Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2012 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

7-15-2012

Effects Of Information Seeking Modes On Users' Online Social Engineering Vulnerabilities

Koteswara Ivaturi
Department of Information S ystems & Operations Management, University of Auckland, k.ivaturi@auckland.ac.nz

Lech Janczewski
Department of Information Systems & Operations Management, University of Auckland, lech@auckland.ac.nz

EFFECTS OF INFORMATION SEEKING MODES ON USERS' ONLINE SOCIAL ENGINEERING VULNERABILITIES

Koteswara Ivaturi, Department of Information Systems & Operations Management, University of Auckland, 1010, k.ivaturi@auckland.ac.nz

Lech Janczewski, Department of Information Systems & Operations Management, University of Auckland, 1010, lech@auckland.ac.nz

Abstract

Hackers are increasingly exploiting the social movement on the Internet, which is responsible for domestication of the web and its associated technologies, by using novel methods of online social engineering (OSE). While most research to date in this field has focused on one type of OSE vector-phishing, there is a need to understand user vulnerabilities to other types of OSE attack vectors. This research in progress proposal first extends prior published classifications and presents a new typology of OSE attack vectors that manifest during the various information seeking contexts that users engage while online. This provides a conceptual starting point to build our empirical model that we propose will be useful in testing variance in human vulnerability to the different OSE attack vectors. The results of this research should be of interest to academic researchers, practitioners, consumer protection agencies and government regulatory authorities.

Keywords: Online social engineering, Human information seeking, human vulnerability, Information security, Typology

1 INTRODUCTION

While talking about information security it is very common to think about threats that can be contained with the help of technical countermeasures such as email filters, network firewalls, anti-viruses etc., albeit there is a more subtle form of threat to which there is no direct solution. Many organizations are learning the fact that technical countermeasures alone cannot provide the required security as ‘social engineering’ provides a means to bypass them (Rhodes 2001). Social engineering allows attackers to psychologically manipulate their victims to change their behavior and divulge important sensitive information (Townsend 2010). Accordingly, ‘online social engineering’ (OSE) is the use of the web in order to influence online user behaviour by exploiting the vulnerabilities in both humans & web applications individually or in unison, usually to the user’s detriment. Unlike other security vulnerabilities that are inherent to man-made software & hardware systems a key aspect of gaining insight into the nature of social engineering attacks involves a significant understanding of how humans interact. The fact that not all humans are unique adds an additional layer of difficulty to understand this esoteric attack methodology.

The advent of the Internet and our increasing dependency on it has expanded the threat landscape of these attacks. According to a recent report released by Symantec in 2010, 65% of the world’s online population has fallen victim to cybercrimes including computer viruses, credit card fraud and identity theft (Merritt 2010). Advances in technology that try to mitigate the effect of these attacks can be best described as ‘lacking’ partly because of the reactive nature of their detection mechanisms and partly because of the irresponsibility or ignorance on part of the user. The target demographic for our research is the casual internet user, who in the recent years has become an important unit of analysis given the range of activities he engages with on the web. Yet, empirical research that focuses on the vulnerabilities of this user has been relatively unexplored. Although there are a few published empirical studies that have analyzed how people respond to OSE attacks a majority of them have used ‘phishing’ as their primary test bed for research (Grazioli 2004; Jakobsson, Tsow et al. 2007; Workman 2007; Vishwanath, Herath et al. 2011). While there are many other vectors that can be categorized as OSE attacks, a question arises whether there is any other way to understand or explain human vulnerability holistically.

We try to achieve this by looking at the issue from a human web information seeking perspective. The objective of this research is to further our understanding of OSE attacks and the variance in human vulnerability to such attack vectors. Accordingly, the primary research question is to find whether different modes of information seeking on the web affect the user’s judgment in detecting OSE attacks. For this, we first built a two dimensional typology that maps OSE attack vectors against three specific modes of information seeking on the web. Based on this typology we then develop a model that could be used to correlate aspects of human vulnerability with the efficiency of different OSE attacks. As such, this study lies at the unique intersection of the fields of information science and information security. The results of this research should be of great interest to academic researchers, practitioners, consumer protection agencies and government regulatory authorities.

2 LITERATURE REVIEW & RESEARCH QUESTIONS

Human vulnerability is central to the success of OSE attacks and many researchers in the past have endeavored to understand aspects of it through various research studies. The objective of most of these studies was to understand why people fall victim for such attacks. As Downs et al. (2006) argue, it is necessary to understand why people fall for phishing attacks in order to build effective countermeasures in the form of tools or procedures. This chapter gives an overview of some of the well citied empirical studies that were conducted in the general area of deception on the web with a focus on attack vectors using social engineering methods.

Study	Methodology	Findings
Grazioli & Jarvenpaa (2000)	Lab experiment & questionnaire	Showed that users are vulnerable despite the presence of obvious signs of deception. Also shows how trust plays a moderating effect on the relationship between user's perceived risk & intention to shop online.
Karakasiliotis et al. (2006)	Questionnaire	Focusses on the user's ability to detect manipulations in phishing emails. Reveals that visual factors & content have an impact on the user's decision making.
Downs et al. (2006)	Interview	Shows that one of the reasons why people may be vulnerable to phishing is because the awareness of the risks is not linked to perceived vulnerability or to detection strategies.
Dhamija et al. (2006)	Lab experiment	Analyses successful manipulation strategies. Finds that a significant chunk of their sample did not heed standard security indicators while exposed to phishing emails
Workman (2007)	Questionnaire& Observation	Found that personality traits such as committment, fear, trust positively influence one's social engineering vulnerability
Jakobsson et al. (2007)	Lab experiment & interviews	Uses the 'think aloud' protocol and captures various user sensitivities that makes them think why phishing emails appear authentic and its contrary.
Tsow & Jakobbson (2007)	Lab experiment	Tests the effect of authenticity enhancing design changes combined with narrative strength as factors to exploit human vulnerabilities in the context of phishing
Jagatic et al. (2007)	Experiment	Tested the effect of a user's social network in increasing the probability of being victimized through a phishing attack
Vishwanath et al. (2011)	Questionnaire	Used OSIR model by including user involvement & motivation as a factor that can affect user vulnerability. Also tests the effects of structural elements of a phishing email like subject line, source, grammar & spelling & urgency cues.
Chen et al. (2011)	Questionnaire	Tests the affects of risk propensity & perception and their antecendents of commercial email reading intention

Table 1 Summary of empirical literature on OSE.

2.1 Prior empirical research on online social engineering

As can be seen from the table above, majority of the research studies relevant to the online social engineering attacks have primarily chosen phishing as the test bed for investigation into human vulnerabilities. While some of these studies have chosen to explore users's phishing detection abilities using descriptive analyses (Downs, Holbrook et al. 2006) some of them have chosen to set up laboratory or field experiments in order to get data (Grazioli and Jarvenpaa 2000). The above studies have also investigated the role of varied stimulus like source of the email, grammar, spelling and email title in affecting the deception detection of phishing emails. Other studies also integrated individual attributes such as self-efficacy, personal knowledge and level of involvement (Vishwanath, Herath et al. 2011). Some of the other examples of individual attributes hypothesized to affect phishing detection accuracy are gender (Dhamija, Tygar et al. 2006), personality traits such as committment, trust & fear (Workman 2007).

While these studies have definitely helped in developing an enhanced understanding of human vulnerabilites in the context of phishing there remain a number of unexplored areas within the realm of understanding OSE vulnerabilities. First, as discussed earlier most of the studies have used phishing as their test beds but when we talk about OSE attacks there are many other types of emerging attack vectors that are gaining popularity with the hackers and being used to victimize the world's internet users. Second, phishing is an attack vector that primarily affects users of email and so the structural elements that were studied in the above mentioned studies are relevant only to the context of deceptive emails. This shows that the effect of structural elements of other attack vectors are relatively unexplored. Lastly, as a result of the unduly focus on phishing we do not know if factors found causative for phishing detection would be useful for detecting other OSE attacks and whether exposure to a combined set of attacks would have an overall effect on the user's deception detection capabilities.

2.2 A typology of social engineering attacks – an information science perspective

A point reiterated in the prior sections is that while phishing as a OSE attack vector has been studied in depth there are many other OSE attack vectors that have been relatively unexplored. So what are the other attack vectors that can be categorized as OSE attacks? A taxonomy is always useful to gain a better understanding of any phenomenon and to build accurate measures that cater to it. A good taxonomy that is mutually exclusive, unambiguous, comprehensive and comprehensible can further explain this distinction (Lindqvist and Jonsson 1997). Laribee (2006) in her thesis suggests taxonomy to classify these attacks based on three broad criteria 'close access techniques', 'online social engineering' and 'intelligence gathering'. However, the list of different attack vectors that especially fall under online social engineering wasn't up-to-date while 'information gathering' is not strictly unique to social engineering. A recent study suggests a revised taxonomy that addresses the issues stated above to a fair extent. According to this taxonomy, OSE attacks entail vectors that propagate malware through email, social network spam, search engine poisoning and pop-ups (Ivaturi and Janczewski 2011). It is to be noted that although what happens after a victim clicks on a malicious link is very much like the traditional technical hacking, the initiation of such attacks is through setting up a situation that lures the user into the trap. This is where the distinction lies between traditional technical security attacks and OSE attacks.

However, the taxonomies mentioned above only enumerate different attack vectors that can be categorized as OSE attacks. What is still missing is a conceptual underpinning that can be used for empirical testing of user behaviour when exposed to these attack vectors. This can only be achieved with the help of an integrated model that reflects scenarios which can be mapped to instances of each of these attack vectors. We argue that the field of information science that studies human information seeking on the web fits our need of that integrated model. Accordingly, an obvious assumption for this research is that users of the web regularly engage in the act of information seeking and while doing so are exposed to OSE attacks. The next section discusses the theoretical premise for our argument.

2.2.1 Human information seeking

During the last decade, the web has become the prime destination for an increasing number of users to find and disseminate information (Martzoukou 2005). As the web moved from its original static and passive version of web 1.0 to the current dynamic and active version of web 2.0 it allowed the user to don a more active role in the whole web ecosystem. This made the study of the user behavior on the web extremely important to gain a richer understanding of the real utilization of the web as an information source.

Information science has evolved into forming strong associations with the fields of information systems, computer science & human computer interaction with design and development of information systems as its core concepts (Keshavarz 2008). This field that deals with human information seeking behavior has been used provide insights into user behavior on the web. The origin of this field is usually attributed to the Royal Society Scientific Information Conference in 1948 that was held due to the post World War II increase in the amount of scientific literature that wasn't published until then due to war time restrictions (Wilson 2000). Although initially the field had a focus on a 'system centric' approach addressing issues related to functionalities of information retrieval systems the focus shifted towards a 'person centered' approach since the early mid-1970s. This allowed other disciplines like psychology and sociology to inform concerns related to information processing and cognition (Wilson 2000). Several researchers like Wilson, Dervin, Ellis, and Kuhlthau were responsible for this change by publishing various human information behavior models during the mid-1980s.

While organizational information seeking was the focus in this field, Savolainen in 1995 developed the Everyday Life Information Seeking model (ELIS) that focuses on a variety of domains in which information seeking occurs in our day-to-day lives (Savolainen 1995). The ELIS model provided a holistic framework to understand source preferences and use patterns of individuals' selection and application of the same to solve problems or to make sense of their everyday world issues. The value of ELIS over the previous models lies in the difference that as the other models try to explain the behavior of information seeking that starts with an uncertainty or knowledge gap the ELIS model starts with a sense of coherence and hence provides a holistic explanation of the phenomenon (Rieh 2004). Pamela McKenzie (2003) in her study of information practices of 19 Canadian pregnant women with twins, used the ELIS framework to develop a two-dimensional model that describes the following four modes of information practices.

The examples used to explain the four modes below are hypothetical but fit the descriptions given in the McKenzie model.

- **Active seeking**: In which users actively seek for information based on a pre-existing need (a goal) and perform a systematic search. Ex: Going into a book store to find a specific book.
- **Active scanning**: In which the users have identified a particular source as a place they are likely to find useful information. They do not specifically have a particular goal in mind while looking at these sources. Ex: Going into a book store without any specific book or title in mind.
- **Non-directed monitoring**: In which users serendipitously find information in an unlikely place or while scanning information sources that they use daily. Here, users do not have any goal in mind and their need triggers when they are exposed to information that they had no intention to look for. Ex: Finding a book that you like at a roadside vendor on your way to work etc.,
- **By proxy:** In which users find information through the initiation of another agent. Ex: Learning about a new book or title through a friend.

Based on this model and combining it with our research on different OSE attacks we developed the following two-dimensional typology, see Table 2 below, and submitted our analysis as a paper to PACIS 2012 conference. As can be seen one of the dimension is a list of current attack vectors that can be categorized as OSE attacks while the other dimension is the different information seeking modes from the McKenzie model of information seeking. The grouping was done based on user behavior in each of the three modes and the likelihood of being exposed to the attack vectors. This typology also serves as a conceptual starting point to the empirical stage of the research. The 'By proxy' mode is not used as part of our typology because we are interested in analyzing individual human vulnerability and not the proxy state of it.

2.3 Research questions

The objective of this research is to further our understanding of OSE attacks and the variance in human vulnerability to different attack vectors. Accordingly, the primary research questions for this research are:

1. What are the various OSE attack vectors and how can we present them in an integrated model? - addressed by the two dimensional typology mentioned above

2. How will the different types of information seeking modes affect user judgment in the context of OSE attacks – addressed by an empirical study that we propose to carry out using a lab based experiment.

3. How can we improve the design of current countermeasures to improve the accuracy of OSE attack detection? – Addressed by the same empirical study mentioned above.

	Active seeking	Active scanning	Non-directed monitoring
Phishing		**X**	
Search Engine Poisoning	**X**		
Clickjacking		**X**	
Malvertising			**X**
Malicious downloads	**X**	**X**	
Popups			**X**
Money laundering		**X**	

Table 2 A typology of OSE attack vectors based on Information seeking modes

3 RESEARCH MODEL & EXPERIMENT DESIGN

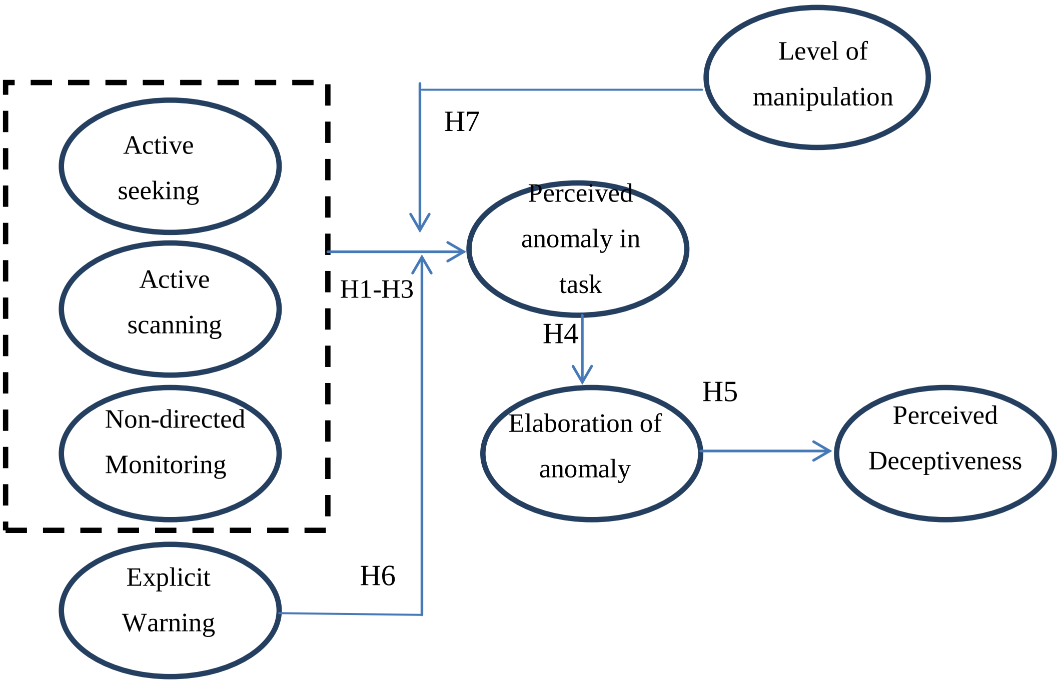

Fig 1 Research model and the proposed working hypotheses.

As illustrated in the research model the three modes of information seeking are hypothesized to have an affect on deception detection capabilities of the user (H1-H3). The deception detection process is layered as a two step process that first allows users to notice anomalies in the given task which is operationalized by the “perceived anamoly in task” construct which then affects the construct “elaboration of anamoly ” which is a measure of how users evaluate and make conclusions about the anomalies that they’ve encountered (H4). The two step deception detection process is inspired by the theory of deception (TOD) (Johnson, Grazioli et al. 1993) which proposes a four step detection process of activation, hypothesis generation, hypothesis evaluation & global assessment when a user is exposed to deception. This theory has a lot of similarities with the mediated cognition and learning model that focuses on the user’s information processing abilities. This model proposes two distinct sub-processes of attention & elaboration when a user is exposed to a stimulus (Eveland, Shah et al. 2003). The attention construct of the mediated cognitions model is similar to the first two steps of theory of deception – activation and hypothesis generation. Elaboration on the other hand is defined as the process through which individuals make connections between cues they observe and their prior knowledge (Perse 1990). This process draws similarities with the later two steps of TOD – hypothesis evaluation & global assessment.

Based on whether or not users notice anomalies and make relevant elaborations regarding these anomalies will directly affect the extent to which they believe in overall deceptiveness of the tasks (H5). We also propose that explicit warning about the manipulations & level of manipulation moderates the effect of deceptive manipulations on users' ability to detect anomalies in task (H6-H7).

3.1 Independent variables & experimental design

The three main independent variables are 1) Information seeking modes, 2) Warning & 3) Level of manipulation. A 3 (Information seeking modes: Active seeking, Active scanning & Non-directed monitoring) x 2 (Warning: with warning, without warning) x 2 (Level of manipulation: high manipulation, low manipulation) between-subject factorial design will be used. The experimental design and the associated treatment groups can be found in Fig 3. below. A MANCOVA analysis will be performed in order to find the differences between the various treatment groups with 'involvement' & 'disposition to trust' as the covariates. In addition a structural equation modeling analysis will be carried out to study in depth the causal relations between the various experimental constructs.

Two experimental websites (one with high manipulation and the other with low manipulation) are being custom designed for this study. Each website has links to three tasks that will allow us to simulate user behaviour in the three modes of information seeking. The three chosen tasks are 1) Search - to simulate the active seeking behaviour, 2) Email - to simulate active scanning & 3) Web portal - to simulate non-directed browsing.

The sample that will be used to test the model will be students from an undergraduate class in the business school of the University of Auckland. The students of the class will be invited to the experiment and will be randomly divided into one of the 12 treatment groups. They will then be given a set of instructions relevant to their treatment groups and asked to perform the tasks. The subjects in the groups with a warning will find explicit warning as part of their instruction manual before they start their task. On the other hand subjects will not know whether they are operating in a low level or high level manipulation environment.

Predictors/Independent vaiables	**Treatment groups**											
	1	2	3	4	5	6	7	8	9	10	11	12
Active seeking	X	X	X	X	X	X	X	X				
Active scanning	X	X	X	X					X	X	X	X
Non-directed monitoring					X	X	X	X	X	X	X	X
With warning	X		X		X		X		X		X	
Without warning		X		X		X		X		X		X
High manipulation	X	X			X	X			X	X		
Low manipulation			X	X			X	X			X	X

Table 3 3x2x2 Full factorial experimental design.

This will then be followed up with a questionnaire to capture measures (dependent variables in Table 4) of their perceived performance. Before they perform tasks everyone will be asked to fill a pre experiment questionnaire that will capture basic demographic and control measures.

3.2 Manipulations used to induce deception

Four categories of manipulations are used either in isolation or in combination across the three experimental tasks. These manipulations were adapted from a study that was focused on phishing but the nature of these manipulations could extend to other contexts too (Jakobsson 2007).

- Manipulations on spelling & grammar – Ex: spelling and grammar mistakes induced into the snippets of artificially generated search engine results, rss feeds & content of emails.
- Manipulations on URLs – Ex: Using url shortners to obfuscate the real destination url.
- Manipulation on relevance – Ex: Anchor text of a url would look relevant to your search query but on mouse over would reveal a different destination url (url redirection).
- Manipulation through personalization – Ex: The sender of the email is someone that the user would trust because of a personal association.

3.3 Dependent &Control variables

The following table gives an overview of the dependent and control variables that will be used in our research model. All measurement items for the principal constructs in this study have been adopted from existing measures to enhance validity concerns.

Construct	**Adapted from**
Dependent variables	
Perceived anomaly in task	Bo Xiao, 2010
Elaboration	Eveland et al. (2003)
Perceived deceptiveness	Grazioli & Jarvenpaa (2000)
Control variables	
Disposition to trust	Mcknight et al. (2002)
Involvement	Zaichkowsky 1985

Table 4 Dependent & Control variables and sources from which they are adapted.

4 EXPECTED CONTRIBUTIONS

We expect the results of this thesis will have both theoretical and practical contributions and will be of great interest to academic researchers, practitioners, consumer protection agencies and government regulatory authorities.

The typology can be readily used as educational material to improve end user awareness about different types of OSE attack vectors. From a practitioner standpoint, there is an urgent need to start integrating information about these new vectors into current security programs to help spread the awareness, especially among the home based internet users. A recent paper that studied the adequacy of security policies for online banking reiterates the point discussed earlier that there is significant focus on educating users about phishing while lacking significantly on creating awareness about other vectors (Ivaturi and Janczewski 2011).

The results of the our empirical study can inform current information systems security design standards and eventually lead to implementing appropriate design mechanisms that would help in mitigating the consequences or at least lower the rate of being victimized.

5 REFERENCES

A. Tsow and M. Jakobbson (2007). "Deceit and design: a large user study of phishing." Indiana University.

Chen, R., J. Wang, et al. (2011). "An investigation of email processing from a risky decision making perspective." Decision Support Systems **52**(1): 73-81.

Dhamija, R., J. D. Tygar, et al. (2006). Why phishing works. Proceedings of the SIGCHI conference on Human Factors in computing systems. Montreal, Qubec, Canada, ACM**:** 581-590.

Downs, J. S., M. B. Holbrook, et al. (2006). Decision strategies and susceptibility to phishing. Proceedings of the second symposium on Usable privacy and security. Pittsburgh, Pennsylvania, ACM**:** 79-90.

Eveland, W. P., D. V. Shah, et al. (2003). "Assessing Causality in the Cognitive Mediation Model." Communication Research **30**(4): 359-386.

Grazioli, S. (2004). "Where Did They Go Wrong? An Analysis of the Failure of Knowledgeable Internet Consumers to Detect Deception Over the Internet." Group Decision and Negotiation **13**(2): 149-172.

Grazioli, S. and S. L. Jarvenpaa (2000). "Perils of Internet fraud: an empirical investigation of deception and trust with experienced Internet consumers." Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on **30**(4): 395-410.

Ivaturi, K. and L. Janczewski (2011). A cross geographic content analysis of social engineering security policies for online banking. International conference on Informations technology, Systems & Management, IIM Kozikhode.

Ivaturi, K. and L. Janczewski (2011). A Taxonomy for Social Engineering attacks. CONF-IRM 2011 PROCEEDINGS.

Jagatic, T. N., N. A. Johnson, et al. (2007). "Social phishing." Commun. ACM **50**(10): 94-100.

Jakobsson, M. (2007). The Human Factor in Phishing. Privacy & Security of Consumer Information '07. School of Informatics; Indiana University at Bloomington.

Jakobsson, M., A. Tsow, et al. (2007). What instills trust? a qualitative study of phishing. Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security. Scarborough, Trinidad and Tobago, Springer-Verlag**:** 356-361.

Johnson, P. E., S. Grazioli, et al. (1993). "Fraud detection: Intentionality and deception in cognition." Accounting, Organizations and Society **18**(5): 467-488.

Karakasiliotis A, Furnell S.M, et al. (2006). Assessing end-user awareness of social engineering and phishing. Australian Information Warfare and Security Conference, Perth.

Keshavarz, H. (2008). "Human information behaviour and design, development and evaluation of information retrieval systems." Evaluation of information retrieval systems **42**(4).

Laribee., L. (2006). Development of Methodical Social Engineering Taxonomy Project. NAVAL POSTGRADUATE SCHOOL. MONTEREY, CALIFORNIA.

Lindqvist, U. and E. Jonsson (1997). How to systematically classify computer security intrusions. Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on.

Martzoukou, K. (2005). "A review of Web information seeking research: considerations of method and foci of interest." Information Research **10**(2).

McKenzie, P. J. (2003). "A model of information practices in accounts of everyday-life information seeking." Journal of Documentation **59**(1): 19-40.

Merritt, M. (2010). "Norton's Cybercrime Report: The Human Impact."   Retrieved 1/03/2012, 2012, from http://community.norton.com/t5/Ask-Marian/Norton-s-Cybercrime-Report-The-Human-Impact-Reveals-Global/ba-p/282432.

Perse (1990). "AUDIENCE SELECTIVITY AND INVOLVEMENT IN THE NEWER MEDIA ENVIRONMENT " Communication Research **17**(5): 675-697.

Rhodes, K. (2001). "Operations Security Awareness: The Mind has No Firewall." Computer Security Journal **18**(3).

Rieh, S. Y. (2004). "On the Web at home: Information seeking and Web searching in the home environment." Journal of the American Society for Information Science and Technology **55**(8): 743-753.

Savolainen, R. (1995). "Everyday life information seeking: Approaching information seeking in the context of “way of life." Library Information Science Research **17**(3): 259-294.

Townsend, K. (2010). "The art of social engineering." Infosecurity, **7**: 32-35.

Vishwanath, A., T. Herath, et al. (2011). "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model." Decis. Support Syst. **51**(3): 576-586.

Wilson, T. D. (2000). "Human Information Behavior." Informing Science **3**(2).

Workman, M. (2007). "Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security." Journal of the American Society for Information Science and Technology **59**(4): 662-674.