“The Human Layer of Information Security Defense”

Written by Ugo Emekauwa, MCSE, CCNA

In today’s corporate environment, the topic of information security has become a top concern for several organizations. Due to the various laws and government regulations that have recently been implemented to hold an organization liable for the loss of data, information security is an issue that can no longer be overlooked. Effective information security is comprised of multiple layers of defense which work together to protect information. The premise is that if one layer fails, the following layer will succeed. Often when information security is discussed, the technical layers such as firewalls, software patches, intrusion detection systems, anti-virus programs, and encryption are the only areas addressed. However, an important layer of information security defense that is not given the attention that it deserves is the human layer. The human element is the arguably the most important layer of defense for information security. If an individual with malicious intent is able to effectively bypass the human layer, they can circumvent all of the other defensive layers of information security. The time, money and resources directed towards the other layers of information security defense are wasted if the human layer is breached. Therefore the human layer requires the most attention. It is imperative to ensure the strength of the human layer of defense in one’s information security strategy. To ensure the strength of the human layer in one's information security plan, a company must first recognize and address the human layer's biggest threat which is social engineering. Once a company understands social engineering then it can proceed to put in place policies and countermeasures to fight social engineering.

What exactly is social engineering?

The term social engineering usually incites an inquisitive response as to what exactly it means. Social engineering is the use of any number of techniques to gain access to otherwise restricted areas or confidential data. Simply put, social engineering is the use of con artistry within the realm of hacking. It is "The Art of Deception," as the title of reformed hacker Kevin Mitnick's book on social engineering so eloquently puts it. Social engineering comes in several different forms. One of the more popular forms that have been discussed in the media is phishing. Phishing is the use of fake correspondence to retrieve information. A phishing attack can come in the form of an email from a fraudulent sender, a fake website, or a telephone call with a fake Instant Voice Response system. A primary example of phishing involves receiving an email that appears to be from a major company such as eBay or PayPal. The email will fraudulently inform the recipient that there is a problem with there eBay or PayPal account and will attempt to direct the recipient to a fake website or telephone number to resolve the problem. If the recipient clicks on the fake website or dials the phone number, they will be asked to input sensitive information such as their social security number or account usernames, passwords, and pin numbers under the false pretense of verifying their information.

Sophisticated phishers will construct their website or IVR system to trick their victims into entering their private information multiple times with false incorrect login messages.

Another instance of phishing may involve an email from senders claiming to be a large software vendor such as Microsoft. The fake email will inform the recipient that there is a vulnerability in their software and that they need to click on a provided link in order to download the latest patch or fix. Clicking on the link will then install a backdoor, malware, spyware or virus that can be used to destroy data, monitor or even control the recipient's computer system. This can be very dangerous in a personal or business environment.

Another form of social engineering is pretexting. Pretexting is the attempt to obtain private information or access to restricted areas through the creation of false pretenses. Pretexting often occurs over the phone and primarily involves impersonation tactics, where the attacker pretends to be something they are not. An example of pretexting would be receiving a call while at work from an individual pretending to be a support tech from the IT helpdesk, claiming that there is a virus on your computer system and that they need your username and password to fix it. Another example would be the IT helpdesk at an organization receiving a call from an individual pretending to be a user who lost their email password and needs it reset. A skilled pretexter will use various scenarios to create a sense of urgency or pressure in their request such as claiming to be a company vice president or that they have an important meeting they need to be at in a few minutes and they need access to their email immediately.

Another social engineering technique is the use of a Trojan horse. The Trojan horse technique involves an attacker concealing a malicious object by portraying it as a gift or something of value and then delivering the object to the victim in order to gain access into the victim’s restricted network. Trojan horses can be delivered in several different ways depending upon the creativity of the attacker. An example of a Trojan horse may be an email with a link to an offer for some sort of free prize which in actuality directs the user to a webpage containing a script that silently installs monitoring applications on the victim’s computer. Another example of using a Trojan horse could be a scenario where an attacker pretends to be a salesman and visits an unsuspecting business with free demos of some form of software. During the visit, the demos are given to various employees of the business who unknowingly accept the software and load it onto their computers. Upon loading the software, a background script is installed giving the attacker backdoor access to the business’ network. One especially creative form of the Trojan horse is where the attacker will specifically place media such as floppy discs or flash drives on the grounds of a targeted business in hopes that an employee will find the media and out of curiosity, insert the media into their office computer. Upon the loading of the media, a malicious script is installed on the office PC.

Other methods of social engineering include dumpster diving and shoulder surfing. Dumpster diving is used to describe the rummaging and examination of the trash of a particular target in order to discover confidential information. Dumpster divers will literally enter the trash dumpsters of targets to find documentation. In some instances, dumpster divers will instead opt to steal their targets trash when it has been placed outside for pickup and rummage through it at another location. Dumpster diving has been an effective way for attackers to gain trade secrets, passwords, network infrastructure layouts and other private data about their targets.

Shoulder surfing is used to describe the general act of observing a target as they login or access a system and taking note of their authentication credentials and any other available information. This for of social engineering is often performed at ATM's. While a target is entering their PIN number, an individual using shoulder surfing will watch from behind and record the PIN number entered.

What are some examples of social engineering incidents?

Social engineering attacks are a common occurrence, although this is not reflected in the media. Often, organizations may not be aware that they were targeted or the incident was unreported because the embarrassment could potentially hurt the reputation or image of the company. Three prominent companies that were affected by social engineering are Microsoft, T-Mobile, and Hewlett-Packard.

During the anti-trust case against Microsoft in 2000, Larry Ellison, the CEO of the rival software company Oracle, hired a private detection company named Investigative Group International (IGI) to examine the relationship between Microsoft and several policy trade groups that publicly supported Microsoft. Three of the trade groups that were investigated by IGI are the Independent Institute, the National Taxpayers Union, and the Association for Competitive Technology. What follows is not only a very real example of how effective social engineering is in obtaining information, but also how the strength of the human layer of a company's information security defense can determine whether or not a social engineering attack will be successful.

During the investigation of the three above mentioned trade groups, IGI engaged in the use of the social engineering technique, dumpster diving. Through dumpster diving, IGI was able to examine the trash of the Independent Institute and in doing so discovered evidence that Microsoft had funded the group by as much as $153,000. IGI used the same technique of dumpster diving on the National Taxpayers Union and was able to produce more evidence of funding from Microsoft in the form of $200,000. Critically valuable information was obtained through the simple technique of merely sifting through trash. No malicious scripts were needed, no ports were scanned. No computer was used. The most robust firewall and intrusion detection system did not have to be breached. It was a weakness in the human layer of the information security defense of these two companies that allowed for the disclosure of such highly confidential information.

The third company of this group, the Association for Competitive Technology (ACT), was also the target of dumpster diving by IGI, but this time the attack would prove to be unsuccessful. IGI went as far as renting a building space in Washington, near the offices of the Association for Competitive Technology. In IGI's attempt to obtain the trash of ACT, IGI indirectly arranged to pay the cleaning crew of ACT's offices $1,200 to bring to them any trash removed from the ACT offices. The cleaning crew for ACT's offices refused the offer and instead contacted the authorities. IGI's social engineering attack was prevented due to the integrity of the cleaning crew. This highlights the importance of a strong human layer of defense and one of its underlying aspects which is personnel security. The benefits of good personnel security promotes the hiring of trustworthy qualified individuals. Had the cleaning crew for ACT accepted IGI's offer, the social engineering attack would have succeeded. This is a real life example of how critical the human layer is to information security defense.

Another highly publicized incident of social engineering involves the wireless telephone service provider T-Mobile and their paid celebrity endorser Paris Hilton. Through the use of social engineering techniques, a group of hackers, which included members as young as 16 years old, were able to gain access to T-Mobile's intranet website used for customer account management. Through information obtained on the internal T-Mobile website, the hackers were ultimately able to access Paris Hilton's cell phone account and publish nude photos found in her cell phone account folders.

The social engineering technique used by the hackers was pretexting. With the pre-determined goal of hacking Paris Hilton's cell phone account, the hackers called a T-Mobile sales and service store located in California. A reportedly 16 year old member of the group of hackers initiated the phone call. By pretending to be a member of IT support for T-Mobile, the 16 year old was able to get the sales rep at the California store to not only give him the address the of the internal T-Mobile website for customer account management, but also a username and password. The following is an excerpt of an account of the phone conversation from one of the hackers as reported by the Washington Post:

> “The conversation -- which represents the recollection of the hacker interviewed by washingtonpost.com -- began with the 16-year-old caller saying, "This is [an invented name] from T-Mobile headquarters in Washington. We heard you've been having problems with your customer account tools?"
>
> The sales representative answered, "No, we haven't had any problems really, just a couple slowdowns. That's about it."
>
> Prepared for this response, the hacker pressed on: "Yes, that's what is described here in the report. We're going to have to look into this for a quick second."
>
> The sales rep acquiesced: "All right, what do you need?"
>
> When prompted, the employee then offered the Internet address of the Web site used to manage T-Mobile's customer accounts -- a password-protected site not normally accessible to the general public -- as well as a user name and password that employees at the store used to log on to the system” (Krebs, 2005).

After gaining authentication to T-Mobile’s customer account management website, the hackers used the directory services on the internal website to lookup the phone numbers of various famous celebrities, as they now had access to the phone number of any T-Mobile subscriber. According to the hackers, they first looked up the phone number of well known actor, Laurence Fishburne. The hackers revealed how the made several prank phone calls to the actor in relation to the role he played as 'Morpheus' in the Matrix film trilogy. The hackers then decided to take their actions a step further. Through T-Mobile’s website, the hackers looked up the phone number of Paris Hilton and issued a password reset of her account. Through this password reset, the hackers were able to gain access to Paris Hilton’s cell phone account which contained private data such as personal notes, photos, and an address book which contained the contact information of several other celebrities. Seeking to gain notoriety by making their exploit public, the young hackers published the contents from Paris Hilton’s account, which included nude photos, to various websites.

When the news was first reported that Paris Hilton’s cell phone account had been hacked, among the initial reactions were questions as to how one was able to hack a cell phone. There was a frenzy of concern about how firewalls and anti-virus tools would be needed to protect cell phones from intrusion. Upon further investigation, it was discovered that a simple phone call employing the use of social engineering was all that was needed to ‘hack’ the cell phone. With a simple phone call, hackers were able to breach the customer account records of a major telecommunications company and then access individual accounts. Imagine the damage that could have been done if these hackers had truly malicious intentions and were not just a group of kids.

The Hewlett-Packard scandal which made news in September of 2006 is another high profile example of social engineering. Executives of Hewlett-Packard were accused of approving the use of social engineering tactics to investigate the members of the company's board of directors and various journalists. In response to media leaks that were suspected to be from a board member, then HP chairman, Patricia Dunn, hired a private investigation company to discover who exactly the source of the leak was. In order to find the leak, the private investigation team used pretexting to obtain the phone records of all the HP board members and suspected journalists. The private investigators called the telephone service providers of each board member and were able to obtain specific phone records by pretending to be the targeted board member. Tom Perkins, former HP board member, came forward with letters from his telephone service provider AT&T which documented fraudulent online accounts set up in his name and records of a support call where an individual pretending to be him received assistance in obtaining his long distance phone call records. The private investigation team also used the social engineering technique of phishing by pretending to be an employee of HP and sending emails containing tracers to various journalists. This scandal was another instance that once again displayed how sensitive data can be obtained without having to breach technical controls. The security of information was broken by bypassing the human layer.

What are some solutions and countermeasures for combating social engineering?

There are three major steps a company should take to countermeasure the threat of social engineering. These three steps are education, training and policy. By addressing these three components, an organization can increase the strength of the human layer in its information security defense plan.

For many individuals, especially those not familiar with information security, social engineering is a foreign concept. When the average person thinks of hacking, the stereotypical images of some mastermind writing malicious programs on a computer are most likely to come to mind. Educating employees about social engineering creates awareness of the problem and its dangers. The topic of social engineering should be apart of the standard orientation process for new employees. Current employees should also be required to attend mandatory sessions discussing social engineering. Some may view mandatory sessions as an extreme, but when the possible consequences of social engineering are realized, it is not. Mandatory sessions are already used by several companies to educate their employees on other topics such as sexual harassment. This is due to the damaging impacts that such incidents can have on an organization such as lost customers, internal disorder, and major lawsuits that can destroy a company's image and financial stability. The aftermath of social engineering attacks can have the same effects and should be taken as seriously. The costs alone for notifying customers of a data breach can reach millions of dollars.

With training on social engineering, employees would learn how to recognize social engineering attacks and how to respond. Employees should know who within the organization they should alert if they suspect a social engineering attempt. Learning how to recognize and respond to a social engineering attack reduces the chances of its success and can help assist it the finding and prosecution of attackers. Reporting the attack to the proper officials in the organization can aid in building documentation that will lead to the creation of new controls to prevent a similar attack from occurring again. Employees should also be trained on the next component which is policy.

Policy is critical to counteracting social engineering. By having standard policies in place, guidelines are set that let an employee know exactly what they can and cannot do. For example, if policies are in place that prevents an employee from giving out their password, this can help reduce the chances of such disclosure occurring during a social engineering attack. Policies eliminate ambiguity and important decisions or actions from being made by judgment calls. Policies should be put in place to address key areas such as email use, telephones, and internet access, and building entry. There should be disposal policies requiring the use of shredders for discarded confidential documents and hard drive erasures for obsolete computer systems. Strict polices should be in place for dealing with outside vendors. All vendors should be escorted while on site. Vendors should also be required to call ahead before arriving with preferably a twenty-four to forty-eight hour notice. Where possible for service contracts, a request should be made for a specific tech to be assigned to the business. Also, it should be specified that service requests should not be accepted unless they are initiated by a particular point of contact. Policies should also be in effect in regards to the introduction of external systems on to the internal network. Employees should be required to have their personal systems inspected for viruses and spyware before introduction to the network.

As mentioned earlier effective personnel security can also prevent social engineering. To strengthen the human layer of information security, an organization should start from within. Social engineering primarily works by taking advantage of an opening from the inside of an organization, so any measures that can be taken to eliminate internal weaknesses should be taken. A business needs to ensure that its own employees are trustworthy, qualified, and reliable. Potential employees should have thorough background checks performed. Credentials should be verified and timely performance evaluations conducted.

Although this paper has focused on the human layer of information security defense, the technical layer can assist in mitigating inevitable human errors in regards to social engineering. The lowest level of access rights necessary for an individual to perform their job should be given. Rules should be put in place to not show the last username on client workstations. Strong passwords should be enforced and mandatory rules for password replacement should be in effect. Also rules for minimal login attempts and automatic account locks should be implemented. Account management should be diligently performed and strictly monitored. Human resources should notify IT immediately upon the release of an employee so that their account and any codes can be disabled upon leave or termination.

Single IPs and domains known for malicious activity should also be blocked from the business network. This includes internet websites and email. This can be done through firewall access lists and email spam filters. Lists of such domains and networks can be obtained from blacklists available on the internet. These steps can help prevent users on the inside business network from being able to access a malicious website that they may be directed to by a perpetrator of social engineering. Also the amount of email with social engineering attempts such as phishing and spoofing can be reduced from reaching users on the internal network.

In closing, to implement an effective information security strategy, a multi-layered layered defense model should be used. While technical controls are an important layer of defense, the human layer is just as if not more important and should not be ignored.

References

Bridis, Ted, & Mangalindan, Mylene. (2000, June 28). Oracle-MS Flap – how it happened. *Wall Street Journal Online.* Retrieved July 4, 2007, from http://news.zdnet.com/2100-9595_22-502575.html

Cohen, Adam. (2000, July 2). Peeping Larry. *Time.* Retrieved July 4, 2007 from http://www.time.com/time/magazine/article/0,9171,49039,00.html

Fontana, John. (2006, November 02). Average data breach costs companies $5 million. *Network World.* Retrieved July 4, 2007, from http://www.networkworld.com/news/2006/110206-data-breach-cost.html?page=1

Granger, Sarah. (2001, December 18). Social Engineering Fundamentals, Part I: Hacker Tactics. *SecurityFocus.* Retrieved July 4, 2007, from http://www.securityfocus.com/infocus/1527

Granger, Sarah. (2002, December 19). Social Engineering Fundamentals, Part II: Hacker Tactics. *SecurityFocus.* Retrieved July 4, 2007, from http://www.securityfocus.com/infocus/1533

Granger, Sarah. (2006, March 14). Social Engineering Reloaded. *SecurityFocus.* Retrieved July 4, 2007, from http://www.securityfocus.com/infocus/1860/1

Idaho National Engineering and Environmental Laboratory. (2004, September 30) Personnel Security Guidelines. Retrieved July 1, 2007, from http://www.us-cert.gov/control_systems/pdf/personnel_guide0904.pdf

Kaplan, David. (2006, September 6). Intrigue in High Places. *Newsweek.* Retrieved July 7, 2007, from http://www.msnbc.msn.com/id/14687677/site/newsweek/page/0/

Krebs, Brian. (2005, May 19). Paris Hilton Hack Started With Old-Fashioned Con. *Washington Post.* Retrieved July 7, 2007, from http://www.washingtonpost.com/wp-dyn/content/article/2005/05/19/AR2005051900711_pf.html

Noguchi, Yuki, & Nakashima, Ellen. (2006, September 29). House Panel Digs Deep in HP Case. *Washington Post.* Retrieved July 7, 2007 from http://www.washingtonpost.com/wpdyn/content/article/2006/09/28/AR2006092800231.html

Stone, Brad. (2006, September 18). A ‘Pretexter’ and His Tricks. *Newsweek.* Retrieved July 7, 2007, from http://www.msnbc.msn.com/id/14736384/site/newsweek

Wikipedia: The free encyclopedia. (2007, July 11). FL: Wikimedia Foundation, Inc. Retrieved July 11, 2007, from http://en.wikipedia.org/wiki/Pretexting

Winkler, Ira. (2006). Case Study of Industrial Espionage through Social Engineering. Retrieved July 4, 2007, from the Computer Security Resource Center website: http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper040/WINKLER.PDF

Zetter, Kim. (2006, September 5). Phone Scam Charge Rocks HP. *Wired.* Retrieved July 4, 2007 from http://www.wired.com/gadgets/pcs/news/2006/09/71727