# Avoiding Social Engineering Attacks through Security Education Training and Awareness

Robert Martin

East Carolina University

## Abstract

This paper focuses on avoiding Social Engineering attacks through Security Education Training and Awareness (SETA). Hackers continue to exploit the weakest asset in IT security, which is the human asset. This paper will outline four Social Engineering attacks that are designed to manipulate the emotions of the victim. These four attacks are: Spear phishing/whaling, Drive/CD baiting, In-person Pretexting, and Wi-Fi Evil Twin. The purpose of this paper is to show how SETA can help users and businesses avoid the costly impact of Social Engineering attacks.

Avoiding Social Engineering Attacks through Security Education Training and Awareness

According to reuters.com, the cost of data breaches continues to increase year after year. The article states, “the total average cost of a data breach is now $3.8 million” (Ruvic, 2015). Many data breaches result from a hacking technique called Social Engineering. Social Engineering is defined as “the use of social skills to convince people to reveal access credentials or other valuable information” (Whitman & Mattord, 2010, 2014). Social Engineering attacks have existed since the 1970s. These attacks have been executed by notorious computer hackers, like Kevin Mitnick. According to forbes.com, “Kevin Mitnick was once known as the ‘World’s Most Wanted’ social engineer and computer hacker” (Coleman, 2013). Well-trained employees are formidable opponents to even the best social engineer attack.

## Literature Review

There are two questions that must be answered when addressing the issue of avoiding Social Engineering attacks. First, what are the Social Engineering attack techniques currently used by hackers? Second, how do organizations avoid those attacks?

Tetri and Vuorinen (2013) point out three goals in their article that help to support this paper. The first goal is “to create an analytical and critical concept of Social Engineering.” The second goal is “to gather all the individual acts” and “the techniques of intrusions” that attackers use. The third goal is “to discover how Social Engineering has been studied.” The only issue that I find with this material is the low probability that the authors were able “to gather all the individual acts” of Social Engineering that an attacker would use (Tetri & Vuorinen, 2013).

The Official (ISC)$^2$ Guide to the CISSP® CBK® lists Social Engineering as one of the topics that should be part of a formal security awareness training program. The book points out that security training “may result in the partial or complete offset of the risk within an organization” (Gordon & Malik, 2015). This resource not only provides the current definition of Social Engineering attack methods, but it also offers methods to combat Social Engineering attacks.

Sjouwerman (2015) supports the value of this paper by identifying that “email spear phishing is now the number one source of data breaches.” Additionally, this journal focuses on leading sources of data breaches and how security training can reduce data loss. This author is the CEO of a security awareness training company and has over 30 years of experience working in the IT industry (Sjouwerman, 2015).

Krombholz et al. (2015) use the term “knowledge worker” to describe an employee “whose main capital is knowledge.” In doing so, this journal resource lends credibility to this paper by demonstrating that knowledge is key to protecting data. The journal also discusses how Social Engineering can affect the knowledge worker, the “taxonomy” and “attack” vectors of Social Engineering, and real-life Social Engineering attacks that were successful (Krombholz, Hobel, Huber, & Weippl, 2015).

Whitman and Mattord (2010, 2014) outline the importance of, and the need for, Security Education Training and Awareness programs. The textbook refers to security awareness as “one of the least frequently used but the most effective security methods” (Whitman & Mattord, 2010, 2014). This source provides supporting details on the importance of SETA in the management of information security.

## Social Engineering Attacks

Social Engineering attacks are designed to take advantage of the victim's emotions. Each hacker has their preferred modus operandi. Common emotions exploited by Social Engineering are fear, curiosity, anger, pity, and trust. Peter Hewitt, Raleigh ISSA board member and GIAC Certified Incident Handler stated, "the top Social Engineering attack methods currently used to deceive victims and steal data are Spear phishing/whaling, Drive/CD baiting, in-person Pretexting, and Wi-Fi Evil Twin (P. Hewitt, personal communication, July 5, 2015). Each of these techniques focuses on one or more of the victim's emotions.

### Spear Phishing/Whaling

During a Spear phishing /whaling campaign, the attacker, "posing as a trustworthy organization," sends the victim an email that is specifically designed to appeal to the victim as an individual (Gordon & Malik, 2015). For instance, the attacker will go to social media sites such as Facebook or Linkedin, or background-check sites such as pipl.com or thatsthem.com to gather victim information. Attackers also use Google to identify a victim's likes and dislikes. For example, if the attacker finds out the victim contributes to a charity then the attacker will compose an email using automated programs, such as Social Engineering Toolkit, or just manually using HTML. The intention is to craft the email to look as legitimate as possible. The pictures and language used in the email must mirror the website of the legitimate charity website. The attacker's goal is to appeal to the victim's emotions such as, curiosity and pity, so that the user clicks on a link to visit the fake website, which contains the attacker's malicious code or opens an attachment contained in the email, which contains malicious code (Tetri & Vuorinen, 2013).

**Drive/CD Baiting**

With a drive/CD baiting attack, the attacker must gain physical access to the target's office or surrounding areas. This attack is accomplished by placing one or more devices such as USB drives or CDs/DVDs in frequently trafficked locations such as parking lots, lunch rooms, smoking areas, and bathrooms (Krombholz, Hobel, Huber, & Weippl, 2015). The devices are often labeled with text designed with company logos or familiar executive names to trigger the victim's curiosity. To enhance the effect, the contents of the drive or CD will contain folders with names like, “Vacation Photos" or "2015 layoff projections," which may pique the victim’s emotions of curiosity, anger, and fear. Additionally, the folders may even contain files that closely match the same naming scheme the victim uses.

One way an attacker can mask the true purpose of the file is to label it something intriguing, such as “Vacation Photos,” add a significant number of spaces, and then an .exe file extension. Windows operating systems will often shorten the file name so the victim will not realize that file is really an executable. The executable file contains code that will conduct malicious operations. For example, Cobalt Strike, a commercial software, can be used to generate a file that will make the victim's computer send a signal out to the attacker's listening computer (Strategic Cyber, n.d.). Once the attacker responds, full control of the victim's computer is taken.

The traffic from this type of attack evades many firewall policies because many organizations only restrict inbound traffic and do not log outbound traffic. To ensure that the malicious code is not blocked by antivirus programs, the attacker can use other open source hacking tools to obfuscate the code (P. Hewitt, personal communication, July 5, 2015).

### In-person Pretexting

With in-person pretexting, the attacker must be able to gain physical access to the target's location. The attacker impersonates a trusted person, typically an employee of the company whose position allows unfettered access inside the target's organization to access private data (Gordon & Malik, 2015). The attacker takes advantage of employee’s desire to trust, or have pity for, a person. For example, in a medical facility, an attacker would wear a lab coat and a stethoscope and pose as a doctor. Employees often trust someone in a position of authority and healing, so if the attacker looks the part, their authority could be accepted without question. In another example of in-person pretexting, the attacker might pose as a delivery person who is late in getting a package to a VIP within an organization. The victim may sympathize with the delivery person and want to look good in front of the VIP and permit access due to the urgency of the package.

### Wi-Fi Evil Twin

“Evil twin hotspots are on the rise and are starting to appear most anywhere that a business, such as a coffee shop, retail establishment or restaurant provides free Wi-Fi access to its patrons” (Ohlhorst, 2014). For a Wi-Fi Evil Twin attack, the attacker goes to a location where a Wi-Fi signal is publicly available and sets up a wireless access point using a common name that matches a business within that vicinity. “Cybercriminals build evil twin hotspots to allow them to both eavesdrop on network traffic and insert themselves into the data conversation between the victims and their destination servers” (Ohlhorst, 2014). Many victims’ computers will retain such network names in their memory and will automatically connect when presented with an available network with the same name. With open source hacking tools, the attacker can even set up a fake "login" screen so the victim thinks a form of authentication is occurring to gain access to the Wi-Fi network. Once the victim's device connects, the attacker's computer will simply pass the connection on to the legitimate Wi-Fi network. However, the attacker will be able to record passwords, bank account information, login credentials, and other private data that the victim supplies (P. Hewitt, personal communication, July 5, 2015).

## Security Education Training and Awareness

To help avoid Social Engineering attacks, an organization must develop and maintain an effective security education training and awareness program. Sjouwerman (2015) states that, “training reduces losses.” His research shows that “businesses that have security-awareness programs experience significantly lower average financial losses from cybersecurity incidents” (Sjouwerman, 2015).

Spear phishing/whaling attacks can be avoided by teaching employees what to look for in an email or instant message. This email message may look as if it is from a trusted source. Employees should be trained to think before opening attachments. The employee should question if the document that they have received is something they should actually be receiving. If a document is received during a time when it is not expected, then employees should call the sender to verify the attachment.  Attackers can use a technique called spoofing to disguise their identity in an email. “As SMTP does not possess an adequate authentication mechanism, email spoofing is extremely simple” (Gordon & Malik, 2015). Employees should also be trained to avoid giving out their work email address to people outside of the organization. It is also a good security practice to not use company email to register with websites that may sell or share contact information with partner companies. This practice helps to not only avoid incoming spam but reduces the likelihood of receiving spear phishing/whaling type emails. A best practice to avoid spear phishing/whaling attack is to create one or many “throw away” email accounts. The purpose of these email accounts is to provide employees a way to register and receive information relevant to their job, from outside sources. This way the employee is able to use those accounts to obtain the necessary information, without putting the company in harms way.

This type of training can be accomplished by constructing computer-based training that contains spear phishing/whaling simulations. The employees are shown what a real attack looks like in the safety of a simulated environment. These simulated environments can be accessed through computer-based training that can be accessed by employees on a global scale. The simulations can produce the effects of clicking on a malicious link without the real repercussions. This training can be further augmented by sending out internal phishing attacks to employees and rewarding those who report the malicious message to the proper security department. An employee can be designated for each department within a company to act as a point of contact for the security department. Employees acting as the point of contact can be incentivized via a bonus or other means to maintain security awareness.

Drive/CD baiting attacks can also be avoided by teaching employees that removable media can pose a threat to the company, if used improperly. This training should show employees how to properly use and secure company assets like removable media. Drive/CD baiting can take many forms and can be found in seemingly harmless places. Mobile employees should be specifically trained on what is acceptable to receive from third-party vendors or exhibitors at conferences or meetings. Many attackers will pose as legitimate businesses at conferences and distribute removable media as prizes to unsuspecting attendees. The bait offered could be a CD, DVD, flash drive, a smart phone, or an mp3 player (DARA SECURITY, n.d.).

Employees should be shown examples of the types of malicious media that could be encountered in and around the business, as well as outside events. Employees should be given clear direction, from appropriate security personnel within the company, as well as appropriate contacts to reach out to in the event that they encounter suspicious media. Additionally, this type of security training can produce trust relationships between the employees and security personnel. This trust relationship empowers employees to consider the needs of the company and to realize the potential negative impacts of a data breach on the company and the company's reputation.

In-person pretexting can be overcome by teaching and empowering each employee to be the "eyes and ears" of the organization. Employees can be trained to take a person that does not have a badge to the proper location to obtain a badge. Through scenario-based training, employees can be taught what company information is appropriate to share with people outside the company. Mobile workers can be targeted in places like restaurants and airports.  Many times employees on long flights can be befriended by a hacker and craft conversations that help reveal information about the company. An attacker can claim that they are having an issue with their operating system and ask questions in the hope that the employee will reveal what version of the operating systems the company is currently using. If the operating system that the company is using is a Windows version and has a weakness, the attacker can later exploit that weakness in an attack. With proper security training, employees will feel confident in refusing access to anyone that does not have the proper credentials to gain access. They will also feel confident in refusing to release any data that may compromise the security of the company.

Wi-Fi Evil Twin attacks can also be avoided by providing training to all employees that use company devices outside of the work environment. Employees should be trained on what the correct company Service Set Identifier (SSID) is and what procedures should be expected during the WiFi login process. If an employee finds their device connected to an unauthorized access point at work then they should know the proper procedure to document the SSID, disconnect the device, and report the incident to the proper security personnel.

Mobile employees should be trained to “disable their Wi-Fi adapters by default.” If the mobile device WiFi is only turned on when needed, then the likelihood of connecting to a WiFi Evil Twin is greatly reduced. Mobile employees can also be trained to connect to the company VPN when connected to external WiFi connections to reduce the risk of a man-in-the-middle attack (Ohlhorst, 2014). Employees should have the correct motivation to not take the risk of using public Wi-Fi. Companies can also provide their mobile workforce with mobile hotspots so they will not feel tempted to use public WiFi and risk exposing company data to attackers.

## Conclusion

Social Engineering techniques will continue to advance as the technology we use advances. Security Education Training and Awareness should advance as the technology that company utilizes, advances. The training must continue to focus on new methods that attackers are using to exploit their victims. The only employees that the attackers will be able to exploit are employees that are not properly trained. Untrained employees can pose the greatest risk or be the greatest security asset to an organization. That security decision is ultimately left up to the company. Considering the rising number of data breaches and the costs associated with those data breaches, organization certainly need each and every employee focused on the security.

Well developed security training should “help users understand their role in InfoSec and how a breach in that security can affect their jobs” (Whitman & Mattord, 2010, 2014). It is much less expensive to train staff than suffer the consequences of a data breach to your bottom line and the company’s reputation. As Derek Bok, former Harvard University president, was said to have stated, “If you think education is expensive, try ignorance.” (Sjouwerman, 2015).

# References

Coleman, T. W. (2013, April 11). Kevin Mitnick: The Hacking Hamburglar. Retrieved July 18, 2015, from http://www.forbes.com/sites/singularity/2013/04/11/kevin-mitnick-the-hacking-hamburglar/

DARA SECURITY. (n.d.). Social Engineering - Would You Take the Bait? Retrieved July 21, 2015, from https://www.darasecurity.com/article.php?id=32

Gordon, A., &amp; Malik, J. (2015). <i>Official (ISC)2® guide to the CISSP® CBK®: Certified Information Systems Security Professional</i> (4th ed.). Boca Raton, FL: CRC Press.

*Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl, Advanced social engineering attacks, Journal of Information Security and Applications, Volume 22, June 2015, Pages 113-122, ISSN 2214-2126, http://dx.doi.org/10.1016/j.jisa.2014.09.005. (http://www.sciencedirect.com/science/article/pii/S2214212614001343)

Ohlhorst, F. (2014, September 8). Minimizing the threats of public Wi-Fi and avoiding evil twins. Retrieved July 21, 2015, from http://www.techrepublic.com/article/minimizing-the-threats-of-public-wi-fi-and-avoiding-evil-twins/

Ruvic, D. (2015, May 27). Cost of data breaches increasing to average of $3.8 million, study says. Retrieved July 17, 2015, from http://www.reuters.com/article/2015/05/27/us-cybersecurity-ibm-idUSKBN0OC0ZE20150527

*Sjouwerman, S. (2015). Confronting 'spear phishing' etc. Privacy Journal, 41(7), 3-4. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1691260002?accountid=10639

Strategic Cyber. (n.d.). Features - Cobalt Strike. Retrieved July 18, 2015, from http://www.advancedpentest.com/features

*Tetri, P., &amp; Vuorinen, J. (2013). Dissecting social engineering. <i>Behaviour &amp; Information Technology,</i> <i>32</i>(10), 1014-1023. doi:10.1080/0144929x.2013.763860

Whitman, M. E., &amp; Mattord, H. J. (2010,2014). <i>Management of information security</i>. Stamford, CT: Cengage Learning.