

# the Social Engineering Threat

By Dan Timko

**To effectively defend against social engineering, we must involve human psychology just as much as technical and administrative solutions.**

Social engineering is not a new threat brought about by the rise in computing popularity; it is, in fact, as old as the human race itself. Social engineering is just another term for fraud, con, or scam, and it highlights the weaknesses of users themselves as opposed to those of the systems. Management of this threat requires a mix of solutions from wide ranging disciplines, much more so than for other threats. To effectively defend against social engineering, we must involve human psychology just as much as technical and administrative solutions. I intend to give a background of the threat itself, and then discuss methods for an organization to protect itself from this highly effective attack vector.

## Social engineering background

Social engineering in the security sense is the art of deceiving people into giving confidential, private or privileged information or access to a hacker.<sup>1</sup> It has occurred throughout history, and fundamentally has nothing to do with technology. Technology can be a tool of a social engineer, but by no means is that his only option. Information security has historically been a very technology-centric discipline. Through the use of firewalls, intrusion detection systems and access controls, inexperienced security managers feel protected. Those who have been around know the real dangers are lurking in areas

much harder to protect – with the users themselves. In fact, as the security technologies get better, the attackers will utilize social engineering more and more. Reformed social engineer Kevin Mitnick<sup>2</sup> wrote that “as developers invent continually better security technologies, making it increasingly difficult to exploit technical vulnerabilities, attackers will turn more and more to exploiting the human element.”

Social engineering is already far more damaging than the traditional sense of hacking or cracking. Richard Mogul of The Gartner Group states that “Many of the most-damaging security penetrations are, and will continue to be, due to social engineering, not electronic hacking or cracking.”<sup>3</sup> He goes on to state that the greatest security risk facing large companies and individual Internet users over the next 10 years will be the increasingly sophisticated use of social engineering. This is an incredible risk to face, and one that most organizations are not effectively defending against currently. In order to prepare defenses, it is crucial to understand why humans are so vulnerable to this avenue of attack. With that knowledge in hand a solid defense can be built.

1 D. Gragg, “A Multi-Level Defense Against Social Engineering,” SANS (December 2002). Retrieved July 1, 2007, from [http://www.sans.org/reading\\_room/whitepapers/engineering/920.php](http://www.sans.org/reading_room/whitepapers/engineering/920.php).

2 K. D. Mitnick and W. L. Simon, *The Art of Deception*, Wiley Publishing, Inc. (2002).

3 K. Munir, “What’s the greatest security risk? Social engineering, says Gartner,” Silicon.com. Retrieved July 2, 2007, from <http://software.silicon.com/malware/0,3800003100,39125457,00.htm>.

## Psychology of social engineering

Social engineering takes advantage of human weaknesses and not technology weaknesses, so one must look to the field of psychology to help understand the reasons that people are so easily taken advantage of. Distinguished psychology researcher Robert B. Cialdini studied the psychology of influence. He determined that six basic tendencies of human behavior come into play in generating a positive response: reciprocation, consistency, social validation, liking, authority and scarcity.<sup>4</sup> By understanding these six tendencies, we can better prepare ourselves to prepare defenses against social engineering attacks.

### Reciprocation

Reciprocation can easily be summed up as “returning a favor.” People are more likely to assist someone when that person has done something for them. The original favor does not even need to be something the person even wanted. This strong tendency to reciprocate exists even in situations where the person receiving the gift has not asked for it.<sup>5</sup> Everyday examples of this are mailed donation requests from charities in which a small gift is included. Something as simple as personalized address labels has been shown to nearly double the donation rate.<sup>6</sup>

Reciprocation is commonly used as part of a social engineering attack. An attacker may call the user claiming to be a member of the help desk staff. The attacker informs the user that a virus is going around that may cripple the user’s workstation. He may direct the user to install a patch or update his system to protect it from this virus. Even though the virus threat may never have existed, the user feels that the attacker has now done him a favor and will be more likely to comply with the next request, which may not be so benign.

Reciprocity includes more than gifts and favors; it also applies to concessions that people make to one another.<sup>7</sup> An attacker may make a request that is completely out of the question, which the user will reject. He will then make a concession and only ask for part of the original request, or a smaller request. In this case, the user is more likely to reciprocate the concession and comply with the smaller request.

### Consistency

People are more likely to comply after endorsing or making a commitment to a cause. Once a commitment has been made, people do not wish to seem untrustworthy or dishonest by backing down. For this reason, people tend to follow through even when they originally would not have. Cialdini wrote of

4 R. Cialdini, “The SCIENCE of Persuasion,” *Scientific American Special Edition*, 14(1), 70-77, (2004, Jan 2004 Special Edition). Retrieved July 2, 2007, from Academic Search Premier database.

5 K. D. Mitnick and W. L. Simon, *The Art of Deception*, Wiley Publishing, Inc. (2002).

6 R. Cialdini, “The SCIENCE of Persuasion,” *Scientific American Special Edition*, 14(1), 70-77, (2004, Jan 2004 Special Edition). Retrieved July 2, 2007, from Academic Search Premier database.

7 Ibid.

a study in Israel in which researchers nearly doubled contributions to a charity for the handicapped. The key factor in their work was that two weeks prior to asking for donations they asked residents to sign a petition supporting the handicapped. After making this public commitment, the residents were more likely to contribute money than if they had been approached otherwise.<sup>8</sup>

As part of a social engineering attack, consistency can be used by an attacker claiming to be from the compliance department. The attacker will remind the user of her agreement to the company’s security policy and tell her that he needs to verify that she is following the standard on complex passwords. Due to the attacker reminding the user of the policy agreement and her commitment to that policy, the user is more likely to reveal her password to the attacker.

### Social validation

Social validation is a tendency that most are very familiar with. It is used regularly in advertising. People are more likely to do something if they think that everyone else is doing it too. It does not necessarily even have to be the truth; as long as people believe it is the social norm, they will be more likely to comply.

An attacker may take advantage of social validation by calling the user with a survey. He will then proceed to tell the user that he is almost done with the survey and has already spoken with most of the user’s other coworkers. The user is likely to follow through with the survey thinking that everyone else has done it as well. This simple lie by the attacker gives his survey some credibility. He can then go on to ask numerous questions, some of which may reveal confidential information about the company.

### Liking

It should come as no surprise that people are more likely to help people they like. They do not need to actually know the person, as long as the requestor can make himself seem likeable or form some sort of bond with the user. It can be made through sheer physical attractiveness, similarity, complimenting or cooperation.

Physical attractiveness is a form of liking that we see every day. Advertisements constantly take advantage of our tendency to like attractive people. Advertisers barrage audiences with ads featuring attractive people pushing new products. Due solely to liking, one can be influenced to purchase or do something. An attractive social engineer could take advantage of this by appearing on-site well dressed. People would be more likely to allow access or grant requests due to the person’s perceived attractiveness.

People are more likely to build a rapport with someone who shares similarities with them. This can be as simple as having the same hometown, favorite sports team, or common enemies. Through these connections, a social engineer can

8 Ibid.

take advantage of an increased trust based on false pretenses. By doing some initial homework on the target, a social engineer can build a wealth of knowledge that he can then use to appear more similar to the user. By sharing these stories or traits, he can gain the user's trust and then take advantage of it.

Complimenting someone is also a good way to gain their liking. Research at the University of North Carolina at Chapel Hill found that compliments produced just as much liking for the flatterer when they were untrue as when they were genuine.<sup>9</sup> With a quick compliment to a secretary, a social engineer is more likely to get a helpful response to his request.

Cooperation is another method for a social engineer to gain trust. If an attacker can make someone believe that he is on the same side of an issue, he will be more likely to help out. Cialdini gives an example of the car salesman who is "on your side" when trying to negotiate a price with the evil sales manager. This cooperation leads to the buyer liking the salesperson, which in turn increases sales.<sup>10</sup> A social engineer may take advantage of this by fabricating a story and convincing the user that he is cooperating and trying to help the user out.

### Authority

People are conditioned to obey authority figures from early childhood. This is a response that can easily be taken advantage of. A person can be convinced to comply with a request if that person believes it is from a person of authority, or someone authorized by a person with authority to make the request.<sup>11</sup>

This tendency is easy to understand. The user is fearful that if she does not do as the requestor asks, she is at risk of losing her job. Company employees very rarely defy a CEO and stick around for long. This concern causes people to blindly comply with the request, taking the attacker at his word that he is authorized to make such a request. Cialdini gives an excellent example of this tendency in a paper written for the *Harvard Management Communication Letter*:

In one study, researchers tested the willingness of well-trained nurses to give up their decision-relevant responsibilities regarding a patient once the "boss" of the case – the attending physician – had spoken. To perform the experiment, one of the researchers made a call to twenty-two separate nurses' stations on various surgical, medical, pediatric, and psychiatric wards. He identified himself as a hospital physician and directed the answering nurse to give 20 milligrams of the drug Astrogen to a specific ward patient. In 95 percent of the instances, the nurse went straight to the ward medicine cabinet, secured the ordered dosage of the drug, and started for the patient's room to administer it – even though the drug

<sup>9</sup> Ibid.

<sup>10</sup> Ibid.

<sup>11</sup> K. D. Mitnick and W. L. Simon, *The Art of Deception*, Wiley Publishing, Inc. (2002).

---

## The awareness of the social engineering threat needs to be instilled in each employee so that she may defend herself and the company in the face of an attack.

---

had not been cleared for hospital use, the prescribed dosage was twice the maximum daily dose set by the manufacturer, and the directive was given by a man the nurse had never met or even talked with before on the phone. It appears that the nurses unhooked their considerable professional intelligences in deferring to the doctor. Yet the nurses' actions are understandable. Regarding such matters, the attending physician is both *in* authority and *an* authority.<sup>12</sup>

Highly trained nurses were easily convinced into giving a dangerously high dosage of an unapproved medication by a person none of them had ever met, simply by stating that he was a doctor. This is a dangerous vulnerability. It is all too easy for a social engineer to claim that he is either higher ranking or authorized by someone higher ranking to do what he is asking. Most people will not ask for any proof and will comply with the request to protect their job.

### Scarcity

People are more likely to comply if it is believed that there is a time limit or short supply of something. In daily life, this is seen when stores advertise something as "limited supply" or when a restaurant advertises a new dish as "limited time only." If one thinks that he is competing with others for a limited supply item, he is more likely to purchase or go out of the way to obtain it.

A social engineer can take advantage of this by sending an email to the target with a link to a website. If the email includes something free for the first 100 respondents, the user is more likely to follow the link to hurry up and sign up before thinking through the action. This link could contain malicious software or could require the user to register on the site before entering. Out of convenience, most people use the same password for multiple logins. By registering on a seemingly trustworthy site, the user may use his normal login ID and password for the company network to access the site. This information is now in the hands of the attacker.

### Methods of defense

Social engineering is a wide ranging threat that can come at the company through many different vectors. For this reason it is important to educate the user with the core concepts instead of deploying countermeasures to handle individual threats. The awareness of the social engineering threat needs

<sup>12</sup> R. Cialdini, "The Perils of Being the Best and the Brightest," *Harvard Management Communication Letter*, 1(2), 3-5, (2004, Spring). Retrieved July 3, 2007, from Business Source Premier database.

to be instilled in each employee so that she may defend herself and the company in the face of an attack. Without adequate preparation the chances of successfully thwarting the breach is low.

There are many different ways to protect an organization from social engineering, and they are all important. Security should be modeled around the *defense in depth* model, in which multiple security layers exist around information assets. If one fails, the defense in depth model ensures that other layers are there to continue protecting the asset. For a social engineering defense, these layers will consist of both non-technical and technical methods. However, since the problem itself is not technical, usually the non-technical methods are the most effective in stopping social engineering.

### Non-technical defense

Social engineering is a people issue. By no means can it be solved without involving those people. There are many different administrative controls that can combine to form a solid defense against social engineering. For one, *a security policy must be in place*. This is the foundation of any organizational security program. With that being said, that policy cannot be written and then stored away in a file cabinet waiting for auditors to come looking. The policy must be disseminated to the users and they must be educated. User awareness is by far the best defense against social engineering.

### Information security policy

Simply defined, an information security policy provides rules for the protection of the information assets of an organization.<sup>13</sup> This policy is the foundation of any organizational security program. Without it, there is no standard to follow and the organization will attack security problems in an ad hoc and unorganized fashion. This will not be effective.

The security policy must be made clear to all employees at the organization. They must understand that they are responsible for following the policy and that consequences exist for violations. Security policies, even if religiously followed by all employees, are not guaranteed to prevent every social engineering attack. Rather, the reasonable goal is always to mitigate the risk to an acceptable level.<sup>14</sup>

An important part of the security policy is data classification. If sensitive information is marked as such, users will be less likely to give it away easily. If it is clear to be private and there are policies for the release of private information, it will allow the user to refuse the request or at least verify the identity of the caller further.

### Security education training and awareness

As stated above, a security policy is useless if the end users are unaware of it and the reasons for its existence. This is where Security Education, Training and Awareness (SETA) programs help. SETA is an especially big part in the defense against social engineering attacks. Users must be made aware of the threat and how to know what the symptoms and warning signs are. Without this knowledge, they are left vulnerable.

Security awareness training cannot be a onetime event. It is insufficient for an employee to get security training when joining the company, but never again. Security is a process, and so is security education. Users must be regularly reminded of the threats they face and how to stay vigilant. They must be made aware of new attacks and whether these attacks have been seen in the organization yet. Updating employees with information about successful or thwarted attacks will increase their awareness of the issue and their understanding of the real dangers.

### Technical defense

While social engineering is primarily a people issue, there are technical countermeasures to help when humans fail. Simple countermeasures like email filtering, web filtering, host antivirus and host intrusion prevention can help prevent the social engineering from ever occurring, or save the day when the human has been tricked. These technology solutions work far better when paired with education and awareness programs for users. This is why the defense in depth model is so widely used and successful.

### Conclusion

The threat of social engineering attacks will only increase in the future. The relative ease of most social engineering attacks, coupled with the low likelihood of being caught, makes social engineering the path of least resistance for attackers to gain access to company information. Through policy and training, users should be made aware of the threat and know their responsibilities when it comes to defense. Technical solutions should also be considered to bolster the administrative controls. The threat is real; however, with the correct knowledge and understanding an information security manager should be able to create a security management program that can reduce that risk to an acceptable level.

### About the Author

Dan Timko, CISSP, CCSP, MCSE, is a Senior Engineer at Blue-Wave Computing, LLC, specializing in information security consulting. He is a member of the Atlanta chapters of ISSA and ISACA and is currently finishing his MS in Information Security at The Georgia Institute of Technology. He may be reached at [timko@bluewave-computing.com](mailto:timko@bluewave-computing.com).

13 M. Whitman and H. Mattord, *Management of Information Security* (2nd ed.), Thompson Course Technology, (2007).

14 K. D. Mitnick and W. L. Simon, *The Art of Deception*, Wiley Publishing, Inc. (2002).