Proceedings of the 14th Colloquium for Information Systems Security Education
Baltimore Marriott Inner Harbor
Baltimore, Maryland June 7 - 9, 2010

Use of Spear Phishing Exercises to Increase Security Awareness

Allen M. Smith, Nancy Y. Toppel, *Northrop Grumman Corporation*

Abstract – Spear phishing, targeted e-mail that attempts to extract sensitive information without authorization, is a growing concern for individuals who need to protect their personal information and companies that need to safeguard their intellectual property. Technical controls on networks and systems cannot totally prevent spear phishing e-mail from reaching users' e-mail inboxes, thereby requiring the e-mail recipients to understand how to recognize spear phishing attempts. To underscore the risks and importance of handling spear phishing e-mail appropriately, a security awareness method with immediate impact is needed. This paper describes one company's success in using internal spear phishing exercises to raise security awareness among its employees.

Index terms – advanced persistent threat, espionage, information security awareness, spear phishing

I. Introduction

"Phishing" refers to mass amounts of spam e-mails that typically include urgent language or a persuasive offer, and are sent by cyber criminals in an attempt to elicit a response from recipients. "Spear phishing" is a targeted phishing attempt in which the recipients make up a specific target population and the content of the e-mail is crafted toward that population. The e-mail includes an attachment or a link to a Web site that, when launched, downloads and installs malicious software that potentially allows the cyber criminal access to the recipient's computer and login credentials. Although spear phishing is not a new attack vector, the ubiquitous use of the Internet has made it a profitable business for transnational organized crime operations [1][2] and competitive and state-sponsored espionage [3][4].

Targets of spear phishing attempts vary based on the motivation of the cyber criminals involved. Individuals are targets of spear phishing attempts seeking to steal personal information, such as Social Security Numbers, credit card numbers, PIN numbers, usernames, and passwords, which can be used to gain access to online accounts, steal funds, and create new identities. Spear phishing e-mails have spoofed a wide range of well-known government and service organizations, including financial institutions, the Monster.com career site [5], United States Department of Justice, Internal Revenue Service, and Better Business Bureau [2].

College students are often targeted because they are perceived to have an innate trust in the Internet and may be looking for ways to make money. Student e-mail addresses are easy to compile because they are often publicly available on school Web sites. Spear phishing e-mails may appear to be from the student's school and urge the student to verify username and password information [6][7][8].

Social media sites that are popular with college students have become a breeding ground for spear phishing attacks attempting to steal personal information and login credentials. Victims follow URLs in e-mails that request personal information [9] or display a fake login page to the social media site, making it easy for the cyber criminal to steal the user's login credentials. Since many people use the same passwords for multiple accounts, the cyber criminal can then proceed to hack into other accounts held by the victim, such as bank accounts [10].

Opportunities to work from home or earn money quickly also target students. The "tweet for cash!" scam claims to allow individuals to earn money by sending tweets on Twitter, but requires the individual to enter a credit card number [9]. Another advertisement targets students interested in becoming "mystery shoppers" for a consulting firm, but requires personal and credit card information [11].

Organizations such as corporations and academic institutions are targets of spear phishing attempts intent on stealing intellectual property and research and development data. A 2009 study by Intrepidus Group that implemented 32 phishing scenarios on 69,000 employees worldwide found that 23% were vulnerable to spear phishing attacks [12]. Recent spear phishing attacks on Google, Adobe, and other U.S. companies have focused on the theft of intellectual property [13]. Attacks targeting law firms and public relations companies have also been on the rise, concentrating on large corporate clients with international business deals [1]. Senior corporate executives may be targeted (sometimes referred to as "whaling") because of their access to highly sensitive company information [14].

ISBN 1-933510-99-4

Spear phishing is a commonly used attack vector used in the "advanced persistent threat," extremely complex, foreign state-sponsored attacks that aim to obtain financial, strategic, technology, national defense, and personal information [3] [15]. The U.S. government, U.S. defense contractors, and critical infrastructure are key targets of advanced persistent threat actors. As one of the top providers of information technology for the federal government and the nation's second largest defense contractor [16], Northrop Grumman is acutely aware of these threats. Northrop Grumman is a leader in cyber security and has extensive experience in cyber threat analysis and intelligence.

II. The Case for Spear Phishing Exercises

Spear phishing is difficult to thwart because the e-mails involved appear to be legitimate and can evade an organization's perimeter and e-mail security controls. Unlike traditional spam e-mail, spear phishing attempts are targeted to the individual and can be spoofed to look like they are from a familiar source. Cyber criminals are now doing reconnaissance ahead of time to ensure that e-mails look legitimate in order to get a higher percentage of recipients to respond [17]. A recent spear phishing experiment by PacketFocus reported that a spoofed LinkedIn invitation purported to be from Bill Gates reached its recipients 100 percent of the time, bypassing various industry standard e-mail filtering products and services [18]. Since the onus is on the recipient of the e-mail to recognize it as a malicious attempt to gain sensitive information, security awareness of spear phishing attacks and their risks is a critical component in mitigating spear phishing attacks.

To increase awareness of the advanced persistent threat and spear phishing attacks, Northrop Grumman instituted an internal security awareness campaign which includes regular communications to employees, mandatory annual security awareness training, and an internal Web site [19]. In addition to these traditional security awareness methods, the security awareness team researched additional methods that would have more immediate impact on employees in identifying the risks, consequences, and desired behaviors. Implementation of spear phishing exercises - sending fake spear phishing e-mails to employees within an organization to educate them – was considered.

The efficacy of spear phishing exercises is not well-documented in the media, but there are a few examples:

- In 2005, The United States Military Academy conducted a proof-of-concept spear phishing test of 400 cadets, involving an e-mail that appeared to come from an Army colonel [2]. Eighty percent clicked on the Web link. With subsequent tests, the click rate was reportedly reduced.

- In 2005, the New York State Office of Cyber Security and Critical Infrastructure Coordination sent a fake e-mail to 10,000 state employees in five agencies [20]. The e-mail appeared to be from the Office of Cyber Security and instructed recipients to check the security of their password by clicking on a link to a Web site. Seventeen percent clicked on the link, and 15 percent entered their password. Two months later, the same population was sent a similar e-mail, and 8 percent attempted to enter their password.

- July, 2009 articles indicate that the United States Military Academies have engaged Intrepidus Group's PhishMe to assist them in executing mock phishing exercises against employees [21].

The two cases from 2005 indicated that implementing regular spear phishing exercises can result in increased awareness of spear phishing among targeted individuals. Northrop Grumman determined that this was a viable method to pursue, and created a team to establish a step-by-step process for planning and implementing internal spear phishing exercises.

III. Methodology

A. Initial Approval and Preparation

Before executing a spear phishing exercise, approval must be obtained from the appropriate management, including security, legal, and human resources. The implementation team must ensure that they are following company policies and procedures, and not violate copyright or other laws when conducting spear phishing exercises.

Deceiving recipients with fake e-mail in order to educate them may result in unhappy individuals, so the response should be considered ahead of time. It must also be determined whether there will be any remedial action (such as mandatory training) for those who fall victim to the exercises.

In order to maintain the element of surprise, the implementation team should be kept as small as possible. The number of other individuals in management and operations that need to know about the details of each exercise should also be kept to a minimum.

Relevant policies, procedures, and best practices regarding handling potential spear phishing e-mail should be documented and well-communicated to the

organization prior to the implementation of the first exercise. These documents are also used as references during the exercises.

B. Spear Phishing Exercise Planning

For each spear phishing exercise, a basic set of parameters needs to be determined:

Target audience and basic premise: To ensure a higher percentage of responses, the spear phishing e-mail must be from what appears to be a familiar sender and include content that is relevant to the recipients. If the entire organization is the target, a premise such as an internal helpdesk request to verify account information can be employed if not considered by the organization to be too "easy" to recognize. Limiting the exercise to a subset of the population (such as those who have elevated privileges to a system or those may attend a particular industry conference) will allow a wider range of premises to be used that will appeal to all targeted recipients.

Clues that make the e-mail suspicious: As the details of the e-mail content and the other parts of the user experience are identified, it is important to consider what "clues" will be included that recipients should recognize as suspicious. For initial exercises, more obvious clues should be provided, in order to emphasize that distinguishing suspicious e-mail is within the recipient's capabilities. The list of clues should be included in the Web page or other documentation that notifies the victim of the exercise that he should have recognized the e-mail as suspicious.

E-mail content: The subject line and the content should include urgent or enticing language that will prompt the recipient to respond quickly. Examples include the threat of preventing access to a critical system until account information is verified, or the promise of a free gift. Spoofing other organizations using real company logos and other copyrighted information should be prohibited for legal reasons, in the event that an e-mail is somehow sent outside of the organization's intranet.

Use of an embedded Web link in the body of the e-mail is a simple mechanism to track whether a recipient was taken in by the spear phishing attempt. Hits to that Web page can be tracked and should include the victim's network login information. The URL should be spoofed by making required temporary changes to the Domain Name System and be designated one of the clues for the recipients.

Flow of e-mail through the network: In order to replicate a true spear phishing attack, the e-mail must either be sent from outside the organization's intranet or appear to be. The sender information of the e-mail can be spoofed to align with the premise of the exercise and appear to be either an internal or external e-mail.

If the e-mail is sent from outside of the intranet, perimeter and e-mail security controls may need to be temporarily adjusted to allow those e-mails to bypass existing security filters. Recipients may attempt to reply to the sender or forward the e-mail to their personal e-mail accounts on the Internet; both replies and forwards should be intercepted so that they do not leave the intranet.

Registration Web page: The chosen premise of the exercise may be conducive to attempting to extract personal information from victims. Clicking on the embedded Web link in the e-mail could display a registration Web page where the victim can enter personal information such as location, job title, etc. This could give the exercise greater impact when victims realize their personal information would have fallen into the hands of cyber criminals had the exercise been a real spear phishing attack.

Metrics: As part of the planning process, the required metrics should be determined and collection mechanisms implemented and tested. Possible metrics include:

- Number of e-mails that were read: A percentage of recipients will not read the e-mail during the metrics collection period (e.g., they are out of the office or they decide to delay processing that particular e-mail). Metrics should be reported based on the number of e-mails read rather than the entire target population.
- Number of e-mails deleted and not read: Deleting the e-mail without reading it can be considered a desired behavior.
- Number of replies to the e-mail: Replying to a malicious sender is an undesirable behavior.
- Number of victims: Clicking on the embedded link in the e-mail is an undesirable behavior. If a separate registration page is used, additional metrics can be collected on those who entered personal information.

Notification Web page: In order to reinforce desired behaviors, a mechanism should be in place to notify and educate victims. Depending on the premise used, a notification Web page can be presented to the victim either after the embedded Web link in the e-mail is clicked or after personal information is submitted into a separate registration Web page. The key components of the notification Web page are:

- Notification that the e-mail was part of a spear phishing e-mail and that no remedial action would be pursued.
- Description of the consequences that could have occurred had the e-mail been part of a real spear

phishing attack. Screen shots of the spear phishing e-mail and any Web pages used should be included for clarity.
- Description of the clues in the e-mail that the victim should have recognized as suspicious.
- Reinforcement of the desired behaviors, including instructions on any internal mechanism for reporting spear phishing e-mail. Relevant policies and procedures should be cited. Additional resources on spear phishing threats and risks should be provided.
- Contact information so the victim can follow up with questions or comments.

Notification of exercise details to management and internal support organizations prior to implementation: Notification of the date and time of the exercise to specific management may be required. Minimal notification is suggested in order to keep the secrecy of the exercise intact.

The efficacy of internal incident response processes can be tested as part of the exercise. Determine if internal support organizations such as helpdesk/desktop support and the incident response team will be notified prior to the implementation of the exercise.

C. Post-Exercise Reporting

Participation in the exercise should be strong at the initial onset and drop off considerably after a few hours. Metrics collection can be halted after a day, and can be analyzed based on the subset who participated (those who took some action). A review of the exercise parameters and results should be reported to management and include any actions that the security awareness team will take based on the results. A communication summarizing the results should be distributed to the entire organization as part of the security awareness effort.

IV. Spear Phishing Exercises Conducted at Northrop Grumman

Two spear phishing exercises were successfully conducted at Northrop Grumman in 2009, directed at two employee populations that are potential targets of advanced persistent threat actors due to their specialized access to company information and systems.

A. Constraints and Assumptions

The following constraints and assumptions were made when planning and implementing the spear phishing exercises at Northrop Grumman:

Subsets of the employee base targeted: The large employee base of 120,000 employees made it tactically difficult to implement a company-wide spear phishing exercise. Instead, subsets of the employee population have been identified, based on information gathered from media reports.

Company culture: Because of its lines of business, Northrop Grumman has a company culture that is generally security-aware. Policies and procedures surrounding physical, computer, and information security are relatively aggressive in an effort to maintain a secure culture and protect sensitive information. Employees are provided with security awareness information on a regular basis, from various organizations and levels of management, and in diverse formats. Participation in the third-party consulting firm Information Risk Executive Council's end user survey [22] in 2009 resulted in Northrop Grumman's recognition as having a leading user security training and awareness program.

Internal incident response processes tested: In order to test internal incident response processes, the desktop support helpdesk and the security operations center staffs were not notified prior to the two exercises described below. The management of those teams had requested that their response processes be tested as part of the exercises.

B. Goals

The main goal of the spear phishing exercises was to test employees' awareness of fraudulent e-mail messages. Employees should scrutinize e-mail and recognize relatively obvious clues that an e-mail is not legitimate. They should not click on attachments or Web links within the e-mail if they are not expected or appear suspicious. Suspicious e-mails should be reported immediately to the company security operations center. Deletion of the e-mail without reading it was also considered an acceptable response.

A secondary goal was to test effectiveness of the incident response process. Immediate action should be taken by the incident response team to determine if the e-mail is part of a spear phishing attack, block any subsequent e-mails from entering the company e-mail system, and implement automated e-mail and voice response indicating that the attack is being investigated.

C. Exercise #1: Managers Asked to Verify Credentials

The first spear phishing exercise focused on approximately 16,000 Northrop Grumman managers. The e-mail was sent from the Internet, and the sender of the e-mail was spoofed to appear as if it originated from a

popular Internet service provider. The body of the e-mail was crafted to look like internal e-mails used to notify employees of network issues. Recipients were urged to connect to a Web site to verify their network login credentials within three business days or their accounts would be suspended. No contact information was included in the e-mail.

Clicking on the link connected the recipient to a notification Web page, which notified him that the e-mail had been a test, described the clues in the e-mail and the risks of clicking on the Web link, and indicated how suspicious e-mail should be reported.

D. Exercise #2: System Administrators Receive Free Gift with Whitepaper Download

Almost 3,000 employees with elevated privileges on company servers were targeted in the second spear phishing exercise. The e-mail appeared to be from an online publication whose name was similar to a real well-known publication. The e-mail promised a free 32GB flash drive in return for downloading a technical whitepaper, if the recipient was one of the first 3,000 to respond to the e-mail that day.

The embedded Web link with an external URL connected the recipient to registration page which requested personal information, such as job title, address, and phone number. Both the sender address in the e-mail and the embedded Web link contained zeroes in place of the letter "o," a telltale sign of a spoofed e-mail.

Clicking on the "Submit" button on the registration Web page connected the recipient to a notification Web page. Similar to the first spear phishing exercise, the notification Web page described the clues, risks, and reporting process.

For this test, a follow-up e-mail was sent to the population the next day, requesting information on why they did or did not click on the link. This additional metric was tabulated and presented along with the rest of the metrics.

V. Results

Baseline results: A moderate degree of response was observed in the management group, whereas a minimal response was observed in the system administration group. Future exercises will target these populations again to measure any change in response.

A common comment received from victims of the exercises was that employees are inundated with e-mail and do not always take the time to scrutinize them carefully before reacting to them. They asked for tools or automated alerts that could help them recognize suspicious e-mail quickly and easily.

Internal incident response: Over the two exercises, improvements were observed in the internal incident response teams' recognition of the spear phishing attack and implementation of countermeasures to block subsequent e-mails from entering the company e-mail system. Future exercises may involve notifying these teams prior to implementation in order to focus the exercises solely on the response of the e-mail recipients.

Response from target populations: Participants were able to send comments via e-mail, and after implementing spear phishing exercises that targeted in total approximately 20,000 employees, the overall feedback about the exercises has been markedly positive. Many appreciated the reminder to take the time to scrutinize e-mail more carefully. Others indicated that this type of exercise was both a practical and proactive way to increase security awareness. Several wanted further clarification on reporting procedures, and some provided comments that precipitated further research into additional e-mail security measures.

New security measures: As a result of suggestions and comments received by the exercise participants, tactical projects were implemented to determine what could be done to further secure e-mail.

VI. Lessons Learned

Each spear phishing exercise has provided data that can be used to improve future exercises.

Use of a registration Web page is very effective: A registration Web page allows the participants to provide, in some cases, more detailed information than can be gathered easily from network or e-mail account information.

End-to-end testing is critical: When all of the parameters for the exercise are in place, an end-to-end test should be implemented within the team to ensure that all aspects of the exercise are working as planned. This includes checking the flow of the e-mail from the Internet through the company perimeter and e-mail security devices to the company e-mail system; testing the user experience of processing the e-mail and navigating the associated Web pages; and ensuring that the metrics are being gathered as planned.

Testing internal response procedures can affect participant response metrics: Because the internal helpdesk and incident response staffs were not notified of the exercises prior to their implementations, there was a danger that the incident response team would block the incoming spear phishing e-mails before they reached the

entire target population. The staffs had to be monitored carefully during the exercise in order to ensure that all spear phishing e-mails were allowed to reach their targets.

Sufficient metrics can be gathered within one day: Once a few participants realize that the e-mail is an exercise and not a real spear phishing attempt, they may notify their management and co-workers, subsequently reducing participation in the exercise. Also, a percentage of the population may never read the e-mail if it is not perceived as relevant or of interest. Indeed, an Intrepidus Group study in 2009 reported an average of 60 percent of corporate employees that were found susceptible to targeted spear phishing responded to the spear phishing e-mails within three hours [12]. Metrics can be reported based on the subset of the population that processes the e-mail.

Metrics can be skewed by Outlook delegates: During the exercise targeting managers, some of the identified victims did not appear on the original recipient list. In some cases, administrative assistants who were delegates for their managers processed the spear phishing e-mail. This was noted in the metrics reports.

Heightened awareness can have a backlash effect: After each exercise, there was an increase in reporting of suspicious e-mail, including valid internal e-mails. Participants were afraid to respond to any external or internal e-mails with attachments or Web links prior to verification by an internal security organization.

VII. Future Direction

Based on the results in 2009, Northrop Grumman has instituted these exercises as quarterly events as part of the standard annual training and awareness activities. New subsets of the employee population may be targeted based on attack vectors observed on the Internet. Previously targeted populations may also be exercised again to further measure the efficacy of these exercises.

Other security awareness vehicles, such as regular communications and mandatory security awareness training, will continue. Areas of focus may be adjusted based on feedback received from subsequent spear phishing exercises. Future victims may be required to complete additional security awareness training specifically related to spear phishing.

Additional methods of securing e-mail and alerting employees of suspicious e-mail are being aggressively pursued.

VIII. Conclusion

E-mail has become an essential part of both academia and business operations, making it a popular target of cyber criminals who want to steal sensitive personal information and intellectual property. Spear phishing is a particularly insidious attack vector because there are no technical controls that can completely filter spear phishing e-mails and prevent them from arriving in recipients' e-mail inboxes. The e-mail recipient must be able to recognize and not be deceived by spear phishing e-mails.

Because individuals are the critical link in preventing spear phishing attempts from being successful, security awareness is the best defense. In addition to traditional communications and training methods, spear phishing exercises can have an immediate impact on individuals and provide direct feedback to the security awareness team to help identify which segments of the population require additional attention. Northrop Grumman has successfully used these exercises to raise awareness of spear phishing consequences and prompt the implementation of additional technical solutions to help its employees recognize spear phishing attempts.

IX. References

[1] *Hackers Have New Technique: 'Spear Phishing.'* November 17, 2009. Associated Press. Retrieved February 5, 2010 from http://www.foxnews.com/scitech/2009/11/17/hackers-new-technique-spear-phishing/

[2] Krebs, Brian. *Spear Phishing Gang Resurfaces, Nets Big Catch.* June 10, 2009. Washingtonpost.com. Retrieved February 5, 2010 from http://voices.washingtonpost.com/securityfix/2009/06/spear-phishing_gang_resurfaces.html

[3] Grow, Brian, Epstein, Keith, Tschang, Chi-Chu. *The New E-spionage Threat.* April 10, 2008. Business Week. Retrieved February 4, 2009 from http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm

[4] Greenberg, Andy. *Cyberspies Target Silent Victims.* September 11, 2007. Forbes.com. Retrieved February 8, 2010 from http://www.forbes.com/2007/09/11/cyberspies-raytheon-lockheed-tech-cx_ag_0911cyberspies.html

[5] Koman, Richard. *Monster.com Hit by a Monster Phishing Scam.* August 22, 2007. Enterprise Security Today. Retrieved February 5, 2010 from http://www.enterprise-security-

today.com/story.xhtml?story_id=13300EWTF5DI&page=1

[6] University of Connecticut. *Phishing E-mails Target Students' Accounts at UConn.* November 11, 2008. Retrieved February 11, 2010 from http://www.spamfighter.com/News-11268-Phishing-E-Mails-Target-Students-Accounts-at-UConn.htm

[7] Cal Poly Pomona. *Scams and Phishing.* January 6, 2010. Retrieved February 11, 2010 from http://www.csupomona.edu/~ehelp/scams_phishing.shtml

[8] Penn State. *Beware of Phishing Scams and Holiday Spam.* December 14, 2009. Retrieved February 11, 2010 from http://live.psu.edu/story/43483

[9] Hernandez, Sharon. *Scams Target Facebook, Twitter Users.* Ball State University Daily News. November 16, 2009. Retrieved February 11, 2010 from http://www.bsudailynews.com/news/scams-target-facebook-twitter-users-1.2084552

[10] Choney, Suzanne. *Facebook Hit Again with E-Mail Phishing Attack.* May 21, 2009. Msnbc.com. Retrieved February 5, 2010 from http://www.msnbc.msn.com/id/30874530/

[11] Lamb, Tyler. *College Students a Target for Identity Theft, Financial Scams.* Royal Purple. January 21, 2009. Retrieved February 11, 2010 from http://media.www.royalpurplenews.com/media/storage/paper1225/news/2009/01/21/News/College.Students.A.Target.For.Identity.Theft.Financial.Scams-3590275.shtml

[12] Interpidus Group. *One-Quarter of Worldwide Population at Risk of Spear Phishing Attacks: Report.* March 9, 2009. Retrieved February 5, 2010 from http://www.darkreading.com/insiderthreat/security/app-security/showArticle.jhtml?articleID=215801372

[13] Higgins, Kelly Jackson. *Spear-Phishing Attacks out of China Targeted Source Code, Intellectual Property.* January 15, 2010. Informationweek.com. Retrieved February 5, 2010 from http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=222301157

[14] Goodin, Dan. *Fake Subpoenas Harpoon 2,100 Corporate Fat Cats.* April 16, 2008. The Register. Retrieved February 5, 2010 from http://www.theregister.co.uk/2008/04/16/whaling_expedition_continues/

[15] Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee, February 27, 2008. Retrieved February 11, 2009 from http://www.dni.gov/testimonies/20080227_testimony.pdf

[16] Northrop Grumman Corporation Web site. Retrieved February 6, 2010 from www.northropgrumman.com.

[17] Savage, Marcia. *User Education Key Defense Against Spear Phishing.* August 17,2005. SC Magazine. Retrieved February 5, 2010 from http://www.scmagazineus.com/user-education-key-defense-against-spear-phishing/article/32458/

[18] Higgins, Kelly Jackson. *Spear-Phishing Experiment Evades Big-Name Email Products.* January 5, 2010. Darkreading.com. Retrieved February 5, 2010 from http://www.darkreading.com/insiderthreat/security/client/showArticle.jhtml?articleID=222200326

[19] Smith, Allen, Toppel, Nancy. *Case Study:Using Security Awareness to Combat the Advanced Persistent Threat.* June 1, 2009. Proceedings of the 13th Colloquium for Information Systems Security Education.

[20] Perlman, Ellen. *The Phishing Catch.* July 15, 2008. Governing.com. Retrieved February 5, 2010 from http://13thfloor.governing.com/2008/07/whens-the-last.html

[21] Kol, Derek D. *United State Military Academies to Use PhishMe to Combat Spear Phishing.* July 24, 2009. Marketwire. Retrieved February 5, 2010 from http://www.marketwire.com/press-release/United-States-Military-Academies-to-Use-PhishMe-to-Combat-Spear-Phishing-1021627.htm

[22] Information Risk Executive Council (IREC). *Focus on User Motivation to Drive Compliance.* 2008. Retrieved February 8, 2010 from https://www.irec.executiveboard.com/Public/Documents/ExecutiveSummary/IREC1AM9TRJ_Awareness_ExecSum.pdf. Note: IREC publishes details of its end user surveys only to its members. This reference is a publicly available datasheet on IREC's services related to end user security awareness.