SANS | GIAC CERTIFICATIONS

WHITE PAPER

Methods for Understanding and Reducing Social Engineering Attacks

Michael Alexander

Methods for Understanding and Reducing Social Engineering Attacks

GIAC (GCCC) Gold Certification

Author: Michael Alexander, michael6933@yahoo.com
Advisor: Rick Wanner
Accepted: April 30, 2016

Abstract

Social engineering is widely recognized by cyber criminals as one of the most effective methods of penetrating an organization's infrastructure. Information security professionals are aware of this as a threat but to date have never seemed to focus their efforts on studying and understanding in depth how and why cyber criminals are using this as a weapon. Electronic means of penetration are far easier to focus on because they are straightforward in their techniques and thus their prevention. But hacking the "wetware" tends to be viewed as much more difficult to prevent due to the seemingly unlimited number of variables humans present. While prevention is all but impossible, more research and better methods of understanding how and why an organization's representatives are easy targets would go a long way to reduce the success of these penetration efforts.

1. Introduction

> *"The biggest threat to the security of a company is not a computer virus, an unpatched hole in a key program or a badly installed firewall. In fact, the biggest threat could be you."* - *Kevin Mitnick*

Social engineering is arguably the easiest way for an attacker to penetrate the defenses of an organization. As part of protecting an organization, most experts agree that training the end point users to be aware of the types of threats they may encounter is essential to an effective information security strategy (Mitnick & Simon, 2002).

But most training for end point users is centered on electronic threats such as how to detect a phishing or spear phishing attack or how to avoid downloading and installing malware. While these threats are still considered social engineering due to their deceptive element, perhaps a seemingly benign phone call from an alleged internal technician claiming to need access so they can verify a problem is more of a threat. Electronic-based social engineering is potentially easier to train for as it happens more regularly and users can be taught not to open emails from anyone they do not recognize. But human-based social engineering, for example a phone call from a seemingly trustworthy person or even letting a stranger tailgate into the office simply because they have on what appears to be an official uniform can be a much more serious threat. Yet the reality is most organizations do not properly train their employees to recognize these potential hazards (Hadnagy, 2011).

By contrast, human-based social engineering attacks, that is, attacks either by phone or in person, are much more subtle and more difficult to detect because they involve the very complex and seemingly unlimited scenarios that come about from day-to-day interaction with other human beings. These complexities are exploited because of the innate desire of humans to be trusting, helpful and just generally a "good person" (Peltier, 2006). Attackers use these desirable traits in people and leverage them for their own purposes.

The root cause of this problem lies with the type of training that most organizations provide for their employees (Johnston, Warkentin, McBride, & Carter, 2016). As a rule,

Michael Alexander, michael6933@yahoo.com

organizations are primarily interested in how to generate more sales. Additionally, any issue encountered that becomes a detriment to that objective also becomes a high priority. In the 21st century economy, prospective clients in a business-to-business market often use security questionnaires to determine if a potential vendor is secure enough to form a partnership (Lord, 2016). One of the questions on that questionnaire that must be answered in the affirmative for the partnership to proceed is, "Do you require security awareness training for all employees at least annually?". Most experts agree that being able to truthfully answer "Yes" to that question is the primary motivation for having any type of security awareness training at all. And therein lays the problem. Organizations are more interested in "checking the box" to be able to answer that question truthfully than they are in actually preventing breaches that could result in data loss (Winkler and Manke, 2013).

2. What is Social Engineering?

Most industry professionals are very familiar with social engineering and its dangers. But it should be noted that social engineering has many definitions depending on one's experience and how it may have manifested itself in the past. If one were to perform an internet search on *"*What is Social Engineering in Information Security*?",* one may be presented with a nice, concise definition such as this one from Whatis.com:

"*Social engineering is an attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures."*

While all of this is true, it presents a very simplistic view of a much more complex problem. That problem, at least in part, involves training employees to recognize and understand a social engineering attack when, where and how they see it.

However social engineering is defined it is important to note the key ingredient to any social engineering attack is deception (Mitnick and Simon, 2002). The attacker must deceive either by presenting themselves as someone that can and should be trusted or, in the case of a phishing attack for example, by deceiving the user into thinking a correspondence has a benign or even useful purpose when it was intended all along to gain access to sensitive information (Peltier, 2006).

3. Real Life Examples of Successful Social Engineering Attacks

Social engineering attacks are much older than the internet, the electronic age or even the industrial revolution. Generals and military leaders have been using some form of deception in warfare almost since the beginning of warfare itself. Probably the most famous of these, as depicted in many books and movies, is the instance of the Greek-Trojan war (Bryce, 2005). Most are familiar with the story of the ten-year long campaign between the two nations. The Greeks appear to have been defeated and, as a parting gift, built a large wooden horse and left it at the gate of Troy and then appeared to have retreated. The Trojans, thinking that they were the victors, brought the horse into the city and began their victory celebration (Peters, 2015). Unbeknownst to the Trojans, the Greeks had hidden a small military unit of a few soldiers inside the horse. After the celebration ended and while the Trojans slept, the Greek soldiers simply slipped out of their hiding place and opened the gates for the Greek army who had returned in anticipation of a successful deception. The ensuing battle was very short and ended in the resounding defeat of the Trojans. Whether this is truth or fiction, the story has made such an impression on the information security community that a particular form of malware now bears the name “Trojan horse” (Peters 2015).

While that story is a profound cautionary tale, there are at least two recent examples of attacks that can only be described as ironic. One happened in 2011 to security company RSA. RSA had a two-factor authentication product they sold under the name SecurID. The attacker sent two different phishing emails over a two-day period. The two emails were sent to two small groups of employees. These users were not high profile or high value targets. The email subject line read "2011 Recruitment Plan" (Heyden, 2011).

The email was crafted well enough to entice one of the employees to open the attached Excel file. It was a spreadsheet titled "2011 Recruitment plan.xls" containing an Adobe Flash exploit. Once inside the network, the attacker performed privilege escalation attacks to gain access to higher value administrator accounts. Such stepping stone attacks allow hackers to escalate from compromised access to a low value account into accounts with administration-level privileges before carrying out the end purpose which is often the extraction of commercially or financially sensitive information. According to reports, RSA detected the

attack in progress but the attackers still managed to extract sensitive data (Schwartz, 2011). The exact data that was extracted is unknown but what is known is that there were serial numbers of the SecurID token product that would allow the attacker to gain access to any system that the approved user is attempting to authenticate against using that token.

A second case of irony was the breach at information security white-listing company Bit9. In 2013, the "Hidden Lynx" cyberespionage group in China used water-holing attacks to compromise security firm Bit9's digital code-signing certificates, which later were used to target some Bit9 customers (Krebs, 2013).

Watering holes are much more subtle than phishing attacks. Malware is injected into a legitimate website that organizations in the target industry are likely to visit. The deception, and what qualifies this as a social engineering attack, is that users working in the target industry are known to frequent the target site and have done so many times without incident, thereby making them unsuspecting of anything nefarious.

The attackers accessed Bit9's file-signing infrastructure in order to sign malware and make it seem legitimate. They then used it to attacked Bit9 itself, at least three of its customers, and three defense industrial base organizations that were customers of Symantec (Peters, 2015).

And finally, social engineering attacks are not just limited to ancient warfare or information security companies. The consequences of a successful security breach generated by a social engineering attack can be massive to an organization. Case in point: the retail giant Target.

In December 2013 in the midst of a busy holiday shopping season, Target experienced a breach on their point of sale system that allowed attackers to steal some 40 million credit card numbers (Olavsrud, 2014). Forensic evidence shows that the point of sale system was not the original target, but because Target was PCI-compliant, they were not storing credit card numbers in their database. So while the attackers were able to access the database and thus extract millions of customer's personally identifiable information, they were thwarted in their efforts to extract their ultimate target; the credit card numbers of millions of Target customers.

This all began not with a breach at the retailer initially but by breaching an HVAC vendor that Target was using at the time. The initial compromise occurred via a phishing

attack on the vendor. The attack allowed the attackers to access to a web service that Target had set up for vendors to submit invoices (Olavsrud, 2014).

4. Methods Used by Social Engineers to Gain Access to Sensitive Information

4.1 Electronic access

As previously discussed, social engineers use myriad ways to gain access to sensitive information. But the one common element in all the techniques is deception. Whether they are attempting to deceive by sending a phishing email or by posing as a technician on the phone or by standing outside the office door wearing an official-looking uniform armed with knowledge that appears to indicate familiarity, it is all about deceiving a target into giving them sensitive information (Ashford, 2016).

Most people feel they are immune to such trickery because they are somehow smarter or more aware than others. The fact is almost everyone will fall victim to some form of social engineering in their lifetime. It may not lead to a massive data breach. It could be as simple as a child using a smile or a compliment on a parent to manipulate them into allowing the child to stay up just a little longer. The compliment may have been heartfelt and genuine but if the purpose of giving the compliment is anything other than to make the recipient feel better about themselves, that is manipulation, deception and, therefore social engineering. The fact is any form of deception for personal gain falls into the category of social engineering.

The techniques used by social engineers fall into the following basic categories. There are potentially others but these seem to be the most common.

4.1.1. Phishing

Phishing scams might be the most common types of social engineering attacks used today. Most phishing scams tend to have the following characteristics (Bisson, 2015):

- They seek to obtain personally identifiable information (PII), such as names, addresses and social security numbers.

- They tend to use shortened URLs or embed links that redirect users to sites that appear legitimate.
- They usually attempt to instill a sense of urgency in the user by using some sort of fear tactic or a threat in an attempt to get the user to act immediately.

Some phishing emails are more poorly crafted than others to the extent that their messages oftentimes exhibit spelling and grammar errors but these emails are no less focused on directing victims to a fake website or form where they can steal user login credentials and other personal information (Workman, 2008).

A recent scam sent phishing emails to users after they installed cracked APK files from Google Play Books that were pre-loaded with malware. This specific phishing campaign demonstrates how attackers commonly pair malware with phishing attacks in an effort to steal users' information (Whitwam, 2015).

4.1.2. Spear Phishing

Spear phishing is very similar to phishing attacks with one major difference. Whereas phishing attacks tend be very scattered by nature; that is a phishing email can be sent to thousands of domains, spear phishing is much more targeted. Usually a spear phishing attack will focus on a single organization, a group of individuals within an organization or even a single individual (Zitter, 2015). The intent is the same a phishing but the success rate is often higher because the attacker will often research the organization or individual for weeks or months to find any vulnerability they can exploit. For example, if an attacker learns via social media that a certain CEO has a soft spot for a certain charity, they can fabricate an email that will exploit that and maybe even dupe the CEO into revealing sensitive personal or organizational information.

In an actual spear phishing attack attempt, KnowBe4, a Security Awareness Training and Simulated Phishing platform company in the Tampa, FL area, received a spear phishing email in September 2015. It was received by KnowBe4's Controller allegedly from the "CTO" requesting a wire transfer. Since the Controller, was well trained in what to look for, she immediately went to the CEO. The CEO decided to engage the attacker and to appear to comply with the request. The attacker apparently had performed some cursory research on the

company and was able to identify the Controller and CTO but clearly not enough research to know they were dealing with experts in spear phishing techniques (KnowBe4 press release, 2015).

"Since we send millions of simulated phishing emails to our 2,000+ enterprise customers every year, we decided to have some fun with these scammers", said KnowBe4's CEO Stu Sjouwerman. Had the attacker spent a little more time to see what we actually do, he might have changed his mind from his attempt at wire fraud."

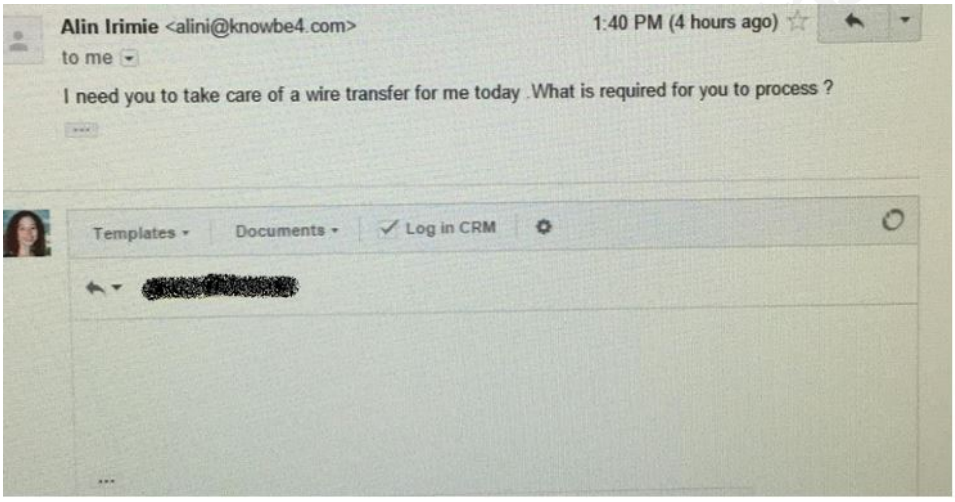

Figure 1. Screenshot pf actual email sent to KnowBe4 in an attempt to have funds wire transferred.

KnowBe4 analyzed the attackers email. The email headers revealed that the attacker created a hosting account with GoDaddy to get access to an email delivery system. The attacker then used an open source mail client to spoof email headers and pick up the replied to emails on an AOL account.

The CEO had the Controller reply back and to the attacker and simply ask "How much and where to?" The attacker's reply back contained the bank wire information with real bank info but a fake company name and address. KnowBe4 decided to phish back the attacker and created a fake AOL email account which claimed the attacker's account was locked. The attacker then made a fatal error and clicked on the link which allowed KnowBe4 to get his IP address. This data was then sent over to the AOL security team and the FBI's Internet Crime Complaint Center (KnowBe4 press release, 2015).

Michael Alexander, michael6933@yahoo.com

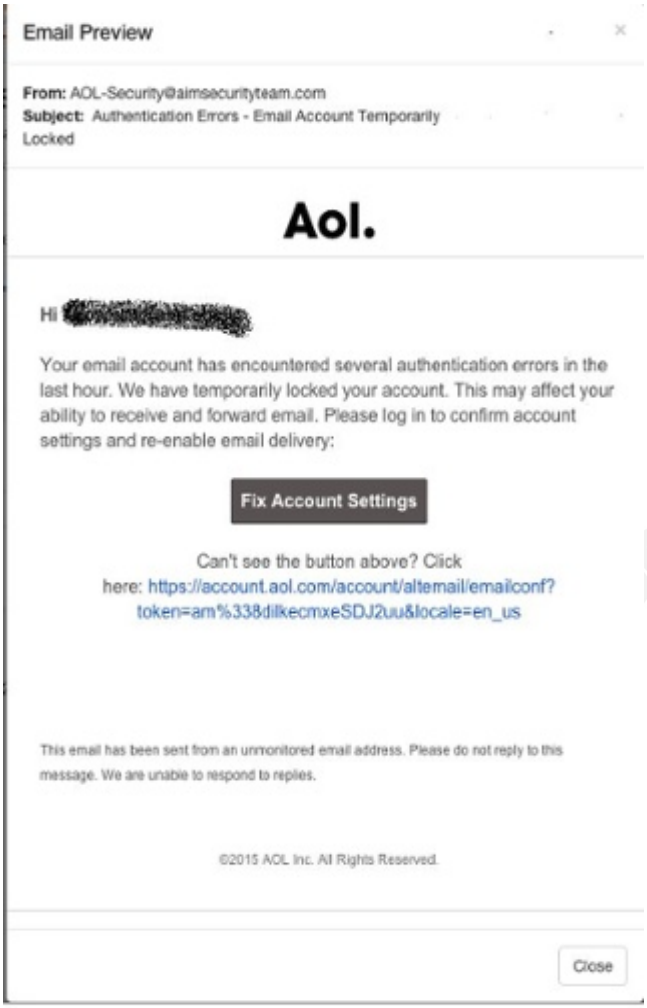

Figure 2. Actual email sent from KnowBe4 back to the attacker. When the attacker clicked on the link, KnowBe4 captured their IP address which they forwarded to the FBI to investigate.

4.1.3. Baiting

Baiting is in many ways similar to phishing attacks. However, what distinguishes baiting from other types of social engineering is the promise of an item or good that hackers use to entice victims. Baiters may offer users free music or movie downloads if they provide their login credentials to a certain application or web site (DeWolf, 2013).

Baiting attacks are not restricted to online schemes, either. Attackers can also focus on exploiting human curiosity via the use of physical media.

One such attack was documented by Steve Stasiukonis, VP and founder of Secure Network Technologies, Inc., back in 2006. To assess the security of a financial client, Steve and his team infected dozens of USBs with a Trojan virus and dispersed them around the organization's parking lot. Curious, many of the client's employees picked up the USBs and plugged them into their computers, which activated a key logger and gave Steve access to a number of employees' login credentials (Johansson, 2008).

4.2. Physical Access

4.2.1. Pretexting

Pretexting is another form of social engineering where attackers focus on creating a good pretext, or a fabricated scenario, that they can use to try and steal their victims' personal information. These types of attacks commonly take the form of a scammer who pretends that they need certain bits of information from their target in order to confirm their identity (Henry, 2014).

More advanced attacks will also try to manipulate their targets into performing an action that enables them to exploit the structural weaknesses of an organization or company. A good example of this would be an attacker who impersonates an external IT services auditor and manipulates a company's physical security staff into letting them into the building (Ashford, 2016).

Unlike phishing emails, which use fear and urgency to their advantage, pretexting attacks rely on building a false sense of trust with the victim. This requires the attacker to build a credible story that leaves little room for doubt on the part of their target (Bisson, 2015).

Pretexting attacks are commonly used to gain both sensitive and non-sensitive information. In one such instance, a group of scammers posed as representatives from modeling agencies and escort services, invented fake background stories and interview questions in order to have women, including teenage girls, send them nude pictures of themselves (Workman, 2008).

4.2.2. Tailgating

Another social engineering attack type is known as tailgating or "piggybacking" (Bisson, 2015). This type of attack involves an unauthorized individual following an employee or other authorized individual into a restricted area.

In a common type of tailgating attack, the attacker impersonates a courier and waits outside a building. When an employee gains security's approval and opens the door to their office area, the attacker asks that the employee hold the door, thereby gaining access off of someone who is authorized to enter the company.

Tailgating does not work in all corporate settings, such as in larger companies where all persons entering a building are required to swipe a card. However, in mid-size enterprises, attackers can strike up conversations with employees and use this show of familiarity to successfully get past any badge-based security in place (Peltier, 2006).

4.3.3. Quid Pro Quo

Similarly, quid pro quo attacks promise a benefit in exchange for information. This benefit usually assumes the form of a service, whereas baiting frequently takes the form of a good.

One of the most common types of quid pro quo attacks involve attackers who impersonate IT service people and who "vish" call as many direct numbers that belong to a company as they can acquire. These attackers offer IT assistance to each and every one of their victims. They will promise a quick fix in exchange for the employee disabling their AV program and for installing malware on their computers ostensibly as a software update (Bisson, 2015).

It is important to note, however, that attackers can use much less sophisticated quid pro quo offers than IT fixes. As real world examples have shown, office workers are more than willing to give away their passwords for a cheap pen or even a bar of chocolate.

In fact, Colin Greenless, a security consultant at Siemens Enterprise Communications, used these same tactics to gain access to several different floors, as well as the data room at an FTSE-listed financial firm. He was even able to base himself in a third floor meeting room, out of which he worked for several days (Bisson, 2015).

Michael Alexander, michael6933@yahoo.com

Allowing physical access to a server room or even an endpoint is extremely dangerous from an information security perspective. Once a bad actor has this level of access they can easily install USB devices such as a WAN turtle or a rubber ducky that will either allow them access via a shell or can automatically run simple scripts that will infect an end point and give an attacker access from anywhere.

4.3. Social Media

And finally, beyond electronic and physical means of social engineering, there is a third category. It can be considered "electronic" access but it is really more of a hybrid between electronic and physical/virtual access because it requires electronics to access an individual's information but using that information to an attacker's advantage may include some sort of "virtual" interaction i.e. a message on Facebook or a comment on an Instagram post (Algarni, Xu, Chan, & Tian, 2014).

Many people online today tend to be way too free in sharing of what they see as harmless or benign information. But hackers view this information quite differently; especially those whose preferred attack vector is identity theft. And to exacerbate the situation, the sharing of personal information is usually encouraged by the social media sites themselves. That is their way of knowing how to target an individual for advertising. The more a social media site knows about a person's interests and habits, the more likely they are to present advertising that will be enticing and effective and, ultimately, the more revenue they will generate. Advertisers want more targeted advertising because targeted advertising equates to more revenue per advertising dollar spent.

Below are some types of information to avoid sharing on social media as they tend to be used as answers to security questions and often tend to be included in passwords (Lewis, 2014).

- Full name (especially middle name)
- Date of birth
- Pet's name
- Home town
- School locations and graduation dates

- Other affiliations, interests and hobbies

But social engineering on social media is not about targeting information about users. It can also be used to create fake profiles that appear legitimate for the purposes of garnering connections and trust (Algarni, Xu, Chan, & Tian, 2014).

In 2015, security researchers discovered more than two dozen bogus LinkedIn profiles that were apparently created with the intent of compromising the security of organizations involved in various industries including telecommunications, utilities, defense and government (Paganini, 2015).

The eight core profiles of the group claimed to be employees of such firms as Northrup Grumman, Airbus, Teledyne and South Korean holding firm Doosan. The rest of the fake profiles were created to fill out the network and make the core profiles seem more legitimate.

According to InfoWorld, five of the eight core profiles claimed to be corporate recruiters, a role that would justify cold-contacting potential targets of the hack. It could make those targets more likely to believe the profiles and potential job offers were authentic.

Security researchers were able to identify the fake profiles through close examination of profile details. For example, some of the profile photos turned up elsewhere on the Web, often on adult sites, while job descriptions used text from help wanted ads (Robinson, 2015).

By the time the fraudulent network was exposed and taken down, it had developed connections to upwards of 500 real individuals, located primarily in the Middle East, North Africa and South Asia.

The challenge for firms and their employees is that the sort of scrutiny that exposed this hacking effort is tedious, time-consuming and generally beyond the means of many individuals or even entire organizations (Robinson, 2015).

5. The Psychology of Social Engineering

Now that social engineering has been defined and the tools and techniques social engineers use to exploit the "wetware", the next step is to understand why humans fall prey to those tools and techniques. The questions this section seeks to address are as follows:

1) Do all humans fall victim at some point to social engineering attacks?
2) Are certain people with certain personality types or other innate qualities more susceptible to these types of attacks?
3) Are certain people with certain personality types or other innate qualities more susceptible to these types of attacks?

5.1. Question 1: Do all humans fall victim at some point to social engineering attacks?

The first question has to do with common general tendencies and human nature. The fact is that social engineering is rooted in deception and all humans are susceptible to being deceived. There are a few reasons for this but the one most relevant to this topic stems from how most parents' in today's society teach children to be, as the Boy Scouts' motto states, Trustworthy, Loyal, Helpful, Friendly, Courteous, Kind, Obedient, Cheerful, Thrifty, Brave, Clean, and Reverent.

Notice that there are at least four characteristics that society considers valued in that list that are preyed upon by social engineers (Peltier, 2006.) The first is trustworthy. As part of a civilized society, most strive to be trustworthy. And in doing so, expect that most others are attempting likewise. So when a social engineer approaches an individual to gain unauthorized entrance into an office, what makes that individual unsuspecting is the fact that they, themselves attempt to be honest and trustworthy and tend to assume that of a total stranger (Workman, 2007). Even after successful completion of a security awareness training program that specifically addressed this as a threat, the engrained teachings from childhood are often too much to overcome. The target will often have initial pangs of skepticism and then relent after just a few seconds without any further evidence that the attacker is legitimate. When asked later about why they allowed the attacker to gain access, the answer is often "They appeared to be legitimate" or "They had an honest face" (Hadnagy, 2011).

The second valued characteristic that social engineers prey upon is loyalty. That may seem contradictory because an employee who goes against company-sponsored security awareness training is displaying the opposite of loyalty. In fact, the behavior being displayed appears to be betrayal. But the question is one of motivation. The target perceives that by

allowing access to the facilities to someone who appears to be a vendor or contractor, they are being a good employee (Peltier, 2006). In their own mind, they are being loyal so loyalty, not betrayal is the motivation that is being preyed upon by the social engineer even though the end result is, in fact, a betrayal.

Valued characteristic number three that is often exploited by social engineers is probably the most preyed upon. It is the tendency and desire of people to want to be helpful (Peltier, 2006). Most people feel that being helpful is a true win-win. Helping others provides a service that is clearly desired and needed at the time but it also makes us, as humans, feel good about ourselves. From the time a dad asks a son to help with the yard work to helping mom carry in groceries to just being a good employee, being helpful is engrained in the DNA of humans. Social engineers exploit that innate desire to be a helpful by appearing to be in desperate need of help. Even if that means an employee bends the rules a bit to provide that help, it seems like the "right thing to do" (DePaul, 2013). A typical ploy of a social engineer would be to stand outside an office waiting for an authorized employee to enter and then declare to them that they are new and have forgotten their badge. Often the employee will allow them entrance without the slightest hesitation or confirmation that they even work there.

And finally, the desire of humans to be obedient is a characteristic often exploited by social engineers (Henry, 2014). This is certainly a learned characteristic as it not intuitive for any child to be obedient. As individuals, people tend to want to do what they want to do when they want to do it without any regard for the wishes of others. Parents have to fight this tendency in young children in order to contribute to a society of order. If this were not taught, the result would be children who grow up to do whatever they like whenever they like. It is easy to imagine that a society filled with these individuals would quickly devolve into chaos.

Once learned and understood, this characteristic becomes more of an instinct. This is particularly true in a professional setting where the livelihood of an individual could be at stake if they are insubordinate. Almost always, the adaptive personality of an individual in a professional setting includes that of being obedient. As a professional, tasks are assigned and expectation of management is that those tasks are to be completed in the time provided. A social engineer often uses that tendency enhanced by the environment of the workplace and

coupled with a deception of some sort to manipulate an employee (Huang, Ryan, Zabel, & Palmer, 2014). A typical exploit would be a social engineer posing as someone who has authority granted to them by the leadership. The attacker seems legitimate in that they know something about the processes and the chain of command. Posing as having direct orders from someone the target knows to be in charge and seemingly having enough information about the situation to appear credible, the target feels that being "obedient" to the demands of the attacker is in their best interest professionally.

There is little doubt that the answer to Question 1 is a resounding yes; all humans are susceptible to social engineering because social engineering is based on deception and all humans are susceptible to being deceived. It is important to note that social engineering in this context does not necessarily have to be an attack. Any form of manipulation through deception can be considered social engineering.

5.2. Question 2: Are certain people with certain personality types or other innate qualities more susceptible to these types of attacks?

5.2.1 Overview

As previously noted, certain experiential or cultural factors can and do contribute to the likelihood of a successful social engineering attack. These are learned responses or responses as a result of one's environment. But are there innate factors built into one's personality or behavioral tendencies that contribute to a successful attack as well? If so, can these innate tendencies be overcome by targeted training?

Personality traits and tendencies vary greatly from person to person. By nature, some people are more trusting as opposed to more suspicious (Johnston, Warkentin, McBride, & Carter, 2016). Some people are more giving as opposed to more selfish. As this applies to social engineering, the attacker seeks to exploit those who, by their very nature, tend to be more helpful and more trusting (Abraham & Chengalur-Smith, 2010). Unlike learned responses from our previous topic, understanding the tendencies an individual possesses takes time and effort. A social engineer may not target an individual soon after meeting them but as the relationship matures, the attacker may see an opportunity based on observation that an individual is more likely to be susceptible to attack based on their tendencies. This is

especially true after a trust has formed over a period of time. In fact, the "attacker" may never have intended to become an attacker. At some point, however, based on months of observation, they saw an opportunity to exploit a particular tendency of an individual and they took advantage.

Just as with learned responses, the innate tendencies of humans can be overcome by training and awareness (Johnston, Warkentin, McBride, & Carter, 2016). The person who leaves their wallet open and unattended must be trained that this habit creates a risk. Often this training is most effective in the form a scare to the target. If an honest colleague notices the wallet being left open and unattended, they could temporarily take a credit card to train the target. When the target notices it missing, the trauma of that makes an indelible impression that is not soon forgotten. The next time they start to leave the area with their wallet open, they will no doubt be reminded of that incident and take the appropriate action to secure their belongings.

5.2.2 Determining personality types scientifically

As discussed in the previous section, tendencies of individuals can be observed, documented and ultimately exploited by individuals who are so inclined. The problem with determining an individual's tendencies using this method is that is it reactive (Aitel, 2012). Only after an exploitation has occurred will the tendency be recognized and corrected and, perhaps, not even then.

To address the problem of being reactive, an organization must become proactive. If those risky tendencies could be tested for, analyzed, and accounted for in advance of such a breach, the breach could be prevented or at least minimized (Johnston, Warkentin, McBride, & Carter, 2016). One way to do this is to scientifically assess the personality types and behavioral patterns of individuals. Many organizations already do this for other purposes such as placing the employee with the right personality in a role that is best suited for their personality (Bariff & Lusk, 1977). Or to ensure that they are placed on a team or teams that will create a synergistic work environment with other team members with either similar or complementary personalities to avoid conflicts or even promote conflict which often fuels creativity and competition.

There are several tools and techniques that have been created over the years that can scientifically help determine the personality traits of an organization's human resources. For the purposes of this discussion, the focus will be on the method outlined in Table 1 below. It is referred to as the Big Five or OCEAN. OCEAN is an acronym for the five primary personality traits: Openness, Conscientiousness, Extraversion, Agreeableness and Neuroticism (Zhuang, 2006).

Big Five Trait	Trait Description
Openness to experience	"[People scoring high on the openness scale are] characterized by such attributes as open-mindedness, active imagination, preference for variety, and independence of judgment."
Conscientiousness	"People [scoring] high on the conscientiousness scale tend to distinguish themselves for their trustworthiness and their sense of purposefulness and of responsibility. They tend to be strong-willed, task-focused, and achievement-oriented."
Extraversion	"People scoring high on the extraversion scale tend to be sociable and assertive, and they prefer to work with other people."
Agreeableness	"People [scoring] high on the agreeableness scale tend to be tolerant, trusting, accepting, and they value and respect other people's beliefs and conventions."
Neuroticism	"People [scoring] high on the [neuroticism] scale tend to experience such negative feelings as emotional instability, embarrassment, guilt, pessimism, and low self-esteem"

Table 1. The primary personality traits and their descriptions.

The table below is references the OCEAN table above. It outlines how certain personality types based on the OCEAN frameset are more or less likely to violate cybersecurity policy. It takes into account other factors as well such as Threat Severity, Self-Efficacy, Sanction Severity and Response Cost. It clearly demonstrates the correlation between personality types and their likelihood of falling victim to a social engineering attack (Johnston, Warkentin, McBride, & Carter, 2016).

Individuals who are less likely to violate cybersecurity policies	Individuals who are more likely to violate cybersecurity policies
• Open individuals with a low sense of Self-Efficacy • Open individuals with a low sense of Threat Severity • Open individuals with a low sense of Response Cost • Conscientious individuals with a low sense of Threat Severity • Extroverted individuals with a low sense of Sanction Severity • Agreeable individuals with a low sense of Self-Efficacy • Agreeable individuals with a low sense of Sanction Severity • Neurotic individuals with a low sense of Self-Efficacy • Neurotic individuals with a low sense of Sanction Severity	• Open individuals in general • Open individuals with a low sense of Sanction Severity • Conscientious individuals with a low sense of Response Efficacy • Extroverted individuals with a low sense of Threat Severity • Extroverted individuals with a low sense of Threat Vulnerability • Extroverted individuals with a low sense of Response Cost • Agreeable individuals with a low sense of Sanction Certainty • Neurotic individuals with a low sense of Sanction Certainty

Table 2. The breakdown of how some personality types based on OCEAN are more or less likely to violate security policies.

5.3. Question 3: Can a security awareness training program be customized based on the personality type, experiential commonalities or other traits that will reduce the likelihood of successful attacks?

Many organizations tend to perform security awareness training by using a third party of some kind. This is accomplished typically by either contracting a security firm to perform this training live or by purchasing a third party training tool such as software or videos. This, of course, implies that the third party provides a "canned" solution that covers the basics at a high level but does not take the time or effort to understand the detailed training needs of the organization. From the organization's perspective, this is a necessary evil. Often the organization is just "checking the box" so when a client asks if they have a security awareness training program, the organization can truthfully answer yes (Winkler and Manke, 2013).

As attackers become more sophisticated and more targeted in their attacks as with spear phishing or advance persistent threats, this approach is quickly becomes grossly inadequate. In the near future, security awareness training must become as sophisticated as the attacks. Otherwise, there will be little use in having it all. To do this, security awareness training must train at the same level at which the attacks occur. For example, if an attack targets a particular individual based on their position in the company or their privileged access, security awareness training must train those individuals separately and in greater detail and specifically for how they are likely to be attacked. A system administrator, for example, is likely to be attacked because of their privileged access in a very different way than an administrative assistant. An accounts payable employee may be attacked differently than a CFO because the AP person has the ability to create and print checks or has certain sensitive bank account information readily available whereas this is rarely the case for a CFO. Security awareness training as a "check the box" exercise will not adequately train the individuals in an organization that are most likely to be targeted based on their access to sensitive information (Winkler and Manke, 2013)..

Even end users security awareness training needs to be overhauled to take into account the innate personality traits and tendencies as previously noted. If an attacker has compromised a particular user and monitors their behavior, the attacker may notice that they frequent a particular website that is not related to the company but that is a personal interest of the employee. In this scenario, it would be reasonable to assume that the attacker could perform some type of man-in-the-middle attack that spoofs the site and asks for certain sensitive information (Lewis, 2010). The user then enters their sensitive information and submits it thinking it was securely handled by a trusted site. What actually happened is the user just sent their sensitive information to the attacker. End users are almost never trained to be wary of legitimate websites that everyone frequents such as Google or Amazon and how to tell the difference between the legitimate site and a spoofed one. But an attacker can spoof almost any site. Very few users are aware of this even though most of them go through "security awareness training" annually (Bullée, Montoya, Pieters, Junger, & Hartel, 2015).

This is just one example of how, unless security awareness training becomes more sophisticated, organizations will remain vulnerable to attackers especially through social

engineering. There are literally of hundreds of other social engineering scenarios not mentioned. And while it may impractical to train all employees on every potential threat, it is possible to modularize training based on certain threat vectors such as access level, internet usage or even personality types.

6. The Solution

Ultimately the solution is to create an in-house, custom built security awareness and training program. It must take into consideration all the factors that affect the organization as well as the behavioral and personality factors previously discussed. It must be planned, designed, implemented and measured. It must be "baked-in" to the everyday processes of the organization until it becomes part of the culture of the organization.

6.1. Plan the training

The first step in planning the training is to establish the goals of the training. The goals must realistic, attainable and measurable (Gupta, n.d.). The actual goals will vary from organization to organization but some examples might include:

- Ensure all employees learn the security policies and procedures by the end of Q2.
- Reduce use of internet for personal reasons by 30%.
- Reduce the number of security-related incidents due to social engineering by 30% by the end of Q3.

The next step is to plan the personality testing. Plan time to research and select the best personality test for the organization. The OCEAN method mentioned previously is just one example (Johnston, Warkentin, McBride, & Carter, 2016). Others include Myers-Briggs, The Caliper Profile and DISC. There are countless others. Care should be taken to select the best testing for the organization.

Finally the format and delivery method of the training should be determined. This should take into account all factors such as training facilities available, training materials, location of employees if organization is global, various languages. A project plan should be laid out to determine all relevant tasks, planned start and end dates for each task, predecessors and projected complete date of the training.

Michael Alexander, michael6933@yahoo.com

6.2 Perform the personality testing

Once the proper testing vendor has been selected, the personality testing should begin as soon as possible. This is because the design of the program itself cannot begin until the personality testing is complete.

Once the testing is complete, analyze the results to categorize employees based on personality type (Johnston, Warkentin, McBride, & Carter, 2016). There can be as many or as few as makes sense but it should be noted that a custom training program will be created for each category.

6.3 Design the security awareness program

Once the testing and analysis is complete, the design of each program can begin (Gupta, n.d.). The design should be tailored to focus on the potential strengths, and more importantly, the weaknesses of each personality type.

For example, if a particular employee tests that they fall into the Extroverted personality type and it is known that Extroverts with a low sense of Threat Severity are more likely to violate company security policies; they will be trained to fully understand all known threats and the consequences of those. This is not to say that all employees will not receive that training as well but for Extroverts it will be a point of focus.

6.4 Develop the security awareness training

Now that personality and design are complete, the development of the training can begin (Gupta, n.d.). The design should be tailored to focus on the potential strengths, and more importantly, the weaknesses of each personality type. From the planning process, training materials must be created, facilities must be secured and schedules must be finalized. A testing of the materials should be performed on a small cross-functional group of employees and feedback should be collected and incorporated where appropriate. Also, this is where success criteria should be determined so that when results are measured, management will know whether or not the program is a success.

Michael Alexander, michael6933@yahoo.com

6.5 Implement the security awareness training

This is culmination of the previous steps. Planning is complete, personalities have been determined and categorized, and training materials have been written and rewritten. Assuming all those were done properly, the delivery of the training should go smoothly. It is important to note that the delivery of the training will (and should) evolve over time (Gupta, n.d.). Also, this is when the corporate culture should begin to shift. Policies and timelines should be implemented to ensure security awareness becomes engrained in the mindset of each employee and it becomes a natural part of the organization's processes.

7. Conclusion

Social engineering is more prevalent and more of a threat than it has ever been. As Figure 3 indicates, attacks as a result of social engineering began to skyrocket in 2004 and it does not appear that a slowing of this trend is happening in the near future.

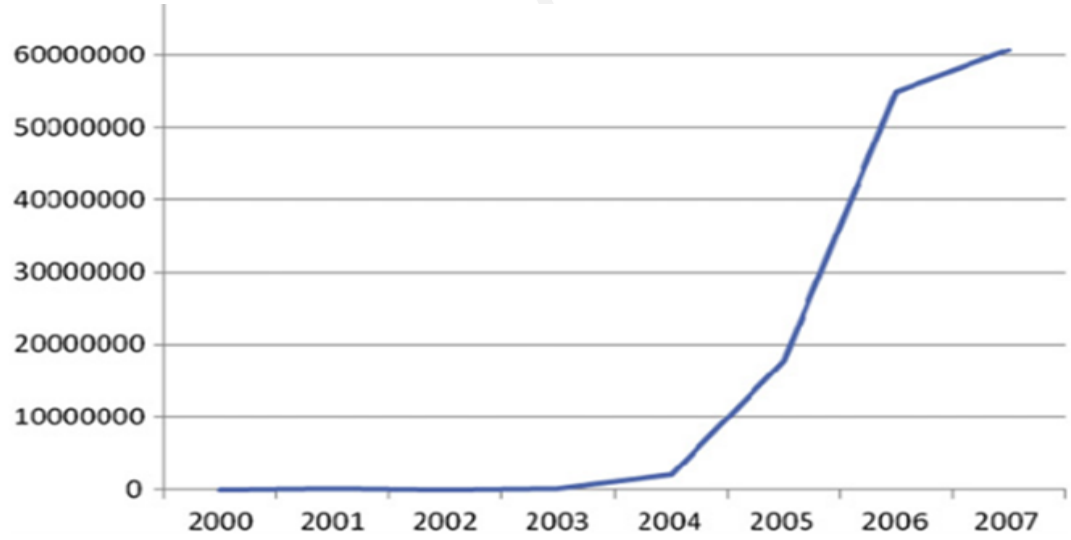

Figure 3. Number of security incidents as a result of social engineering.

Attacks on an organization's sensitive information using social engineering are more targeted and more sophisticated than ever before. Security awareness training has not kept pace with the level of social engineering sophistication. Despite this fact, the cybersecurity community refuses to recognize the seriousness of the threat. In fact, in the latest version of

the 20 Critical Controls, released October 2015 by the Center for Internet Security, the ranking of the relevant control, namely "Security Skills Assessment and Appropriate Training to Fill Gaps", fell from number 9 in Version 5 to number 17 in Version 6. It is important to note that these controls are ranked in order of severity of threat. It stands to reason if the cybersecurity community does not recognize the threat as critical, then the organizations to which they offer consulting services will not either. As a result, employees continue to fall for social engineering attacks at an alarming rate and are costing organizations billions annually (Ashford, 2016). While it is impossible to prevent all attacks on the wetware because there are so many complexities and variables within the human mind, security awareness training can and should be improved.

The challenge for an organization is to review their current security awareness training program objective. Determine if its real purpose is to prevent breaches and potential data loss or is it just to "check the box" and be able to truthfully answer a prospect's security questionnaire. Once that question has been answered, the next challenge is to proactively determine which of an organization's employees are most susceptible to social engineering attacks by scientifically determining their personality traits and tendencies. One way to determine this would be to document which employees over a given time period have been victimized by social engineering attacks and test them to determine their personality types and tendencies. Then review the personality profiles of the victims and cross reference for similarities. Then once every employee has been tested, it should be obvious which of the employees are most likely to become victims. Finally, the last challenge is too customize and tailor their security awareness training program to address the tendencies of the highest risk employees. This effort should be based on several factors such as what type of social engineering was used to victimize the target (phishing, quid pro quo, etc.). Then tailor a targeted training program to just those employees that focuses on the exact type of social engineering that was used.

It should be noted that not every cybersecurity professional agrees with this approach. There is a school of thought that states that spending money on security awareness training is wasteful. The argument is that any budget allocated for security awareness training would be better spent on the security of networks, servers and workstations (Aitel, 2012). The theory is

that better security of the hardware and software would prevent any employee from being allowed to compromise an organization's data. It should further be noted that this opinion is in the vast minority. Most credible cybersecurity professionals agree that more and better training will prevent some social engineering attackers from reaching their objectives.

Proper security awareness training takes time and is costly. It requires a strong commitment from an organization to follow through on all the steps outlined above. But compared to the potential cost of a breach in both dollars and reputation to the brand, it is insignificant. With information security much more of a front-and-center topic than it has ever been, with companies spending millions securing their data, does it make sense to leave this area so exposed to threat?

References

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, 32(3), 183-196.

Aitel, D. (2012). Why You Shouldn't Train Your Employees for Security Awareness. *CSO*. Retrieved April 14, 2016 from http://www.csoonline.com/article/2131941/security-awareness/why-you-shouldn-t-train-employees-for-security-awareness.html?nsdr=true

Algarni, A., Xu, Y., Chan, T., & Tian, Y. (2014). Social engineering in social networking sites : how good becomes evil. In *Proceedings of The 18th Pacific Asia Conference on Information Systems* (PACIS2014), The Association for Information Systems (AIS), Chengdu, China.

Applegate. S.D. Major. (2009). Social Engineering: Hacking the Wetware! *Information Security Journal: A Global Perspective*, 18:1, 40-46, DOI: 10.1080/19393550802623214

Ashford, W. (2016). Social engineering is top hacking method, survey shows. *ComputerWeekly.com*. Retrieved March 22, 2016 from http://www.computerweekly.com/news/4500272941/Social-engineering-is-top-hacking-method-survey-shows

Bariff, M. L., & Lusk, E. J. (1977). Cognitive and personality tests for the design of management information systems. Management Science, 23(8), 820-829.

Bisson, D. (2015). 5 Social Engineering Attacks to Watch Out For. *Tripwire.* Retrieved March 13, 2016 from http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

Michael Alexander, michael6933@yahoo.com

Bryce, T. (2005). The Trojan War: Myth or Reality? The Kingdom of the Hittites, 357-371. doi:10.1093/acprof:oso/9780199281329.003.14

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. Journal of experimental criminology, 11(1), 97-115.

Burgess, C. (2015). Three Reasons Social Engineering Still Threatens Companies. *Security Intelligence*. Retrieved April 15, 2016 from https://securityintelligence.com/three-reasons-social-engineering-still-threatens-companies/

Chatterjee, C. (2015). 5 personality tests hiring managers are using that could make or break your next job interview. *MSN Money*. Retrieved March 30, 2016 from http://www.msn.com/en-nz/money/careersandeducation/5-personality-tests-hiring-managers-are-using-that-could-make-or-break-your-next-job-interview/ar-BBl1TRB#page=2

Cullina, M. (2012). 9 Alarming Statistics About Identity Theft. *IDT911*. Retrieved March 12, 2016 from http://idt911.com/education/blog/9-alarming-statistics-about-identity-theft

Dattner, B. (2014). Most Work Conflicts Aren't Due to Personality. *Harvard Business Review*. Retrieved from https://hbr.org/2014/05/most-work-conflicts-arent-due-to-personality/

DePaul, N. (2013). Hacking the Mind: How & Why Social Engineering Works. *Veracode*. Retrieved March 12, 2016 from https://www.veracode.com/blog/2013/03/hacking-the-mind-how-why-social-engineering-works

DeWolf, J. (2013). 5 Types of Social Engineering Attacks. *Datto*. Retrieved April 20, 2016 from http://www.datto.com/blog/5-types-of-social-engineering-attacks

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, *59*, 26-44.

Gardner, B., & Thomas, V. (2014). *Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats*. Elsevier.

Goodchild, J. (2011). Social engineering: 3 examples of human hacking. *CSO*. Retrieved March 12, 2016 from http://www.csoonline.com/article/2126983/social-engineering/social-engineering-social-engineering-3-examples-of-human-hacking.html?nsdr=true&page=2

Gupta, M. (n.d.). Designing and developing an effective Security Awareness and Training program. *National Institute of Standards and Technology*. Retrieved April 23, 2016 from http://csrc.nist.gov/organizations/fissea/2009-conference/presentations/fissea09-mgupta-day3-panel_process-program-build-effective-training.pdf

Hadnagy, C. (2011). Social engineering: The art of human hacking. Indianapolis, IN: Wiley.

Huang, J. L., Ryan, A. M., Zabel, K. L., & Palmer, A. (2014). Personality and adaptive performance at work: A meta-analytic investigation. *Journal of Applied Psychology*, *99*(1), 162-179. doi:10.1037/a0034285

Henry, A. (2014). Why Social Engineering Should be Your Biggest Security Concern. *Lifehacker*. Retrieved April 3, 2016 from http://lifehacker.com/why-social-engineering-should-be-your-biggest-security-1630321227

Michael Alexander, michael6933@yahoo.com

Heyden, J. (2011). RSA explains how attackers breached its systems. *The Register*. Retrieved March 9, 2016 from http://www.theregister.co.uk/2011/04/04/rsa_hack_howdunnit/

Johansson, J. (2008). Island Hopping: The Infectious Allure of Vendor Swag. *Technet Magazine.* Retreived April 14, 2016 from https://technet.microsoft.com/en-us/magazine/2008.01.securitywatch.aspx

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: influences on information security policy violations. *European Journal of Information Systems*. doi:10.1057/ejis.2015.15

KnowBe4 Press Release. (2015). KnowBe4 Foils CEO Fraud Attack Thanks to Security Awareness Training. Retreived April 3, 2016 from https://www.knowbe4.com/press/knowbe4-foils-ceo-fraud-attack-thanks-to-security-awareness-training

Krebs, B. (2013). Bit9 Breach Began in July 2012. *KrebsonSecurity*. Retrieved April 12, 2016 from http://krebsonsecurity.com/2013/02/bit9-breach-began-in-july-2012/

Lewis, K. (2014). How Social Media Networks Facilitate Identity Theft Fraud. Entrepreneurs' Organization. Retrieved March 22, 2016 from https://www.eonetwork.org/octane-magazine/special-features/social-media-networks-facilitate-identity-theft-fraud

Lewis, N. (2010). Email, website and IP spoofing: How to prevent a spoofing attack. *TechTarget*. Retrieved April 17, 2016 from http://searchsecurity.techtarget.com/tip/Email-website-and-IP-spoofing-How-to-prevent-a-spoofing-attack

Michael Alexander, michael6933@yahoo.com

Lord, N. (2015). Social Engineering attacks: common techniques & how to prevent an attack. Digital Guardian. Retrieved March 18, 2016 from https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack

Lord, N. (2016). Data Security Experts Reveal the Biggest Mistakes Companies Make with Data & Information Security. *Digital Guardian*. Retrieved April 3, 2016 from https://digitalguardian.com/blog/data-security-experts-reveal-biggest-mistakes-companies-make-data-information-security

Mitnick, K. and Simon, W. L. (2002). The art of deception: Controlling the human element of security. New York: John Wiley & Sons.

Olavsrud, T. (2010). 9 Best Defenses Against Social Engineering Attacks. *eSecurity Planet.* Retrieved March 12, 2016 from http://www.esecurityplanet.com/views/article.php/3908881/9-Best-Defenses-Against-Social-Engineering-Attacks.htm

Olavsrud, T. (2014). 11 Steps Attackers Took to Crack Target. *CIO.* Retrieved March 18, 2016 from http://www.cio.com/article/2600345/security0/11-steps-attackers-took-to-crack-target.html?nsdr=true

Okenyi, P. O. and Owens, T. J. (2007). On the anatomy of human hacking. *Information Systems Security.* , 16(6), 302–314. Retrieved April 8, 2016 from Academic Search Premiere database

Paganini, P. (2015). According to the Symantec firm, a growing number of threat actors in the wild are targeting professionals on LinkedIn with fake LinkedIn profiles. *Security*

Affairs. Retrieved April 2, 2016 from http://securityaffairs.co/wordpress/42498/cyber-crime/fake-linkedin-profiles.html

Pascual, A., Marchini, K., Miller, S. (2016). 2016 Identity Fraud: Fraud Hits an Inflection Point. *Javelin.* Retrieved March22, 2016 from https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point

Peltier, T. (2006). Social Engineering:Concepts and Solutions. *Information Systems Security*, 15:5, 13-21, DOI: 10.1201/1086.1065898X/46353.15.4.20060901/95427.3

Peters, S. (2015). The seven best social engineering attacks ever. *InformationWeek Dark Reading*. Retrieved March 10, 2016 from http://www.darkreading.com/the-7-best-social-engineering-attacks-ever/d/d-id/1319411?image_number=4

Robinson, R. (2015). Social Engineering Attackers Deploy Fake Social Media Profiles *Security Intelligence*. Retrieved April 18, 2016 from https://securityintelligence.com/social-engineering-attackers-deploy-fake-social-media-profiles/

Schwartz, M. (2011). RSA SecurID Breach Cost $66 Million. Information Week Dark Reading. Retrieved April 11, 2016 from http://www.darkreading.com/attacks-and-breaches/rsa-securid-breach-cost-$66-million/d/d-id/1099232?

Vidalis, S. & Kazmi, Z. (2007). Security Through Deception, *Information Systems Security,* 16:1, 34-41, DOI: 10.1080/10658980601051458

Whitwam, R. (2015). Google Play Books Is Crawling With Fake 'Guides' That Promise Cracked Android APKs, Provide Only Malware And Phishing Scams. *Android Police*. Retrieved April 14, 2016 from http://www.androidpolice.com/2015/03/03/google-play-

books-is-crawling-with-fake-guides-that-promise-cracked-android-apks-provide-only-malware-and-phishing-scams/

Winkler, I. and Manke, S. (2013). 7 Reasons for Security Awareness Falure. *CSO* . Retrieved March18. 2012 from http://www.csoonline.com/article/2133697/metrics-budgets/7-reasons-for-security-awareness-failure.html?nsdr=true

Workman, M. (2007). Gaining Access with Social Engineering: An Empirical Study of the Threat. *Information Systems Security*, 16:6, 315-331, DOI: 10.1080/10658980701788165

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the American Society for Information Science and Technology, 59(4), 662-674.

Zhang L. (2006). Thinking styles and the big five personality traits revisited. *Personality and Individual Differences*. 40:1177-11187.

Zitter, K. (2105). Hacker Lexicon: What Are Phishing and Spear Phishing?. *Wired*. Retreived April17, 2016 from https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/