2011

Trends in Phishing Attacks: Suggestions for Future Research

Ryan M. Schuetzler
University of Nebraska at Omaha, ryan.schuetzler@byu.edu

Trends in Phishing Attacks: Suggestions for Future Research

Research in Progress

Jeffrey Gainer Proudfoot
University of Arizona
jproudfoot@cmi.arizona.edu

Justin Scott Giboney
University of Arizona
jgiboney@cmi.arizona.edu

Ryan M. Schuetzler
University of Arizona
rschuetzler@cmi.arizona.edu

Alexandra Durcikova
University of Arizona
alex@eller.arizona.edu

ABSTRACT

One of the most common and costly forms of deception and fraud online is phishing. Due to the ramifications of successful phishing attacks, security experts and researchers seek to better understand this phenomenon. Prior phishing research has addressed the "bait" and "hook" components of phishing attacks, the human-computer interaction that takes place as users judge the veracity of phishing emails and websites, and the development of technologies that can aid users in identifying and rejecting these attacks. Despite the extant research on this topic, phishing attacks continue to be successful as tactics evolve, rendering existing research less relevant. Although numerous tools have been created to aid people in recognizing phishing attacks, users disregard the recommendations of these tools. This paper summarizes the core of phishing research, provides an update on trending attack methods, and proposes future research addressing computer credibility in a phishing context.

Trends in Phishing Attacks: Suggestions for Future Research

Research in Progress

ABSTRACT

Deception in computer-mediated communication is a widespread phenomenon. Cyber criminals are exploiting technological mediums to communicate with potential targets as these channels reduce both the deception cues and the risk of detection itself. A prevalent deception-based attack in computer-mediated communication is phishing. Prior phishing research has addressed the "bait" and "hook" components of phishing attacks, the human-computer interaction that takes place as users judge the veracity of phishing emails and websites, and the development of technologies that can aid users in identifying and rejecting these attacks. Despite the extant research on this topic, phishing attacks continue to be successful as tactics evolve rendering existing research less relevant, and users disregard the recommendations of automated phishing tools. This paper summarizes the core of phishing research, provides an update on trending attack methods, and proposes future research addressing computer credibility in a phishing context.

Keywords

Phishing, Security, Fraud, Cybercrime, Linguistic Analysis, Email, Scam, Human-Computer Interaction, Computer Credibility, Expert Systems

INTRODUCTION

One of the most prevalent and costly manifestations of deception in computer-mediated communication is phishing. *Phishing* is "a form of social engineering in which an attacker, also known as a 'phisher', attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion." The Anti-Phishing Working Group reported that the number of unique phishing websites detected in the first quarter of 2010 was just fewer than 100,000, with the number of brands hijacked by phishing campaigns around 800 . Furthermore, the financial losses associated with this form of attack have been estimated to be between $400 million and $2.4 billion dollars . Due to the prevalence of phishing attacks, and their costly ramifications when successful, security experts and researchers seek to better understand this phenomenon.

This attack methodology typically consists of three separate steps: creating a website that is designed to closely resemble a legitimate site, uploading the spoofed site onto a webserver, and sending the attack email in large volumes in an attempt to direct recipients to the spoofed site . Due to the two primary components (the email and the website) needed for a phishing attack, phishing experts also refer to this approach as the bait and hook method . The deceptive email is referred to as the bait as it is used to attract email recipients to the hook. The ability to identify a phishing email prior to visiting the corresponding spoofed website is critical as 90% of users are unable to distinguish the difference between a legitimate website and a fake website . In other words, if a user accepts a phishing email as being truthful, they are unlikely to identify deception in a fictitious website. In total, 5% of targets will become a victim of the attack .

A significant portion of phishing research has addressed the identification and evaluation of various attributes commonly found in attack emails . Furthermore, as reoccurring attributes are identified, automated tools have been developed to aid users in identifying suspicious websites and emails **cite needed**. However, the effectiveness of these tools is questionable for two reasons. First, the tactics utilized by phishers are constantly evolving , rendering the classification criteria for automated tools less accurate over time. Second, the users of automated phishing tools often question the credibility of computer assessments and disregard their recommendations. Consequently, additional research is needed to identify trending attack methods currently utilized by phishers, and a new research stream is necessary to evaluate computer credibility in a phishing context .

This paper has been organized into the following sections. First, literature is reviewed that addresses the behavioral and technical elements of existing phishing research. Second, the methodology for collecting and analyzing a set of 2,700 phishing emails acquired from a Scamdex database is presented, and reoccurring attributes found in those emails are

identified. Third, these attributes are compared with a prior linguistic analysis of phishing emails. Finally, a new stream of phishing research is proposed.

LITERATURE REVIEW

The existing corpus of phishing research can be segmented into three core emphases: (1) identifying the attack methods phishers employ in fraudulent emails and websites (2) understanding human-computer interaction with phishing emails and websites, and (3) the development and implementation of anti-phishing technologies that aid humans in both identifying and avoiding phishing attacks and emails. Relevant papers pertaining to each section are discussed in the following subsections.

Phishing Attack Methods

As identified earlier in this paper, phishing attacks are generally comprised of two components: the attack email (bait) and the corresponding website (hook).

Research Addressing the "Bait"

The most important element of any phishing attack is the email, as recipients will first judge its veracity prior to being directed to the corresponding fraudulent website. Table 1 identifies and classifies various tactics utilized in phishing emails to deceive recipients into proceeding to the corresponding website. These tactics can be classified into technical and or social engineering categories . Within the social engineering category, an email can have generic content (see Table 1) or it can be content aware . A content-aware approach incorporates personalized information scraped from social networking sites thus making the *bait* more credible to the recipient. Adding content-aware features to an email increase the success of phishing emails from 5% to 72% .

Characteristics of Phishing Emails	
Social Engineering Characteristics	**Technical Characteristics**
E-mail Title	Links to Web Sites That Gather Information
Urgency	Link Text in Email Differs from Link Destination
Impact	Using onMouseOver to Hide the Link
Company Name	Using the IP Address
E-mail Argument Quality	Using the @ Symbol to Confuse
General Content	Reply Address Differs From the Claimed Sender
Company's Image	Hiding the Host Information
Links to a Real Company Site	Redirecting the URL
Email Appears to Be From Spoofed Company	Switching Ports
Response Action	
Justification / Creating a Plausible Premise	
Urgency	
Security Promises	
Collecting Information in the Email	
Impact	
Courtesy	
Event	
Penalty	
Typos	
Personalization	

Content-Aware Approach	

Table 1 Components of Phishing Emails

Research Addressing the "Hook"

While the *bait* component of a phishing attack must be carefully crafted in order to deceive recipients, the corresponding *hook* must utilize similar deceptive strategies for the attack to be successful. Well-crafted fraudulent sites have proven to be very effective and fool from 83% to 90% of the individuals that view them . Table 2 identifies and classifies various tactics utilized in phishing websites to build credibility and deceive targets into divulging their personal information. These tactics can be classified into content-related and or technical categories .

Characteristics of Phishing Websites	
Website Content	**Technical Characteristics**
Spoofed Content	SSL Certificates
Spoofed Layout	Browser Discrimination
Forms to Submit Information	Fake Address Bars
Pup-Up Windows	Disabling Right-Click
Information Processing	Visually Deceptive URL
Account Access Restrictions	Images Masking Underlying Text
Images Mimicking Windows	
Windows Masking Underlying Windows	

Table 2 Components of Phishing Websites

Research Addressing Human-Computer Interaction in a Phishing Context

A wide range of individual characteristics has been examined by researchers addressing the interaction between humans and the attack methods phishers employ. The various individual characteristics relevant to phishing research can be classified as either experiential or dispositional. Experiential factors include computer experience, web-purchasing experience, education level, and Internet experience, which have proven to be ineffective in helping phishing targets distinguish between fraudulent and legitimate websites . Additionally, the gender of targets has been found to be insignificant in predicting the ability of targets to detect a phishing attack . Dispositional factors include sensitivity towards the value of information, concern for privacy or security, obedience to instructions or authority, knowledge of institutional factors, and past experience with fraud, all of which have been identified as contributors to the successful detection of deception in phishing emails . An examination of the personality characteristics of deceived phishing targets found that experiential factors, rather than dispositional factors, are most influential in individuals that successfully identify phishing attacks .

Anti-Phishing Technologies

As the variety and complexity of phishing attacks continue to evolve, researchers and security experts continue to develop tools to aid users in the proper identification and avoidance of phishing emails and websites. The methods used to identify suspicious sites range from machine-learning tools able to correctly classify 96% of phishing emails , to browser add-ons that track user activity and present warnings when users are about to divulge personal information on untrusted sites . Examples of other technologies that have been developed to thwart phishing attacks include: dynamic security skins using images to verify that a website is legitimate , content-based tools used to identify phishing websites , password management tools , and so forth.

While there is a significant number of tools that can be utilized to reduce the dangers of phishing, the most important aspect of any technology is whether or not the end user actually uses it. A study addressing the effectiveness of three different security toolbars found that users tend to consider the warnings they present as trivial as long as the website appears to be legitimate . Users rationalized that their own knowledge and experience was sufficient to make the decision, and the security toolbar was wrong in its recommendation. A different study found similar results as 68% of subjects asked to identify

fraudulent websites disregarded warnings while 23% did not even look at security indicators in the web browser . In other words, even technologies that are highly effective at distinguishing the difference between legitimate and fraudulent sites are ineffective when users fail to heed their warnings.

DATA ANALYSIS AND RESULTS

To obtain a corpus of phishing emails, we scraped 2709 emails from Scamdex.com ("Email Scam, Internet Fraud, Identity Theft & Phishing Resource," n.d.). This corpus contained emails over a 3-year period from November 2006 to June 2009. These emails were submitted to Scamdex by recipients of phishing attacks..

Initially, the emails were formatted for text analysis which was accomplished using the R Text Mining package (Hornik, 2008). Next, HTML tags were removed from the emails and punctuation characters and numbers were removed. We then formatted the remaining text as lowercase characters and removed the stop words contained in the Standard English stop word list in R. Finally, we stemmed the remaining words allowing only core words to be analyzed.

We then put the words into a Term Document Matrix using term frequency and inverse document frequency (TF-IDF) and normalized the terms. This gave us a large list of terms occurring at least once in our corpus. Although we are trying to give a detailed picture of current phishing practices, we also need to make sure that we are not reporting non-relevant categories. Thus our next step was to only retain words that had at most a 90% sparsity (i.e. the words were only found less than 10% of the documents were cut). This left us with 115 terms used in the phishing emails.

Our next step was to categorize the 115 terms into sensible categories. A similar categorization was done with emails from 2003 to 2005 . Wang et al. (2009a) ran an analysis on 210 phishing emails collected from the Anti-Phishing Working Group using CATPAC. We solicited the help of three people to categorize the words. The only direction that these people were given was to categorize the words and name the groups. They were not told the context or purpose of the categorization. After obtaining the results, we grouped their categories into similar categories creating eleven categories to represent tactics that phishers are using (see Table 3).

Politeness	Address, Apologize, Concern, Contact, Dear, Email, Feature, Inconvenience, Mail, Matter, Message, Person, Please, Receive, Regards, Replies, Sent, Sincerely, Thank, User
How to do	Click, Choose, Detail, Internet, Link, Log, Login, Online, Page, Prompt, Restore, Review, Site, System, Visit
What to do	Access, Confirm, Locate, Screen, Step, Verify
Story	Account, Additional, Bank, Card, Change, Record, Reserve, Server, Value
Customer Service	Answer, Assist, Attention, Customer, Experience, Help, Request, Service, Support, Understand
Fraud	Commit, Compromise, Failure, Fraud, Fraudulent, Unauthorized
Time	Active, Due, Future, Hour, Initial, Period, Recent, Regular, Soon, Temporarily, Time, Update
Purpose	Agreement, Attempt, Complete, Continue, Ensure, Follow, Maintain, Measure, Process, Provide, Require, Use, Verification
Security	Copyright, Credit, Identity, Issue, Prevent, Protect, Right, Safe, Secure, Sensitive
Impact	Partial, Result, Suspend, Suspension
Notice	Alert, Department, Inform, Limit, Notice, Notify, Reason, Team, Unusual

Table 3 Phishing Tactics

When comparing our results to Wang et al. (2009), we found that there are several overlapping categories, and some new categories. Wang et al. (2009a) identified seven groups which the authors titled as follows: Event, Impact, Justification, Response Action, Penalty, Urgency, and Courtesy. Their Event and Impact categories coincide with our Story category; their Justification to our Purpose; their Response action to our What To Do and How To Do; their Penalty to our Impact; their Urgency to our Time; and their Courtesy to our Politeness. We also identified four new categories: Customer Service, Fraud, Security, and Notice.

Each email was then classified as either containing each tactic, or not. The evidence shows that these tactics are highly found together with Fraud and Impact occurring at a lesser frequency (see Figure 1). This indicates that phishers are not informing their targets of the consequences of their actions. This may be a successful strategy as people typically don't understand the consequences of phishing, and therefore are not telling them of the consequences may result in higher rates of success. It is also interesting to note that there is a trend of decreasing frequencies of each tactic identified. There are two possible reasons for this: 1) another tactic is emerging that is not a major player in our analysis or 2) phishers are starting to narrow the number of tactics used (from a shotgun approach towards a sharpshooter approach).

Figure 1 also shows that Politeness is a fairly consistent tactic employed by Phishers. Politeness started out as the second most popular tactic in 2006 tied with How to Do. By 2009, Politeness was the most popular tactic losing around 10% frequency. Most other categories lost at least 20%.

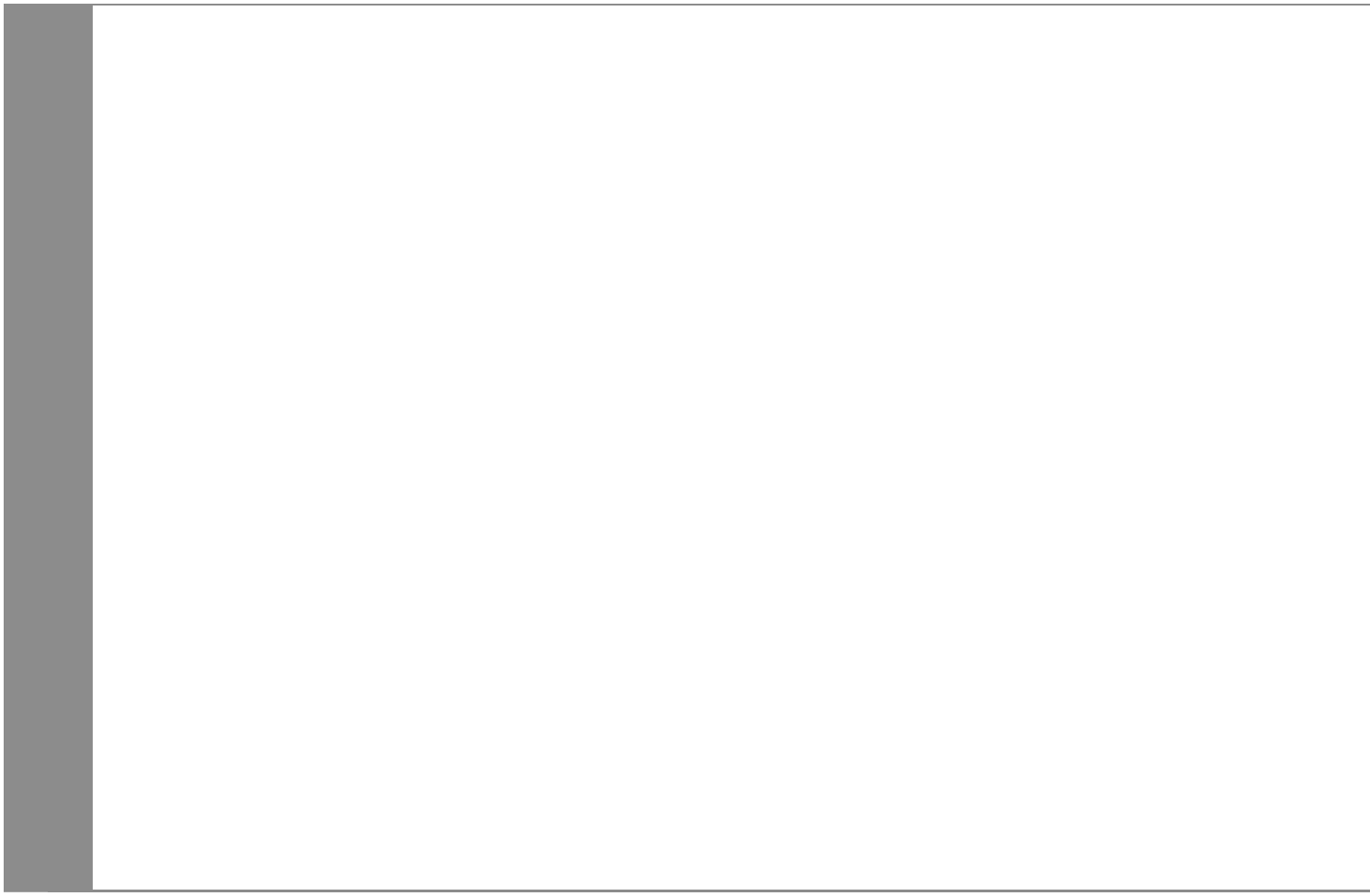

Figure 1 Phishing Tactics Over Time

DISCUSSION

Based on these findings, an important direction for future research will be to identify methods by which anti-phishing technology can be made more credible in the eyes of users. Significant research has addressed the issue of computer credibility . Credibility, or believability, is a perceived quality commonly acknowledged to be composed of at least two primary components: trustworthiness and expertise . When users interact with a website while using a phishing toolbar, the toolbar may provide a recommendation against clicking a link or entering information based on certain cues present on the site. The credibility of the toolbar application is critical in this situation because the system is providing advice. When the computer is giving this type of advice or instruction, the user's assessment of the application's credibility will be a factor in determining if the user follows the advice .

Tseng and Fogg identify four primary types of computer credibility that could be useful in determining the best way to improve the effectiveness of anti-phishing technology. The four types of credibility are presumed, reputed, surface, and experienced. Presumed credibility is a pre-use level of credibility assigned to the technology. Research has been inconclusive about the credibility people assign to computer technology in general, with some studies showing that computers are more credible than humans , and others showing less . Additionally, as people gain more experience with computers, they realize that they are not infallible, and recognize that they are programmed by humans and subject to human-like mistakes . Reputed credibility is based on third party reports. For example, a computer program receiving good reviews from users would likely be perceived as more credible than the same program receiving poor reviews.

The third type of credibility, and perhaps most important to phishing toolbars, is surface credibility. The design of a program's interface can have a significant impact on the credibility and usability . Different aspects of the interface are important for different types of application . For example, privacy was important in building trust in website with high information risk, while navigation was more important for website containing a lot of information to be processed. An important direction for future research will be to determine the most critical components of design for anti-phishing technologies, and incorporate those features into future iterations of the technology.

The final credibility type discussed by Tseng and Fogg is experienced credibility. The experienced credibility is developed by a user over time while using a system. Experienced credibility is gained by providing correct recommendations or information, and lost by providing incorrect information . When systems lose credibility by providing incorrect information, the credibility can sometimes be regained by providing correct information again. However, the regained credibility may never reach the same level as the initial credibility. This, of course, presumes that users continue to use a system. When users lose faith in a system's credibility, they may stop using it altogether .

While the issue of trustworthiness may be important, the users' assessment of the toolbar's expertise may be the most critical factor. Often Internet users will dismiss recommendations from a phishing toolbar because they consider themselves web savvy and think they know better . In a study of computer credibility, drivers were told to use a GPS-like path recommender to find the optimal route to a given location . Drivers who were given a scenario in a familiar city were significantly less likely to follow the recommendations than were drivers in an unfamiliar city. This phenomenon may partially explain why users reject phishing toolbar recommendations. They consider themselves familiar with online territory, and are unsure of the basis for the system's recommendations, thus they ignore the advice of decision support systems. Interestingly, contradictory evidence is presented in a study of users' trust in spell-checking software . Even users who were high in verbal ability were more likely to make grammatical or spelling errors when spell-checking software was turned on, indicating that they put more trust in the computer's recommendations than in their own ability. The underlying phenomenon explaining why users would trust a computer system for a non-critical task like spell-checking, but fail to trust a system when attempting to protect their personal information is an important area for future phishing research.

LIMITATIONS

Begin the limitations section here…

CONCLUSION

Phishers continue to be successful as their attack methods are constantly evolving and users frequently disregard the recommendations provided by expert systems. The results of our empirical analysis support this claim as phishing tactics identified in previous research have changed based on a more recent corpus of phishing emails. This research provides a basis for automated-phishing tools to be calibrated; however, additional research is needed to understand why individuals are willing to disregard expert systems when the privacy of their personal information is at stake.

REFERENCES

1. Andrews, L. W., and Gutkin, T. B. (1991) The effects of human versus computer authorship on consumers' perceptions of psychological reports, *Computers in Human Behavior*, 7, 4, 311-317.
2. APWG (2010) "Phishing activity trends report,," A.-P.W. Group (ed.).
3. Bart, Y., Shankar, V., Sultan, F., and Urban, G. L. (2005) Are the drivers and role of online trust the same for all web sites and consumers? A large-scale empirical study,*Journal of Marketing*, 69, 4, 133-152.
4. Beldad, A., de Jong, M., and Steehouder, M. (2010) How shall i trust the faceless and the intangible? A literature review on the antecedents of online trust, *Computers in Human Behavior*, 26, 5, 857-869.

5. Dhamija, R., and Tygar, J. D. (2005) The battle against phishing: Dynamic security skins, 2005 Symposium on Usable Privacy and Security, Pittsburgh, Pennsylvania, ACM, 77-88.
6. Dhamija, R., Tygar, J. D., and Hearst, M. (2006) Why phishing works, SIGCHI conference on Human Factors in computing systems, Montreal, Quebec, Canada, ACM, 581-590.
7. Drake, C. E., Oliver, J. J., and Koontz, E. J. (2004) "Anatomy of a phishing email," in: *First Conference on Email and Anti-Spam*, Mountain View, California, USA.
8. Emm, D. (2006) Phishing update, and how to avoid getting hooked, *Network Security*, 2006, 8, 13-15.
9. Fette, I., Sadeh, N., and Tomasic, A. (2006) "Learning to detect phishing emails," Defense Technical Information Center, Ft. Belvoir.
10. Fogg, B. J., and Tseng, H. (1999) The elements of computer credibility, Proceedings of the SIGCHI conference on Human factors in computing systems the CHI is the limit - CHI '99, New York, New York, USA, ACM Press, 80-87.
11. Forte, D. (2009) Phishing in depth, *Network Security*, 2009, 5, 19-20.
12. Galletta, D. F., Durcikova, A., Everard, A., and Jones, B. M. (2005) Does spell-checking software need a warning label?, *Communications of the ACM*, 48, 7, 82-86.
13. 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.
14. Grazioli, S., and Jarvenpaa, S. L. (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.
15. Jagatic, T. N., Johnson, N. A., Jakobsson, M., and Menczer, F. (2007) Social phishing, *Association for Computing Machinery. Communications of the ACM*, 50, 10, 94-100.
16. Jakobsson, M. (2005) "Modeling and preventing phishing attacks.," in: *Phishing panel in financial cryptography.*
17. Kantowitz, B. H., Hanowski, R. J., and Kantowitz, S. C. (1997) Driver acceptance of unreliable traffic information in familiar and unfamiliar settings, *Human Factors*, 39, 2, 164-176.
18. Kim, J., and Moon, J. Y. (1998) Designing towards emotional usability in customer interfaces-trustworthiness of cyber-banking system interfaces, *Interacting with computers*, 10, 1, 1-29.
19. Kirda, E., and Kruegel, C. (2006) Protecting users against phishing attacks, *The Computer Journal*, 49, 5, 554.
20. Loftesness, S. (2004) *Responding to "phishing" attacks*, Glenbook Brothers.
21. Martin, C. D. (1993) The myth of the awesome thinking machine, *Communications of the ACM*, 36, 4, 120-133.
22. Muir, B. M., and Moray, N. (1996) Trust in automation. Part ii. Experimental studies of trust and human intervention in a process control simulation, *Ergonomics*, 39, 3, 429-460.
23. Myers, S. (2007) "Introduction to phishing," in: *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft,* M. Jakobsson and S. Myers (eds.), John Wiley and Sons, New Jersey.
24. Tseng, S., and Fogg, B. J. (1999) Credibility and computing technology, *Communications of the ACM*, 42, 5, 39-44.
25. Waern, Y., and Ramberg, R. (1996) People's perception of human and computer advice, *Computers in human behavior*, 12, 1, 17-27.
26. Wang, J., Chen, R., Herath, T., and Rao, H. R. (2009a) An exploration of the design features of phishing attacks, *HANDBOOKS IN INFORMATION SYSTEMS*, 4, 259-288.
27. Wang, J., Chen, R., Herath, T., and Rao, H. R. (2009b) Visual e-mail authentication and identification services: An investigation of the effects on e-mail use, *Decision Support Systems*, 48, 1, 92-102.
28. Wright, R., Chakraborty, S., Basoglu, A., and Marett, K. (2010a) Where did they go right? Understanding the deception in phishing communications, *Group Decision and Negotiation*, 19, 4, 391-416.
29. Wright, R., and Marett, K. (2010b) The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived, *Journal of Management Information Systems*, 27, 1, 273-303.
30. Wu, M., Miller, R. C., and Garfinkel, S. L. (2006) Do security toolbars actually prevent phishing attacks?, SIGCHI Conference on Human Factors in Computing Systems - CHI '06, Montreal, Quebec, Canada.

31. Yee, K. P., and Sitaker, K. (2006) Passpet: Convenient password management and phishing protection, Second Symposium on Usable Privacy and Security - SOUPS '06, Pittsburgh, Pennsylvania, ACM, 32-43.

32. Zhang, Y., Hong, J. I., and Cranor, L. F. (2007) Cantina: A content-based approach to detecting phishing web sites, International Word Wide Web Conference, Banff, Alberta, Canada, ACM, 639-648.