Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2008 Proceedings

Americas Conference on Information Systems (AMCIS)

2008

Unweaving the Phisher's Net: An Exploratory Study

Begona Perez-Mira
Louisiana State University, bperez24@lsu.edu

Unweaving the Phisher's Net: An Exploratory Study

Begoña Pérez-Mira
Louisiana State University
bperez4@lsu.edu

ABSTRACT

Over 29,000 phishing emails are reported each month on average to the AntiPhishing Working Group. If we consider that at least 5% of these emails achieve their target, at least 1,450 distinct email users a month are caught in the phisher's net. This study attempts to understand the basic deception techniques utilized by phishers when creating the phishing emails. Exploratory content and linguistic analyses are performed to elicit the most widely used deception techniques and linguistic features that seem to be prominent in phishing emails. Preliminary results provide evidence to support that phishers utilize a very reduced and recognizable subset of deception techniques. Moreover, paired with these deception techniques, specific linguistic features seem to create a recognizable pattern of phishing emails that can be used to aid detection and filtering.

Keywords

Phishing, deception theory, linguistic analysis.

INTRODUCTION

It was November 2005, Susan, a mathematician with an acute inclination for gardening checked her email for the tenth time. She was quickly answering her student's questions until one email caught her attention; the sender was "EBay – Customer Support Notification." She had discovered a wonderful nursery in Houston, TX, with a well-constructed eBay Store. The store sold rare plants that had quickly became part of her greenhouse. Today, she was expecting a new shipment. She could not wait to open the package and add the new additions to her already award-winning garden. So that email caught her attention with the subject line: "IMPORTANT: Update your eBay information to secure prompt shipment." Susan rapidly opened the email and scanned the contents. There had been an issue with the shipping of her plants; the email referenced a store order number, and it requested a shipment information update. Susan clicked on the provided link, updated her account information, and submitted the form. After taking care of the shipping problem, she went back to her daily grading and emailing routine. A day later, she received the plants as stated in the eBay description. She also received a call from her bank. Her account was overdrawn; a couple of important checks were going to be denied payment. She quickly checked her online bank account, and she realized that charges for more than $1500 had been made with her bank card from a point sale in Poland. The money was gone, and she was in despair. She had been a victim of identity theft, and she did not know how it had happened.

Susan was a victim of identity theft through phishing. According to the AntiPhishing Working Group website (http://www.antiphishing.org), Phishing uses social-engineering and technical subterfuges to steal consumers' identity data and personal financial credentials. The first mention of a the term "phishing" appeared more than 10 years ago[1], and this is a crime that according to the Anti-Phishing Working Group and the Binational Working Group (2006) does not seem to be slowing down. The number of reported phishing attempts reported to the APWG grew from 25,624 in August 2007 to over 38,500 in September 2007[2]. In just a year, the number increased by over 13,000. Moreover, according to the same group, 5% of all the phishing attempts are successful; the number of estimated individual losses from these successful phishing attempts already reaches over a billion dollars. But phishing does not only attack individuals. It also undermines the hijacked companies by reducing individual trust in email communication. Phishing is a real threat, and it is not going away any time soon.

[1] phish, v." OED Online, March 2006, Oxford University Press.. *Oxford English Dictionary Online*.

[2] The Anti-phishing Working Group (http://www.antiphishing.org/)

There have been some attempts to fight phishing. Software companies that specialize in anti-phishing code have developed different tools to attempt to fight phishing emails. Some of the most popular tools are anti-phishing toolbars adopted by the latest Internet browsers (i.e. Internet Explorer); however, a study conducted by the CyLab found that out of the 10 toolbars they examined, even the best ones still failed to identify more than 15% of phishing emails (Lorrie, 2006). This is still a large number, as a 5% success rate in that 15% rate of failure could easily account for millions of dollars in losses. Even with the efforts of software companies, hardware companies, and the government, phishing attacks are on the rise. Perhaps then, we need to better understand phishing at the level of the basic building blocks. We should ask these questions: Why is phishing so powerful? Why, if we know what it is and how it works, can we not seem to be able to fight it properly? And what elements of those phishing emails are so powerful that even an educated and knowledgeable person can be fooled by them?

This study is an attempt to partially answer some of these questions. To understand the basic deceptive techniques of phishing emails, actual phishing emails were analyzed in terms of deceptive techniques and also in terms of linguistic features. This paper presents the results of this preliminary study and suggestions for further research.

LITERATURE REVIEW

Deception Theory

The fields of accounting and finance have a rich history of fraud research. In these studies, fraud is analyzed as a game of deception in which the deceiver introduces a false representation of reality to the target and the target is expected then to take the deceiver's expected action (Buller, Strzyzewski, and Comstock, 1991). In the case of accounting, for example, the deceiver creates fictitious transactions to deceive auditors so that auditors may identify them as authentic and accept them. There have been many studies utilizing deception theory[3], but a particular study by Johnson et al. (1993) is of special interest. The researchers adopt Whaley and Bell's deception taxonomy (1991) to describe a set of deception strategies or tactics. Dissimulative strategies attempt to hide reality, and simulative strategies attempt to show the false as real. Based on dissimulative strategies, the authors propose seven distinct deception tactics: *masking, double lay, mimicking, dazzling, inventing, repackaging,* and *decoying*. These seven deception tactics are used by the deceiver with two main goals in mind: (1) to convince the target that the deception is authentic (incorrect representation of reality); (2) to hide the fact that the deception is false (correct representation of reality). The following table summarizes the deception tactics and their definitions (Johnson, Karim Jamal, 1993).

Deception	Definition
Masking	Deleting elements in the representation that would suggest the correct representation (i.e. deleting an item that would convince the user that the email is a fraud)
Double Play	Manipulating attributes in the environment in a way so as to weakly suggest the correct representation. (i.e. referencing the environment of the item such as a shipping, a payment, or a previous purchase)
Mimicking	Modifying attributes in the environment in a way so as to suggest the incorrect representation (i.e. adding well known organization logos to the email)
Dazzling	Modifying the environment in such a way as to obscure or blur these attributes whose interpretation suggests the correct representation, and to emphasize these attributes whose representation suggests the incorrect one. (i.e. hiding the real URL under a typed up fake one)
Inventing	Adding new attributes to the environment in order to suggest the incorrect representation
Repackaging	Modifying attributes in the environment in order to hinder the generation of the correct representation

[3] See Vrij 2003 for an up to date review of deception theory studies.

Decoying	Adds new attributes to the environment in order to hinder the representation of the correct representation.

Table 1 - Deception tactics (Johnson et al 1993).

This taxonomy has been used to explain deception in fields outside of accounting, as well. Biros, George, and Zmud (2002) utilize this taxonomy to create deceptive data to analyze sensitivity to deception in order to improve decision-making performance. In the marketing field, Burke, DeSarbo, Oliver, and Robertson (1988) analyze the deceptive effects of advertising claims in a set of computer-constructed ads for fake pain reliever medication. In this study, the different levels of deception tactics proposed by Johnson and Grazioli are used to create the deceptive ads presented to the participants. Kauffman and Wood (2000) utilized deception theory to analyze opportunistic behavior in online auction marketplaces. Grazioli and Jarvenpaa published three articles that applied deception theory to Internet fraud. In their first article, "Perils of Internet Fraud," the authors utilized the deception tactics specified by Johnson et al. to create different variations of a fraudulent e-commerce website in an attempt to measure the relationship between deception and trust and the level of perceived risk. In their study, most of their subjects failed to detect the deception tactics utilized in the experiment. Their study showed that by using deceptive tactics the fraudulent sites not only avoided detection but also increased trust (Grazioli, 2000). Their second article, "Consumer and Business Deception on the Internet," was similarly based on the deceptive techniques stated by Johnson et al., but this study added a new layer of understanding to the tactics, analyzing which ones were more likely to be used by the deceiver in the case of a consumer deception or a business deception. Their results suggested that deceivers do select tactics according to targets and their own purported identities (Grazioli, 2003). Finally, the third article looks at Internet deception as a whole to specifically identify what types of deception techniques are the most widely used by deceivers. They analyzed a total of 201 cases collected from magazines, newspaper articles, and court proceedings that occurred between 1995 and 2000. Their study shows that the "inventing" deception tactic (making up the information about the "core"—i.e. electronic auction sellers who simply do not have the promised merchandise to sell) is the most widely used deception tactic in Internet fraud.

Even though Grazioli's 2003 paper analyzed deception techniques widely used by deceivers, the study did not center on phishing attempts. Instead, the data collected is extremely varied, and the study does not reflect any consideration of different group comparison. Generalizations about Internet fraud as a subject are very difficult to make. Hence, it is important to study a specific attempt type and try to understand the mechanics of the deception techniques used in that specific type. For example, in the fight against phishing, it is important to know and categorize what elements inside these phishing emails are most often used by phishers to deceive and influence the target to behave in the desired way. The generalizations stated by Grazioli's 2003 study are not detailed enough to portray this type of detailed information.

Phishing Research

Phishing is still a very young subject. A direct "phishing" library keyword search yields only 12 results: 5 of those are government documents that explain the fraud and give advice to avoid it; 5 refer back to generic Internet fraud; and, only 2 results are specific for phishing fraud (Lance, 2005; Jakobson, 2007). A directed search of the Lexis-Nexis database provides more than 100 articles that contain the word "phishing." Just a few of these articles contain discussions of specific tactics or items used by deceivers in phishing emails. For the most part, the articles focus more on generic ways to describe a sample phishing email, how to avoid being phished, the actual coding procedures, or their distribution and reach (Jagatic, Johnson, Jakobsson, and Menczer, 2007). Not many articles, only 17 of the ones retrieved, discuss the actual deceptive tactics that phisher uses when creating the phishing emails. A result of the most-cited tactics and techniques and how they are categorized in deception theory are summarized in the tables below.

Technique	Deception Tactic
Using IP addresses instead of domain names in hyperlinks that address the fake website (Alliance 2005)	Dazzling
Embedding hyperlinks from the real target web site into the HTML contents about the fake phishing website (Alliance 2005) (Drake et al. 2004)	Decoying

Encoding or obfuscating the fake web site URL(Alliance 2005) (Drake et al. 2004)	Dazzling
Registering similar sounding DNS domains (Alliance 2005)	Dazzling
Using a pop-up window over the real website (Emm 2006)	Decoying
Using well known logos, lettering, and format (Thompson 2006) (Lynch 2005) (Drake et al. 2004)	Mimicking
Grammatical / Spelling Errors (Knight 2005)	(-Mimicking)

Table 2 - Email Formatting Techniques

Technique	Deception Tactic
Asking for account verification (Thompson 2006) (Drake et al. 2004)	Inventing
Threats of account closure (Lynch 2005) (Drake et al. 2004)	Inventing

Table 3 - Email Content Techniques

It is interesting to note that "Grammatical/Spelling Errors" functions as a negative deception technique (-Mimicking) that works to help elicit the deceitfulness core of the phishing attempt. Some of the articles surveyed presented this characteristic as a well-known technique used to spot phishing emails (Knight, 2005) and (APWG, 2006).

Linguistic Features

Burgoon's et al. article "Detecting Deception through Lingustic Analysis" (2003) provides a different perspective on the fight against deception. The article presents results from preliminary tests where linguistic features are utilized to assess the deceptiveness or truthfulness of a piece of pre-fabricated text. The authors utilize four different types of linguistic indicators in their textual fabrications: Quantity (number of syllables, words, and sentences), Vocabulary Complexity (number of "big" words, number of syllables per word), Grammatical Complexity (number of short sentences, long sentences, average number of words per sentence), and Specificity and Expressiveness (emotiveness index, rate of adjectives and adverbs, and number of affective terms). Results from the experiment posit that the indicators are helpful when distinguishing the deceiving utterances from the truthful ones. According to the study, "the deceivers had significantly fewer long sentences, fewer average syllables-per-word, and a lower sentence complexity than truth tellers" (Burgoon et al. 2003). Extending the results of their study, we might consider that since phishing emails are deceiving pieces of text, it seems possible that the same linguistic features may be clues that help distinguish phishing emails from authentic ones. If these indicators proved significant for phishing emails when compared with other written texts, the linguistic analysis could give us another level of understanding of the deceiving creations.

In the fight against phishing, it is important to know and categorize what elements inside these phishing emails are most often used by phishers to deceive the target and what techniques are most often used by these deceivers to influence the targets to behave in the desired way (basically, click the link and give the information out). The generalizations stated by Grazioli's 2003 study are not detailed enough to portray this type of detailed information and the studies discussed above are just pieces of the overall phishing realm. It is necessary to have a systematic approach to the research and analysis of phishing emails. As such, we need to understand and know (1) what deception tactics are most widely used by phishers and (2) how are phishing emails different to "normal" emails. If we understand these features a bit better, maybe we will have a better position in spotting the phishing emails, filtering them out, and ultimately reducing the amount of phishing emails that are received by the user.

RESEARCH METHOD

Sample Selection

The data (phishing emails) were collected from 3 different sources: (1) the Anti-Phishing Group (http://www.antiphishing.org/), (2) the European counterpart, MillersMiles.co.uk (http://www.millersmiles.co.uk/), and (3) the researcher's personal collection of phishing emails. The first two sources (website archives) contain the images only (not the actual text files) of phishing emails that had been reported starting as early as the 5th of March 2003.

For the first exploratory analysis (deceptive features), 25 phishing emails were selected. The phishing emails were collected from the phishing archives kept by the MillersMiles and the Antiphising Group website. At the time of this paper, the archival websites contained more than 378,079 examples of phishing scams. The emails were randomly selected from a pool of 100 (a list of 25 random numbers were generated using Excel, and the selection was transposed to the 100 pool of phishing emails provided by the archive). The 25 unique phishing emails were analyzed for accuracy and relevance.

For the second exploratory analysis (linguistic features), 25 unique phishing emails were randomly selected from the researcher's collection of phishing emails following the same random procedure[4].

Data and Analysis Methods

A content analysis was conducted on the first data set (images of phishing emails collected from the archival websites). Two coders simultaneously coded the images following the deception theory techniques proposed by Johnson et al. (1993) as top level codes: *Mimicking (positive and negative), Dazzling, Decoying, Masking, Inventing, Relabeling, and Double Play* . The intent of the analysis was twofold: (1) to elicit more instances and examples of deceitful elements from the sample selected and (2) to determine which of the deceptive techniques were used more frequently by the phishers at the time the sample was retrieved.

The second dataset was examined using linguistic analysis. The analysis was conducted using Oxford WordSmith Tools 4. The phishing emails were analyzed as a single text to account for textual features such as word frequency, sentence length, and word count. The emails were also compared against a well-established corpus of one million words in American Written English (the FROWN Corpus) to elicit any possible differences between mainframe American Written English and the phishing emails. All emails were saved as text files (no markup language was analyzed, just basic text) and imported into the program for analysis.

RESULTS

Deception Techniques

In all the emails analyzed, the main goal of the deceiver was to convince the target to click on the provided link. The core of the deception was the narrative used by the deceiver to convince the user to click the deceiving link. To do so, the deceiver could use one or more of the seven deception techniques outlined by Johnson et al. (1993). The content analysis supported the list of phishing techniques revealed by the phishing articles in non-academic publications (see Table 2). There were many instances of *Mimicking* as described by Thompson (2006) and Lynch (2005), such as the use of logos, lettering, and structures from the real websites, and *Dazzling* as described by Alliance (2005), including hiding the real URL under a text link, a fake URL, or an image. Basically, the analysis showed that out of the seven techniques, *Dazzling*, *Decoying*, *Mimicking*, and *Inventing* were those most used in phishing emails. *Masking* (eliminating crucial characteristics of the core) and *Relabeling* were not used at all in the sample of phishing emails selected. *Double play* (the core is exchanged against the deceiver's will) was linked to emails that contained somebody else's information in them (such as the wrong email or the wrong account number). *Inventing* was present in all emails because the core was essentially "invented" by the deceiver. When the inventing techniques were sub-categorized at a lower level, three main topics arose: 1) inventing an account verification/update with threat of account closure or suspension, 2) account verification/update without any mention of a threat of closure or suspension, and 3) a seemingly innocent help issue. Instances of *Decoying* appeared in the majority of the phishing emails (use of real areas of the website, use of real phone numbers, and use of web addresses to increase perceived security). Table 4 provides a detailed summary of the deception techniques and their instances:

[4] At the time of the data collection, the author's personal collection of phishing emails contained more than 250 specimens.

Deception Technique	Phishing email instance
Dazzling	Hiding the real URL under a fake URL. Hiding the real URL under a hyperlinked background image. Hiding the real URL under a text link.
Decoying	Use of "Email ID" to make it more trustworthy Use of "do not reply". Use of the Identity theft threat. The email provides personal information such as case id number Use of real areas of the real website. All the links except the required ones are valid links from the real website. Piggy back on a real issue that took place: power failure. Use of real phone numbers. Using safe market place tips, links to report spoofing Use of https in the URL. Use of Email notification ID.
Mimicking	Use of financial institution logo. use of a high ranking employee name to make the email sound more official Use of logos, lettering, and structure for a pay-pal payment confirmation.
Inventing	New account info added, confirm/verify/authorize your account. Need for the phone number to ask for account verification. Account issues. Verify your information Question about a non completed transaction on eBay. Need your help. Complete the survey for a $20 credit to your account. Update your personal records for security purposes. Confirm payment. Help us re-gain the data. Unauthorized access from a third party. Please, check your records. EBay unpaid item dispute. Email added to the account, please verify. Add a debit card to your account to reduce fraud. Unusual transaction in the account. Limited access until confirmation. Multiple computers logged in, multiple logon failures. Account suspended. Account ready to expire. Question about a selling item on eBay. Upgrade in security measures, verify your account.
Double Play	The item sent out has a different user name. It may be used to confuse the user and to convince him/her that the account has been breached. The email does not have a username attached to it. It may be used to confuse the user and to convince him/her that the account has been breached.

Table 4 - Deception Techniques.

LINGUISTIC ANALYSIS

The basic linguistic analysis showed some interesting results, as well. Oxford WordSmith 4 provided detailed information about word count, sentence length, and word frequency for the twenty-five analyzed phishing emails. According to the results, the emails ranged from 79 distinct words to 157 distinct words. The number of sentences ranged from 8 to 12, and the content words that appeared more frequently in the five emails were "eBay," "account," and "PayPal." Two non-content words that appeared very frequently in the five emails were "your" and "you," the second-person pronouns. When

compared with the FROWN Corpus of Written American Words, the results showed that words that occur with unusually high frequency in these phishing emails that do not occur as frequently in the reference corpus were "EBay," "PayPal," "Account," "update," and "your." While "EBay" and "PayPal" may not be of interest in this comparison, (they may not appear in the Frown Corpus due to its date) the high frequency of "account", "update", and "your" is significant for our study because these words do appear in the corpus. At the other end of the spectrum, words that do not occur in the analyzed phishing emails at an unusual rate in comparison with the reference corpus were "the" and "a," two of the three English articles.

DISCUSSION

The results from both analyses help to understand the different elements that make up a phishing email. It is very interesting to see how the different deception techniques are methodically applied to the deception attempts. Apart from the obvious techniques of *mimicking* (logos, lettering, structure) and *decoying* (hiding the real URL under an image, text, or a fake URL), the most impressive results are given by the subtle use of *double play* in phishing emails with widely recognized brands such as eBay and PayPal. Due to the large number of users and the fact that these are Internet-based companies, the possibility of reaching a target with an existing eBay or PayPal account is likely to be very high. It would be very easy for an email user to disregard a phishing email from a company with whom the user does not have an existing relationship. The problem usually arises when the user actually has an existing relationship with the hijacked bank or company. In those cases, the mere suspicion of an account breech may convince the target to click the link and meet the deceivers' goal. It seems to me that the *mimicking* and *decoying* techniques would be easier to detect than these *double play* techniques.

Another interesting issue that is elicited by the analysis is the fact that the inventing techniques used are extremely limited. All emails included in the sample can be placed in one of the three categories: 1) inventing an account verification/update with threat of account closure or suspension, 2) account verification/update without any mention of a threat of closure or suspension, and 3) a seemingly innocent help issue. The linguistic analysis also supports this finding by showing the words "Account," "records," and "please" as some of the content words highest in frequency in all twenty-five phishing emails.

The same linguistic analysis provokes an interesting insight into the rhetoric of the phishing emails. The frequent use of the second-person pronouns "you" and "your" indicates an attempt towards a personalization of the phishing email. The deceiver, because the real name of the target is unknown, utilizes the pronouns to identify the target and create a sense of familiarity and closeness, which seems to increase trust. The fact that the phishing emails contain the words "the" and "a" less frequently than normal, also supports this idea. The articles "the" and "a" are more generic and impersonal; hence, they appear less frequently in the phishers' emails.

CONCLUSION, LIMITATIONS, AND FURTHER STUDIES

This preliminary study has attempted to shed some light on the understanding of the mechanics and internal techniques of phishing emails. However, this is not nearly enough. The sample was extremely limited (as this was an exploratory study) and hence, the conclusions are not sufficiently supported to be made general. Further studies should build upon the results of this study. With the information gathered in this study, a corpus of phishing examples and instances that match the deception techniques and are generic across the board could be created. These techniques and examples could then be used in a follow-up study to analyze how these techniques really affect the targets. As an example, this follow-up study could be conducted in two different ways:

1) Examples of real phishing emails containing different deception techniques could be presented to real users in a semi-structured interview setting. The researcher could then ask questions about how real/deceptive the email is perceived to be, and what elements of the email seem to be more or less real/deceptive?

2) The researchers could conduct controlled experiments where only one type of phishing email with different variations of deceptive techniques is presented to the participants at a time. Participants then could rate the deceptiveness level of each individual instance.

An even more ambitious study could be performed by incorporating the constructs and relationships from Buller and Burgoon's "Interpersonal Deception Theory." This theory focuses on the context and environment of the communication exchange, the familiarity between the sender and both the deceptive message and the deceiver, and, of course, on the tactics and techniques utilized by the deceiver to live up to the message expectations (Buller and Burgoon, 1996). Adding the Interpersonal Deception Theory to the study could give the researchers a more complete model of phishing communication.

With a complete model of phishing communication exchanges created, more efficient and effective detection techniques could be developed to help stop the proliferation of successful phishing attempts.

Another important limitation of the study is the fact that the corpus utilized to make the frequency comparisons may lack some of the more technologically advanced texts. For this reason, a study that utilizes the BYU Corpus of American English (updated yearly since 1990) will improve the analysis and offer more insight in the similarities and differences between regular text, regular emails, and phishing emails.

In conclusion, even though some generalizations can be drawn from this preliminary study, there is still a lot to be learned from both the structure of the phishing emails and the communication exchange that takes place in a deceptive situation. More research is needed to better understand these two important issues and hopefully unweave the phisher's net.

REFERENCES

1. Alliance, T. H. P. R. (2005). Know your Enemy: Phishing - Behind the scenes of Phishing Attacks. [Electronic Version]. Retrieved 10/12/2006 from http://www.honeynet.org/papers/phishing/.
2. APWG. (2006). Anti-Phishing Working Group. Consumer Advice: How to Avoid Phishing Scams. Retrieved 12/3/06, 2006, from http://www.antiphishing.org/consumer_recs.html
3. Buller, D. B. and Burgoon, J. K. (1994). Deception: Strategic and nonstrategic communication. In J. A. Daly and J. M. Wiemann (eds.), Strategic interpersonal communication (pp. 191-223). Hillsdale, NJ: Erlbaum.
4. Buller, D. B. and Burgoon, J. K. (1996). Interpersonal deception theory. *Communication Theory,* 6(3), 203-242.
5. Buller, D. B., Strzyzewski, K. D. and Comstock, J. (1991). Interpersonal deception: I. Deceivers' reactions to receivers' suspicions and probing. *Communications Monographs*, 58, 1-24.
6. Biros, D. P, J. F. George., Robert W. Zmud. (2002). Inducing Sensitivity to Deception in Order to Improve Decision Making Performance: A Field Study. *MIS Quarterly, 26*(2), 119-144.
7. Drake, C. E., Oliver, J.J., and Koontz, E. J. (2004). Anatomy of a Phishing Email. *First Conference on Email and Anti-Spam (CEAS)*, Mountain View, CA, USA. . [Electronic Version]. Retrieved from http://www.ceas.cc/papers-2004/114.pdf on April 24th 2008.
8. Emm, D. (2006). Phishing update and how to avoid getting hooked. *Network Security,* 13-15.
9. Grazioli, Stefano, S. L. J. (2000). Perils of Internet Fraud: An Empirical Investigation of Deception and Trust with Experienced Internet Consumers. *IEEE Transactions on Systems, Man, and Cybernetics. Part A: Systems and Humans. , 30*(4), 395-410.
10. Grazioli, Stefano. L. J. (2003). Consumer and Business Deception on the Internet: Content Analysis of Documentary Evidence. *International Journal of Electronic Commerce, 7*(4), 93-118.
11. Hulme, G. (2005). Lack of trust hampering online direct marketing. *B to B, 90*(12), 4-45.
12. Jagatic, Tom N., Johnson, Nathaniel, A., Jakobsson, Markus; Menczer, Filippo.(2007) *Communications of the ACM*, *50*(10), 94-100.
13. Jakobson, Markus & Steven Myers. (2007) Phishing and countermeasures: understanding the increasing problem of electronic identity theft. Hoboken, N.J. : Wiley-Interscience.
14. Johnson Paul E., S. G., Karim Jamal. (1993). Fraud Detection: Intentionality and Deception in Cognition. *Accounting, Organizations and Society, 18*(5), 467-488.
15. Judee K. Burgoon, J. P. B., Tiantian Qin, and Jay F. Nunamaker, Jr. . (2003). Detecting Deception through Linguistic Analysis. *Lecture Notes in Computer Science*(2665), 91-101.
16. Knight, W. (2005). Caught in the Net. *IEE Review*(July), 26-30.
17. Lance, James. Phishing exposed. Rockland, MA ; Syngress, 2005.
18. Lorrie Cranor, S. E., Yason Hong, and Yue Zhang. (2006). Phinding Phis - An Evaluation of Anti-Phishing Toolbars. *CyLab - Carnegie Mellon University*. [Electronic Version]. Retrieved 12/3/06, 2006, from http://www.cylab.cmu.edu/files/cmucylab06018.pdf
19. Lynch, J. (2005). Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks. *Berkeley Technology Law Journal, 20*, 259-300.

20. *Report on Phishing: A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States.* (2006).).
21. Robert J. Kauffman, C. A. W. (2000). *Running up the bid: Modeling seller opportunism in Internet auctions.* . Paper presented at the Proceedings of the 2000 Americas Conference on Information Systems, Atlanta.
22. Stone, A. (2004). Tangled in the Phishing Lines [Electronic Version]. *Business Week Online*, 6/22/2004 - Special Report - High Tech Marketing. [Electronic Version]. Retrieved 12/6/2006 from http://www.businessweek.com/technology/content/jun2004/tc20040622_9153_tc150.htm?chan=search.
23. Thompson, S. C. (2006). Phight Phraud - Steps to protect against phishing. *Journal of Accountancy*(February), 43-44.
24. Vrij, A. (2000). *Telling Lies and Detecting Deceit. The Psychology of Lying and the Implications for Professional Practice.* . Chichester, UK: Wiley.
25. Wahl, A. (2004). Gone phishin'. *Canadian Business, 77*(12), 13-13.