Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2013 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-2013

Countermeasures for Social Engineering-based Malware Installation Attacks

Waldo Rocha Flores
Royal institute of technology (KTH), waldorf@ics.kth.se

Mathias Ekstedt
Royal institute of technology (KTH), mathias.ekstedt@ics.kth.se

Countermeasures for Social Engineering-based Malware Installation Attacks

Waldo Rocha Flores
Royal institute of technology (KTH)
waldorf@ics.kth.se

Mathias Ekstedt
Royal institute of technology (KTH)
mathias.ekstedt@ics.kth.se

Abstract
Social engineering exploits vulnerabilities at different layers (i.e. technical, social layer) in an organizational defense structure. It is therefore important to understand how to defend against these attacks using a holistic defense approach including multiple countermeasures. The literature suggests a plethora of countermeasures, little research has however been done to assess their effectiveness in managing social engineering threats. In this paper we attempt to obtain a deeper understanding of how to defend against a type of social engineering attack that attempts to install malware on computers through e-mail or portable media. We explore commonly proposed countermeasures needed to prevent this type of attack, and if any dependencies between them exist. Through a combined method approach of surveying the literature and conducting semi-structured interviews with domain experts we identified a set of countermeasures that provide empirical input for future studies but could potentially also give organizations guidance on how to manage social engineering-based malware installation attacks.

Keywords
Social engineering, malware installation, countermeasures.

1. Introduction
The increased effectiveness and robustness of technical security components has made it more difficult to successfully introduce malware on computer systems using purely technical means. Many attackers have therefore started to include social means in their malicious efforts and target the humans accessing and using the computers (Applegate, 2009). These types of attacks are commonly known as social engineering attacks. In organizational settings, typical social engineering attacks include deceptive methods to make an organizational member comply with a malicious request, e.g. execute malware on a computer or install malware through portable media (Mitnick & Simon, 2002). Numerous papers have focused on describing social engineering concepts and proposed a plethora of different countermeasure including technical controls, user interventions and organizational security policies. However, the effectiveness of these approaches has largely remained anecdotal. The existing empirical research has largely focused on success rates of certain types of social engineering attacks or analyzing characteristics that

influence an individual's susceptibility to social engineering attacks. In Bakhshi, Papadaki, & Furnell (2009) an experiment was conducted in where a phishing mail was sent out to organizational employees as a mean to assess the probability of malware being successfully installed on their computers. In the study by Pattinson, Jerram, Parsons, McCormac, & Butavicius (2012) it was found that familiarity with computers and cognitive impulsivity affected an individual's susceptibility to phishing. These results provide indications of how susceptible an organization is to social engineering, but no information is given on how to effectively counter these attacks and most importantly, which countermeasures that are effective when employed in an organization given different scenarios, i.e., the type of attack they counter. From a practitioner's point of view, it's challenging to practically assess the effectiveness of countermeasures. It is therefore, with no doubt, useful to know if there are countermeasures that are more effective than others and if some combinations of countermeasure are better than others.

The purpose of this paper is to examine the effectiveness of commonly proposed countermeasures against two types of social engineering-based malware installation attacks: phishing and malware installation through portable media. To effectively defend against social engineering attacks the strategy need to include multiple countermeasures that are structured and combined in a holistic approach (Applegate, 2009). We therefore attempt to understand if any dependencies between countermeasures exist. We aim to fulfill this purpose through a combined method approach in where we first identify relevant countermeasures by performing a literature review and then obtain opinions on the perceived effectiveness of the countermeasures by conducting semi-structured interviews with domain experts.

The rest of the paper unfolds as follows. The next section presents social engineering attacks and countermeasures discussed in the literature. The section that follows presents how the data collection was conducted in order to obtain a deeper understating of social engineering malware installation attacks and countermeasures. Then, the results of the data collection are presented and discussed. The final section concludes the paper.

2. Theoretical framework

While there have been many papers describing social engineering and its components in detail (e.g. (Applegate, 2009)(Hong, 2012)(Mitnick & Simon, 2002)) there is, to the knowledge of the authors, no holistic approach that have examined the effectiveness of countermeasures and their potential dependencies, given different scenarios. This section provides a basis for understanding the linkages between two social engineering-based malware installation attacks (phishing and malware installation through portable media) and countermeasures commonly proposed in the literature that will be discussed during the interviews.

2.1 Social engineering-based malware installation attacks

Phishing is described as the marriage between technology and social engineering in which attackers use spoofed email messages to trick end-users into taking a suggested action that benefits the attacker (Nohlberg & Kowalski, 2008). For instance, the attacker can convince end-users to reply with sensitive information such as user credentials or click on a malicious link where the attacker either: i) automatically introduce malware by exploiting vulnerabilities in the

web browser (e.g. drive by download) or ii) persuade end-users to execute malware on their computers. Malware can also be executed through hidden scripts in attached documents.
Malware installation using portable media is the practice of using a combination of technical and social attack methods. For instance, an attacker can send a valuable gift (e.g. an Ipad) to a potential victim or leave a USB memory stick with a tempting text, outside a building, to entice a victim's curiosity into using the item in their computer (Nohlberg & Kowalski, 2008).

2.2 Countermeasures

Countermeasures against social engineering- based malware installation attacks can be categorized as organizational security policies, user security interventions and technical controls. In the following, countermeasures proposed in the literature are presented.

2.2.1 Organizational security policies

Organizational security policies are developed and maintained to get employees to perform behavior that is conducive to the protection of information assets in the enterprise (A. Da Veiga & Eloff, 2010).
Internet use policy addresses and restricts employee Internet usage (e.g. usage of social network sites during work hours) (Hasan & Prajapati, 2009),(A. D. Veiga & Eloff, 2007).
Acceptable installation policy addresses software installation privileges and restricts additional software installation on users' computers (Nohlberg & Kowalski, 2008).
Hardware policy addresses the acceptable use and disposal of hardware (e.g. computers, portable media) that can contain either sensitive information or malware (Hasan & Prajapati, 2009).
Separation of duties policy has the primary objective to prevent that a single deception or breach of trust is sufficient to compromise a system. In theory, the policy can prevent an attacker from gaining access of information when deceiving one victim as it may require more than one victim to deceive for accessing the targeted information. This may discourage the attacker and thus lower the probability of success (Nohlberg & Kowalski, 2008),(Botha & Eloff, 2001).

2.2.2 User interventions

User interventions are often seen as an important to counter social engineering attacks and often carried out through formal training, workshops, lectures or through IT-based training tools.
Awareness education and training program increases the user knowledge of general IT security threats and threats related to social engineering malware. Further, the training should inform the user on common manipulative techniques and educate the user to recognize and react to an attack (Applegate, 2009), (Mitnick & Simon, 2002).
Verification and authorization procedures educate users that they need verify the identity of the person requesting a type of information or action to be taken, and ensure that the person is authorized to receive the requested information or giving the order to perform an action (Mitnick & Simon, 2002).
Social engineering penetration tests are important for management to assure and monitor that the users have comprehended the security education and training. This could be done through implementing regular security exercises using weaker forms of penetration tests. These exercises reinforce the training and education programs. It also keeps the users alert, and more prepared in the occasion of an actual attack (Barrett, 2003)(Nohlberg & Kowalski, 2008).

2.2.3 Technical controls

Technical controls are countermeasures that are implemented to block a malicious mail at the gateway, prevent a user to browse on malicious web pages, or prevent malware to be installed on a computer.

Sender policy framework works as an email validation system designed to prevent email spam by detecting email spoofing by verifying that a sending host is authorized to send mail on behalf of the source domain. This measure should make it easier for the human recipient to recognize that the sending domain is legitimate for the targeted organization (Tally, Thomas, & Vleck, 2004),(Milletary, 2005).

Content-based email filter is a countermeasure that is installed at the company's network boundary (mail gateway). It analyses the e-mail content and prevents phishing e-mail from reaching the users and thus stopping the attack at an early stage of the attack (Bergholz, 2010),(Huang, Tan, & Liu, 2009).

Blacklist function is a measure that is included in the browser. The browser queries lists of blacklisted and whitelisted domains and makes sure that a user is not accessing any malicious phishing sites. The blacklist requires active monitoring and needs to be updated on a regular basis (Hong, 2012),(Huang et al., 2009).

Little research has been done on the effectiveness of commonly proposed countermeasures against social engineering-based malware installation attacks and if there exists potential dependencies between those countermeasures. In an attempt towards fulfilling the gap, data was collected by interviewing content domain experts.

3. Data collection

Six semi-structured interviews were utilized in order to capture rich, detailed information on content experts' views of the investigated domain in general, and countermeasures against social engineering attacks in particular. The number of respondents was decided due to the following reasons: i) the study is of exploratory nature, and ii) a too high number of respondents will make thorough interpretations of the interviews difficult (Kvale, 1986).

The interviews were carried out from February 2012 to June 2012. All respondents had acquired a deep domain specific knowledge through experience of the topic on a regular basis. Two of the respondents were academics, and are both well-regarded in the research field and have many years of practical experience. Four respondents were practitioners. They were selected on recommendations, and had all worked extensively within the investigated domain. Respondent data is summarized in table 1.

Respondent	Position	Experience (Years)	Time (Hours)
1	Professor and scientist (private industry)	>15	1
2	Senior Consultant	16	1.5
3	Consultant	5	1.5
4	Head of Security (private industry)	12	2.5
5	Associate professor	>10	2
6	Senior security researcher (private industry)	>15	1

Table 1: Respondent data

Three of the interviews were carried out face-to-face at the expert's respective places of business and three over telephone due to geographical issues. Due to the complexity of acquiring assessment on the effectiveness of the countermeasures effort was spent to enforce reliability of results. That is, the original layout and scope of the data collection was somewhat changed according to the focus area(s) of the respondents. For example, no answers were forced, the scales were allowed to be switched for a ranking system, and the respondents were allowed to traverse from the original scope if needed. For example, if they wanted to discuss a particular countermeasure in greater detail. As a consequence, more time was spent on those matters the respondents perceived to be of greater importance for the topic of the study.

The interviews all had the same general approach, and consisted of three main objectives: (i) to gain a deeper understanding of social engineering-based malware installation attacks, (ii) to discuss the relevance (if the experts perceived that the countermeasures are not only useful in theory but will also possible to implement in practice) and comprehensiveness (if there are any countermeasures missing to capture the content domain) of the countermeasures proposed by the literature (cf. section 2.2), (iii) to assess the effectiveness of countermeasures that were the output of objective (ii) through a scale of 1-5, where 1 meant "do not increase the difficulty of successful attack" and 5 "greatly increase the difficulty of successful attack" and (iv) to discuss potential relationships between countermeasures, i.e., if the experts perceive that any combination of countermeasures provides greater effectiveness, and which combinations that they perceive don't provide any greater effectiveness.

4. Data collection results and discussions

During the first interview the expert commented on the importance of clearly defining the profile of the attacker and to clarify what the attacker wants to obtain by attacking an organization or individual, i.e., is the attacker after generic or specific information of an organization. It is expected that the effort required to defend against a targeted attack is much higher than for a generic attack and the experts therefore perceived that the type of attack affect the effectiveness of the countermeasures. Therefore, only when clearly defining the attacker an assessment of countermeasure effectiveness can be done. As a consequence effort was spent on clearly defining the type of attacker and the type of attack that is performed.

Three categories of attacks were defined: a hyper-targeted attack, a semi-targeted attack or a generic attack. In a hyper-targeted attack, the attacker is a professional social engineer with a large amount of resources, has spent time preparing the attack and obtained a considerable amount of context-specific information that makes the effect of any implemented countermeasure rather weak. In a semi-targeted attack, an attacker has obtained some context-specific information, hasn't the same amount of resources and don't spend as much time on preparing the attack (the most common attack according to the experts). A generic attack is usually carried out be a less professional attacker (also known as "script kiddie") which uses a spam-like approach and relies heavily on publically available automated phishing tools.
For the purpose of the present study, the attacker was defined as an attacker that is performing a semi-targeted attack and has obtained some context-specific information. This definition was introduced in the remaining interview sessions.

4.1 Opinions on the type of attacks

The experts agreed that the attack is more likely to be regarded successful if the attack aims to compromise a computer from anyone in an organization than a specific piece of information that a specific person has access to. For instance, clicking on malicious link can be enough to install malware through a drive by download on a randomly chosen user computer. However, if the attacker is after a specific piece of information, the specific information owner needs to install the malware. This will require a targeted attack where context-specific information needs to be obtained. This information can be obtained by gathering information from the target organization in the preparation of the attack.

Regarding the two attack types (phishing and malware installation through portable media), the experts perceived that they have both the same main purpose – to install malware on a user computer. Given the purpose of the study, the experts perceived that it isn't necessary to have two attack types as they both use social and technical means to make users' install malware on their computer and therefore suggested merging these two attack types into one broader attack type. Consequently, the two attack types were aggregated to one variable.

4.2 Opinions on the countermeasures

4.2.1 Opinions on security policies

A policy that restricts Internet usage is perceived to be difficult to implement in an entire organization. Five experts argued that the best way to protect user is to keep them away from malware. Therefore it's suggested that such a policy should be implemented on the computers to control the use of browsers versions and websites that employees are allowed to browse. This policy works to prevent users form accessing hostile content on the Internet and limit access to sites people actually need to access during work hours. The experts recommended replacing the *Internet use policy* with a broader policy denoted as *Technology acceptable use policy* and also include acceptable email usage.

Regarding acceptable installation of additional software the experts suggested that a combination of two measures can be used. The first measure can be a written policy that addresses acceptable installation of additional software (*Acceptable installation policy*) and the second countermeasure is a policy installed on the computer to *Minimize user privileges* (the experts prescribe the change of *Separation of duties policy* to the procedure *Minimizing user privileges).* The latter countermeasure both limit users access rights to information that users need in their daily work and make it impossible for regular users to install software on their work computers without having administrator privileges. The experts further agreed that a policy that addresses the acceptable use and disposal of portable media is useful and can be implemented in practice. However, they suggested renaming the measure to *Device acceptable use policy*.

4.2.2 Opinions on user interventions

Training users to recognize and react to malware attacks is perceived to provide good results. However, the experts' opinions are rather varying. One expert perceived that it's not useful to train users as at least one user will always be fooled by the social engineer and install the malware in spite of educational efforts. For instance, this expert believed that if a device is desirable enough, the user will connect the device to a computer and thereby install malware.

However, the experts agreed that for an attack through portable media, user training is more effective than for a phishing attack as they perceive that it's easier to implement such training in practice. Regarding verification procedures, the experts agreed that if the attack is targeted, the measure is not effective at all as the attacker will bypass the measure using effective manipulative skills. The experts agreed that social engineering penetration tests are well-invested efforts if the results are used effectively. The penetration tests assess how well implemented measures function and identifies weaknesses in the security defense chain. The tests increase the security awareness and make future educational efforts more effective.

Based on the expert recommendations, the measures *awareness education and training program* and *verification and authorization* procedures was aggregated to *User security training*. *Social engineering penetration test* was replaced with *Performance monitoring*.

4.2.3 Opinions on technical countermeasures

The experts agreed that technical countermeasures are important and should be able to recognize if an attached link or software is malicious. The experts suggested three layers of technical measures. The first layer prevents a malicious mail from reaching its target. This layer consists of parameters related to email protection on a mail server level. Anti-spam technology analyzes the structure of an incoming mail at the gateway. Antivirus technology checks for virus signatures, content filter analysis the email to identify any suspicious content, and outbreak filter analyses the attached link to the website (based on blacklist technology). If the filter doesn't recognize the link to the website, it's quarantined and scanned for virus and if virus is identified the mail is blocked. The experts recommended the countermeasure that prevents a malicious mail from reaching its target to be referred as *Email protection*.

The second layer consists of parameters related to the protection against malware installation on a user's desktop computer. This layer consist of measures such as antivirus, antimalware, content filter, outbreak filter and web reputation filter that analyses the IP address to the webserver. If the webserver is listed as malicious, the user is not able to browse to the malicious website. The experts recommended naming the measure *Desktop anti-malware.*

The final measure is activated when a user has installed malware on a computer. The measure works to monitor and detect malicious outgoing traffic. Intrusion Detection Systems (IDSs) usually serve this purpose.

4.2.4 Countermeasures to add according to the experts

Regarding the comprehensiveness of the countermeasures, the experts recommended to add five countermeasures. *Intrusion detection system* was added to monitor and detect malicious outgoing traffic. For data hygiene, two measures were recommended: a formal *Patch management process* that regularly updates used software and a process that monitors the services being used and *Disable unnecessary services* if needed. Thus, minimizing service being used and maximizing software updates. A *Device control* measure was added to handle attempts to install malware through portable media. This measure includes virus scanning when the user connects the media and that the auto-run function is turned off. The experts finally agreed that *Information security leadership* is very important for effective implementation and manage of all other measures, and to get sponsorship for every security effort being made or planned to be made in an organization.

4.3 Effectiveness of countermeasures

The quantitative estimates made by the respondents can be seen in Table 2. These estimates are made under the assumption that no measure other than the one studied is present. The effectiveness of the measures was studied based on the changes as recommended by the experts and their effectiveness against an attacker that is conducting a *semi-targeted* malware installation attack and has obtained some context-specific information. Notable is that the two respondents did not feel comfortable providing quantitative estimates of 1-5, they preferred High (H), Medium (M), and Low (L) instead. The results point to a consensus regarding most measures. There is agreement regarding *Information security leadership* to be the most effective measure. However, the consensus regarding *User security training* is rather low. The respondents perceive it to be important, but the effectiveness depends on the degree of obtained context-information that an attacker can use to gain trust.

Attack	Countermeasure	R1	R2	R3	R4	R5	R6
Malware installation attack	Technology acceptable use policy (TAUP)	-	2	2	2	-	L
	Acceptable installation policy (AIP)	2	4	4	3	L	M
	Device acceptable use policy (DAUP)	-	4	4	2	L	M
	User security training (UST)	2	4	3	4	H	L
	Performance monitoring (Pmon)	2	4	3	3	M	L
	Patch management (Pman)	-	3	3	3	M	H
	Disabling unnecessary services (DUS)	-	-	2	2	M	H
	Minimizing user privileges (MUP)	4	3	-	-	M	H
	Email protection (EP)	3	4	3	4	M	M
	Desktop anti-malware (DAM)	4	4	4	4.5	-	H
	Intrusion detection system (IDS)	3	3	3	3	-	H
	Device control (DC)	3	4	2	4	M	-
	Information security leadership (ISL)	5	4	4	4	-	-

Table 2: Estimates of the effectiveness of countermeasures

4.4 Effectiveness of countermeasures in combination

Oftentimes, the effectiveness of one countermeasure can be thought of as dependent on the presence of another. The result of the data collection on this topic is depicted in table 3. A “0“ means that the combination of countermeasures is not perceived to result in a significant increased effectiveness. A “+” means that the combination is perceived to result in a significantly increased effectiveness. A “*” means that a data collection event did not detail the perceived dependency between two countermeasures. Interview 1 is the first symbol in each cell, interview 2 the second, interview 3 the third, and so forth. For example, the combination between *Acceptable installation policy (AIP)* and *Performance monitoring (Pmon)* has the symbols “0+++*+“. That is, respondent 1 (R1) did not perceive the combination to result in any significant increased effectiveness, and as such the first symbol is “0“. The second, third, fourth

and sixth respondents (R2, R3, R4 and R6) perceived a significant increased effectiveness of the combination, and thus the second, third, fourth and sixth symbols are "+". Finally, the fifth respondent did feel comfortable to assess the effectiveness in combination; and thus the fifth symbol is"*".

Some interesting results are now discussed. All experts perceived that *Information security leadership (ISL)* in combination with the other countermeasures increases the effectiveness of the protection against malware installation. *User security training (UST)* is perceived to increase the effectiveness in combination with all measures except *Patch management (Pman), Disable unnecessary services (DUS)* and *Minimizing user privileges (MUP)*. This is expected as these measures are oftentimes managed by a centralized IT department and do not have a direct interaction with the user. However, *Email protection (EP)* and *Desktop-antimalware (DAM)* for instance, are perceived to have a greater effectiveness in combination with user training. The reason for this is that the experts perceived that the technical measures should work to both prevent a malicious email from reaching its target and make it impossible for a user to install malware on a computer. However, if the mail reaches the user and the computers antimalware is not implemented or well-maintained; the training should prevent the user from installing the attached malware. Therefore it is believed that these countermeasures, together, make it more difficult for an attacker to successfully install malware on a user computer. *Device control (DC)* and *Acceptable installation policy (AIP)* is perceived to increase the effectiveness in combination by five out of six experts. On the other hand, the countermeasure specifically related to malware installed using devices is generally not perceived to be effective in combination with measures implemented for phishing attacks. The reason behind this is logical and based on the fact that these measures are simply not relevant in combination.

In this study we examined the combination of two countermeasures at a time. Examining more than two countermeasures at a time would be interesting, although very time consuming, and there could be a risk that it would be difficult to assess the effectiveness of more than two countermeasures in combination, in particular using human judgment. As the results show, the experts in this study perceive that some combinations do not increase the effectiveness in combination. Future research could examine if these results hold when collecting data from a larger sample.

4.5 Discussions on the interview methodology

To address bias in this study, the data collection was carried out using the same procedure using a structured procedure. Also, no respondent had any previous affiliation with the interviewer. To handle the complexity of the research purpose, the questionnaire was broken down into a sequence of different topics. The sub-session corresponding to each of these topics were introduced by the interviewer at the beginning of each session. Another potential bias is that respondents, if pressured, can provide answers which they do not really believe in. This is of particular significance to a study such as the present, with complex high-level questions that can be perceived as difficult to answer. To counter this issue, no answers were forced. Furthermore, the format of the estimates could be changed to better suit the respondent. These options were utilized twice in the present study: one respondent did not feel comfortable assessing the effectiveness of countermeasures in combination and two respondents did not feel comfortable

with the measurement scale of "mean effectiveness". As a consequence, the interview instrument was revised during these occasions to accommodate their needs.

	TAUP	AIP	DAUP	UST	Pmon	Pman	DUS	MUP	EP	DAM	IDS	DC
AIP	0++***											
DAUP	0000*0	++++*+										
UST	++++*+	++++*+	++++*+									
Pmon	0+++**	0+++*+	0+++*+	0+++++								
Pman	*****0	**00*0	***0*0	***0*0	***0*0							
DUS	***0*0	***0*0	***0*0	***0*0	***0*0	***0*0						
MUP	**00*0	++++*+	++++*+	**00*0	0000*0	0000*0	00++*+					
EP	0+++*+	0+++*+	*000**	++++*+	0++0*+	*****0	**00*0	+**+**				
DAM	0**+**	++++*+	++++**	++++*+	0000*0	*+++*+	0****0	*****0	*+++*+			
IDS	0****0	0**0*0	0**0*0	++++*+	0000*0	***0**	*00**0	*00**0	++++*+	0+++*+		
DC	0000*0	++++*+	++++**	++++*+	0++**0	0****0	0****0	**+**0	0000*0	++++*+	0000*0	
ISL	++++*+	++++*+	++++*+	++++*+	++++*+	++++*+	++++*+	++++*+	++++*+	++++*+	++++*+	++++*+

Table 3: Dependencies between countermeasures. "+"denotes perceived increased effectiveness, "0"denotes no perceived increased effectiveness, and "*"denotes that the combination was not scored.

5. Conclusions

In this study, we have attempted to obtain a deeper understanding of how to defend against social engineering-based malware installation attacks. We have conducted six semi-structured interviews with experts to discuss the relevance and comprehensiveness of a set of countermeasures that were identified be performing a literature review. Data was then collected on the effectiveness of the individual countermeasures that the experts perceived to be relevant and if any dependencies between them exist.

The result of the interviews indicates that experts perceive that some countermeasures are more important and can be more easily implemented in practice than others. The consensus regarding the effectiveness of email protection, desktop anti-malware and intrusion detection system is rather high. However, for some countermeasures (e.g. user security training and device control) the consensus among the experts regarding the countermeasure effectiveness is rather low. The experts perceive that the most important countermeasure is information security leadership as it affects the effectiveness of all other countermeasures.

The study is of exploratory nature and as the field is still immature there is still research left to be conducted. The results from this study can be seen as hypothetical relations between social engineering concepts that can be further validated in future studies. In line with the nature of the study we aim at continuing our research by conducting several validation steps. Currently, we are conducting several case studies were we are collecting survey data, conducting observations and unannounced phishing experiments. Through these studied we will attempt to measure actual effectiveness of measures against a social engineering-based malware installation attack.

References

Applegate, S. D. (2009). Social Engineering: Hacking the Wetware! Information Security Journal: A Global Perspective, 18(1), 40-46. Taylor & Francis.

Bakhshi, T., Papadaki, M., & Furnell, S. (2009). Social engineering: assessing vulnerabilities in practice. Information Management & Computer Security, 17(1), 53-63.

Barrett, N. (2003). Penetration testing and social engineering: Hacking the weakest link. Information Security Technical Report, 8(4), 56–64. Elsevier.

Bergholz, A. B. (2010). New filtering approaches for phishing email. Journal of Computer Security, (1), 7-35.

Botha, R. A., & Eloff, J. H. P. (2001). Separation of duties for access control enforcement in workflow environments. IBM Systems Journal, 40(3), 666-682.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. Computers & Security, 29(2), 196-207. Elsevier Ltd.

Hasan, M. I., & Prajapati, N. B. (2009). An Attack Vector for Deception Through Persuasion Used by Hackers and Crakers. 2009 First International Conference on Networks & Communications (pp. 254-258).

Hong, J. (2012). The state of phishing attacks. Communications of the ACM, 55(1), 74-81.

Huang, H., Tan, J., & Liu, L. (2009). Countermeasure Techniques for Deceptive Phishing Attack. 2009 International Conference on New Trends in Information and Service Science (pp. 636-641).

Kvale, S. (1986). Interviews. An introduction to qualitative research interviewing. Thousand Oaks, CA: Sage Publications.

Milletary, J. (2005). Technical Trends in Phishing Attacks (pp. 1-17).

Mitnick, K., & Simon, W. (2002). The art of deception (p. 368). Indianapolis, Indiana: Wiley Publishing.

Nohlberg, M., & Kowalski, S. (2008). The cycle of deception – a model of social engineering attacks, defenses and victims. Proceedings of the Second International Symposium of Human Aspects of Information Security & Assurance (HAISA 2008) (pp. 1-11).

Pattinson, M. R., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why Do Some People Manage Phishing Emails Better Than Others? Information Management & Computer Security, 20(1), 18-28. Emerald Group Publishing Limited.

Tally, G., Thomas, R., & Vleck, T. V. (2004). Anti-Phishing□: Best Practices for Institutions and Consumers. Technical Report # 04-004 (pp. 1-28).

Veiga, A. D., & Eloff, J. H. P. (2007). An Information Security Governance Framework. Information Systems Management, 24(4), 361-372. ACM Press.

Workman, M. (2008). A test of interventions for security threats from social engineering. *Information Management & Computer Security*, *16*(5), 463-483.