Usable Security Policies + User Training:
The Best Method to Counter Social Engineering Attacks

Rebecca Long

Eastern Washington University, Cheney, WA, USA
rebecca.long@gmail.com

Abstract. Security is a foremost concern for any institution. Investing in the best technological and physical security products only go so far to protect a system and often forget to take the users into account. A social engineer can fairly easily manipulate a system user into granting him or her access despite all the security measures taken. The best method to counter a social engineering attack is to implement usable security policies so users know what to do, and to give all users proper training so they know why they need to follow the policies.

Keywords: Security, social engineering, usability, training

1 Introduction

Securing a system involves many components:

> "A secure system is part of a wider socio-technical system whose goal is the achievement of a production task … [it] has both human and technical components working together to achieve [this goal]…, as well as achieving the enabling task of securing that system effectively" [1].

Security policies work to regulate the system and the users of the system. For example, a policy may require users to change their system password every month. Some policies may seem unreasonable to a user and this can result in users not following them. Without proper user training, the user may not understand the purpose behind all the security policies resulting in security holes.

1.1 Importance

An attacker interested in breaking into the secure system will find the easiest way in. This often means breaking in through the users of the system. Kevin Mitnick, renowned computer hacker specializing in social engineering attacks, testified before congress stating:

> “The human side of computer security is easily exploited and constantly overlooked … Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted, because none of these measures address the weakest link in the security chain” [2].

The users are the ‘human-factor’ of security. It is considered to be the weakest-link in any security system; making it ever more important to remember to take it into consideration. As stated by Bruce Schneier, a leading security expert: “People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems” [3].

It is critical that the users are properly managed to maintain a secure system. Without proper management and cooperation with the users, no system will ever be properly secured. One popular method used by attackers that takes advantage of users who are improperly managed is social engineering:

> “… a critical aspect of many forms of cybercrime that typically involves getting victims, such as employees of a firm or agency, to reveal confidential personal, financial, or security information or otherwise grant an attacker authority to access a computer system or physical environment in which valuable information may be stored” [4].

1.2 Solutions

The best way to combat social engineering is with user training that teaches users to be aware of social engineers and what to do when an attack happens. As stated by one expert, Johnny Long: “Without awareness of the problem and without an understanding of how our minds can be fooled, there is little defense against social engineering" [5].

The training may teach users about security policies and how to handle a social engineering situation, but usable security must be in place for the users to adhere to the training. This is a factor that is often forgotten when creating security policies. Policies need to cover how to use the security technology but also include how to properly dispose of documents, how to handle email and phone calls, and generally how to manage a social engineering situation.

If the security policies and technology are not user-friendly, users are going to have a difficult time following the policy and using the technology correctly or they may decide to not follow the policy at all:

> "… security policies that require the impossible create resentment and lower people's general willingness to comply with security policies … it reduces their motivation to be dependable" [1].

This could be a password policy that requires users to have 8-10 characters including at least one number and at least one symbol that needs to be changed to a new, unused password every two weeks. This may be a very secure policy, but one that is very difficult for users to follow.

To ensure that security can be properly followed, usability must be taken into account. Unfortunately, "usability and security are often seen as competing design goals in security" and yet "when users fail to comply with the behavior required by a secure system, security will not work as intended" [6]. This is why it is so important to not only train users in security policies and the specifics of social engineering, but to have usable security that the users can properly follow.

2 Social Engineering

Social engineering is a serious threat to any secure system. Even with the highest level of technological and physical security, a social engineer can convince someone to allow them access to the system.

Social engineering has many different, but similar, definitions. One definition is: "…the exploitation of psychological triggers and cognitive biases as a means to gain unauthorized access to information or information systems" [7].

Another definition is: "… the art and science of getting people to comply with your wishes" [8, 9].

Kevin Mitnick has a more detailed definition:

> "Social engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology" [10].

Social engineers use a variety of tricks to gain the trust of the unsuspecting users of a system. The attacker convinces a legitimate user to grant them access to the system. An untrained user can easily fall for the social engineer's tricks creating a serious security hole in any system.

2.1 Social Engineering Cycle

Social engineers tend to use a basic "cycle" for performing an attack (see Figure 1). This cycle includes four stages:

1. Information Gathering
2. Developing Relationships
3. Exploitation
4. Execution [7, 8]

Each of these stages will be described in the following sections.

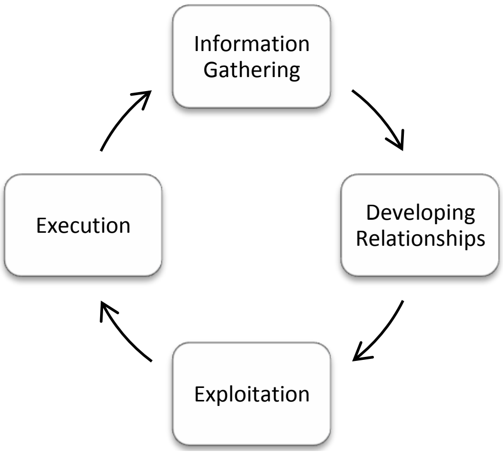

Fig. 1. Social Engineering Cycle [8]

2.1.1 Information Gathering

In order for an attacker to sound legitimate, background research on the target is necessary. This allows the social engineer to obtain the lingo of the company, names and positions of employees, and any other information that a legitimate user would probably know. Having this knowledge in the attacker's tool-belt allows him or her to sound more believable resulting in fewer questions and greater trust by their target.

Information collected on the target may or may not seem sensitive to the average person but could prove invaluable to a social engineer. This could include phone lists (current or outdated), birth dates, an organization's organizational chart, and other types of seemingly harmless information [8]. Given that most of this information is viewed as this being non-sensitive it often gets discarded without a second thought and without taking any security precautions (i.e. shredding of documents). This makes it trivial for an attacker to collect this information for social engineering attacks.

Methods of gathering this information can vary. It can be as simple as doing a Web search or dumpster diving, to a more complicated forensic analysis on hardware that was thrown out. Table 1 below shows a list of many of the possible information gathering techniques used by social engineers [7].

Table 1. Information Gathering Techniques [7]

Asking for Favors	Mail-Outs	Simple Requests
Cold Calling	Photography	Shoulder-Surfing
Contriving Situations	Pharming	Surveys
Dumpster Diving	Phishing	Tailgating
Forensic Analysis	Pretexting	Theft
Giving out Free Software	Reverse Social Engineering	Trojan Horses
Impersonation	Reconnaissance	

As an example, a social engineer interested in Financial Institution A would do his or her research on this business before moving onto the next step in the cycle. Information can be easily gathered from looking on their Web site and doing a Google Web search to find blogs, news articles, videos, or any other related information regarding Financial Institution A. Just from these simple activities, a social engineer can gather enough surface (or public) information to dig deeper.

Digging deeper can include using the surface information to perhaps make phone calls to the help desk or customer support to get more names and numbers of managers, support software, and other employees. This is where the information gathering stage begins to phase into the next stage: Developing Relationships.

2.1.2 Developing Relationships

With the information gathered, the attacker will now begin to use the information to develop relationships with employees within the target organization. This can be accomplished by making phone calls to employees within the target. The attacker can either pretend to need help from the employee or pretend to be an employee at another location (i.e. another campus or off campus such as working from home). Another tactic could be to make up a situation where the real employee will need help and then offer to help fix the made-up problem.

Multiple phone calls to the same employee within the target can build trust and a relationship. Making small requests for help that seem within reason build that relationship. Chatting with the employee and relating with what they have to put up with at work, or what they enjoy outside of work also help build the relationship. Over time trust is gained with this employee making it more likely they will help the attacker when they are ready for the next stage of the cycle.

To continue the example, the social engineer could call a teller at Financial Institution A pretending to be a teller themselves at a different financial institution that frequently works with Financial Institution A. The social engineer could pretend to be new and have a question about the application used by the tellers, such as how to transfer money between the two institutions. After a few calls like this and a very grateful social engineer, a relationship is created on helpfulness. This is the perfect place for a social engineer to be for the next stage: Exploitation.

2.1.3 Exploitation

At this point, the social engineer has information on the target and a good standing relationship with an employee with the target. This is the stage where the social engineer can make a tougher request that gets the employee to reveal more confidential information or to perform some action. The trust built with the employee is exploited by the social engineer, yet the employee may never know they have been used and will most likely walk away feeling good about the whole encounter [8].

The social engineer from the previous example may request information from their helpful teller that gains them remote access to the computer system, such as dial-up access or login information to an intranet. From this spot the social engineer has all the access they need to execute their plan in the next step: Execution.

2.1.4 Execution

Having completed the previous stages of the cycle, the social engineer has all the pieces he or she needs to execute their final attack.
To finish the example, the social engineer may either make a request to the friendly teller to transfer a large sum of money from one of the accounts at Financial Institution A to an attacker’s account or if the

request in the previous step was to gain remote access to the institution, the social engineer could use that access to install a virus to gather financial information on clients.

3 Counter-Measures to Social Engineering

There are many ways to counter and help prevent a social engineering attack. While it is impossible to completely prevent one of these attacks, there are measures to help prevent it from happening. If nothing else, making it harder for the attacker to get in may make it not worth their while to complete the intended attack.

Below in Table 2 is a list of some common intrusion tactics used by a social engineer and strategy ideas for countering the attack according to Sarah Granger in her article from SecurityFocus, a leading Web site in computer security [11]. Strategies include something as simple as shredding all documents being thrown out and keeping it in a locked container for professional disposal. Simply keeping private rooms locked and monitored, such as a mail room or server closet, can prevent or deter an attacker from gaining access.

Table 2. Common Intrusion Tactics and Strategies for Prevention [11]

Area of Risk	Hacker Tactic	Combat Strategy
Building Entrance	Unauthorized physical access	Tight badge security, employee training, and security officers present
Dumpsters	Dumpster diving	Keep all trash in secured, monitored areas, shred important data, erase magnetic media
General - Psychological	Impersonation & persuasion	Keep employees on their toes through continued awareness and training programs
Intranet-Internet	Creation & insertion of mock software on intranet or internet to snarf passwords	Continual awareness of system and network changes, training on password use
Machine Room / Phone Closet	Attempted to gain access, remove equipment, and/or attach a protocol analyzer to grab confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment
Mail Room	Insertion of forged memos	Lock & monitor mail room
Office	Shoulder surfing	Don’t type in passwords with anyone else present (or if you must, do it quickly!)
Office	Wandering through halls looking	Require all guests to be escorted

	for open offices	
Office	Stealing sensitive documents	Mark documents and confidential & require those documents to be locked
Phone & PBX	Stealing phone toll access	Control overseas & long-distance calls, trace calls, refuse transfers
Phone (Help Desk)	Impersonation and persuasion	Train employees/help desk to never give out passwords or other confidential info by phone
Phone (Help Desk)	Impersonation on help desk calls	All employees should be assigned a PIN specific to help desk support

3.1 Security Policies

Proper strategies should be included in the security policies for any company. The policies must be made with consideration of usability and the users who will be using the policies. The best policies are those that "institute simple, reliable rules for mutual authentication and a supportive point of contact for no-fault reporting and clarifying rules" [1].

3.2 Training and Usable Security

Proper training for all employees, those who use a computer or have access to private rooms or not, must be done regularly to ensure everyone knows the rules. Training should work toward "developing a culture in which … security is adopted as a shared concern by all employees" [12].

Training must include a usability component. Users must be informed not only on specific knowledge about social engineering, but why it is important to follow the security policies. Users who know and understand the implications behind a social engineering attack are more likely to follow the security policies willingly and perhaps even be an advocate for security. It is common for users without training to think "the data stored on their system is not important enough to become the target of a hacker or industrial spy" or if it was they "do not think that somebody getting into their account could cause any serious harm to them or their organization" [12].

User training should give the users the ability and knowledge to behave properly within the security policies, provide appropriate motivation to behave within these boundaries. The studies cited throughout this paper have indicated some success with these social engineering mitigation strategies.

4 Summary

The human-element of security is the weakest-link in any secure system. It is vitally important to secure it in order to combat social engineering attacks. Social engineers can easily manipulate a user into giving up confidential information or granting access to a secure location.

With proper user training on social engineering and good usable security policies, in addition to a technologically and physically secured system, the human-element can be secured against an attacker using social engineering techniques. This is the best way to fully protect against this attack vector.

5 References

[1] Flechais, I., Riegelsberger, J., & Sasse, M. A. (2005). Divide and Conquer: The role of trust and assurance in the design of secure socio-technical systems. New Security Paradigms Workshop '05. Lake Arrowhead, CA: ACM.

[2] Poulsen, K. (2000, March 2). Mitnick to Lawmakers: People, Phones are the Weakest Links. Retrieved July 11, 2009, from Politech: http://www.politechbot.com/p-00969.html

[3] Schneier, B. (2004). Secrets & Lies: Digitial Security in a Networked World. Indianapolis, Indiana: Wiley Publishing, Inc.

[4] McQuade III, S. C. (2006). Understanding and Managing Cybercrime. Pearson Education.

[5] Long, J. (2008). No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Burlington, MA: Syngress Publishing, Inc.

[6] Cranor, L. F., & Garfinkel, S. (2005). Security and Usability. O'Reilly Media, Inc.

[7] Twitchell, D. P. (2008). Social Engineering and its Countermeasures. In M. In Gupta, & R. Sharman, Handbook of Research on Social and Organizational Liabilities in Information Security (pp. 228-242). Idea Group Inc.

[8] Allen, M. (2007). Social Engineering: A Means to Violate a Computer System. SANS Institute.

[9] Harl. (1997). The Psychology of Social Engineering. Access All Areas III.

[10] Mitnick, K., & Simon, W. L. (2002). The Art of Deception: Controlling the Human Element of Security. Indianapolis, Indiana: Wiley Publishing Inc.

[11] Granger, S. (2002, January 9). Social Engineering Fundamentals, Part II: Combat Strategies. Retrieved from SlashDot: http://www.slashdot.com

[12] Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security. BT Technol , 19 (3).