Social Engineering

Alvin Cheung

ACC 626 – Spring 2012

Introduction to Social Engineering

As we continue to increase our reliance on computer systems by using them to store and process the world's information, they have become increasingly popular targets for attackers looking to disrupt, or steal from, the target company. In response to this threat, companies around the world are projected to invest over 151 billion dollars on IT security projects in 2012[1] in an attempt to protect their businesses. So why, despite these large investments, do we often see constantly see large companies with strong IT systems suffer from service disruptions and leaked information? According to Kevin Mitnick, described by the US government as the most dangerous hacker in the world[2], the cause of this could be because "it is much easier to trick someone into revealing a password for a system than to exert the effort of hacking into the system".

Social Engineering, according to Mitnick, is the use of influence and persuasion to deceive people into divulging information[3]. While Mitnick was the first to coin the term, the art of social engineering itself is nothing new; in a crude example, International Intelligence claims that social engineering started "way back in time when man started to lie to woman."[4] However, the art of social engineering has enjoyed a strong resurgence due to the low cost of attacks, anonymity of electronic communication and the ease of researching potential targets thanks to the popularity or email and social engineering sites.

The widespread use of social engineering is undeniable. In the few years alone, we have seen social engineering play a critical role in a number of high profile attacks such as in the government-sponsored attacks that have crippled a highly secure nuclear reactor in Iran[5] and amateur attacks that have been responsible for the leakage of over 500,000 client records by a cloud application provider[6]. These attacks clearly show that in many cases, exploiting the human mind is easiest way to breach an organization's defenses and that social engineering has made IT security a pervasive problem that cannot simply be solved through the provision of hardware or software.

As auditors, we are uniquely positioned to protect our organizations and those we service against social engineering. Unlike most parties within an organization, we are already familiar with the entire organization's internal controls and have an understanding of day-to-day operations. This helps in the identification of soft spots that a social engineer could exploit when attempting to use social engineering to steal information, passwords or even tangible goods. While auditors may not necessarily possess the technical competency to advise on attacks that incorporate the latest software exploits, the ability to

[1] (Wheatman)
[2] (SEO ARTWORKS)
[3] (Paul)
[4] (International Intelligence Limited)
[5] (Farivar)
[6] (Office of Inadequate Security)

identify potential targets of social engineering, prepare the potential targets from attack and to promote a culture of vigilantly skepticism makes auditors an excellent candidate to address the risks posed by social engineering.

This report will serve as a primer on social engineering by discussing several key aspects of social engineering:

- The psychology that powers social engineering
- The Broad categories of social engineering attacks
- Common areas of vulnerability
- Notable cases of social engineering
- Steps to prevent social engineering attacks from succeeding
- Methods to limit the damage caused in a security breach.

The Psychology of Social Engineering[7]:

Although social engineering results in employees simply handing valuable information, products or access to an attacker, it is important to note that the employee generally does not do so maliciously. For example, when social engineers need to gain physical access to an organization, a common tactic is to tailgate an employee into the building in order to bypass the ID scan that opens the door, an automated control. In this case, the employee holding the door for the attacker would not feel as if they were doing anything wrong; the employee was just following normal social conventions that one holds the door for people behind them.

As the aforementioned example demonstrates, in order to understand why social engineering is so effective, we must first understand the qualities of human nature that social engineers prey upon. Thomas Peltier, the author of several books on information security, suggests that there are four fundamental aspects of human nature that social engineers prey upon: the desire to be helpful, the tendency to be trusting, the fear of offending others and the tendency to cut corners:

The desire to be helpful to others

One of the most popular targets for social engineers is an organization's customer facing personnel[8] that provide information and support to external customers because they tend to be easily accessible to an attacker. While companies typically attempt to train these employees to guard confidential information and access to the company's systems by providing detailed conversation scripts, social engineers have found that these employees are easy to manipulate. Customer facing personnel spend every day continually

[7] This section is based on Peltier's paper, "Social Engineering: Concepts and Solutions", Information Systems Security
[8] (Striek)

helping a never-ending line of customers and psychological research has shown that it is incredibly difficult in this situation to question the validity of every interaction[9]. Instead, the customer-facing employee will display a tendency to try to help the customer with his or her problem, even if it deviates from the controls put in place by the company to prevent social engineering from succeeding.

For example, a social engineer could take advantage of this by feigning a strong accent or a poor ability to communicate in English in hopes that a call center employee will circumvent the controls in place to better assist the troubled "customer". If successful, the social engineer may be able to bypass security questions put in place to verify the caller's identity.

The tendency to trust others

In his book, The Art of Deception, Kevin Mitnick describes a fatal flaw that most people share: a tendency to have trust and faith in each other[10]. This blind trust in others has resulted in thousands of people believing stories as ridiculous as a Nigerian prince that needs to enlist the help of a random stranger to transfer vast amounts of money out of his own country[11]. While it is possible that the popularization of the Internet has hardened our defenses against such obvious attempts at social engineering such as advance fee fraud perpetuated by "Nigerian prince"[12], this has not changed the fact that we are still very vulnerable to well-crafted social engineering attacks.

In fact, as presenters hold up obvious cases of social engineering in their organization's awareness campaigns, they unfortunately reinforce a tragic misconception that the average person possesses: that they are too smart to be deceived. The result is that the person has an inflated sense of security and will be easily exploited by social engineers that are discreet enough to only make reasonable requests that will draw no suspicion until it is too late.

The fear of offending others

Being raised in a world of political correctness, we have a tendency to worry about offending others through our words or actions. For example, many people would reluctantly spend several minutes listening to a telemarketer's monologue instead of simply hanging up and/or hesitate to stop a uniformed repairman in their place of business.

Social engineers have been able to exploit this characteristic by gathering information on their targets over "telephone surveys" that can be used to reset the target's password on sites that incorporate security questions[13]. For example, common security questions such as, "what is your hometown" or "what is your first pet's name", could easily be captured by posing as a surveyor asking about a target's pets.

As we are so hesitant to stop a uniformed employee from doing their jobs, it is not surprising that social engineers frequently put on disguises to gain access to employee-only areas. By walking confidently across hallways, the social engineer could gather information or breach systems without any interference at all. For example, by donning the uniform of an electrical technician, a security auditor was able to trick a

[9] (Gragg)
[10] (Mitnick)
[11] (PammingSodom)
[12] (419 Eater)
[13] (Mann)

dozen bank branches into allowing him to wander freely around the premises and install miniature computers onto the organization's network that allowed the auditor to remotely access computers within the network after his departure[14].

The tendency to cut corners

Above all else, social engineering is incredibly successful because of the inherent laziness present in the average person and their willingness to cut corners, especially when the shirking appears to be relatively harmless or inconsequential. This is because people, unlike computerized controls, will naturally become tired and distracted, especially near the end of a shift[15].

A social engineer can exploit this tendency of human nature by observing the employees within an organization and making a note of employees that frequently cut corners in their duties. This process could lead to the discovery of a critical control weakness, which will allow the social engineer to develop a plan of attack to bypass the control. For example, a social engineer could notice that a certain clerk at the post office was erroneously not verifying the identity of patrons that came in with delivery slips. The social engineer could then collect other peoples' delivery slips from nearby apartment buildings to claim as his or her own.

Categories of Social Engineering Attacks[16]

While the term social engineering is often used to describe all trickery used to manipulate people into performing actions or giving up information, the rapid development of electronic means of deception have led some security professionals to believe that social engineering should be segregated into human-based and technology-based components.

Human-based attacks

The human-based type of social engineering relies exclusively on person-to-person communications in order to achieve the desired result. The defining element of these attacks is that they do not require any special technical knowledge and rely completely by gathering information through exploiting the fundamental flaws in human nature previously discussed; For that reason, these techniques are timeless and have been successfully employed throughout human history.

Human-based attacks typically employ one or more of the following methodologies:

i. Impersonation: By finding out the reporting relationships in an organization, the attacker impersonates a person within the organization with power over someone with the necessary information or access privileges and asks the subordinate to gather the information or perform

[14] (McMillan)
[15] (Lineberry)
[16] This section is based on Peltier's paper, "Social Engineering: Concepts and Solutions", Information Systems Security

the task required. For example, a university student could attempt to boost his or her mark by impersonating a professor on the phone to the teaching assistant.

ii. Third Party Authorization: Through research into the organization, the attacker finds the name of a person that has the authority to authorize a certain course of action and attempts to trick a subordinate to do so. For example, a person trying to gain unauthorized access to a club could attempt to convince the bouncer that the owner personally invited him or her in.

iii. In Person: The attacker can simply walk into a building pretending to be an employee, visitor or a contracted service personnel and gather information left unattended. For example, a social engineer notes that by simply wearing a "Xerox" promotional shirt and carrying a toolbox, he is able to walk into secure areas of almost any company[17].

iv. Dumpster Diving: The attacker attempts to gain valuable information about the target by going through the company's trash. This typically leads to valuable information such as discarded bank statements or price lists that are carelessly discarded.

v. Shoulder Surfing: With the rising popularity of laptops in public spaces, a perceptive social engineer could gain information by simply sitting at a coffee shop and watching unsuspecting people reveal their email username and passwords. Using this core piece of info, the social engineer could then gain access to the person's entire online identity.

Technology-based attacks

On the other hand, the advent of modern computing has brought along a new type of technology-based social engineering. Taking advantage of vulnerabilities by using malware or other computer-based exploits, a social engineer attempts to use technology to complement human-based social engineering by either:

i. Tricking the user into installing malware that provides the attacker with remote access to a computer that would otherwise be too secure to breach. This allows the social engineer to gain a level of access to information almost impossible under human-based techniques.

ii. Tricking employees into sending confidential information to the attacker by using technology to create the appearance of legitimate communications. While it can be argued that phishing is nothing new and has existed in traditional mail, the rise of inexpensive anonymous communications has resulted in sophisticated phishing techniques unique to the computer.

Technology-based attacks tend to fall under one of the following methodologies:

i. Software exploits: Technology-based social engineering attacks are constantly evolving in response to new exploits that are found. For example, about a decade ago, Internet Explorer

[17] (Laflotte)

had a flaw that allowed a website owner to read visitors' clipboard contents without their knowledge – social engineers were quick to exploit this vulnerability by finding ways to convince people to copy and paste important information and viewing their webpages.

ii. Email Phishing: By using an email address that looks legitimate, for example, admin@UWATERL00.CA, an attacker may be able to trick a user into responding with confidential information such as their username and password. Alternatively, the attacker may be able to trick the user into opening infected attachments contained within the email message by naming the attachment with a tempting filename such as "Quest Username/Password List 2012".

iii. Website Phishing: An attacker could redirect a person to a website with a URL that appears to be legitimate at first glance. As with the email phishing example, this is usually done by swapping out a letter with a similar looking number or inserting a character into a long URL. This would allow an attacker to direct the user to a login screen that is used to harvest passwords from unsuspecting victims.

Common Areas of Vulnerability[18]

One of the first things that a social engineer does is to create a list of the potential targets within the organization. This list tends to be generated through publically available information such as the company website, employee profiles on LinkedIn, or a call to the company itself. In order to narrow down the list of candidates, a social engineer needs to consider a number of factors:

i. Appropriate access: The social engineer must know that the person being targeted has the appropriate credentials to manipulate or access the information or system that is of interest. For example, if a social engineer is attempting to steal confidential information about software being developed by a firm, gaining access into the secretary's computer may not yield results if the secretary's computer is not connected to the server that holds the software's code.

ii. Assessed resistance: Although only 11 of the 138 people put up any resistance to the social engineering attempts demonstrated at DEFCON 18 security conference, the social engineer must evaluate the selected target's resistance to an attempt at social engineering in order to determine whether the target's viability. For example, a social engineer attempting a technology-based attack would be interested in factors such as the employee's level of technical knowledge while an attacker using a human-based approach may seek out disgruntled ex-employees that will not hesitate to share information about their past employer.

[18] This section is based on Hadagy et al's paper, "DEFCON 18: Social Engineering Capture the Flag Results"

iii. Information availability: Google, Facebook and LinkedIn are three sources of information that are universally used by social engineers in order to obtain background information on their targets. For example, attackers at DEFCON 18 all used LinkedIn to recreate organizational charts by piecing together the profiles of employees at a given company so that they could select an ideal target.
Using this information, attackers are able to develop a plan of attack tailored to the employee. For example, if it is discovered through a search of Facebook that a certain employee plays Farmville during work hours, an attacker may choose to call this employee while pretending to be from the company's IT department noting that an unauthorized site has been visited so that the employee believes that that the attacker must be legitimately IT personnel due to the knowledge of his or her browsing history.

Therefore, it is no surprise that we often find that secretaries, assistants and call-center personnel are often targeted for their access to large amounts of sensitive information and low perceived amount of technical knowledge about information security. Despite the higher likelihood that security experts within the organization would be more likely to spot technology-based attacks, they remain a high-value target to social engineers because of their nearly unlimited access to the company's information systems[19].

Notable Cases of Social Engineering

Since social engineering relies on deceiving an insider into proving access or information, the target company may never notice a perfectly executed attack. Even when the company is aware of an attack, in most cases, the company will do everything in their power to keep the breach a secret in fear of lawsuits and an overall weakened reputation[20]. However, this secrecy shrouds the community as a whole from the importance of effective defenses against social engineering and its power to completely bypass both hardware and software defenses.

Attacks against individuals

Developers of online games use unique CD keys in order to prevent pirated versions of their game from accessing online content. In order to obtain a valid CD key, many pirates turn to social engineering to get a valid key by tricking legitimate customers on online communities. As seen in exhibit I, the attacker does this by posting a set of instructions on how to convert one CD key into multiple keys online, waiting for people to email with the resulting key that doesn't work, and reversing the process to find the legitimate key.

[19] (Damle)
[20] (Panda Security)

Another common attack is to send a phishing email in an attempt to trick the recipient into entering their username and password into a site that is controlled by the attacker. This is done by sending an official looking email to the target, urging them to log onto the bank's site, along with a fake link that leads to the attacker's site as shown in exhibit II.

Attacks against organizations

One of the most high profile cases of social engineering in recent history involved the destruction of components of an Iranian power plant through a joint American-Israeli cyber-espionage operation. Critical infrastructures such as these power plants were once through to be absolutely impossible to hack because they are not connected to the Internet at all. However, through social engineering, the Americans and the Israelis were able to trick plant workers into bringing infected USB drives into the plant[21]and plugging them into the machines that once were isolated from the outside world.

The result of this breach is that the US and Israeli government was able to completely destroy critical pieces of equipment and set the Iranian nuclear program back by months without stepping foot inside the facility. In addition, if the governments did not later choose to claim responsibility for the attack, it would have been completely untraceable.

Preventing Social Engineering Attacks

As auditors, we have already assumed a great deal of responsibility by ensuring that our organizations' systems meet the control objectives as identified by the CICA IT Control Guidelines[22]. Notably, the control objectives that directly relate to security over IT are as follows:

I. We must ensure the integrity, confidentiality and availability of information technology processing throughout the enterprise
II. We must ensure that access to the enterprise's systems and information is reliably controlled
III. To ensure that appropriate consideration is given to security issues and technical skills when management and staff are hired into IT positions

Despite this responsibility, the results from the DEFCON 18 social engineering contest have clearly demonstrated that all companies are vulnerable against social engineers[23]. The following are a series of practical solutions to common social engineering techniques.

i. Human-based controls should be replaced with electronic controls where possible. This will eliminate the ability of employees to be tempted into circumventing the system by a social engineer. For example, if the company's call-center policy is that no information can be

[21] (Langner)
[22] (Boritz)
[23] (Hadnagy)

released prior to a caller verifying their name, address and credit card number over the phone, the company can implement a control where the employee must enter all three pieces of information correctly before being able to view the information within the system.

ii. Despite lectures and workshops about security and password protection, people have been shown to constantly write their passwords down or refuse to use different passwords for their various accounts. As a result, two-factor authentication should be considered.

Two-factor authentication uses a token with a constantly changing second password that must be entered in conjunction with the user's static password. A social engineer would have great difficulty convincing an employee that there is any legitimate reason why the token's password is required, especially if a warning is printed on the token itself. See exhibit III for an example of a strong implementation of two-factor authentication.

iii. Regularly educate employees on the techniques that are employed by social engineers, conduct internal audits regularly to show employees how an attacker could have potentially gained access to the system, and ensure that employees that fail to follow best practices are reprimanded. It is simply not good enough to show employees any single case of social engineering: it is critical to train the employee to be able to heuristically identify when they are being targeted and alert the company to the attack.

iv. Every employee with access to confidential information should be provided with a shredder at his or her desk. Given the human nature to be lazy, sensitive information will invariably end up in garbage cans or a shred pile of sensitive information will end up piled up in an easy-to-steal box otherwise. While this may appear to be a relatively silly idea, such an initiative would have prevented Oracle's investigators from uncovering Microsoft covert antitrust activities[24].

Mitigating the Damage of Social Engineering Attacks

While the best practices mentioned above are likely to prevent many social engineers from successfully breaching an organization, Kevin Mitnick laments that you simply cannot stop a determined social engineer because "You can't go and download a Windows update for stupidity... or gullibility".[25]" As a result, a proper security plan should incorporate safeguards designed to mitigate the extent of damage that a social engineering attack could cause.

Segregation of access

By ensuring that users only have access to the information and systems that they absolutely require for their jobs, the organization can limit the amount of damage that a social engineer with access to the system could cause. For example,

[24] (Bort)
[25] (Gedda)

Maintain access logs

By ensuring that the company retains an access log, it will be possible for the company to find out what the attacker was able to access before the company was able to cut off his or her access. This will allow the company to make informed decisions about the extent of the damages that the company is facing and whether any immediate response is necessary. For example, if a pharmaceutical company notices that research for a particular unpatented drug was stolen, it can work with its lawyers on defending that particular drug from being infringed upon.

Ensure that backups occur regularly

While some intruders may be content to simply steal as much information as possible from a target company, others may be more interested in simply harming the company by deleting the company's data. Companies need to perform backups on a regular basis and ensure that an intruder on the network would not be able to also destroy the backup. An example of an attack that could have been mitigated by backup procedures occurred on March 31, an ex-employee of a data storage company was able to break into the servers and delete over 304 gigabytes of data that could not be recovered[26].

Automatically revoke user privileges if suspicious activity is detected

When an intruder enters a system, he or she will immediately search for the files or applications of interest by browsing around the computer's directories or performing searches of the drive and transfer as much information as possible back to his or her own computer. Using anomaly-based intrusion detection systems, companies can automatically monitor the normal levels of disk and network usage and shut down a suspicious account's access within seconds[27].

[26] (Nemani)
[27] (Zanero)

Exhibits

Exhibit I: Social Engineering: CD Key

This is a technique to create an unused Warcraft III CD key. The technique will work for both the Frozen Throne and Reign of Chaos. This technique would be good if you had two computers, and you wanted to play on Battle.net at the same time. The CD key you create will be free and unused.

NOTE: Make sure the CD Key you use is from the actual Warcraft III CD case. This technique will not work if you use a fake CD key. Don't e-mail me saying it didn't work if you didn't use an authentic CD key.

Instructions

1. Find an authentic Warcraft III: Reign of Chaos or the Frozen Throne CD key. It should look something like this: XXXXXX – XXXX – XXXXXX – XXXX – XXXXXX.
2. With the first set, add one to each **number**, but if it becomes a 10, make it a zero.
3. On the second set, subtract one from each **number**.
4. On the third set, leave it alone.
5. On the fourth set, flip it backwards. If it was 1A2B, it would become B2A1.
6. On the fifth set, leave it alone.
7. Now, use your CD key, or give it to one of your friends. If the CD key doesn't work, e-mail the CD key you created to Flam3_Spr3ad3r@yahoo.com. Make sure you do **not** send your original. You should never give **anyone** your original CD key. I will try to make your CD key work and e-mail you back the results.

Exhibit II: Phishing Attempt

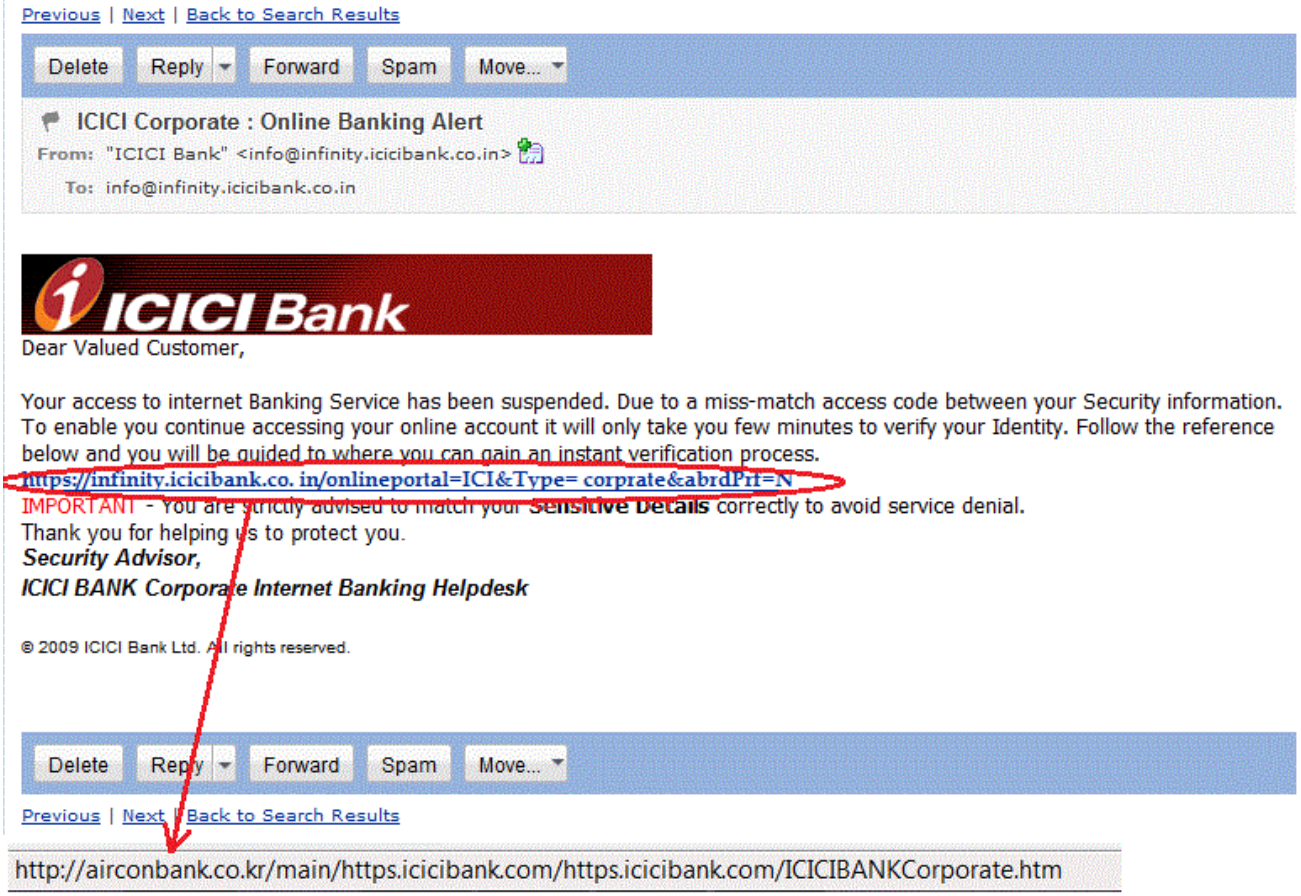
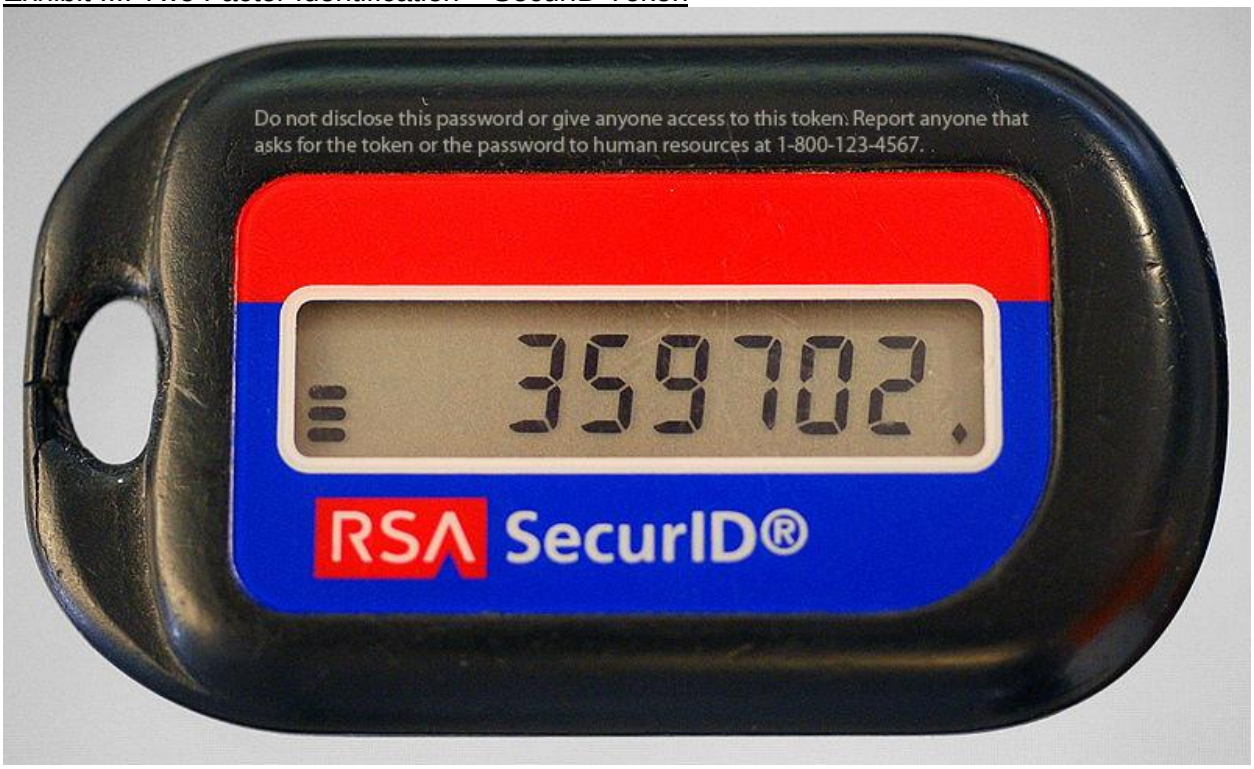


Exhibit III: Two Factor Identification – SecurID Token



Works Cited

419 Eater. What is the '419' scam? 20 June 2012. 20 June 2012 <http://www.419eater.com/html/419faq.htm>.

Boritz, Efrim. Information System Security and Availability. 1997. 20 June 2012 <http://accounting.uwaterloo.ca/ccag/6CHAP97.htm>.

Bort, Julie. The 10 Most Outrageous Stories About Larry Ellison. 17 January 2012. 20 June 2012 < http://www.businessinsider.com/the-10-most-outrageous-larry-ellison-stories-2012-1?op=1 >.

Damle, Pramod. Social Engineering: A Tip of the Iceberg . 2002. 20 June 2012 <http://www.isaca.org/Journal/Past-Issues/2002/Volume-2/Pages/Social-Engineering-A-Tip-of-the-Iceberg.aspx>.

Farivar, Cyrus. Stuxnet expert calls US the "good guys" in cyber-warfare. 6 June 2012. 20 June 2012 <http://arstechnica.com/tech-policy/2012/06/stuxnet-expert-calls-us-the-good-guys-in-cyber-warfare/>.

Gedda, Rodney. Hacker Mitnick preaches social engineering awareness. 21 July 2005. 20 June 2012 <http://www.computerworld.com.au/article/136508/hacker_mitnick_preaches_social_engineering_awareness/>.

Gragg, David. A Multi-Level Defense Against Social Engineering. 1 January 2003. 20 June 2012 <http://www.sans.org/reading_room/whitepapers/engineering/multi-level-defense-social-engineering_920>.

Hadnagy, Christopher J. Defcon 18: Social Engineering Capture the Flag Results. 2010. 20 June 2012 <http://www.social-engineer.org/resources/sectf/Social-Engineer_CTF_Report.pdf>.

International Intelligence Limited. Social Engineering. 8 December 2008. 20 June 2012 <http://www.hg.org/article.asp?id=5778>.

Laflotte, Duane. The Dark Art of Social Engineering. 6 October 2005. 20 June 2012 <http://www.informit.com/articles/article.aspx?p=417272&seqNum=3>.

Langner, Ralph. How did Stuxnet reach its target? CBS Online. 4 March 2012.

Lineberry, Stephen. The Human Element: The Weakest Link in Information Security. November 2007. 20 June 2012 <http://www.journalofaccountancy.com/Issues/2007/Nov/TheHumanElementTheWeakestLinkInInformationSecurity.htm>.

Mann, Ian. Hacking the human social engineering techniques and security countermeasures. Aldershot: Ashgate, 2008.

McMillan, Robert. The Pwn Plug is a little white box that can hack your network. 3 March 2012. 20 June 2012 <http://arstechnica.com/business/2012/03/the-pwn-plug-is-a-little-white-box-that-can-hack-your-network/ >.

Mitnick, Kevin. The Art of Deception. Indianapolis: Wiley, 2002.

Nemani, Purna. Hacker Deleted Entire Season, TV Station Says. 31 March 2011. 20 June 2012 <http://www.courthousenews.com/2011/03/31/35406.htm>.

Office of Inadequate Security. WHMCS victim of social engineering; over 500,000 client records stolen, deleted from server, and dumped publicly. 22 May 2012. 20 June 2012 <http://www.databreaches.net/?p=24284>.

PammingSodom. Nigerian prince wants my help? 20 June 2009. 20 June 2012 <http://answers.yahoo.com/question/index?qid=20090807194219AALXAcZ>.

Panda Security. Crimeware: the silent epidemic. 2011. 20 June 2012 <http://www.pandasecurity.com/homeusers/security-info/types-malware/crimeware/>.

Paul, Mano. Phishing: Electronic Social Engineering. 1 January 2009. 20 June 2012 <http://www.certmag.com/read.php?in=3594>.

Peltier, Thomas R. Social Engineering: Concepts and Solutions. 20 June 2012. 20 June 2012 <http://www.infosectoday.com/Norwich/GI532/Social_Engineering.htm>.

SEO ARTWORKS. KEVIN MITNICK, the most dangerous hacker in the world. 1 January 2009. 20 June 2012 <http://www.seo-artworks.com/CYBERSPACE/Kevin Mitnick.htm>.

Striek. Classic Social Engineering Attacks. 15 December 2003. 20 June 2012 <http://www.social-engineer.org/framework/Common_Social_Engineering_Attacks>.

Wheatman, Victor. Corporate spending on IT security. 8 November 2011. 20 June 2012 < http://www.ft.com/cms/s/0/83f39434-0a23-11e1-92b5-00144feabdc0.html - axzz1xzFGwSNd>.

Zanero, Stefano. Anomaly-Based Unsupervised Intrusion Detection HelpNet Security. 5 June 2007.

Annotated Bibliography

Previously Used Sources

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link	Added in the final paper?
Peter Bright	Anonymous speaks: the inside story of the HBGary hack	Ars Technica		2011		May 12, 2012	http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/	Not Explicitly
	Annotation Background information regarding the intrusion of HBGary, a technology security company by employing social engineering techniques. This was partially due to the use of SQL injection to gain information to gain trust from the person's assistant and retrieve additional control of the system. That is, this was a mix between conventional hacking attempts and the use of social engineering where the system was too secure to penetrate otherwise. This article shows that even security professionals who are aware of best practices are at risk of social engineering because they may not follow the practices they recommend to others and not all personnel within an office will be trained to spot an social engineering attempt							

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link	Added in the final paper?
Joshua Brower	Which Disney© Princess are YOU?	SANS Institute Reading Room		2010		May 25, 2012	http://www.sans.org/reading_room/whitepapers/privacy/disney-princess-you_33328	Not Explicitly
	Annotation This paper explores the ease of harvesting personal information from social networking sites and the ways that the information gained. It explains that the internet has caused social engineering to become more prevalent because of the anonymity that reduces the risk to social engineers more than ever before. For example, the researcher was able to trick 800 people into filling out a survey called, "what does your password say about you" in which the user gave out information such as the number of characters and numbers there are in the password as well as other hints as to what it could be. Another example that the research has found is the "What Type of Personality are You?" quizzes on Facebook that provides the crafter of the online survey to be able to gain valuable information about the user in order to break into other accounts that the user has. While the creation of a quiz on Facebook is a trivial task for most technically competent people, a person that wishes to set up a quiz to gain information about potential targets could license the code to existing applications for as little as $500. Techniques used by social engineers 1. Spear Fishing: A highly targeted phishing attempt that incorporates knowledge about the person in order to craft a communication that he or she would be likely to respond to. For example, an employee could be tricked into opening an excel file named, "2012 Layoffs" which is actually filled with a virus. 2. Impersonation and Identity theft: Using information gained about the target to impersonate the target. For example, using the information gathered through social networking sites, an attacker could attempt to gain access to a person's email account or banking site through the security question. 3. In person attack: By using information gained about the target, a person could determine when a person leaves for work in order to find the perfect time for a break in.							

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link	Added in the final paper?
CSO Magazine	The Ultimate Guide to Social Engineering	CSO Magazine		2012		May 13, 2012	http://assets.csoonline.com/documents/cache/pdfs/Social-Engineering-Ultimate-Guide.pdf	Not Explicitly
	Annotation Useful statistics: - A survey of 850 IT and security professionals located in the U.S., Canada, U.K., Germany, Australia and New Zealand found almost half, 48 percent, had been victims of social engineering and had experienced 25 or more attacks in the past two years. - Social engineering attacks cost victims an average of $25,000 - $100,000 per security incident - 86 percent of IT and security professionals recognize social engineering as a growing concern, with the majority of respondents, 51 percent, citing financial gain as the primary motivation of attacks, followed by competitive advantage and revenge. - New employees are the most susceptible to social engineering, followed by contractors (44 percent), executive assistants (38 percent), human resources (33 percent), business leaders (32 percent) and IT personnel (23 percent) - Among those polled, 34 percent do not have any employee training or security policies in place to prevent social engineering techniques Prevention techniques: - Awareness can be raised by making information visible, requiring training sessions and reinforcing positive behavior such as keeping sensitive material locked up at night							

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link	Added in the final paper?
Christopher J. Hadnagy	Defcon 19 – Social Engineering Capture the Flag Results	CSO Online		2011		May 16, 2012	http://www.social-engineer.com/downloads/Social-Engineer_Defcon_19_SECTF_Results_Report.pdf	Yes
	Annotation The paper outlines the results of the Defcon 19 (security conference) social engineering competition. Of the fourteen large companies that were called, all of them gave up varying amounts of information to the social engineers that would compromise the security of the company's data. An analysis of the sources of information used indicates that social engineers largely rely on the company's site, general web searches and employees' personal social networking accounts in order to perform their attacks. Support and customer service employees were the weakest targets and gave up the most information to the social engineers. The report speculates that this is because The "customer is always right" type of attitude was prevalent and that many companies will tend not to invest in much awareness training for high turnover positions. The results show that AT&T, which held monthly security awareness training sessions, fared the best in the test. Despite this, the company was still tricked into handing over sensitive information to the social engineers.							

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link	Added in the final paper?
Pramod Damle	Social Engineering: A Tip of the Iceberg	Information Systems Audit and Control Association	2	2002		May 16, 2012	http://www.isaca.org/Journal/Past-Issues/2002/Volume-2/Pages/Social-Engineering-A-Tip-of-the-Iceberg.aspx	Yes
	Annotation Although this is a very old paper, it provides an very high level overview of what social engineering is and the roots of social engineering. The article segregates human based social engineering techniques such as impersonation of IT staff from computer based techniques such as creating fake pop-up windows on a target's computer. It acknowledges that security must begin in the user's mind and cannot be embedded in the technology alone – a change from conventional thinking because the security architecture could cannot protect the organization from this type of attack.							

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link	Added in the final paper?
Dimensional Research	The risk of social engineering on information security	Dimensional Research		2011		May 16, 2012	http://www.checkpoint.com/press/downloads/social-engineering-survey.pdf	Not Explicitly
	Annotation There is a lack of proactive training to prevent social engineering attacks within organizations despite 97% of security professionals knowing about the seriousness of this threat. Additionally, the article states that only 16% of companies were able to confidently state that they have not been targeted by a social engineering attack. The motivations behind these attacks were reported to be generally for financial gain or access to proprietary information. The report states that phishing attempts through emails were the most popular social engineering source while social networking sites were the second most used way to target individuals.							

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link	Added in the final paper?
Joan Goodchild	Social Engineering Attacks Costly for Business	CSO Online		2011		May 12, 2012	http://www.csoonline.com/article/690167/social-engineering-attacks-costly-for-business	Not Explicitly
	Annotation Social engineers attempt to target the weakest link in an organization with access to sensitive information. In many cases, this is the administrative staff that may not be as well trained as the executives that they serve but hold almost the same amount of information. The two most common methods to extract sensitive information from employees have been to use phishing emails to trick users into believing forged emails or links or to through gathering f information through social networking sites.							

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link	Added in the final paper?
Joel Hruska	IRS easily baited, vulnerable to social engineering-based attacks	Ars Technica		2007		May 10, 2012	http://arstechnica.com/business/2007/08/study-finds-irs-vulnerable-to-social-engineering-based-attacks/	Not Explicitly
	Annotation An article that states some of the reasons why people fall for social engineering attacks – in the example, the attacker tricked the users into changing their passwords into something of the attacker's choosing. The top reasons that were mentioned were that the attacker seemed to be legitimate and believable or that while others though that changing a password was not the same thing as disclosing it, indicating a lack of knowledge.							

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link	Added in the final paper?
Information Systems Audit and Control Association	IS Auditing Procedure: Security Assessment – Penetration Testing and Vulnerability Assessment	Information Systems Audit and Control Association		2004		May 22, 2012	http://www.isaca.org/Knowledge-Center/Standards/Documents/P8SecAssess-PenTestandVulnerabilityAnalysis.pdf	Yes
	Annotation This document is the requirements that Certified Information Systems Auditors (CISA) must abide by in order to conduct a proper audit of a company's information systems. While it is quite old, it is still in effect today and is therefore, still relevant. Section 7 specifically discusses social engineering in order to "assess the ease of extraction of critical information from internal organization resources and employees/contractors, or others with detailed knowledge of the organization, without their becoming aware of the significance of the information obtained." Examples of the guidelines that the association has set include telephone access and garbage viewing: - Impersonating a consultant/auditor and reaching IT staff directly without any introduction is another approach. Management should be aware and agree to this approach to prevent unnecessary troubles. - Review of garbage disposal areas and bins for information can be a valuable source of sensitive security and overall organizational information that could be useful in a social engineering examination - Without authentication as an employee, one should attempt to obtain unimpeded access. For those organization sites with physical security via mechanical, electronic or physical guard, this testing can be accomplished in multiple ways including piggybacking into the site with a legitimate employee or signing in without an escort and walking directly into the data center or business work sites. - Test controls to prevent social engineering or circumvention of logical security measure in place by masquerading as an individual calling over an internal phone with a business need requesting critically sensitive information or access to basic computing services.							

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link	Added in the final paper?
Robert McMillan	Five Things You Need to Know About Social Engineering			2009		May 12, 2012	http://www.cio.com/article/511100/Five_Things_You_Need_to_Know_About_Social_Engineering	Yes
	Annotation Brief article about social engineering. Of particular note is that, “social engineering is on the rise” and that sophisticated social engineers were using a technique called “spear phishing”, carefully crafting email messages to select recipients that trick them into downloading Trojan horses. Increasingly, social engineers use information gained from Social Networking sites such as Facebook in order to deceive their targets. Steve Santorelli, formerly a Scotland Yard detective states that: A few years ago hackers were more focused on the quality of their code. Now, he says, "they are putting an equal effort into social engineering."							

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link	Added in the final paper?
Mike Rothman	Are senior level executives a target for social engineering attacks?	Search Security		2007		May 22, 2012	http://searchsecurity.techtarget.com/answer/Are-senior-level-executives-a-target-for-social-engineering-attacks	Not Explicitly
	Annotation One of the emerging attack trends is for high-level executives at larger companies to be individually targeted by phishing and other email-oriented attacks because they have access to sensitive corporate data and are not as security aware as they need to be. The article recommends that a curriculum be set up for senior personnel due to the fact that they are targeted frequently and that the executives must realize the importance of the security training in order for it to be effective.							

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link	Added in the final paper?
Elinor Mills	Q&A: Kevin Mitnick, from ham operator to fugitive to consultant	CNET		2009		May 25, 2012	http://news.cnet.com/8301-1009_3-10269348-83.html	Not Explicitly
	Annotation Kevin Mitnick, one of the most well-known computer hackers (who was actually a social engineer), interviews with CNET and provides his opinion on computer security. In particular, he mentions that despite advanced security at Motorola where their entire campus was protected by SecureID, a rotating password required for access into the system, he was able to trick a manager in operations to get an employee to read the new password to him whenever he needed it. The takeaway is that while advanced security systems can protect against some forms of attack, they do little to stop a social engineer from tricking an employee to bypass the company’s defenses.							

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link	Added in the final paper?
Treasury Inspector General for Tax Administration	Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers	Treasury Inspector General for Tax Administration		2007			http://www.treasury.gov/tigta/auditreports/2007reports/200720107fr.html	Not Explicitly
	Annotation Background information to confirm that social engineering has been proven to be able to target large institutions that hold sensitive information. Posing as the organization's helpdesk, In 61 of 102 cases, the auditor was able to convince an IRS employee to change his or her password to one of the helpdesk's choosing. The article also mentions that these employees were already warned about the risks of social engineering: "The IRS has adequate password policies and procedures...The IRS has posted these requirements and password security policies on its internal web site. The web site also has a document that describes social engineering and provides examples of social engineering attempts, specifically mentioning the use of telephone calls to conduct this type of attack." Alarmingly, based on the small sample size, managers appeared to be more susceptible to the social engineering attacks than regularly employees. The report recommended three safeguards: continuation of security awareness activities, conduct internal tests regularly to raise employee awareness and penalize employees for security violations							

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link	Added in the final paper?
Safelight	Safelight Challenges RSA Conference Participants to Cultivate a Security Culture Within their Organizations	Safelight Security		2012		May 25, 2012	http://safelightsecurity.com/news/2012/02/22/safelight-challenges-rsa-conference-participants-to-cultivate-a-security-culture-within-their-organizations/	Not Explicitly
	Annotation Safelight is an organization that provides educational seminars to companies and government organizations. The company. The company states that the best way to protect information is to have people that "adopt a security mindset and are educated on how to protect valuable information on a daily basis" Some of the sessions that the company offers include showing employees how to "piggyback" employees to gain access to the building and giving employees practice with screening malicious emails in the midst of legitimate ones.							

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link	Added in the final paper?
Yahoo!	How can I identify a phishing web site?	Yahoo! Security Center		2012		May 22, 2012	http://security.yahoo.com/article.html?aid=20060102503	Not Explicitly
	Annotation The paper gives recommendations to use in order to determine whether a website is a legitimate site or a phishing site and steps that should be taken to ensure that information is not sent to the attacker. For example, it states that you should check the URL of the site to ensure that it is not spelt incorrectly and owned by an attacker instead. A technique identified is to use an obviously incorrect password to sign into sites that appear to be fraudulent and pay attention to whether the site tries to trick the user into thinking that he or she has signed on successfully.							

New Sources

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
419 Eater	What is the '419' scam?	419 Eater		2012		June 20, 2012	http://www.419eater.com/html/419faq.htm

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
Efrim Boritz	Information System Security and Availability	I N/A		1997		June 20, 2012	http://accounting.uwaterloo.ca/ccag/6CHAP97.htm

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
Julie Bort	The 10 Most Outrageous Stories About Larry Ellison	Business Insider		2012		June 22, 2012	http://www.businessinsider.com/the-10-most-outrageous-larry-ellison-stories-2012-1?op=1

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
Cyrus Farivar	Stuxnet expert calls US the "good guys" in cyber-warfare	Ars Technica		2012		June 21, 2012	http://arstechnica.com/tech-policy/2012/06/stuxnet-expert-calls-us-the-good-guys-in-cyber-warfare/

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
Rodney Gedda	Hacker Mitnick preaches social engineering awareness	Computer World Australia		2005		June 22, 2012	http://www.computerworld.com.au/article/136508/hacker_mitnick_preaches_social_engineering_awareness

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
David Gragg	A Multi-Level Defense Against Social Engineering	Sans Institute		2003		June 23, 2012	http://www.sans.org/reading_room/whitepapers/engineering/multi-level-defense-social-engineering_920

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
Hadnagy, Christopher J	Defcon 18: Social Engineering Capture the Flag Results	N/A		2010		June 20, 2012	http://www.social-engineer.org/resources/sectf/Social-Engineer_CTF_Report.pdf

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
International Intelligence Limited	Social Engineering	HG Global Legal Resources		2008		June 24, 2012	http://www.hg.org/article.asp?id=5778

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
Duane LaFlotte	The Dark Art of Social Engineering	Inform IT		2008		June 20, 2012	http://www.informit.com/articles/article.aspx?p=417272&seqNum=3

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
Ralph Langner	How did Stuxnet reach its target	CBC Online		2005		June 20, 2012	http://www.youtube.com/watch?v=7r6bZKirOfw

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
Stephen Lineberry	The Human Element: The Weakest Link in Information Security	Journal of Accountancy		2007		June 22, 2012	http://www.journalofaccountancy.com/Issues/2007/Nov/TheHumanElementTheWeakestLinkInInformationSecurity.htm

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
Ian Mann	Hacking the human social engineering techniques and security countermeasures	N/A		2008	53 – 57	June 21, 2012	N/A

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
Kevin Mitnick	The Art of Deception	N/A		2002	Various	June 21, 2012	N/A

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
Purna Nemani	Crimeware: the silent epidemic	Panda Security		2011		June 18, 2012	http://www.pandasecurity.com/homeusers/security-info/types-malware/crimeware/

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
Office of Inadequate Security	WHMCS victim of social engineering; over 500,000 client records stolen, deleted from server, and dumped publicly	Office of Inadequate Security		2012		June 18, 2012	http://www.databreaches.net/?p=24284

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
PammingSodom	Nigerian prince wants my help?	Yahoo Answers		2009		June 19, 2012	http://answers.yahoo.com/question/index?qid=20090807194219AALXAcZ

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
Panda Security	Crimeware: the silent epidemic	Panda Security		2011		June 19, 2012	http://www.pandasecurity.com/homeusers/security-info/types-malware/crimeware/

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
Mano Paul	Phishing: Electronic Social Engineering	Certification Magazine		2009		June 16, 2012	http://www.certmag.com/read.php?in=3594

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
Thomas R. Peltier	Social Engineering: Concepts and Solutions	Information Security Today		2012		June 14, 2012	http://www.infosectoday.com/Norwich/GI532/Social_Engineering.htm

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
SEO ARTWORKS	KEVIN MITNICK, the most dangerous hacker in the world	SEO ARTWORKS		2009		June 15, 2012	http://www.seo-artworks.com/CYBERSPACE/KevinMitnick.htm

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
Striek	Classic Social Engineering Attacks	Social Engineer.org		2003		June 18, 2012	http://www.social-engineer.org/framework/Common_Social_Engineering_Attacks

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
Victor Wheatman	Corporate spending on IT security	Financial Times		2011		June 19, 2012	http://www.ft.com/cms/s/0/83f39434-0a23-11e1-92b5-00144feabdc0.html - axzz1xzFGwSNd

Author	Title of Article	Periodical/ website	Vol. / No. / Edition	Year published	Page #	Date accessed	Location, data base, link
Stefano Zanero	Anomaly-Based Unsupervised Intrusion Detection	Youtube		2007		June 20, 2012	http://www.youtube.com/watch?v=cZ2f0_gY19M