Spamming, spoofing and phishing

E-mail security: A survey among end-users

Peter Hoonakker[*], Pascale Carayon[*] & Nis Bornø[#]
[*]Center for Quality and Productivity Improvement, University of Wisconsin-Madison, USA
[#] IT University, Copenhagen, Denmark

Considering that many organizations today are extremely dependent on information technology, computer and information security (CIS) has become a critical concern from a business viewpoint (Knapp, Marshall, Rainer, & Morrow, 2006). Much research has been conducted on CIS in the past years. However, the attention has been primarily focused on technical problems and solutions. Only recently, the role of human factors in CIS has been recognized (Kraemer & Carayon, 2007). End-user behavior can increase the vulnerability of computer and information systems. In this study, we present the results of a large study among end-users and show how end-users' e-mail behavior can affect computer vulnerability.

INTRODUCTION

There is very little reliable information about the costs and impact of security breaches to companies and end users. Most of the information is either anecdotic or stems from commercial surveys among companies and end users. For example, results of a recent study among 5000 consumers by Javelin Strategy & Research (Monahan, 2007) revealed that identity fraud (defined as access to personal account information that leads to fraud) affects nearly 5% of consumers, or nearly 10 million people in the USA per year, and on average costs more than $6,000 per victim. The total one-year cost of identity fraud in the United States was more than $55 billion in 2006 (Monahan, 2007). Contrary to belief, most data compromise still takes place through offline channels (91%) and not via the Internet (9%). Lost or stolen wallets, checkbooks or credit cards continue to be the primary source of personal information theft when the victim can identify the source of data compromise (30%). Nevertheless, computer viruses, spyware or hackers account for more than 5% of all identity fraud cases; phishing for 3%; and online transactions for 0.3% (BBBOnline, 2007; Monahan, 2007).

BACKGROUNDS

Evidently, using electronic or e-mail has many advantages. E-mail is usually a faster alternative to other forms of communication (i.e. letters, phone calls, meetings, etc.) and users can decide when to use and respond to e-mails. The popularity of e-mail is shown by its use: extrapolations by the Radicati Group estimate the number of e-mails sent per day in 2008 to be around 210 billion (Tschabitscher, 2008). Other sources confirm these estimates and show that users are sending more than 180 billion e-mails per day. 180 billion messages per day means that more than 2 million e-mails are sent every second. About 70% of them may be spam and/or contain viruses. The genuine e-mails are sent by around 1.3 billion e-mail users. Results of the Pew Internet & American Life Project Study (Fallows, 2005; Rainie & Fallows, 2004) show that 60% of employees receive 10 or fewer e-mail messages on an average day; 23% receive more than 20 and only 6% more than 50. However, there are also disadvantages of using e-mail, such as receiving Spam e-mail (also known as "unsolicited commercial e-mail"), phishing and spoofing scams.

Spamming is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. Spam in e-mail started to become a problem when the Internet was opened up to the general public in the mid-1990s. It grew exponentially over the following years, and today comprises some 80 to 85% of all the e-mail in the world, by conservative estimate (Kanich, et al., 2008). Results of studies by Fallows (Fallows, 2005; Rainie & Fallows, 2004) on the effects of the CAN SPAM Act (a law aimed at controlling non-solicited commercial and pornographic e-mails) in the USA on January 1, 2004, show that the CAN SPAM Act did have some positive effects. Users who say they have ever received porn spam have decreased from 71% in 2004 to 63% in 2005. However, results of the study by Rainie & Fallows also show that 52% of internet users consider spam a big problem; 22% of e-mail

users say that spam has reduced their overall use of e-mail; 53% of e-mail users say spam has made them less trusting of e-mail; and 67% of e-mail users say spam has made being online unpleasant or annoying (Rainie & Fallows, 2004). Apart from annoying, Spam messages can also contain malware. Malware (malicious software) are programs designed to harm or compromise a computer. Malware includes a wide array of computer code that can wreak havoc to computers, computer networks and even the Internet itself. When end-users open an e-mail attachment they can inadvertently download the malicious computer code on their computer, and it can spread to the computer network or the Internet. Some common forms of malware include:

- *Computer viruses* - programs that disable the victim's computer, either by corrupting necessary files or hogging the computer's resources
- *Worms* - programs that spread from one machine to another, rapidly infecting hundreds of computers in a short time
- *Trojan horses* - programs that claims to do one thing, but actually either damage the computer or opens a back door to your system
- *Backdoors* - methods of circumventing the normal operating-system procedures, allowing a hacker to access information on another computer
- *Rootkits* - a collection of programs that permits administrator-level control of a computer; not necessarily malware on its own, but hackers use rootkits to control computers and evade detection
- *Key loggers* - programs that record keystrokes made by a user, allowing hackers to discover passwords and login codes.

Apart from the indiscriminately sent unsolicited bulk messages (Spam) there are more sophisticated ways of getting the users' information or access to their computer and network. *Phishing*, or a *phishing scam,* means that someone or a website tries to get personal information from the end-user, for example by accidently signing into a website or filling out a form placed on web site. It is an example of a social engineering technique used to fool users. Gartner Inc. (2006) conducted a study among 5,000 online adults in 2006 on phishing attacks. According to the results of the survey, approximately 109 million U.S. adults have received phishing e-mail attacks in 2006, up from 57 million U.S. adults in 2004. The average loss per victim has grown from $257 to $1,244 per victim in 2006. The average amount of money consumers recovered from phishing attacks in 2005 was 80%, but in 2006, recovery amounts dropped to 54%. Recently, security vendor Cyveillance reported a significant increase in phishing attacks during the last months of 2008. Cyveillance reported that the average number of phishing attacks in the first quarter of 2008 was around 400 per day. In September and October that number rose to over 1,750 with record peaks as high as 13,209 phishing attacks in a single day. Techniques, targeted at special populations, such as *spear phishing* or context aware phishing, are targeted scams, where the attacker uses knowledge learned about an individual victim in order to fool more victims (Jakobsson & Stamm, 2006). For example, a users' browser history can be used to determine what websites an user has visited (for example to access his or her bank account) and subsequently an e-mail can be sent to that user, appearing to come from that particular bank, containing the bank's logo, etc., asking the user for sensitive information.

Spoofing, creating hoax websites that closely mimic real sites in order to extract personal information from web visitors, is an increasingly popular form of online scam (Dinev, 2006; Federal Bureau of Investigation (FBI), 2003; Felten, Balfanz, Dean, & Wallach, 1997). In 2000, Ye at al., (Ye, Yuan, & Smith, 2000) estimated that 30 hoax attack sites were detected each day. According to the Anti-Phishing Work Group (Anti-Phishing Work Group (APWG), 2008), that number has increased to nearly 1000 sites a day in the first quarter of 2008.

Network administrators and end-users can protect computer systems in different ways from spamming, spoofing and phishing attacks. Some of the soft- and hardware protections are described below:

- *Anti-virus software* is used to detect and if possible to remove malware. Typically, anti-virus software works by maintaining a list of virus signatures which are used for comparison with the content of scanned files. Modern anti-virus software uses a real time scanner to protect a system at all times and is also able to detect possible threats by analyzing for suspicious program behavior. This method can detect some unknown threats.
- *Intrusion detection systems* (IDS) are soft or hardware solutions used to detect all sorts of attacks, such as intruders and malicious software. This is typically done by monitoring systems and networks with sensors and agents. For example, agents can monitor modifications to system files or analyze network traffic and look for certain patterns previously known as generated by malicious traffic. IDS can detect known and some unknown threats.

- *Intrusion prevention systems* (IPS) can be considered an extension of the IDS technology. The purpose of an IDS is to detect intruders and make a notification. An IPS takes a step more and tries to prevent an intruder or attack by taking a prevention action instead of only making a notification. Actions are taken real time and examples of actions are dropping packets from offending systems and blocking ports or IP addresses.

Despite the technological efforts described above to counteract malware, computer and information systems remain vulnerable because the systems need to interact with human beings, who have their own needs and preferences. It is the human-computer interaction that often creates the biggest vulnerabilities. To quote Mitnick and Simon (2002): "A company may have purchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business. The company is still totally vulnerable... the human factor is truly security's *weakest link*". Especially the use of e-mail and working from remote locations make computer systems vulnerable, partly because it is not under control of the organization.

With regard to e-mail, end-users can protect the system by being careful and not open unknown or suspicious e-mail. However, sometimes that is difficult. The latest viruses can "spoof" the sending e-mail address so that it looks like it is coming from someone other than the computer that infected it. If an e-mail is not from someone the end-user knows, it is usually best to simply delete it without looking at it. If the e-mail appears to be from someone they know, end-users should read the message carefully before opening any attached files. Estimates show that more than a million computer users use *Web-based e-mail programs or webmail* (Yahoo, Microsoft, AOL, Google, etc.), (Brownlow, 2008). One of the advantages of webmail is that you can access your e-mail, everywhere, anytime. However, webmail creates a security issue for the organization because sensitive data can easily be transferred outside of the organization's control and stored on third party servers, meaning that the organization will lose track of the data. Often end-users do not use their own computer, but computers in hotels, airports etc., to access their webmail, which can involve risks. Some services keep caches of Web pages accessed on the local system, including those accessed over a secure link. These caches may allow other users of shared computers to view the e-mail messages other users viewed over a Web-based link (Chapple, 2005). Webmail programs often have less strict security settings than "corporate" mail. Passwords used for webmail can often be simple, and are not updated on a regular basis. Further, allowing employees to use webmail, also means that corporate content filters are bypassed. If organizations are subject to requirements of the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPPA) or other regulatory requirements that limit the types of communications their employees have with the outside world, they need to consider the legal impact of the decision to grant access to external Web-based e-mail services. All of the content controls that they place on their "official" e-mail servers may be rendered moot by an employee's ability to access web-mail. Estimates show that around 30 percent of employees are using private e-mail accounts in the office, even though the company's Internet policy prohibits it (Stone, 2007). Webmail is also vulnerable to malicious actions. Examples are session hijacking (Noiumkar & Chomsiri, 2008), password cracking, cross-site scripting, worms, viruses, and all sorts of scams. Often attached files will never be deleted but remain in the user's e-mail archive even after employment has been terminated.

Working from remote locations, including using the home computer for work, can also make computer and information systems more vulnerable (Landau, 2005). Many organizations depend on mobility of their employees to work from remote locations such as their home or when on the road (Morgan, 2004). Opening the organization's network to employees working from remote locations means greater flexibility as well as an increased amount of security risks (Orme, 2004) and identity and access management is a must for organizations of all types and sizes (Witty, Allan, Enck, & Wagner, 2003).When working from a remote location, the exchange of data typically is done through e-mail, USB devices or a direct connection to the corporate network, for example through a Virtual Private Network (VPN) connection (Venkateswaran, 2001). Especially using the home computer to access the organization's network can increase security risks (Ellison, 2002). The computer at home obviously is not as well protected as the office computer, and is not under the control of the organization. Often other members of the family use the home computer as well, for playing games, downloading files, etc. This creates the possibility of transferring infected files or unauthorized connections into the organization's network (Dyer, Perez, Sailer, & Van Doorn, 2001). When employees use external storage devices such as USB keys, these can easily be forgotten or misplaced (Gorge, 2005).

Some solutions, most technically, exist to eliminate and lowering the risks of remote access. Examples are to require all communication with the organization's network to run through encrypted connections, and limiting access to the data and applications that can be accessed remotely. However, this can cause the user to access restricted data by other means. Providing webmail access to the organization's e-mail account limits the need to use an external webmail service and eliminates a potential security risk, but the user can still have local copies and caches of sensitive files and it is very difficult if not impossible to control user behavior at home (Newman, 2007). Providing secure equipment, such as laptops, which only are intended for work related tasks and restrict the user from, for example, installing applications, is another possibility. Little is known about end-users' e-mail behavior and how it can increase vulnerability of computer an information systems. Therefore, in this study we examine end-users' e-mail behavior and how this behavior can affect computer security vulnerability.

METHODS

Focus Groups

Because relatively little is known about Computer and Information Security (CIS) behavior of end-users, we first conducted focus groups with network administrators and CIS experts (Hoonakker, Carayon, Deb, El Desoki, & Veeramani, 2008). Two rounds of focus groups interviews were conducted with the two different groups (CIS experts and network administrators). During the first focus group, participants were asked to describe non-malicious CIS deviations, and elaborate on contributing factors and possible consequences. During the second round of focus groups, we gave feedback on the results of the first focus group and tried to reach a consensus on the most important deviations from the security rules. The focus groups were conducted over the phone, consisted of 5-7 participants and lasted each one-and-a-half hour. The focus groups were audio taped and the tapes were transcribed in anonymized text files. The text files were analyzed using qualitative data analysis software.

Questionnaire Survey

Based on the results of the focus groups, we developed a survey questionnaire to measure end-users' deviations from the rules and possible contributing factors to these deviations. Analysis of the focus group data showed 10 major areas that are related to CIS deviations: 1) Accessing the computer system and password use; 2) Security settings of the computer; 3) System maintenance and downloading software; 4) Electronic mail; 5) Help with computer problems; 6) Remote access and working from home; 7) Sharing the computer and social networking; 8) CIS training; 9) CIS policy; and 10) beliefs and attitudes towards CIS. In this paper we focus on the results with regard to Electronic mail.

Sample

A representative sample of employees of a large organization was asked to fill out a web-based survey. The organization handles very sensitive private information and has experienced computer security problems in the past. All employees at the organization are requested to participate in a Computer and Information Security training. Totally 836 employees filled out the questionnaire survey (response rate 52%). More than two-thirds of respondents are female (70%). Average age is 50 years. On an average, respondents have 18.5 years of computer experience. Three percent of respondents categorizes themselves as novice users (just started using computers); 68% as average users (use word processors, spreadsheets, e-mail, surf the Web, etc.); 23% as advanced users (can install software, setup configurations, etc.); and 6% as expert users (can setup operating systems; know some computer programming languages, etc.). Respondents had varying educational backgrounds: high school or GED (9%); some college (14%); 2-year college (13%); 4-year college (37%); Master's degree (MA, MS: 21%); professional degree (MD, JD: 3%); and doctoral degree (PhD: 3%). On an average, respondents have worked more than 14 years for the organization. Ninety-five percent of the respondents are normal end-users; 3% super-users (they do have some administrator rights to change the computer settings); and 2% network administrators.

RESULTS

E-mail behavior

We use the questions in the questionnaire about e-mail behavior and questions about vulnerability, i.e. self-reported occurrences of viruses, spyware, phishing scams and identity theft. In the questionnaire, 5 questions were asked about e-mail behavior. Table 1 summarizes the results.

Table 1: E-mail behavior

	Yes	No	DK	NA
Do you sometimes open e-mails if you do not know who the sender is?	45%	55%	0%	0%
Do you sometimes open e-mail attachments if you do not know who the sender is?	9%	91%	0%	0%
Do you use *web-based e-mail software* such as Yahoo mail, Hotmail, Gmail, etc. at work?	39%	59%	1%	1%
Do you use *web-based calendar software* such as Google calendar at work?	7%	92%	1%	0%
If you use web-based e-mail or calendar software, do you pay attention to the security settings of the web-based software?	20%	22%	5%	54%

Results show that more than half of the respondents open e-mails and nearly 10% open e-mail attachments if they do not know who the sender is. Forty percent of respondents use web-based e-mail software and 7% use web-based calendar software, while only a small percentage of the respondents who use web- and calendar based software pay attention to the security settings of the web-based software.

Vulnerability

In the questionnaire, 4 questions were asked about vulnerability to viruses, spyware and adware, phishing scams and identity theft. The results are summarized in Table 2.

Table 2 Self-reported viruses, spy- and adware, phishing scams and identity theft

	Yes	No	DK	NA
Have you ever had a ***virus*** on your computer?	34%	42%	24%	0.1%
Spyware and adware are software programs that quietly sit on your computer and can deliver pop-ups or other advertisements to you. Based on this description, do you think you have any spyware or adware on your computer right now?	16%	57%	26%	0.5%
A *phishing scam* means that someone or a website tries to get personal information from you, for example by accidently signing into a website or filling out a form placed on web site. Have you, or do you believe you have, ever fallen victim to a phishing scam?	6%	81%	13%	0.1%
Do you think your *identity or financial information was stolen online?*	2%	86%	11%	0.9%

Results show that more than a third of respondents (34%) ever had a virus on their computer, nearly a sixth have spyware or adware on their computer (16%), 6% have, or believe they have, fallen victim to a phishing scam, and 2% think that their identity or financial information was stolen.

E-mail behavior and vulnerability

Table 3 summarizes the relation between e-mail behavior of end users and vulnerability (viruses, spyware, phishing scam, and identity theft).

Table 3: E-mail behavior (yes/no) and vulnerability for viruses, spyware, etc in percentages

	Virus (V)		Spyware (S)		Phishing (P)		Identity theft (I)	
Open e-mails?	Yes **50%**	No **40%**	Yes **26%**	No **19%**	Yes 9%	No 6%	Yes 2.6%	No 1.7%
Open e-mail attach-ments?	Yes **58%**	No **43%**	Yes **35%**	No **21%**	Yes **20%**	No **6%**	Yes **6.9%**	No **1.7%**
Use web-mail software?	Yes 46%	No 43%	Yes **26%**	No **20%**	Yes **10%**	No **6%**	Yes 2.9%	No 1.6%
Use web-based calendar?	Yes 55%	No 43%	Yes 30%	No 22%	Yes 15%	No 7%	Yes 2.7%	No 2.1%
Pay attention to security settings?	Yes 44%	No 39%	Yes 24%	No 23%	Yes 9%	No 13%	Yes 2.2%	No 3.9%

*Percentages in **bold** are statistically significant different*

Results of analysis at group level show that respondents who open e-mail, and in particular respondents who open e-mail attachments if they do not know who the sender is, are more vulnerable. They report significantly more viruses and spyware on their computer, and have more often been the victim of a phishing scam and identity theft. Results show that respondents who use web-based software are more vulnerable to phishing scams. However, when analyzing the data at group level, we did not take individual differences such as gender, age, education, years of computer experience, and computer skills into account. Table 4 summarized the results of logistic regression analysis, with these factors taken into account.

Table 4 Results of logistic regression of personal characteristics and e-mail behavior on increased vulnerability for computer and information security risks, statistically significant Odd's ratios

	V	S	P	I
Gender (1=Male, 2=Female)	2.88			
Age (1=<25 years, 2=25-34, 3=45-54, 4=≥55 years)				
Years of computer experience (0-46 years)				
Computer skills (1=Novice user, 2=Average user, 3=Advanced user, 4=Expert user)				
Education (1=less than high school, 2=High school/GED, 3=Some college, 4=2 year college degree, 5=4-year college degree, 6=Masters degree, 7=Professional degree, 8=PhD)				
Open e-mails (Yes/No)				
Open e-mail attachments (Yes/No)		3.02	8.96	8.10
Use web-based e-mail software? (Yes/No)				
Use web-based calendar software? (Yes/No)				
Pay attention to the security settings of the web-based software? (Yes/No)				

Results of logistic regression analysis show that opening an e-mail without knowing who the sender is, significantly increases the vulnerability to malware and hacking. Respondents who open en e-mail if they do not know who the sender is, have a 3 times higher odds to have spyware and adware on their computer; nearly 9 times higher odds to be victim of a phishing scam; and more than 8 times higher odds to have their identity stolen online.

CONCLUSION

Until recently, Computer and Information Security (CIS) was predominantly technology-oriented. Only recently, the role of human factors in CIS has been recognized. Despite all technological hard- and software to make computer and information systems less vulnerable, the interaction of the user with his or her specific needs and the computer system, makes the system vulnerable. End-users often do not realize that their actions, or lack of actions, can endanger computer and information systems. Therefore, end-users should be made more aware of the potential risks of their behavior, for example trough training. End-users can greatly reduce the risks by:

- Installing, using and regularly updating anti-virus programs;
- Using the SPAM filters of their e-mail program;
- Not opening e-mails and in particular attachments to e-mails if they do not recognize the sender, and even if they recognize the sender, think twice before opening the attachment;
- When they are not 100% sure that the e-mail attachment is from a trusted source, they should save it to their hard disk, scan the file using anti-virus software, and only then open the file. As an extra precaution they can disconnect their computer from the network;
- Use their organization's e-mail account instead of web e-mail to access their e-mail, even when working from remote locations through a secure (e.g. VPN) connection
- If the actions above are too complicated, they should ask the network or system administrator, or the help desk to help them perform these actions

With regard to so called cloud computing (using web-based program, such as web-based e-mail and calendars), end-users can reduce the risk by:

- Not use web-mail, and use their corporate e-mail accounts instead, and preferably connect to their organization's network through a secure connection
- If they have to use web-mail, make sure that they adjusted the security settings of the web-based programs. For example, end-users do not always realize that if they do not change the security settings of their Google mail, all information will be open for everyone.

To summarize, end-users should be more aware that their e-mail behavior can increase CIS vulnerability and expose their computer and computer network to all kind of security risks. That does involve sometimes dealing with very user-unfriendly and awkward technology, but it also means using common sense. As pointed out by Reznor (2007):

- No, you have not won the Irish Lotto, the Yahoo Lottery, or any other big cash prize.
- No, there is no actual Nigerian King or Prince trying to send you $10 million.
- No, your bank account details do not need to be reconfirmed immediately.
- No, you do not have an unclaimed inheritance.
- No, you never actually sent that "Returned Mail".
- No, you have not won an iPod Nano.

Acknowledgements

This research was made possible with a grant from the National Science Foundation (NSF # EIA-0120092, Pascale Carayon, PI). We would like to thank our respondents and the organization they belong to, for participating in the survey.

References

Anti-Phishing Work Group (APWG) (2008). Phishing Activity Trends Report, Q1/2008, 2008, from http://www.antiphishing.org/

BBBOnline (2007). New Research Shows Identity Fraud Growth Is Contained and Consumers Have More Control Than They Think Retrieved February 6 2007, from http://www.bbbonline.org/IDtheft/safetyQuiz.asp

Brownlow, M. (2008). Email and webmail statistics Retrieved Dec 11, 2008, from http://www.email-marketing-reports.com/metrics/email-statistics.htm

Chapple, M. (2005). Top five risks of Web-based e-mail. *SearchSecurrity.com* Retrieved Dec 11, 2008, from http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1087968_tax305608,00.html

Dinev, T. (2006). Why spoofing is serious Internet fraud. *Commun. ACM, 49*(10), 77-82.

Dyer, J. G., Perez, R., Sailer, R., & Van Doorn, L. (2001, November). *Personal Firewalls and Intrusion Detection Systems.* Paper presented at the 2nd Australian Information Warfare and Security Conference (IWAR), Perth, Australia.

Ellison, C. (2002). Home network security. *Intel Technology Journal, 6*(4), 37-48.

Fallows, D. (2005). *CAN-SPAM a year later*. Washington D.C.: Pew/Internet.

Federal Bureau of Investigation (FBI) (2003). FBI Says Web "Spoofing" Scams are a Growing Problem Retrieved Dec 1, 2008, from http://www.fbi.gov/pressrel/pressrel03/spoofing072103.htm

Felten, E., Balfanz, D., Dean, D., & Wallach, D. (1997, Oct 7-10). *Web spoofing: An Internet con game.* Paper presented at the 20th National Information Systems Security Conference, Baltimore, MD.

Gartner (2006). Number of Phishing E-Mails Sent to U.S. Adults Nearly Doubles in Just Two Years Retrieved Dec 8, 2008, from http://www.gartner.com/it/page.jsp?id=498245 .

Hoonakker, P. L. T., Carayon, P., Deb, J., El Desoki, R., & Veeramani, R. (2008). The use of focus groups to examine human factors in computer and information security. In L. I. Sznelwar, F. L. Mascia & U. B. Montedo (Eds.), *Human Factors in Organizational Design and Management - IX* (pp. 377-382). Santa Monica, CA: IEA Press.

Jakobsson, M., & Stamm, S. (2006). *Invasive Browser Sniffing and Countermeasures.* Paper presented at the World Wide Web Conference 2006, Edinburgh, Scotland.

Kanich, Kreibich, C., Levchenko, K., Enright, B., Voelker, G. M., Paxson, V., et al. (2008). *Spamalytics: an empirical analysis of spam marketing conversion*. Paper presented at the Proceedings of the 15th ACM conference on Computer and communications security.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Morrow, D. W. (2006). The top information security issues facing organizations: What can government do to help? *Information Security and Risk Management, 34*(4), 51-58.

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics, 38*(2), 143-154.

Landau, S. (2005). Security, wiretapping, and the internet. *IEEE Security & Privacy, 3*(6), 26-33.

Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. New York, NY: John Wiley & Sons.

Monahan, M. T. (2007). *2007 Identity Fraud Survey Report: Identity Fraud Is Dropping, Continued Vigilance Necessary*. Pleasanton, CA: Javelin Strategy & Research.

Newman, K. (2007). Home invasion: Securing home access to business networks. *Network Security, December 2007*(12), 8-10.

Noiumkar, P., & Chomsiri, T. (2008). *Top 10 free web-mail security test using session hijacking.* Paper presented at the 2008 Third International Conference on Convergence and Hybrid Information Technology, Washington, DC.

Orme, B. (2004). Work anywhere, any time, securely. *Infosecurity Today, 1*(1), 44-45.

Rainie, L., & Fallows, D. (2004). *The impact of CAN-SPAM legislation.* Washington D.C: Pew/Internet.

Reznor, T. (2007). The 25 Most Common Mistakes In Email Security. *Digg* Retrieved April 3, 2009, from http://digg.com/d168a2

Stone, B. (2007, January 11). Firms Fret as Office E-Mail Jumps Security Walls. *The New York Times*. from http://www.nytimes.com/2007/01/11/technology/11email.html?ei=5090&en=b5c526a9fea2200f&ex=1326171600&partner=rssuserland&emc=rss&pagewanted=all .

Tschabitscher, H. (2008). How many Email users are there? *About.com* Retrieved Dec 2, 2008, from http://email.about.com/od/emailtrivia/f/how_many_email.htm

Venkateswaran, R. (2001). Virtual private networks. *Potentials, IEEE, 20*(1), 11-15.

Witty, R., Allan, A., Enck, J., & Wagner, R. (2003). *Identity and access management defined* (No. SPA-21-3430). Stamford, CT: Gartner Research.

Ye, Z., Yuan, Y., & Smith, S. (2000). *Web Spoofing Revisited: SSL and Beyond* (No. Technical Report TR2002-417). Hanover, NH: Department of Computer Science, Dartmouth College.