was the No. 1 problem inside large organizations. Yet less than half of the respondents said their companies had a formal training program to meet that threat.

Most companies feel they've trained workers if they've sent them an e-mail with a list of do's and don'ts. Some include a five-minute bit of slideware as part of new-employee orientation.

Neither approach is worth much. You might as well tell workers, "We just don't care that much about IT security. Do whatever you want."

How stupid is that?

Martin Bean, chief operating officer at New Horizons Computer Learning Centers, says companies "only pay lip service" to end-user security training. And, he adds, when he talks to the boards of directors at major companies about securing their IT infrastructures, "the toughest part of the conversation is about the need to retrain every single employee" to be secure computer users.

Many IT folks like to believe that all problems created by technology can be solved with more technology. In many cases, sad to say, it's true. But not this time. Technology is a small part of the security solution. People are the big part. (Hall, 2005).

Companies can help to ensure security by conducting ongoing security awareness programs. Organizational intranets can be a valuable resource for this approach, particularly if on-line newsletters, e-mail reminders, training games, and strict password changing requirements are included. The biggest risk is that employees may become complacent and forget about security. Continued awareness throughout the organization is the key to ongoing protection and establishing a security conscious culture within the company.

Increasing the odds for success.

Changing the psychological response of employees, as it relates to social engineering, can be a daunting task for any large organization. In essence, you are asking employees to be less trustful and less helpful in situations where employees are being asked to provide information. Companies should proactively orient their employees toward the notion that "questioning" is part of the security process. This change goes against basic human nature to

trust and to help. Employees need to be convinced that information security is good for the organization, good for them, and then effective, long-term behavioral change will occur. A more responsible and vigilant security culture within the organization will develop.

Test your security awareness program. Generally tests of system security have focused on hardware and software vulnerabilities. Remember, users are considered the weakest link in the security system. Test your system against social engineering attacks. Do your employees readily give out information over the phone? Do they attempt to ascertain the legitimacy of a call? (Garceau, 1997).

Conclusion

Social engineering is a serious problem and is one of the greatest security threats to enterprises. As technology continues to raise the level of enterprise security, more hackers will turn to social engineering using psychological tactics. Hackers know that the best way around any security system is to manipulate a human target into giving them what they want. A trusting employee may provide information to a hacker, skilled in social engineering techniques, and your company's latest security defenses can become useless. Security conscious employees are the most effective methods to defend against internal and external social engineering attacks.

Security awareness training and education is the most important aspect of preventing social engineering attacks. Educate employees to the perils of social engineering and to recognize when a social engineering attack may be occurring. This is key to avoiding social engineering attacks. A security awareness program should be continuous and dynamic. A continuous program will benefit your organization for the long term. Organizations can reduce the impact of social engineering attacks by implementing this security strategy.

References

- D'Agostino, D. (2003) *What is Social Engineering*. Retrieved June 21, 2005 from CastleCops web site: <http://castlecops.com/article2934.html>
- Chin, P. (2003). The Spy Who Flubbed Me: Intranet Security Begins with Education. *The Intranet Journal*. Retrieved July 3, 2005 from The Intranet Journal web site: http://www.intranetjournal.com/articles/200312/ij_12_12_03a.html
- Damie, P. (2002). How Social Engineers Fool. *The Hindu Business Line*. Retrieved July 3, 2005 from The Hindu Business Line web site: <http://www.blonnet.com/mentor/2002/05/06/stories/2002050600571000.htm>
- Garceau, L. (1997) The Threat of Social Engineering. *The Ohio CPA Journal*. Retrieved June 21, 2005 from HighBeam Research web site: <http://www.highbeam.com/library/index.asp>
- Granger, S. (2001). *Social Engineering Fundamentals, Part I: Hacker Tactics*. Retrieved July 1, 2005 from SecurityFocus web site: <http://www.securityfocus.com/infocus/1527>
- Granger, S. (2002). *Social Engineering Fundamentals, Part II: Combat Strategies*. Retrieved July 1, 2005 from SecurityFocus web site: <http://online.securityfocus.com/infocus/1533>
- Gulati, R. (2003). *The Threat of Social Engineering and Your Defense Against It*. Retrieved June 21, 2005 from SANS Institute web site: <http://www.sans.org/rr/whitepapers/engineering/1232.php>
- Hall, M. (2005). Secure the People. *Computerworld*. Retrieved June 21, 2005 from Computerworld web site: <http://www.computerworld.com/securitytopics/security/story/0,10801,100448,00.html>
- Kotadia, M. (2004). Old scams pose 'the greatest risk.' *ZDNet Australia*. Retrieved June 21, 2005 from ZDNet News web site: http://news.zdnet.com/2100-1009_22-5435199.html
- McDowell, M. (2004) *Avoiding Social Engineering and Phishing Attacks*. Retrieved June 28, 2005 from Virtual DR web site: <http://discussions.virtualdr.com/showthread.php?t=169454>

Mitnick, K. (2002) *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, Indiana: Wiley Publishing.

Mogull, R. (2004). *Danger Within – Protecting Your Company from Internal Security Attacks*. Retrieved June 21, 2005 from CSO Online web site: <http://www.csoonline.com/analyst/report400.html>

Morrison, J. (2004). *Social Engineering As Fraud*. Retrieved June 21, 2005 from The Institute of Internal Auditors web site: <http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5480>

Rogers, M. (2001). *Social Engineering: The Forgotten Information Assurance Risk*. Retrieved July 3, 2005 from Vero Tek Systems web site: <http://www.verotek.com/SecureSD/marcrogers-isc2.ppt>

Rusch, J. (2000). *The “Social Engineering” of Internet Fraud*. Retrieved June 21, 2005 from Internet Society web site: http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm

Stich, P. (2005) IT Security: The Human Factor. *ISSA Journal*. February, 2005.