Mitigating the risk of social engineering attacks

Matthew Spinapolice

Follow this and additional works at: https://scholarworks.rit.edu/theses

Recommended Citation

This Thesis is brought to you for free and open access by RIT Scholar Works. It has been accepted for inclusion in Theses by an authorized administrator of RIT Scholar Works. For more information, please contact rit scholarworks@rit.edu.
Mitigating the Risk of Social Engineering Attacks
by
Matthew Spinapolice

Committee Members
Daryl Johnson
Peter Lutz
Bill Stackpole

Thesis submitted in partial fulfillment of the requirements for the degree of

Master of Science in Master of Science in Networking and System Administration

Rochester Institute of Technology
B. Thomas Golisano College
of
Computing and Information Sciences

11/15/2011
Abstract
Social engineering is a topic that is briefly covered in today’s system administration and security coursework. With emphasis primarily on securing and administering computer network technologies, ample time has not been given to discussing how to administer the users. In addition to their technical training, administrators need to comprehend the potential severity and likelihood of social engineering attacks. Teaching administrators how to minimize the risk of hacking attempts or computer virus infections does not fully equip administrators with the knowledge to defend their networks. Administrators need to be able to answer the question of how they can also mitigate the risk of social engineering attacks against their network.

To properly answer the question of how to mitigate the risk of social engineering attacks, several facets of social engineering needed to be discussed to fully understand how it works. These topics include the:

- Definition of social engineering
- Human factors social engineers exploit
- Motivation for using social engineering
- Types of social engineering attacks

Defining social engineering was necessary to have a firm basis of what is social engineering. For the context of this thesis, social engineering is defined as using subversive tactics to elicit information from end users for ulterior motives.

Research into exploitable human factors is necessary to understand how social engineers think. Understanding concepts such as friendliness, authority, or helpfulness enable administrators to
devise methods to protect themselves, and their users, from having these traits exploited. These traits were defined to give a clear picture of what attackers look for in an individual when planning their method of attack.

Methods of attack were researched to clearly define attack types and make administrators aware of how attacks are typically carried out. By knowing these methods, best practices for administrators can be determined.

A three vector approach is necessary to successfully combat social engineering attacks. Using this approach, administrators must focus on:

- Creating best practices for themselves
- Training users on the dangers and methods of social engineering
- Reviewing organization’s policies and procedures

The creation of best practices for administrators allows administrators to have a checklist of items to ensure proper protection. This best practice guide covers physical security implementations, personnel security measures and network security hardware, software and policies. All three levels of security must be given equal assessment to ensure there is no weak link in the security chain.

Training end users, part of the personnel security best practices, is very crucial if administrators are going to successfully mitigate the risk of social engineering attacks. The users need to have a knowledge transfer of what social engineering is, how attacks can happen, and what needs to be
done if an attack occurs. Like any emergency preparedness training, users must be reminded time and again of the risk of attack and precautions to take.

In today’s age of digital security, it is the users who pose the weakest link to information security and computer networks due to their lack of knowledge of the potential risk. Armed with the knowledge of social engineering methods and tactics, administrators can be better equipped to protect their networks from attack. Apart from understanding the knowledge themselves, an administrator must be able to train the end users about the dangers of social engineering. Today, ensuring a fully protected computer network cannot be done by administrators alone. It takes the entire organization to realize each individual is responsible for ensuring information security. By implementing best practices, conducting regular training classes, and auditing current policies and procedures for compliance, accuracy, and effectiveness, system administrators can mitigate the risk of any social engineering attack.
# Contents

Abstract ............................................................................................................................................ i  
List of Figures and Tables.............................................................................................................. vi  
Introduction ..................................................................................................................................... 1  
Social Engineering Defined ............................................................................................................ 2  
  Why Use Social Engineering? .................................................................................................... 3  
What Social Engineers Prey On ...................................................................................................... 4  
  Reciprocation .............................................................................................................................. 4  
  Commitment ................................................................................................................................ 5  
  Social Proof ................................................................................................................................. 5  
  Friendliness ................................................................................................................................ 6  
  Authority ..................................................................................................................................... 7  
  Scarcity ....................................................................................................................................... 8  
Attack Vectors ................................................................................................................................ 9  
  Carelessness ................................................................................................................................ 9  
  Comfort Zone ............................................................................................................................ 10  
  Helpfulness ................................................................................................................................ 10  
  Fear ........................................................................................................................................... 10  
Ultimate Goal for Successful Attacks: Trust ................................................................................ 11  
Taxonomy of Social Engineering Attacks .................................................................................... 12  
  Dumpster Diving ....................................................................................................................... 12  
  Pharming ................................................................................................................................... 13  
  Phishing ..................................................................................................................................... 15  
  Pretexting .................................................................................................................................. 18  
  Quid Pro Quo ............................................................................................................................ 19  
Reverse Social Engineering ........................................................................................................... 20  
  Shoulder Surfing ....................................................................................................................... 21  
  Trojan Horse/Gimmies .............................................................................................................. 22  
Mitigating the Risk ....................................................................................................................... 24  
  Determine Value ....................................................................................................................... 24  
  Risk vs. Threat .......................................................................................................................... 25  
  Security Measures ..................................................................................................................... 26  
Best Practices ................................................................................................................................ 28  
  Physical Security ....................................................................................................................... 28
List of Figures and Tables
Figure 1 - How Pharming Works................................................................................................. 14
Figure 2 - Phishing Email Example............................................................................................ 16
Figure 3 - Phishing Email Example 2........................................................................................ 17
Figure 4 - Best Practice Security Model.................................................................................... 27

Table 1 - Greening Responses (Greening, 2006, p.11)................................................................. 45
**Introduction**

Network and systems administrators are faced with the potential of having to deal with any number of network attacks. These attacks may come in the form of viruses, worms, hackers, malware, and “bot nets.” When it comes to these types of attacks, administrators have a number of tools at their disposal to defend their network. For example, routers can be deployed utilizing Network Address Translation (NAT) to hide their systems from the external Internet. For filtering and blocking, administrators can employ high-end firewalls to block unsolicited traffic or Access Control Lists (ACLs) to block traffic from unwanted locations. With all these tools in place, many administrators feel they are adequately protected, from attack. At the very least, they feel if an attack is to happen, they would be notified immediately and be ready to act. The problem with this heavy reliance on technology is that administrators now focus solely on the technology to solve their problems. As information security author Bruce Schneier stated, “If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology” (Schneier, Secrets & Lies, 2002, p. xxii).

The problem administrators face today when dealing with security is not a technical one. Kevin Mitnick emphasized this after attending his first Rivest, Shamir and Adleman (RSA) conference:

“No sessions were offered covering physical attacks or social engineering. You could spend a fortune purchasing technology and services from every exhibitor, speaker and sponsor at the RSA Conference, and your network infrastructure could still remain as vulnerable to old-fashioned manipulation” (Mitnick K., 2001).

The issue revolves around the human aspect of the network, not the technological aspect. Like any system, it is only as strong as the weakest link (Schneier, Beyond Fear, 2006). With today’s
advances in network security, humans are now the weakest link in the chain. Attackers have
time on their side. Attackers can take as long as they want in planning out their attacks. These
attackers will plan out their attacks and attempt to go for the weakest link in the security chain
with the hopes of gaining the most information or inflicting the most damage. In contemporary
networks, this weakest link is the end user him or herself (Orgill, Romney, Bailey, & Orgill,
2004). Routers, firewalls and other defenses are meaningless if an attacker is standing in front of
a client’s machine, or worse, gains physical access to the server room. If an attacker can exploit
a user to gain information, administrators need to devise new measures to secure their networks
and data. An administrator’s arsenal of network security tools and software is rendered useless
if those tools can be circumvented simply by the attacker walking through the organization’s
front door.

Social Engineering Defined
When attackers focus on the human element of a computer network, they typically employ social
engineering tactics. Social engineering relies predominately on establishing and exploiting trust
(Russell, et al., 2003). By building trust with an individual the attacker may be able to gain
privileged information he or she would not otherwise be able to attain. The ultimate goal of a
social engineering attack is to gain direct access to the targeted information system (Thornburgh,
2004). Successful social engineering attacks allow attackers to gain the information they want
without having to resort to hacking. Based on what social engineering attempts to accomplish,
when dealing with computer network administration, the following definition of social
engineering can be surmised: using subversive tactics to obtain information from an individual or
individuals for nefarious uses against a computing system.
Why Use Social Engineering?
With social engineering defined, the next question to ask is why would one conduct such an operation in the first place? Lafrance (2004) identifies four distinct motives that may drive one to conduct a social engineering attack.

- Economic Profit
  An attacker may see the information that could be obtained as a quick means of earning money whether by attempting to then blackmail the victim or sell the information to the highest bidder.

- Personal Interest
  An attacker may simply be curious as to what goes on with an organization and see social engineering as the best means to obtain information without causing alarm.

- Revenge
  Former employees, competitors, or someone who disagrees with a corporation’s business or its practices may resort to social engineering in an attempt to damage the corporation or its reputation.

- External Pressure
  External pressure may come from other hackers where hacking is viewed as a game to see who can obtain the most information or do the most damage for notoriety within the group or subculture.
What Social Engineers Prey On
Before one can understand and attempt to identify the tactics social engineers may employ, it is important to understand what human traits social engineers prey on to exploit their victims. The research by Robert Cialdini (2001) gives insight into just these traits.

In his book, *Influence*, Cialdini (2001) listed several innate human conditions that practitioners of social engineering will prey on (and exploit any combination of) to gain a victim’s trust in an effort to obtain desired information. The six conditions described are:

- Reciprocation
- Commitment
- Social Proof
- Friendliness
- Authority
- Scarcity

Reciprocation
Reciprocation is one of the most influential rules ingrained into the human culture. This rule states that people should attempt to repay what another person has provided to them (Cialdini, 2001). When provided with a good or service, the human response is to feel a sense of debt to the provider, so they do not later feel a sense of guilt for getting something for nothing. In most cases of receiving goods or services, this debt is repaid in monitory amounts. Exploiting this rule is easy and one of the most common tactics used by social engineers. The reciprocation rule is exploited so often due to the overpowering strength it has over people.
Besides being an overpowering influence on the human psyche, the reciprocation rule also can result in unequal exchanges of favors or information (Cialdini, 2001). This unequal exchange is typically displayed when a person feels indebted to another. In the course of paying back their debt, the person will pay (monetarily or by actions) more than is owed to relieve their feeling of guilt. Exploiting reciprocation requires the social engineer to make the first move during the attack (rather than waiting for the victim to engage the attacker).

**Commitment**
Commitment is another human condition social engineers prey on. This condition suggests once a person makes a decision, he or she feels a sense of responsibility, whether intrinsically or extrinsically, to commit to it. Social engineers use this to their advantage in numerous ways to coerce their targets into divulging sensitive information. If the target has already been answering questions from the attacker, divulging unnecessary information for future attacks, he or she will feel a sense of pressure when finally asked a question where the answer will yield important information. For example, an attacker could ask a series of questions about a particular employee. Anything from when the employee goes to lunch, how long they take lunch, etc. The attacker could finally ask the office number of the employee. While all this information seems benign, the attacker now has now compiled a window of opportunity to search the employee’s office for useful information.

**Social Proof**
“The principle of social proof states that one important means that people use to decide what to believe or how to act in a situation is to look at what other people are believing or doing” (Cialdini, 2001, p. 140). If an attacker is trying to gain information from several individuals
within an organization, he or she can use the concept of social proof to further coerce someone into divulging information. By instilling a sense of conformity upon the victim, the victim will be more likely to believe others have done what the attacker is asking him or her to do (Manjak, 2006). For instance, the attacker may create a form that asks for the individual’s computer logon credentials, which are needed for an annual security assessment. Upon presenting the form to the target, the attacker may say “Many of your coworkers [dropping names of other members in the organization to help legitimize the request] have already completed this form, it is necessary for you to please do the same.” The victim, now presented with proof (albeit false) of his or her coworkers’ compliance, now feels more at ease thanks to the (false) assumption that others have followed suit in filling out the faux security assessment form. Social proof is very effective when the victim is not around his or her peers. Without being able to confirm the attacker’s statements, lone victims can be more easily persuaded to divulge information than those who are within a group (Orgill, Romney, Bailey, & Orgill, 2004).

**Friendliness**
People tend to be more responsive to others whom they are friendly with and like. This increase in responsiveness aids attackers aiming to exploit the friendliness condition. Responsiveness means that people will be more willing to say “yes” to requests from friendly acquaintances. Due to this likelihood, an attacker utilizing social engineering will compliment and befriend a target during their interactions. A person is more willing to divulge information to someone who is kind, social, and courteous.

A receptionist at an organization may be the most likely target for the friendliness exploit due to his or her job as the effective gatekeeper to the other members within the organization in addition
to high visibility and ease of access. For example, an attacker will walk in mentioning how he is late for a meeting with an executive within the organization. He cannot remember the office or phone number of the higher up and asks the receptionist for the executive’s information, remembering to be polite and smile. Whether the receptionist is male or female, the attacker will attempt to interject a compliment to further the friendliness façade.

Within the concept of friendliness lies the idea of similarity and familiarity. Increased familiarity with someone and discovery of similarities are factors that lead people to like another (Cialdini, 2001). During attacks that take several months or more, the attacker can put the victim at ease by remaining in contact, being friendly, or finding (or more commonly falsifying) similarities between the attacker and victim. The more at ease and friendly the victim is with the attacker, the more likely he or she will be willing to give up proprietary information.

**Authority**
The concept of authority lends itself to obedience (Cialdini, 2001). When someone is seen as an authoritative figure, others will follow the figure’s rules, requests, or orders for one of two main reasons:

- Hope of reward
- Fear of reprimand

Social engineers strive to illicit responses based on these two stimuli. To do so, one must first convey the sense of authority. People associate several visual cues with authority status:

- Titles (such as director, president, sergeant, professor, or dean)
- Money
• Clothing
• Automobiles

Having (or pretending to have) any combination of these and other status symbols allows a social engineer to feign a higher authority and increase the chances of getting sought after information. Arriving to a target organization in a freshly pressed suit and stepping out of an expensive car will help convey the sense of authority and therefore the assumption that the attacker is privileged to otherwise inaccessible information. The same is true over the phone (or computer) if the attacker uses managerial titles such as “Director of Information Security” or “Manager of Information Systems.”

**Scarcity**

Scarcity affects people every day thanks to advertisements on television and on the Internet claiming limited inventory. People are bombarded every day with advertisements claiming, “Act quickly, supplies limited!” or “Hurry, this is a limited time offer!” (The advertisements themselves are examples of social engineering, but in the pursuit of corporate profit, not necessarily deception). Cialdini’s scarcity rule states, “…people assign more value to opportunities when they are less available…. The scarcity principle holds for two reasons. First, because things that are difficult to attain are typically more valuable…. Second, as things become less accessible, we lose freedoms” (Cialdini, 2001, p. 231).

Nefarious social engineers will use the same tactics as their legitimate counterparts. A social engineer may set up a bogus website offering a rare, once in a lifetime available item on sale for a very low price. This website will be in the form of either a fake online retailer, or more deceptively, a recreation of a legitimate online retailer. A person, enticed by the offer and the
thought of being one of a few people to own such a rare item, buys the item, sending the social engineer his or her name, address, and credit card information. In return, the buyer receives a false receipt. Meanwhile, the attacker quickly buys multiple items with the newly acquired credit card information.

**Attack Vectors**
Building upon these six human conditions, Charles Lively, Jr., (2004) states social engineers prey on and utilize four primary attack vectors:

- Carelessness
- Comfort Zone
- Helpful
- Fear

These attack vectors help link what social engineers prey on to the types of attacks social engineers will use.

**Carelessness**
The carelessness vector is exploited by having victims fall prey to their own false sense of security. Not properly disposing of sensitive material or not following security guidelines allows an attacker to exploit a victim’s carelessness and gain access to potentially damaging information. Carelessness often aids social engineers in pre-social engineering attacks when they are in the planning phase of the attack and need information on how to gain the more lucrative information during the main attack. Lively (2004) states, “[Carelessness] is often the first phase of a more complex overall attack” (p. 2).
Comfort Zone
A victim’s comfort zone is exploited only after the attacker has made the victim at ease both with
the attacker and the environment. By being in a more comfortable, relaxed state, the victim’s
threat perception is lowered, making it easier for an attacker’s exploit to succeed. This vector
relies heavily on locations to conduct the attack such as a victim’s office. Friendliness and social
proof conditions are more easily exploited via the comfort zone vector. These attacks are more
commonly used from within the organization. A survey conducted in 1998 found that up to two-
thirds of all social engineering attacks emanate from within an organization (Lively Jr., 2004).

Helpfulness
The helpfulness vector exploits the victim’s compassionate side. Relying on the notion that
people generally want to help another (Jones, 2003), attackers will pose as someone in need of
assistance in an attempt to solicit information. Posing as a new employee, the attacker may ask
where certain resources are located throughout the organization, such as the server room or
security office. Both of these locations should be red flags that a potential social engineering
attack is taking place.

Fear
The fear vector exploits a victim by exploiting the emotions and states that make up fear, such as
anxiety and stress. Lively states the fear vector is often the most aggressive type of attack a
social engineer can perform (Lively Jr., 2004). Using the fear vector often means exploiting the
victim’s conditioned sense of authority and preying on the victim’s fear of reprimand. Social
proof exploits also help in these scenarios as victims want to be seen as team players and can be
fearful of not being seen in such a light by their peers.
Ultimate Goal for Successful Attacks: Trust

The previous human conditions and attack vectors social engineers exploit and utilize all build up to one ultimate goal (aside from gaining information): trust. If the attacker can gain the trust of the victim, the attacker will have a much easier time obtaining any information he or she desires. The more a person trusts another, the less likely they are to have their suspicions raised (Mitnick & Simon, 2002). Once the attacker has the trust of the victim, the hard work of the attack is over. The attacker can now ask for more information while raising little, if any, suspicion on the victim’s part.
**Taxonomy of Social Engineering Attacks**
Focused on exploiting the above human characteristics and learned social behaviors, social engineers have come up with many intuitive ways to trick their prey into divulging information. Social engineering attacks typically combine any number of methods in hopes of obtaining as much information as possible. While commonly used in a combined state, the attack types themselves can be categorized into several distinct methods with unique features.

**Dumpster Diving**
Technically, dumpster diving is not considered a method of social engineering since there is no human interaction while gathering data. Even so, it warrants mentioning as it can play a vital role in deciding which type of future social engineering attack (or attacks) to use. Dumpster diving is defined as searching through, or “diving”, through the trash of a person or organization in an attempt to gain potentially useful information (Authurs, 2003). Names, phone numbers, email addresses, physical addresses, credit card numbers and other personal or proprietary information can be easily obtained by one or more dumpster diving sessions.

While it is in the attacker’s best interest to stay hidden during a dumpster diving session, so as to not to blow his or her cover for future attacks, in most cases the would-be attacker does not have to worry about any legal issues if spotted. In the Supreme Court decision of California v. Greenwood (1988) the Court found that the fourth amendment prohibiting warrantless searches does not apply to trash left outside of a residence or Curtilage (an enclosed area on property but not housed within a building). The Court’s ruling stated that Mr. Greenwood relinquished the right to reasonable expectation of privacy to any belonging he put into the trash. As a result of this case, people are free to inspect one’s trash for any useful items or information. The only
exception to this expectation of privacy is if the trash is on private property with posted “no trespassing” signs (Robinson, 2007).

**Pharming**
Pharming is an example of a passive attack where the victim comes to the attacker. Pharming is the recreation of an otherwise legitimate website, such as a bank or online retailer. The goal is to trick the victim into thinking he or she is on a real, legitimate site and have the victim enter confidential information. Depending on the type of website, this could be one’s social security number, credit card information, or username and password for a legitimate website (Filte, 2006).

Setting up the malicious website is typically not enough for an attack to be successful. For the ruse to be completely hidden, attackers may opt to make the address of their website appear legitimate too. This deception could be accomplished via several means. The most common methods involve registering a domain name with a slight variation on the legitimate website’s address or using a different domain name suffix.

An even more intrusive pharming attack would compromise files locally on the victim’s computer. By editing the “hosts” file of the computer (limiting the range of the attack only to machines that are compromised), or by exploiting Domain Name Service (DNS) servers, attackers can create false domain records so that the legitimate DNS entries for a given website direct victims to a malicious website’s IP address (otherwise known as DNS poisoning). By compromising the DNS server(s), attackers will be able to bring many more users to their website, since any requests the DNS server(s) receives for the legitimate website will be redirected to the fraudulent website.
Figure 1 shows how this type of pharming attack is conducted.

Figure 1 - How Pharming Works

1. The attacker targets the DNS service used by the customer. This server can be a DNS server on the LAN or the DNS server hosted by an ISP for all users. The attacker, using various techniques, manages to change the IP address of ‘www.nicebank.com’ to the IP address of a webserver which contains a fake replica of nicebank.com.

2. User wants to go the website ‘www.nicebank.com’ and types the address in the web browser.

3. User’s computer queries the DNS server for the IP address of ‘www.nicebank.com’.

4. Since the DNS server has already been ‘poisoned’ by the attacker, it returns the IP address of the fake website to the user’s computer.

5. The user’s computer is tricked into thinking that the poisoned reply is the correct IP address of the website. The user has now been fooled into visiting the fake website controlled by the attacker rather than the original www.nicebank.com website.

(Chaudhari, 2006)
An example of pharming would be a malicious site of www.bankofamerica.net instead of the correct www.bankofamerica.com. When a user arrives at the bankofamerica.net website, he or she should not see much difference to the legitimate .com site. Unaware of this being a pharming site, the victim inputs his or her confidential information (username/password/credit card number) as well as identifiable pin number(s) to gain access to the site. After submitting the information, the malicious website may report an error saying the page temporarily cannot be found due to technical errors. More advanced websites may even pass the information to the legitimate website and forward the user to the site. Either way the victim is unaware of falling victim to the attack.

**Phishing**
Phishing is arguably the most common computer based form of social engineering. Unlike pharming, where the attacker waits for the victim to come to him, phishing attacks seek out the victim (McQuade III, 2006). These attacks typically prey on the friendliness and scarcity human conditions. Phishing is most commonly attempted through email but can also come in the form of an instant message, phone call, or even in person. In almost all attempts, the attacker impersonates someone to exploit the idea of authority and gain the victim’s trust and acceptance.

The most common examples of phishing are the Nigerian email scams. These scams usually involve a supposed high-ranking member of an organization or government based in Nigeria stating a large sum of money is available to the victim due to some odd circumstances. All the victim needs to provide is specific personally identifiable information. Typically this information consists of, but is not limited to a name, social security number, checking account and routing numbers, and address. In some cases, the victim is even asked for a modest sum of money in advance for “processing fees.”
Figure 2 shows an example of a phishing email received by the author during the research of this thesis.

**Figure 2 - Phishing Email Example**

From: mrabiidebe0@citcotrust-online.de
Sent: Tuesday, November 06, 2007 9:28 PM
To: ********************
Subject: I Request Your Urgent Consent

Dear Friend,

I am Mr. Abii Debe, staff of Citco Trust & Finance House Accra Ghana. I am the Credit management and recovery manager with the Company office in Ghana before I was transferred to our head office here in Abuja Nigeria. Late Engineer Wilson was my personal Client before he died in an accident, he was a contractor with Shell Development Company and he is from your Country.

On the 21st of April 2004, Engr. Wilson, his wife and their two children were involved in a car accident along Platue express road and all occupants of the vehicle unfortunately lost their lives. Before the time of his death, he had a deposit of $14.5 Million which he declared as family treasure in the Finance House Accra office where I was working then, which is only I and his lawyer knows the true content, Unfortunately, till this moment no person has come as his relation for his chattels with us. I humbly request your attention to this matter so that I can present you as his next of kin and beneficiary to his chattels. It is not a very difficult thing to do and it will not take time.

All I will need is to put your name and particulars as his next of kin to in our computer database and we file in an application for the release of the fund in Ghana to conclude the deal, we may request that the money be sent to Europe for your collection.

Please contact me as quickly as possible through this email address (ab_debe21@yahoo.com.hk) treat this matter as very important and confidential.

When I hear from you, we shall discuss the terms of sharing of the money after the claim. Contact me now so that I can delegate the Attorney who is also going to be part of the deal.

I await your urgent response.

Best regards,
This email has several signs of being a phishing scam. First, there are constant grammatical errors and punctuation mistakes. A second red flag is the reply email address. The sender says he is located in Nigeria, yet the email address ends in the suffix ".hk" which is the domain for addresses emanating from Hong Kong. Finally, the use of a “Yahoo!” email address when the sender says he works for a division of Citco Trust is yet another item to note.

The email in Figure 3 goes one step further and even details what information is desired from the victim. The attacker could then easily commit identity fraud if the victim provided all of the requested information.

Figure 3 - Phishing Email Example 2

From: worthsman kalvin [worthsman_kay1@yahoo.com]
Sent: Saturday, July 21, 2007 12:46 PM
To: ******************
Subject: part time worker needed

Hello,
My name is Worthsman Kalvin and I am an artist. I live in England, with my two kids and the love of my life. It is definitely a full house. I have been doing artworks since I was a small child when I was in Canada, that should give me about 23 years of experience. I majored in art at high school and took a few college art courses.
Most of my work is done in either pencil or airbrush mixed with color pencils. I have recently added designing and creating artwork on the computer. I have been selling my art for the last 4 to 5 years and have had my work featured on trading cards, prints and in magazines. I have sold in galleries, museums and to private collectors from all around the world. I am always facing serious difficulties trying to sell my art works to Americans and Canadians, they are always offering to pay with a US POSTAL MONEY ORDER, which is difficult for me to cash here in England. I am looking for a representative in the states or Canada who will be working
for me as a partime worker and i am willing to pay for every transaction, which
wouldn't affect your present state of work. Basically someone who would help me
receive payments from my customers in the states/Canada. I mean someone that
is responsible and reliable, because the cost of coming to the states and
getting payments is very expensive. Presently I am working on setting up a
branch in the states and Canada, but for now I need a representative in the
united states who will be handling the payment aspect.
These payments are in money order and they would come to you in your name, so
all you need to do is cash the money order deduct your percentage and wire the
rest back. But the problem I have is trust, but I have my way of getting anyone
that gets away with our money, I mean the Security gets involved. It wouldn't
cost you any amount, you are to receive payments which will be sent to you by
fedex or ups from my business partners, which would come in form of a money
order then you are to cash it and send the cash to me via western union money
transfer. All western union charges will be deducted from the money.
If you are interested your percentage is 10% out of any transaction, please
provide this information below as this assures our partnership.

FIRST NAME--------
LASTNAME--------------
ADDRESS--------
CITY----------
STATE-----------------
ZIP CODE----------------
COUNTRY-----------------
PHONE NUMBER (S)------------------
GENDER------------------- MARITAL STATUS-----------------
OCCUPATION-------------------
AGE-----------------
NATIONALITY-----------------

Regards
Susana
BEACON ST, BIRKBY, HUDDERSFIELD,
WEST YORKSHIRE HD2 2RS,
Worthsman
Phone--+447024095475

Pretexting
Pretexting is a technique used by many social engineers. The United States government defines
pretexing as “the practice of getting personal information under false pretenses” (Pretexting:
Your Personal Information Revealed, 2006). Pretecting is used in phishing and pharming attacks
since the people behind the emails and websites are not actually part of the legitimate organizations they claim to be a part of. Because Not all social engineering attempts are made under false pretenses. Therefore social engineering is not synonymous with pretexting.

**Quid Pro Quo**

The Latin word, quid pro quo, is defined as “something for something.” When used for social engineering purposes, the attacker promises the victim something in return for cooperation. This method is often aided by an impersonation, where the attacker will pretend to be another worker within an organization (mixing in pretexting techniques). If necessary, the attacker will impersonate a superior if the attack is not in person (preying on the realm of authority). The attacker’s goal is to make the victim feel as if he or she will benefit from helping the attacker complete his or her goals. These goals are often not seen as malicious in nature to the victim, while the “reward” is seen as very tantalizing. The classic example of a quid pro quo attack comes in the form of a survey. Manjak (2006) explains why surveys provide such an easy means for staging a social engineering attack,

> “Surveys are an information gathering instrument tailor made for attackers. They require no special relationship between the attacker and the victim, and are by their very nature designed to elicit information in a question and answer format” (p. 9).

In a notable study, organizers of the Infosecurity Europe conference conducted three surveys from 2006 through 2008 asking random people in London, England if they would divulge their work usernames and passwords in return for a chocolate candy bar. The organizers also hired attractive females to administer the survey to further entice people. After reviewing the data, the surveyors discovered that in 2006, 81% of people surveyed were willing to give up their
passwords in exchange for a candy bar. In 2007, that percentage decreased to 64%. In 2008, the percentage dropped again to 21% out of 576 people asked (Infosecurity Europe, 2008). While the research shows there are many people willing to part with sensitive, private, and potentially damaging information, these surveys also suggest that people are beginning to be more cautious when giving out personal information. However, it must be noted that the organizers were not able to determine if the usernames and passwords recorded were legitimate.

**Reverse Social Engineering**
Reverse social engineering aims to gain information by having the victim ask the questions rather than the attacker. Typically, when employing this type of attack, the attacker will don the persona of an authority figure within the organization. Utilizing this authority characteristic can yield a great deal of information to the social engineer based on the questions asked by the victim.

Reverse social engineering attacks are one of the hardest types of attacks to perform due to the time and patience necessary to properly prepare one’s self to step into the authority figure’s role. A social engineer needs to make his or her ruse believable to the victim or else he or she will be exposed. Employing this attack method usually means having to give up some information to ensure the victim never knows an attack took place.

Malcolm Allen (2007) describes a reverse social engineering attack as being comprised of three parts: sabotage, marketing, and support. With sabotage, the attacker will attempt to corrupt or give the appearance of corruption to a user’s workstation or other device. The attacker will then use marketing to ensure the victim contacts the attacker by leaving business cards or by name
dropping. Once contacted, the attacker will then switch into support mode and “assist” the victim with the problem while gaining the desired information.

A typical scenario for reverse social engineering involves the attacker impersonating a member of an organization’s Information Technology (IT) helpdesk. Selecting his or her victim, the attacker may sabotage the victim’s computer. This sabotage can be as simple as unplugging the user’s network cable. The attacker will then make himself or herself known to the victim as the person who can help fix the computer’s problem. A simple, “Hi, I’m Henry, the IT guy, can I help you?” will do. Once the attacker is in direct contact with the victim, the final phase, support, or assisting, begins (Dubin, 2003). Throughout the conversation, the attacker listens to and attempts to answer questions asked by the victim. As the victim asks questions related to the issue, the attacker can gain valuable information that may aid in further attacks. When ending the dialog with the victim, the attacker fixes the victim’s computer problem, obtains the desired information and break contact. The victim is unaware of the attack because his or her computer is back up and operational. Additionally, a trust has been established between victim and attacker that could be used for further information gathering attacks.

**Shoulder Surfing**
Shoulder surfing is the act of watching what someone is typing or doing on the computer by watching the screen (or keyboard) with or without the victim’s knowledge (Robinson, 2007). The act of shoulder surfing itself is not a true form of social engineering, as the attacker is not actively engaging the victim (Allen, 2007). Even so, other social engineering methods are used to lead up to this attack, as the attacker needs the victim’s trust and must make the victim feel at ease to allow the attacker to get so close. Attackers find it difficult to walk up and shoulder surf
without a sense of trust by the victim. This action will almost surely cause the potential victim to ask what on the attacker’s motive is and why the attacker is standing behind them. Gaining the victim’s trust, engaging the victim in conversation and finding (or creating) similarities between attacker and victim will increase the chances of this attack succeeding. As the victim falls into a false sense of trust around the attacker, he or she will be less likely to notice, or care, if the attacker happens to be watching what he or she is typing into the computer. Once this trust is established, the attacker only needs to watch for usernames, passwords, or other valuable information, and then disappear. Once again, the victim has no idea an attack has taken place.

Trojan Horse/Gimmies
Trojan horse attacks, also known as “gimmies,” aim to exploit the victim’s curiosity as well as exploit the victim’s sense of scarcity. Trojan horse attacks are unique in that they may never require contact (directly in person or indirectly via email) to be accomplished. The attack is performed by leaving something the victim will find as valuable laying around such as a CD or flash drive. The item is the Trojan Horse.

While at first sight it appears to be nothing more than a harmless piece of technology, it is the software contained on it that is a danger. Prior to planting the device in a location where the victim will find it, the attacker will load any number of malware utilities on it. These utilities include key loggers, spyware viruses, root kits, etc. Once the victim finds the item and inserts it into his or her computer, the software will automatically install and/or activate without the victim’s consent or knowledge. The scarcity condition is exploited when the victim picks up the item after seeing it lying in an inconspicuous space. The victim’s curiosity is exploited when the victim puts the device into his or her computer to see if there is any data on the device.
This exact scenario was tested in June of 2006 by Secure Network Technologies Inc. during a security audit of a credit union. Twenty USB flash drives were preloaded with a Trojan Horse that would collect user’s passwords, logins, and computer system information and then email that information back to the auditors. The USB drives were placed in various areas throughout the credit union’s parking lot. After letting the “attack” go for three days, the auditors found that 15 out of the 20 flash drives were found by credit union employees and were plugged into the company computers, giving them access to all the information they would need to further compromise the stability and security of the credit union’s network (Stasiukonis, 2006).
Mitigating the Risk
Armed with the knowledge of what human conditions social engineers exploit during their attacks, as well as the methods they use, administrators can begin to mitigate the risk of social engineering attacks. In devising such methods, administrators must first determine the value of the data they are trying to protect. Administrators must also understand the difference between risk and threat when dealing with prioritizing their data. Administrators must take into account users’ daily needs to create a ratio of usability to security. As Schneier (2008) has stated:

“Procedures are a tough balancing act. If they're too lax, there will be security problems. If they're too tight, people will get around them and there will be security problems”

(Schneier on Security - People and Security Rules).

Only after understanding a risk verses a threat can administrators effectively implement security measures that would be best suited for their environment.

Determine Value
One key detail administrators must first review is determining what has value in their organization. Administrators should learn to think beyond the traditional terms of value such as a computer costing $2,000 to replace. In addition to such asset values, one needs to think of what the data they manage could be worth. Most organizations tend to underestimate the value of their data, only to realize this error after an attack (Gragg, 2002).

Determining the value of information and resources will help prioritize the level of protection given to the information. By prioritizing and ranking systems by a value metric, administrators can better allocate safeguards and countermeasures to protect them. Administrators should also look at the cost to secure a resource vs. its estimated value. If the cost to secure a resource
greatly outweighs the value of the resource itself, it may not be in the best interest of the organization to spend the money to protect it (Dubin, 2003).

**Risk vs. Threat**
The difference between risk and threat is very important for an administrator to understand. Not fully grasping the definition of these terms can lead to weak security measures that will not provide adequate safeguards when tested.

Bruce Schneier (2006) identified risk and threat as the following:

“A threat is a potential way an attacker can attack a system” (p. 20).

A risk takes “into consideration both the likelihood of the threat and the seriousness of a successful attack” (p. 20).

To summarize, the threat is the type of attack that can be used, while the risk is the chance or the probability that the attack will occur and be successful.

In today’s post 9/11 world, think of the threat as a terrorist attack. The media constantly states how another terrorist attack is a threat to the United States. The risk, however, can vary greatly. For instance, a terrorist attack would be more likely to occur in Washington, D.C. than Bismarck, ND. Therefore, it can be said that the risk of a terrorist threat is greater in Washington, D.C. than in Bismarck.

This same reasoning is used when dealing with social engineering. In a new startup organization, there is the threat that someone could use social engineering to discover the username and password of a given employee; however, the risk of such an attack is low because the company is fairly new and unknown. The argument could be made that the risk of a social
An engineering attempt against an employee of a high profile, well established company is greater than that of a company that was created recently.

Administrators need to evaluate the data to be protected and place values on it. Using the information’s determined value will help in deciding risk if the information were to be compromised. Higher value information may be at greater risk from the same attack than lower value information. Establishing these criteria is what will lead to being able to apply the necessary security measures on the appropriate data.

Security Measures
If a Systems Administrator is to protect the assets of his or her network, he or she must think like an attacker. What data would be sought? Which people would easily give up information? These questions should be asked and answered before any specific policy or procedure is put in place. Even after policies or procedures are implemented, administrators must still remember that they and their network are never one hundred percent protected. When it comes to social engineering, the administrator must strive to mitigate every attack attempt. An attacker need only be successful once.

To combat social engineering attacks, an administrator’s best practices guide has been developed and have been divided into three separate categories:

- Physical Security
- Personnel Security
- Digital Security
These three categories, working from the top down should form a shell around valuable network resources and data, as seen in Figure 4.

Figure 4 - Best Practice Security Model

This “onion” layered approach to mitigating the risk of social engineering attacks aims to ensure that if the outer layer of protection is broken, the damage an attack can cause will be limited to that layer and stopped before access to network resources has been achieved. Once network security measures have been breached, an attacker will have access to any and all desired information.
**Best Practices**
Detailed practices and procedures that can be implemented are broken down under each of the three security layers. A quick reference version of these best practice guidelines can be found in Appendix A.

**Physical Security**
Physical security includes all physical entry and exit points to the facility, including exterior building access as well as access to network resources such as datacenters and wiring closets. These assets must be protected and monitored to ensure only properly authorized personnel can gain access. Being vigilant and ensuring only authorized personnel have permission helps to lower the risk of physical security breaches stemming from social engineering attacks.

Physical security should employ multiple means to secure and monitor all entrances to a facility. Such methods and tools are:

- Auto locking doors
- Closed Circuit video surveillance equipment

Utilizing auto locking doors provides a failsafe against users. These types of doors help to alleviate the user forgetting to lock entrance ways that lead to sensitive areas or resources. Auto locking doors can be classified as the counterparts to the auto lock feature on a user’s workstation, ensuring no one can access network resources without proper access in the event the user forgets to lock his or her workstation while away.

Administrators should emphasize the danger of tailgating users when entering or exiting secured locations. Attackers may attempt to exploit an individual’s courtesy of holding a door open for someone in hopes of entering an unauthorized area (Brainard, Juels, Rivest, Szydlo, & Yung,
2006). Users may find it rude to let the door shut behind them when another individual is trying to pass through the door as well. This tactic further ensures the locking doors are not defeated via any social engineering attempt.

- Photo identification (ID) badges
  Issue ID badges that incorporate copy protection countermeasures, such as printed holograms or microscopic text. These badges should also contain technology such as mag-stripe or RFID encoded information linked the user’s name and access permissions to grant/deny the user access to various areas throughout the organization.

- Biometric access devices
  Using biometric access devices such as hand scanners or retina scanners offer another level of security that has proven to be very difficult, but not impossible to defeat. Using this technology in tandem with photo ID badges establishes a multifactor authentication scheme for ensuring a secure physical environment.

- Security cameras
  Security cameras add a logging mechanism to physical security. Not only can video recordings provide a log of successful logins and logouts of users from the premises, but they also serve to review the events leading up to, during, and after an attempted or even a successful breach of physical security.

- Visitor badges
Badges should be issued to every visitor that enters the premises, no matter how trusted the individual is. Assigning visitor badges to every visitor establishes an auditable policy that shows all visitors are accounted for during their visit.

- **Sign-in sheets**
  
  In addition to visitor badges, guests should be required to fill out a sign-in sheet, or visitor log, recording, at a minimum, their name, organization they are from, who they are visiting, their time checking in, and their time checking out (see Appendix C for an example sign in sheet). Sign-in sheets provide an auditable log of all visitors to the organization and provide information on who in the organization is accountable for a given visitor. An example visitor log with recommended fields can be found in Appendix B.

**Personnel Security**

Strong personnel security is critical, as it is the last barrier before physical access to a network.

There are several policies that can bolster the effectiveness of personnel security.

- **Protect user information**

  Inform users not to give out their personal information or others’ via the Internet in person, or over the phone to unknown parties. If someone calls asking for an associate who is unavailable, instruct users not to tell the caller how to contact the individual. Instead instruct users to ask the caller for callback information and to provide that information to the individual once he or she is available.
• Conduct background checks on potential employees

Background checks should be conducted on all potential new employees before they start to check for criminal records and get a better idea of the character and ethics of the individual (Dolan, 2004).

• Training

Training the members of an organization helps to support both the physical and digital security measures. Training personnel on what signs to watch out for that could signal an attack and what information is acceptable to give out is crucial. Sample training course outlines are discussed in the “User Workshop” section of this paper.

Prior to implementing personnel training, meetings with leadership should be held to reviewing what the organization deems as sensitive information. Meeting hosts should review steps organization members should take to verify a person’s identity before granting anyone access to material or information.

Digital Security
The final barrier in mitigating social engineering attacks is the digital one. Securing the network is the administrator’s last hope of stopping an attack from. Administrators should employ multiple security measures to make it as difficult as possible for an attacker to successfully infiltrate the network. At the very least, such measures should be:

• Strict password policies
Ensure passwords meet a predetermined complexity requirement. Also, force users to change their passwords at a predetermined interval to ensure compromised passwords do not become a significant liability. Establishing a policy on password delivery retention will ensure users cannot soon reuse a password (Mitnick & Simon, 2002).

Randomly generated passwords consisting of a variety of key types (i.e., capitals, special characters, and numbers) and at least 8 characters in length are considered very secure from a technological perspective, but are not necessarily secure from a user perspective. When working with most users, the more complex a password becomes the less secure it may become. For example, the password “1_Lik3_T@c03s!” can be considered to be more secure from a user perspective than “&G9f4jh8%vcS,” as it meets typical password complexity requirements as well as can be easily remembered compared to the second, randomly generated password. While the second password is more secure from a technical perspective, it illustrates the dilemma of how the more complex a password becomes, the less likely users will remember it. If they cannot easily remember their password(s), users will resort to writing it down; defeating is purpose of being secure. Social engineers know this. The classic location to check is for a sticky note stuck under one’s keyboard, or worse, on the side of a user’s monitor.

In an everyday environment, it may be better to compromise. Dissuade users from choosing easily guessed passwords such as birthdays or a pet’s name. At the same time, provide users with tips to make secure, easy to remember passwords. Suggest users substitute numbers for letters, such as using 3 instead of E. Another simple solution is to
recommend users reverse the password string to make it less likely to be guessed by an attacker or broken by a password cracking program, utilizing brute force or dictionary based attacks.

- **Strict firewall rules**
  Configuring and maintaining strict firewall rules helps to keep an attacker out. Ensure content filters are up to date when utilizing website blocking technology to help prevent users from stumbling across websites that could be a source of Trojan Horses or are known pharming sites.

- **Strong email filtering**
  Setting up and maintaining email spam filters will further ensure users do not become prey to phishing attacks, chain emails, viruses, or worms that could harm or steal personal information.

- **Multifactor authentication**
  Multifactor authentication, commonly implemented as two-factor authentication, provides challenges to ensure the user is allowed access. In two-factor authentication, a user is challenged with what he or she knows and what he or she has. Under this method, the user (determined by the username) must enter what he or she knows (e.g., a password) and provide information on what he or she has (e.g., a token that generates a key string).
Incorporating two-factor authentication via the use of a token such as a SafeWord or RSA token helps to protect users in the event their username and password are compromised. Even with their account information in the wrong hands, the risk of that information leading to a further breach is unlikely without the acquisition of the security token.

To establish three-factor authentication, the user must also provide information pertaining to who they are. This third authentication step can incorporate biometric security, as discussed in the physical security section of this paper.

- **Strong (128+bit) encryption**
  
  For sensitive information, protecting it with at strong encryption scheme of at least 128bit provides another safeguard against information tampering. Encryption should be used whenever possible, if the data warrants it, to ensure the data’s confidentiality if it were to fall into unauthorized hands. Encryption should also be used to secure websites, emails, VPN tunnels, hard drives, or any resource that can be accessed from outside the physical location.

- **Limited wireless network access (none if possible)**
  
  Wireless network access significantly increases the risk of a breach by removing the need to be on the premises to access the local network. If a social engineer were able to obtain a user’s login credentials, he or she would not even need to step foot into the building if a wireless access point was present. If the need for wireless access cannot be avoided, then several steps should be taken to mitigate the risks it creates. First, use a strong encryption
method such as WPA 2. WEP has proven far too easy an encryption protocol to break. In independent testing, weaker WEP key strings (64bit WEP keys) were able to be passively sniffed and cracked within several minutes (Kaliburn, Sienkiewicz, & Spinapolice, 2007). Second, choose a strong passphrase, similar to a password, but typically longer, to be used with the encryption method. Third, use a RADIUS server to help authenticate users onto the wireless network. Finally, segment the wireless network onto its own subnet or VLAN. This subnet should be created especially if the wireless network will be available to visitors and provide only limited internal network access.

- Access control lists

Create policies to manage and enforce access control lists. Whether device-based, role-based, or user-based, access controls are one of the final lines of defense against losing information. Ensuring people do not have global access to important information helps mitigate the risk that a user’s stolen credentials will compromise the entire network. It cannot be said enough that administrators need to ensure devices and users are only granted access to the information they need and nothing more. Users should never be granted administrative rights to their own workstations, no matter how tech-savvy they claim to be. Even the administrator should not use the administrator or root account unless it is explicitly necessary. Do not use these accounts for day to day activities.

Implementing and maintaining these policies and procedures at the administrative level will greatly lower the risk of a successful social engineering attempt on one’s network. To ensure these policies and procedures remain a strong deterrent to social engineers as well as strong
protection against attack attempts, administrators still need to provide adequate training to users to ensure they follow similar best practices in protecting the network. Establishing guidelines for future audits to test the policies and procedures will further solidify their effectiveness by revealing any weaknesses in the current setup. The audit results will then aid in rectifying any discovered issues.

**User Training**

In addition to following their own best practices, administrators need to ensure users are aware of the practices and that they obey security guidelines. If users do not see administrators following their own best practices, then the users will follow suit (Dubin, 2003). To combat a weak security atmosphere, administrators should develop several strategies to train and remind users of the danger of attacks and best practices on how to mitigate them. One method of preventing users from letting their guards down is to educate them as to what social engineering is and how to protect against it is via a series of communication, training, and awareness workshops (Twitchell, 2006).

These user workshops enable the administrators to teach users signs to look out for regarding potential attacks and what to do when they identify them. Mitnick (2002) states:

“The central goal of any security awareness program is to influence people to change their behavior and attitudes by motivating every employee to want to chip in and do his part to protect the organization’s information assets” (p. 250).

Before any training begins, it is recommended that the entire IT staff, including helpdesk personnel, network/systems administrators and IT security personnel, be introduced to the users.
In doing so, administrators can reduce the risk of an impersonation attack where an attacker may pose as a helpdesk worker or other staff member. Far too often the network support staff is segregated from the rest of the organization’s population.

Manjak (2006) argues, “Employees will not be motivated to change behaviors if they see no reason to change” (p. 12). During user training sessions, Mitnick (2002) notes one way to motivate users to protect an organization’s information is to make them understand that doing so not only helps protect the organization but also themselves, since the organization retains personal information about all employees. This point is particularly important with payroll information containing salaries, social security numbers, and contact information.

During these training sessions, administrators should cover four basic topics:

- **Social engineering terms**
  
  When gauging users’ knowledge of social engineering, Gross and Rosson (2007) found while many users knew terms such as phishing, none had heard of social engineering nor did they fully understand its meaning. To this end, users must be educated as to what social engineering is and what aspects of the human condition social engineers prey on. Simply being aware of such information will begin to make users more vigilant in their day-to-day activities.

- **Types of social engineering attacks**
  
  The training should highlight to users various attack methods, starting with the most common attacks such as phishing and pharming. Other methods, such as
reverse-social engineering, may require a role playing demonstration to fully illustrate the anatomy of such an attack.

- Ways to defend against attacks
  After users understand the types of attacks and how they occur, administrators must review prevention methods. This section of the training session can focus on various techniques pertaining to the best practices security model (see Figure 4).

- Steps to take when an attack is suspected
  Emphasize that while the goal is to prevent an attack, security can never be one hundred percent effective. In light of this, users should be instructed to notify support staff when they think an intrusion is taking place. Typically, the personnel to be notified would be the network administrative and security teams. If the attack is happening in person, advise users to notify any onsite security personnel.

Classroom-Based Course
To further examine the benefits and structure of a social engineering training session, the author collaborated with an instructional design consultant at ICF International, located in Fairfax, Virginia. The goal laid forth was to devise an outline for a classroom-based course to educate employees with little to no knowledge of social engineering methods and attacks.
Course Objectives

Three main objectives for the course were isolated. By the end of this training session, learners will be able to:

1. Recognize social engineering techniques.
2. Describe techniques for mitigating the risks of social engineering attacks.
3. List security rules of the organization.
4. Describe the importance of following corporate security policies, practices, and procedures.

Course Layout

The devised course was broken down into four main sections:

1. Introduction and knowledge transfer
2. Class participation and activities
3. Review of organization’s rules and policies
4. Objectives review and Q&A

Introduction and Knowledge Transfer

The course would commence with introductions from the security, systems and network team, allowing employees to put names to faces and know who manages the organization’s IT infrastructure. Definitions of social engineering would follow accompanied by reasons employees should care about and be aware of social engineering attacks. Students would be taught the various human conditions attackers attempt to exploit as well as methods employed to exploit said conditions.
**Group Participation Activities**

The activities section of the course would open with several case studies of successful attacks. Details and examples would be given describing the attacks, including information attackers were after, methods used, and their motivation for the attack.

Several questions were devised to ask to the class after each case study to verify participants understand the anatomy of the attack and can actively devise ways to identify and prevent the attack. Three such questions are:

1. What was the objective of the social engineering attack?
2. What techniques were used?
3. How could the victim(s) have prevented the attack?
4. What would you do if you detected or suspected this attack in your office?

**Review of Organization’s Rules and Policies**

After the case studies and class discussions, review of the organization’s policies and procedures would commence. Types of sensitive information that could be compromised would be discussed. Additionally, incentives for following rules in addition to consequences for lack of compliance would be disseminated to the group.

**Objectives Review and Q&A**

Following the review of the organization’s policies, students would be asked to answer questions reviewing the objectives of the course. Students would be asked to define social engineering in their own words as well as to describe steps they would take to prevent themselves from falling victim to an attack.
Following the course review, the floor would be open to questions and answers by the class. The questions would be directed to both the instructor as well as the network and systems administrators.

**Course Length and Recurrence**
In discussion with the instructional designer, it was agreed that such a proposed course would last for approximately two hours in length. Maximum students per session should be kept to roughly 30-50 employees to ensure adequate time and resources for knowledge transfer and any questions from the students. Employees should be required to repeat the course once a year as part of their annual employee training schedule. Such a course could be classroom-based either on or offsite of the organization. Web-based training for such material was deemed unacceptable, since emphasis should be placed on face-to-face introductions of and interactions with the IT staff to the organization’s general population.

An example agenda for such a training session can be found in Appendix C. Additional sample questions to either ask users during the training or have them answer on their own can be found in Appendix D.
Audit Guidelines
Implementing a strong set of policies and procedures and properly training personnel, does not mean an administrator’s network is now secure from social engineering attackers. These new guidelines must be tested to ensure their effectiveness. To ensure proper testing, appropriate auditing techniques must be used. Since social engineering focuses less on the technology and more on the users of the technology, regular system security audits may not properly ensure quality social engineering attack protection. Most security audits simply do not cover aspects of an organization that are vulnerable to social engineering attacks (Jones, 2003). Current security audits should be modified, or new ones created, to deal with the issues surrounding social engineering.

Audit Preparation
Chris Jones (2003) states it is important that an audit focused on social engineering address four key items:

- Define mission and objectives – focus the audit on important aspects within the organization.
- Obtain permission – ensure proper trust between auditors and staff before any action is taken that can be seen as unauthorized activity.
- Notify employees – ensure that auditors are not mistaken for legitimate social engineers. It should be noted that if the audit is being performed under the guise of a mock social engineering attack, only key employees (such as the systems administrators and department heads) should be notified beforehand.
• Review current policies and procedures – allows administrators to review current guidelines for accuracy and relevance and make comments or suggestions where appropriate.

When deciding what information the audit will attempt to gather, administrators should also decide whether such information will be quantitative or qualitative (Manjak, 2006). In most cases, administrators will seek a combination of both data types. Some audit findings, such as password length and complexity, will be quantitative. Other audit findings, such as users’ reactions to the audit process, will be qualitative.

A proper audit for social engineering preparedness should be conducted under two methods:

• Procedure review
• Procedure testing

Procedure review audits consisting of reviewing all policy and procedure documentation. This audit can be performed by internal control auditors (with the help of the system administration staff). While internal auditors may have the most knowledge about the inner workings of an organization, using outside auditors can be beneficial as they bring a unique perspective. This audit should be seen as a good way of maintaining a current set of policies and procedures for all personnel to follow. Information such as defining high priority systems and identifying access verification procedures, and breach response policies should all be reviewed and updated as needed. No policy or procedure will help protect an organization’s assets if it is irrelevant to the organization’s physical and virtual configuration.
In addition to organizational relevance, no policy or procedure will protect an organization’s assets if the policies and procedures are not executed by the organization’s staff. To ensure staff members are adhering to the organization’s best practices, procedure testing auditing is needed. To perform this type of audit correctly, outside, trusted auditors must be used, since this audit, in effect, conducts one or more social engineering attacks against the organization to gauge the effectiveness of the policies, procedures, or personnel preparedness. Unlike the policy review audit, where it is permissible for other staff to be aware of the audit, this audit should be conducted with few people’s knowledge. This faux attack will help expose any lapses in security policies and identify what personnel or resources are weak points real attackers may target. An example audit attack can be found in Appendix F.

Many organizations are leery of these types of audits, as it can be seen as a lack of trust in the organization’s staff by not informing them of such audits. To minimize the fear many organizations have to a social engineering attack simulation, conducting a survey may be a desirable alternate attack method rather than attempting a covert breach (Orgill, Romney, Bailey, & Orgill, 2004). Properly conducted, surveys can prey on aspects such as friendliness and quid pro quo while being a variant of phishing for information. An example of audit survey questions auditors can ask can be found in Appendix E. A sample audit survey attack can be found in Appendix G.

**Audit Timeline**
A timetable should be established on when either type of audit should be conducted. While the procedure review audit be scheduled at fixed intervals, either yearly or bi-yearly, the procedure testing audit should have a more flexible schedule. Administrators can establish policies to
determine the number of testing audits to do per year, but they should not be on a fixed annual schedule. This floating schedule will allow the audits to be more effective as users will not know exactly when to expect the audit(s).

**Example Audit**
Tony Greening (1996) provides a detailed example for a quick social engineering audit to demonstrate the power of impersonation mixed with exploiting authority roles. For his test, Greening sent an email to college students asking them to email him their computer lab account passwords to verify their accounts because they had received word of an intruder accessing the network. Out of the students who were believed to have read the email (estimated to be 291 students), 175 replied. Greening then took the passwords they emailed and compared them to their true computer lab account passwords. Greening found that out of the 175 passwords collected, over 78% of them were legitimate. Table 1 shows Greening’s breakdown of received passwords.

<table>
<thead>
<tr>
<th>Password Type</th>
<th># of Replies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legitimate</td>
<td>138</td>
</tr>
<tr>
<td>Possible</td>
<td>12</td>
</tr>
<tr>
<td>Fake</td>
<td>18</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>175</strong></td>
</tr>
</tbody>
</table>

This high percentage of correct passwords shows that while not all students were willing to divulge their true passwords, more than three fourths did so without any consideration as to who was sending the email and if the recipient could or should be trusted.
Conclusion

Impact of Social Engineering
Social engineering attacks can severely damage an individual’s or organization’s reputation and revenue very quickly (Gulati, 2003). There have been numerous stories in the past years about unprotected laptops being stolen containing confidential or personal information such as social security numbers, credit card information, or health records. Social engineering, to some degree, was used to obtain those devices either by people within the organization or by outside individuals eager to obtain any data they could.

The concept of social engineering for deceitful purposes is nothing new nor is its application to gain access to computer systems and networks. While it certainly is not a new avenue of attack, new methods of performing such attacks are being devised. While no router or firewall will be 100% hack proof, the stronger and more powerful these and other devices become, the more attackers will resort to alternate means to get their desired information. Increasingly, attackers will resort to relatively low tech attack methods as technology continues to advance. An attacker will look for the easiest method with the largest possible payoff and not spend countless hours trying to hack into a network appliance or server when engaging someone in conversation (in other words, hacking the person) will yield the same information in minutes.

Social engineering attack attempts (regardless of the medium) will continue to increase if organizations continue to invest and focus solely on new technology to solve their IT security dilemmas. Administrators must shift focus from the technology to the users of the technology that will help mitigate social engineering attacks. From defining best practices to conducting thorough risk vs. threat analysis, administrators can arm themselves with the tools and
knowledge necessary to mitigate such attacks. Administrators should not aim for a blanket “trust no one” approach to attack prevention, but they should always strive to keep in mind that, unfortunately, not everyone can be trusted.
Appendices

Appendix A – Administrator’s Best Practices

Physical Security Practices

☐ Issue photo ID badges to all staff (combine with RFID or mag-stripe with user information)

☐ Create policies around ID badges (e.g., uniform badge symbols, colors for department divisions, etc.)

☐ Use biometric access if possible (e.g., fingerprint ID, hand scan, etc.)

☐ Mandatory sign-in sheets for all visitors

☐ Issue ID badges to all visitors

☐ Install surveillance cameras and form retention period for recorded video

☐ Install auto locking, ID required doors
Personnel Security Practices

☐ Conduct staff training workshops to teach and review user best practices on a scheduled basis

☐ Create confidentiality policy (e.g., what records are kept, who has access to records)
  - Disable systems administrator access to HR records so only essential personnel can access them

☐ Keep a regularly updated list (including photos) of all personnel

☐ Create policy to revoke user rights on user termination (e.g., disabling account, removing permissions, notifying employees of departure)
Digital Security Practices

☐ Enforce complex password policies and password age policies (including administrator password(s))

☐ Establish firewall rules to lower the hacking risk

☐ Block known malware websites

☐ Filter for possible malware websites/pharming websites

☐ Establish email filters to cut down on spam/phishing emails

☐ Require multifactor authentication to all systems (e.g., username & password + RSA or other authentication tokens)

☐ Encrypt sensitive data (e.g., databases, confidential emails, wireless transmissions)

☐ Establish role-based access to provide for easier administration

Audit Best Practices

☐ Schedule yearly security audits to ensure best practices are being followed

☐ Conduct mock attacks to check for vulnerabilities annually

☐ Conduct legitimate surveys to gauge user’s knowledge and preparedness of attacks biannually

☐ Conduct yearly cleanup of systems to expunge unused/obsolete accounts
Appendix B – Visitor Log Example

*BASIC EXAMPLE COMPANY VISITOR LOG*

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
<th>Guest of ___</th>
<th>Time in</th>
<th>Time out</th>
<th>Visitor badge ID #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visitor’s name</td>
<td>Visitor’s organization</td>
<td>Who is responsible for the visitor’s whereabouts*</td>
<td>Time the visitor arrived</td>
<td>Time the visitor left</td>
<td>Badge number assigned to visitor</td>
</tr>
</tbody>
</table>

* Responsible party shall remain with guest at all times during their visit
Appendix C – User Workshop Agenda

The following is a general agenda of topics and activities that should be covered in an employee workshop to ensure proper security awareness training to the staff:

- Introduction of network and systems administration staff
- Motivations for protecting organization’s information
- What is at stake if information security and/or confidentiality is breached
- Contacts for reporting potential breaches
- Overview of policies and procedures
  - Password policies
  - Physical security policies
  - Guest admittance policies
  - Person verification practices
- Importance of verification and authentication and personal/organizational/legal consequences of internal breach of policies and procedures
- Overview of human conditions attackers will prey on
  (e.g., commitment, social proof, friendliness)
- Overview of tactics attackers may use
  (e.g., phishing, impersonation, pre-texting)
- Sample scenarios
- Review of what was discussed/question and answer session
Appendix D – User Workshop Sample Questionnaire

1. What is social engineering?

____________________________________________________

____________________________________________________

____________________________________________________

2. Name at least 3 human factors social engineers prey on and attempt to exploit?

____________________________________________________

____________________________________________________

____________________________________________________

3. Name at least 3 types of social engineering attacks

____________________________________________________

____________________________________________________

____________________________________________________

4. What are at least 5 things you can do to protect yourself from social engineering attacks?

____________________________________________________

____________________________________________________

____________________________________________________

____________________________________________________

5. Why is protecting the organization’s information relevant to you?

____________________________________________________

____________________________________________________

____________________________________________________

____________________________________________________
6. Who should you contact (name & phone number) if you feel someone is trying to use social engineering on you to gain information? ________________________________

______________________________
Appendix E – Sample Procedure Review Audit Form

- What are the current password policy settings for the domain (including password age/complexity/length)?
- List of users with domain admin rights
- List of users with database admin rights
- List of all servers that manage financial/personal/proprietary information
- List of users with access to financial/personal/proprietary information systems
- Current firewall rules
- Current network access rules
- List of users with physical access to server room
- List of all current employees with photo ID
- Visitor logs kept since prior audit
- Log of all potential breaches reported to security team
## Appendix F – Sample Procedure Testing Audit

### Basic Sample Attack Scenarios

<table>
<thead>
<tr>
<th>Auditor Name</th>
<th>Name used</th>
<th>Contact name &amp; title</th>
<th>Information Desired</th>
<th>Description of Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>auditor 1</td>
<td>John Smith</td>
<td>Sara: Systems Analyst</td>
<td>User's username:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>User's password:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Manager's contact info:</td>
<td></td>
</tr>
<tr>
<td>auditor 2</td>
<td>Larry Jones</td>
<td>Tom: accountant</td>
<td>User's username:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>User's password:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Manager's contact info:</td>
<td></td>
</tr>
<tr>
<td>auditor 3</td>
<td>Julie Meadows</td>
<td>Gregg: paralegal</td>
<td>User's username:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>User's password:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Manager's contact info:</td>
<td></td>
</tr>
<tr>
<td>auditor 4</td>
<td>Mike Richards</td>
<td>Johanna: junior sales</td>
<td>User's username:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>associate</td>
<td>User's password:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Manager's contact info:</td>
<td></td>
</tr>
</tbody>
</table>
Appendix G – Sample Audit: Survey Method

Cover story: new systems administrator conducting survey for head administrator.

Does not want to let new manager down with this task to complete network usage survey.

<table>
<thead>
<tr>
<th>Name</th>
<th>Username</th>
<th>Last time changed password</th>
<th>Last password used</th>
<th>Current password length</th>
<th>Title</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Works Cited


http://www.ftc.gov/bcp/conline/pubs/credit/pretext.shtm


Infosecurity Europe. (2008, April 16). Women 4 times more likely than men to give passwords for chocolate. Retrieved April 17, 2008, from Infosecurity Europe:
http://www.infosec.co.uk/page.cfm/T=m/Action=Press/PressID=1071

http://www.giac.org/certified_professionals/practicals/gsec/3521.php


Retrieved July 12, 2007, from SANS Institute:
http://www.sans.org/reading_room/whitepapers/engineering/1686.php


http://www.sans.org/reading_room/whitepapers/engineering/512.php


http://www.schneier.com/blog/archives/2008/04/people_and_secu.html


