

Vulnerability of Gullibility

By Javier Soto
jay@sototek.com

Most often, when discussing information security, the attention is on technical threats (viruses, worms, etc). Commonly overlooked is the vulnerability caused by the human aspect of machine control. We tend to forget people-generated threats can be more devastating to information systems than technical attacks. With the focus on security today, addressing manipulative communications—a common attack ploy against people by information thieves—is essential. This is best accomplished when information security officers (ISO) understand social engineering functions to gain cooperation.

Basis of Article

This article is based on experience as supervisor of a federal task force targeting crimes at federal facilities. The task force focused on utilizing undercover operatives (UCO) to convince targets of inquiry to cooperate and provide access/information unknowingly. Experiences here helped in understanding why individuals cooperate with strangers when it's not in their best interest.

Defining Social Engineering

Most ISOs may associate social engineering as “cold calling” techniques to elicit protected information. However, a more practical definition may be “...a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break...security procedures...a con game.”¹ The goal is not so much obtaining information (the end result), but manipulating people. In addition, the growing complexity in application of social engineering makes defining a solution difficult. Social engineering can occur through written materials and through any social contact. Secondly, it may not just occur at work (i.e., local bar after work, where employee is relaxed). Third, social engineering may be used to provoke (explained later). Lastly, this threat can be employed using a piecemeal approach, making it difficult to defend against (combining data from various victims). The problem with technical solutions in a people world is they will not address the “vulnerability creep” that human weaknesses bring to any human interacted task as a result of vulnerability to persuasion—a key social engineering tool.

Understanding Persuasion

Understanding persuasion is key to understanding social engineering. The goal of any covert effort is to gain “voluntary” compliance to protect the effort. Here, UCOs/social engineers share one key method of gaining cooperation—persuasion. Persuasion involves influencing a person through

verbal dialogue so that the result of the encounter favors the attacker's intent. Two written works describe persuasion: Aristotle's “Rhetoric”² (translated by Lee Honeycutt) and “Undercover Operations and Persuasion,”³ by Randolph D. Hicks. Aristotle thought judgment might be swayed by an appeal to the personal traits of the targeted audience. As to persuasive methods, Aristotle adds:

“...The first kind depends on the personal character of the speaker; the second on putting the audience into a certain frame of mind; the third on the proof, or apparent proof, provided by the words of the speech itself. Persuasion is achieved by the speaker's personal character when the speech is so spoken as to make us think him credible...this is true generally...where exact certainty is impossible and opinions are divided...our judgments when we are pleased and friendly are not the same as when we are pained and hostile... persuasion is effected through the speech itself when we have proved a truth or an apparent truth by means of...arguments suitable to the case... The man who is to be in command of them must, it is clear, be able (1) to reason logically, (2) to understand human character and goodness in their various forms, and (3) to understand the emotions...know their causes and the way in which they are excited.”²

Aristotle's theories tell us judgment may be impacted by non-factual stimuli or method of argument. Such dialogue techniques are the weapon of the covert attacker as illustrated in Undercover Operations and Persuasion (UOP). The author of UOP, an experienced “Narc,” describes how he persuaded individuals to feel safe when selling him drugs while undercover. Figure 1 displays goals of the author's communication to the target, in pursuit of the target's trust (areas of psyche influenced during verbal dialogue).

Persuasion affects human behavior by catering to needs, feelings, wants, etc. Social engineers use similar rules as UCOs to trick people: 1) know the target (i.e., target's interests, work tasks, beliefs, etc); 2) know the goal to be achieved (attacker's intent or protected item victim has control over); and, 3) persuade the victim that the attacker and the victim are both working toward a common goal. These three rules provide a great challenge and guide in overcoming the vulnerability of gullibility.

Persuasion to Cooperation

Victims cooperate because they are misled or deceived convincingly through persuasion. Social engineering efforts flood a victim with data to gain a desired reaction or thinking process. Hence a challenge for security is not just providing parameters and references for employees to draw from when confronted with such situations, but motivating them to use given parameters and references. Most of the time, victimization occurs

when victims insist on making decisions based on their own beliefs/needs, ignoring security guidance. Consider the following two tactics for UCOs to gain cooperation/trust:

A. Debt to Attacker

If you owe someone, you may have the desire/interest to “pay up.” This is not about money—favours/other benefits are effective. In one scenario, providing a federal supervisory officer with compliments, and escalating to wine bottles got the UCOs access to a federal facility for “criminal activity” (when the officer should have known better).

B. Moral Duty

Playing into an individual’s beliefs or camaraderie is an effective persuasion tool. In one case, a “religious” criminal was cooperative because the UCO “was of the same religion.” Interestingly, arrested con artists would state during questioning: “I’m Catholic—I am not allowed to lie” in an attempt to gain trust with the interrogator. Fraud/con games using personal characteristics is a common occurrence: “Affinity fraud is when one person gains the trust of others because they share the same religion, race, ethnicity, career or other social characteristic and then deceives them...”⁵

One common method for locating human sources of information was to target low-level employees as “unknowing” or “knowing” informants. Most low-level employees, due to low wages and labor-management strife, did not share a similar focus in the company as management. Such positions usually included security guards, janitors, receptionists, and others with access to the facility and its resources and IT systems. These individuals provided requested information based on simple “personal” rationale: data needed in a hurry, rank (perceived) of requestor, friendliness of requestor, benefits possible from requestor, etc. While difficult to pinpoint a solution here, in our studies, we found these low-level employees most often did not receive security training, or scrutiny for that matter. In trying to indoctrinate employees to prevent such influence, our efforts did reveal one possibly effective approach. Teaching employees to focus on what is being requested, the security classification involved (for data requested), and whether proper policy is being followed, can be a great obstacle for covert operators.

Who’s Vulnerable

Vulnerability may be a matter of how invested we are in the action, idea or communication taking place, and parameters we follow or live by. If we use as a guide attributes determined to make UCOs better able to resist “confidence” attacks—street/people smarts, confidence, and ability to manage stress—we can tune training programs to help ensure employees build effective skill sets. For example, confidence/stress management translates to not allowing anyone to bully/hurry decisions, when bombarded with information. While finding special traits in hires is not easy, providing training to develop similar “skill sets” may help.

Why Be Concerned

A well-balanced security program means attention to potential vulnerabilities. Most often, the focus is on protecting data in computer systems. However, social engineering is a widespread practice in society and business—creating a large vulnerability for any organization. For example, while

<u>Physical</u>	<u>Social</u>	<u>Practical</u>	<u>Ego</u>
Food	Acceptance*	Finances*	Achievement Excitement*
Health	Friends*	Ownership	Aggression* Humor
Safety	Love	Ways/Means*	Beauty Independence
Sex		Creativity	Recognition
Dominance*		Self-Expression	Self-Regard*

*some of the “needs” a UCO can attempt to address during communications with an individual in order to persuade them to do “business”

Figure 1: From Undercover Operations and Persuasion³

we are protecting computer data from disclosure through encryption, someone may be talking to the personnel department to gain information concerning the programmer. How many information security programs focus on other than business information? A similar vulnerability exists with visitors. How many of us ask for personal identification of vendors that come to our businesses to fix things (not just a business card)? Recently in the news, there were stories of imposters showing up at various hospitals stating they were inspectors from the hospital accreditation commission (something a hospital would have a vested interest in). In all the cases, the staffs refused to take their word for it. The imposters simply left.

Second, with information systems involved in many aspects of business and personal life, security strategies may have to involve monitoring electronic channels. For example, some say the “I love you Virus” was titled to induce individuals to “click on it” when they did not recognize the sender. Today, instant messaging, chat rooms, etc. are bringing in individual threats to the business environment. Consider today’s “phishing” efforts.

Many individuals fall for scams by sending cash as security to be part of the scheme and never hear back from the schemer. These are great training case studies ISOs can present to employees to gain an understanding of covert attacks. Poor training means employees learn from television and not fact. These attacks look very real.

Third, most security efforts are so engaged in preventive operations, or response, that rarely is provocation considered a threat. Provocation is the use of misleading/false information to assess how a security apparatus/entity reacts (i.e., hackers flood a network to observe technical response, response time or identify technical personnel who handle certain issues, etc). This is a complex problem. Certain provocations need a response (i.e., a network that is flooded must be secured). In law enforcement street narcotics operations, many “walk-in” informants try to get introduced quickly to surveillance personnel to identify the “narcs” for their friends.

Lastly, “social engineering by proxy” and “insider threats” can complicate not just security efforts, but the atmosphere a good work environment should have. Whether an employee or workplace infiltrator, this individual may have proper recognition/authority for requests they make. Not only will having employees check on each other create problems, but persuasion applied from the inside is different than from the outside because of the camaraderie employees enjoy. During task force operations, UCOs were able to persuade security mechanisms to “loosen” and help with “criminal activity” because they were all “employees in the same boat.” Here, personnel security issues (screening employees) intertwine with information security issues, making coordination vital between differing security entities.

Recommended Responses

“Companies...should focus not on technology but on teaching their employees how to say no,”⁴ stated Kevin Mitnick at one of his security sem-


inars. Stressed should be parameters to follow during interactions—lie requesting contact details, so the call for information can be returned and verified. Two simple procedures can help: establishing contact protocols between employees and business partners and keeping a record of protected information transfers. However, equally vital is for ISOs to identify what data must be protected. Again, we must think in broad terms (with varying importance levels depending on type of data).

Second, internal controls should touch upon trespass and dumpster diving. One treasury agency (a high-threat facility with responsibilities for financial instruments) deploys a “destruction division.” The goal is to track and neutralize anything identified as a critical information item from purchase to disposal (i.e., hard drives, papers, etc.). “Garbage covers” have been key to many successful spy efforts.

Third, a basic counter-intelligence effort may be helpful. Guidance for employees who attend trade shows on con games, security review of employee-authored information published in open sources (i.e., employee articles/training materials), periodic surveys of employees in critical areas, may help close avenues of vulnerability.

Lastly, an operations security (OPSEC) plan can help. A while back, the federal government created the Interagency OPSEC Support Staff (IOSS) under National Security Decision Directive 298 (NSDD 298) to help prop up OPSEC at federal agencies. OPSEC is a process that attempts to limit the ability to gather information by accumulating data from various sources. The goal is to deny as much information as we can by identifying “protected information,” analyzing threats (who wants what), and assessing the risks (matching vulnerabilities to threats to prioritize security). A recommended reading on this matter is the Web site of the Operations Security Professionals Society ([Http://www.opsec.org](http://www.opsec.org)). It promotes OPSEC in government and commercial settings.

Summary

The ability and willingness to say no is probably the best countermeasure against social engineering. However, ingraining this thinking in others is not easy. While we hope our firewalls and anti-virus programs help mitigate e-threats, in confronting social engineering threats, ISOs should realize human assets are the ultimate information security “software/hardware.” 

Javier Soto, CISSP, formerly supervised a special federal task force.

Resources

1. Social Engineering. SearchSecurity.com definition. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html.
2. Rhetoric. A hypertext resource compiled by Lee Honeycutt based on the original work by Aristotle. <http://www.public.iastate.edu/~honeyl/Rhetoric/>
3. Undercover Operations and Persuasion. Randolph D. Hicks. Charles C Thomas Publisher (July 1973).
4. Better Security not about Tech: Mitnick. David Braue, ZDNet Australia. March 4, 2005. <http://www.zdnet.com.au/news/security/0,2000061744,39183334,00.htm>
5. Affinity Fraud Investment Scams. WWW.crimes-of-persuasion.com. <http://www.crimes-of-persuasion.com/Crimes/InPerson/MajorPerson/affinity.htm>