ISSN 2454-8596
www.MyVedant.com

An International Multidisciplinary Research E-Journal

An importance of Antivirus in Computer Security: Specially for Accounting Students

Mr. Vishal Patel

PhD Scholar,Assistant Professor

Sardar Patel College of Administration & Management, BAKROL

DrMehul Patel

Assistant Professor

C P Patel & F H Shah Commerce College, Anand

ISSN 2454-8596
www.MyVedant.com

An International Multidisciplinary Research E-Journal

ABSTRACT

Accountants store personal and money knowledge of purchasers on computers. The loss or exposure of this knowledge will have devastating consequences for the consumer and therefore the business. laptop Antivirus play a significant role for security reason. square measure students making ready to figure an exceedingly in a field that always has access to an individual's Social Security variety, checking account routing numbers, and company money records, ready to stay that knowledge secure through common laptop security practices? This paper analyzes the responses of a gaggle of accounting students to a laptop security survey on the bottom of awareness of laptop antivirus and plenty of a lot of points. The survey was developed to research the safety awareness and practices of faculty students. The results of this study indicate that accounting students might not be sufficiently ready to assist safeguard sensitive knowledge and resources as they become active accountants.

Key Words: Sensitive Knowledge, Square measure, significant, divesting, Antivirus, Account Education

INTRODUCTION

Computers square measure a district of virtually each profession in how Associate in Nursing Associate in nursing integral a part of an accounting profession. Accountants use special purpose software system to perform numerous tasks and information employed by accountants is hold on computers and separate storage devices. The education method is meant to organize students to reach their chosen field. Position Statement No. one in every of the Accounting Education Modification Commission declared that accounting graduates want the potential to find, obtain, organize, report, and use data from electronic sources (American Accounting Association, 1990). The Association to Advance body faculties of Business (AACSB) Standards for Accounting certification lists the "Design and application of technology to money and non-financial data management" as a

traditional learning expertise (2005). several professors have designed their categories to satisfy these goals. the necessity to be educated within the space of pc security is equally essential. The Yankee Institute of Certified Public Accountants includes in its Personal Competencies the necessity to handle "privacy,intellectual property rights and security problems associated with electronic communications" as a part of Leverage Technology to Develop and Enhance Personal Competencies (2005).

Accountants usually have access to non-public and money information of shoppers hold on computers. The loss or exposure of this information will have devastating consequences for shoppers, employees, and also the business. Access to Associate in Nursing individual's personal data will result in determine stealing, one in every of the quickest growing crimes in America. Victims of determine stealing will pay months and years attempting to repair a broken credit history, or recover taken cash. Victims might lose job opportunities, be refused loans, education, housing, cars, or perhaps be in remission for crimes they didn't commit (Federal Trade Commission, 2005). Pc incidents will cause name injury, loss of shoppers, or perhaps liability for the business. It will be long or not possible to recover loss pc information. A study by the National Archives and Records Administration in Washington.D.C. shows 500 of firms that lose information access for ten or a lot of days' file for bankruptcy before long following the loss (Data Centric, N.D.). Lack of access to computers will result in lost revenue and idle staff. the web Security Alliance estimates that companies lose many billions of greenbacks hebdomadally to numerous types of cyber-attacks (2004).

Universities across the country have fully fledged network issues caused by students connecting infected machines to the school's network. The schoolroom computers at the author's establishment were infected with the Sasser worm at the start of the 2004 fall semester. Instructors were unable to use schoolroom computers for the primary week of categories. Student computers were known because the supply of the worm. A computer program infected 2200 computers and slowed e-mail networks on the University of Wisconsin-Madison field. many businesses and state's general assembly that remotely access the university's network were also affected (Nathans and Welch, 2003). The

University of North TX in Denton reported that seventieth of computers closely-held by resident student's coverage for the autumn term were infected with some sort of virus (Krebs, 2003; Nathans and Welch, 2003). Students in the least levels might have poor pc security habits. This became evident to network directors at George Mason University. The director's cut web access for all three,600 students living on field once Associate in Nursing insufficient variety of scholars signed a document confirming that their computers were updated with all the required security upgrades (Krebs, 2003). To assist defend the field network, some universities impose sure measures like requiring antivirus software system on student machines before they will connect with the network.

Dr. Eugene Schultz, Principal pc Engineer, University of California-Berkeley science lab and editor-in-chief of Computers & Security has same that universities square measure among the smallest amount secure places within the universe relative to computers (Foster, 2004). square measure students making ready to figure in an Associate in Nursing exceedingly in a field that always has access to an individual's Social Security variety, checking account routing numbers, and company money records, able to keep that information secure through common security practices? This paper can investigate the pc security awareness of a bunch of accounting students. Results square measure supported Associate in nursing anonymous survey. The survey consisted of twenty- four queries designed to explore however aware and compliant students square measure of wide counseled security precautions. The results are analyzed to see if this explicit cluster of scholars is ready to assist safeguard sensitive information and resources as they become active accountants.

RECOMMENDED SECURITY PRACTICES

A pc incident is associate adverse event that interrupts traditional operative procedures. Viruses area unit only 1 supply of pc incidents. Smart pc security practices by user area unit associate integral a part of preventing computer incidents. One negligent user will cripple a sturdy pc security program. Students as pc users ought to bear in mind of the subsequent essential security practices.

Passwords

Computer users ought to never reveal their passwords as a result of this compromises network security. There's ne'er a reason for users to produce their parole even to system personnel unless they initiated the communication. Approved personnel will access accounts while not user input. If the system doesn't give generated password, then the user ought to bear in mind of the characteristics of an honest password. These embrace employing a combination of higher and grapheme letters, numbers and special characters. Passwords ought to be a minimum of half dozen to eight characters, ought to ne'er be a wordbook word, and may not incorporates info that may be known with the user, like date of birth. Additionally, passwords ought to be modified sporadically, for instance each six months.

Patches and Updates

When security vulnerabilities area unit known, code vendors can usually give patches (a fix to a code defect) or updates (a newer version of existing software) to get rid of the vulnerability. These patches and updates ought to be applied as quickly as attainable following the publication of a replacement vulnerability as a result of attackers begin instantly to do to require advantage of the vulnerability. Users ought to additionally take into account utilizing the automated update feature of code.

E-mail and Antivirus code

The common caution isn't to open e-mail from folks you are doing not understand. However, attackers have the flexibility to channel messages from a compromised machine to everybody in this person's address book. pc users ought to suspect associate e-mail with an attachment they're not expecting, e-mails with intriguing subject lines, and e-mails containing filenames or messages that don't add up, notwithstanding they're from identified addresses. Before gap such a message, users ought to contact the sender to verify that they sent the message. Otherwise, delete the message while not gap it. Once the user has set to open associate e-mail, attachments ought to initial be scanned with antivirus code. Antivirus code makes an attempt to notice and take away pc viruses. Antivirus code definitions ought to be updated a minimum of weekly. Downloaded files ought to even be scanned with antivirus code before they're opened.

Firewall, Spyware, and Popups

A firewall helps stop attackers from examining a machine and victimization existing vulnerabilities to facilitate their attacks. Code firewalls ought to be put in and designed to permit the smallest amount of access whereas still permitting legitimate use. Spyware and popup interference code additionallyhelp shield a pc. Spyware is code that sneakily monitors the user. The term has additionally come back to refer additional generally to code that subverts the computer's operation for the good thing about a 3rd party (Wikipedia) Popups area unit a variety of on-line advertising. additionally, to being irritating, attackers use popups to fascinate phishing. Phishing is a shot to realize sensitive info like passwords and MasterCard info by masquerading as a legitimate business in an officer wanting transmission.

SURVEY METHODOLOGY AND PARTICIPANTS

A pc security survey was developed to assess the pc security awareness and practices of faculty students. The survey consisted of 24 queries addressing passwords, code updates, antivirus code, firewall, backups, spyware interference code, popup interference code, UPS, data of the university's security policies, and varied demographic information. The anonymous survey was administered to students at four universities. Students were of all classifications, freshman through senior with a spread of majors. The results given during this paper area unit of the pc security awareness and practices of the accounting students. 33 accounting students participated within the survey, 28 were seniors, 2 freshmen, one sophomore, one junior, and one didn't specify.

SURVEY RESULTS

Passwords

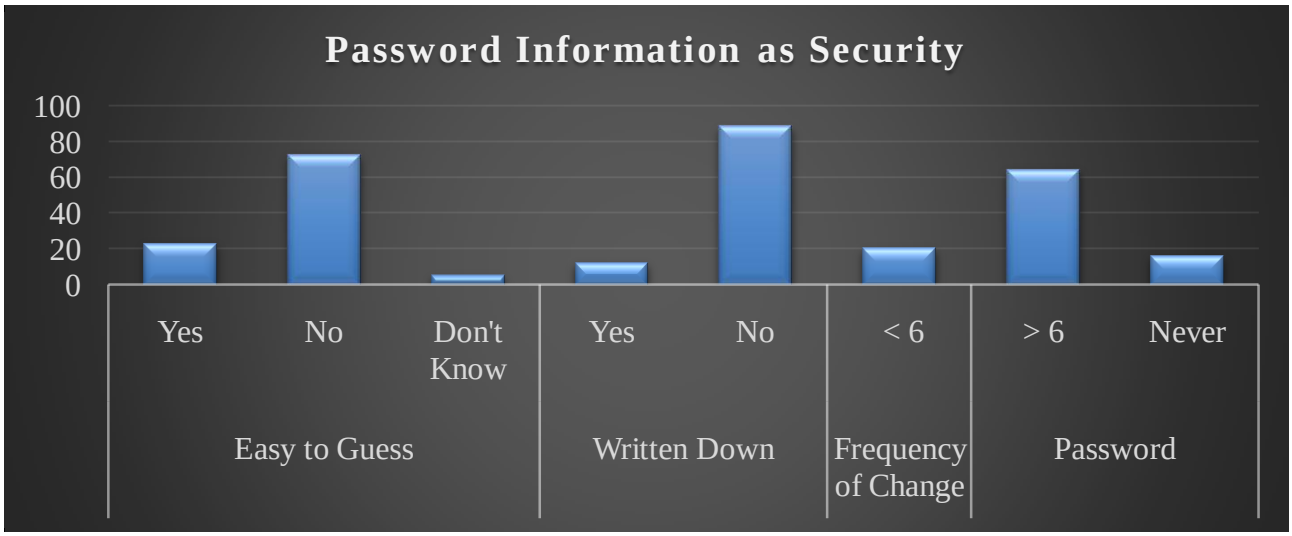
Students were asked multiple questions on their passwords. In response to is your password straightforward to guess (for example a correct name, a wordbook word, your phonenumber)? 72% chosen No. 88%, indicated they didn't write down their password. Students were provided many choices for the question, however usually does one modification your password?just one student chosen a frequency of six months or less. 64 %, indicated they never modification their passwords. Figure one displays the alternatives relative to passwords.

ISSN 2454-8596
www.MyVedant.com
VIDHYAYANA
An International Multidisciplinary Research E-Journal

Table 1: Responses by Percentage of Participants to Password Questions

Easy to Guess	**Yes**	**23**
	No	72
	Don't Know	5
Written Down	Yes	12
	No	88
Frequency of Change Password	< 6	20
	> 6	64
	Never	16

Figure 1: Responses by percentage of participants to password questions

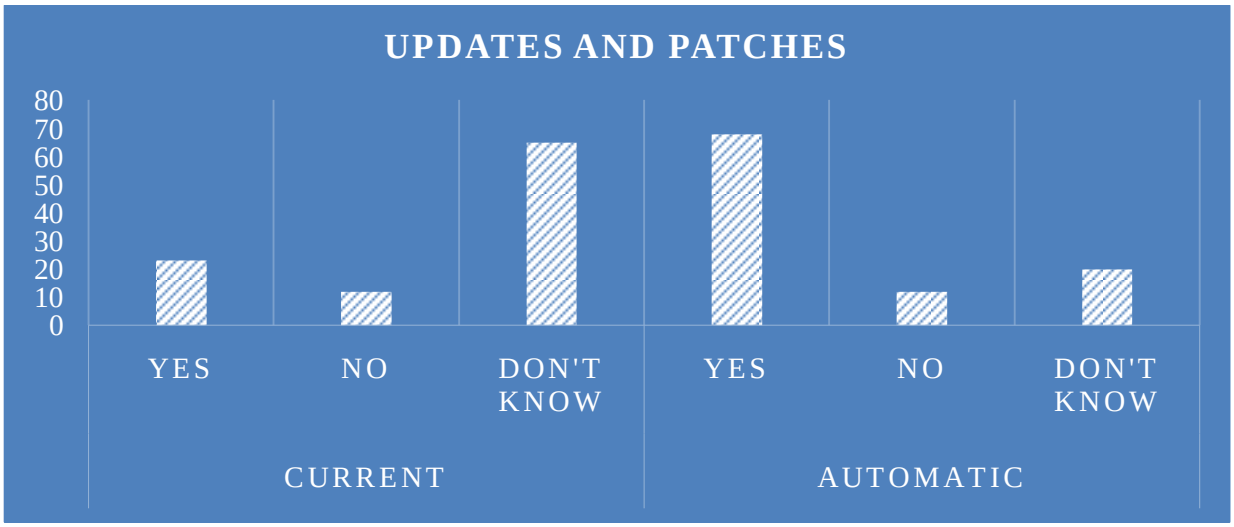


Patches and Updates

Table 2: Patches and Updates

Current	Yes	23
	No	12
	Don't Know	65
Automatic	Yes	68
	No	12
	Don't Know	20

Figure 2: Responses by percentage of participants to updated and patched software



The majority of students, 65%, selected Don't Know when asked if the software on their computer was updated and patched against the latest security threats68%, of students indicated they performed automatic updates of the software on their computer if available. Figure 2 displays the results for the two questions that addressed software patches and updates.

E-mail and Antivirus Software

Students were most aware of antivirus software. Twenty-five or 76% of the students said they had antivirus software installed. Of the students with antivirus software installed, 68% knew the antivirus product name. Those students who identified the product being used were also the students that had a current subscription. Fourteen students indicted they had a current antivirus subscription, all but one of these provided the antivirus product name. Sixteen of the students who knew the product name also indicted the product was set to perform automatic updates. Three students without a current subscription indicated the product is set to receive automatic updates. Unfortunately, because the subscriptions are not current these students are not protected against the latest threats.

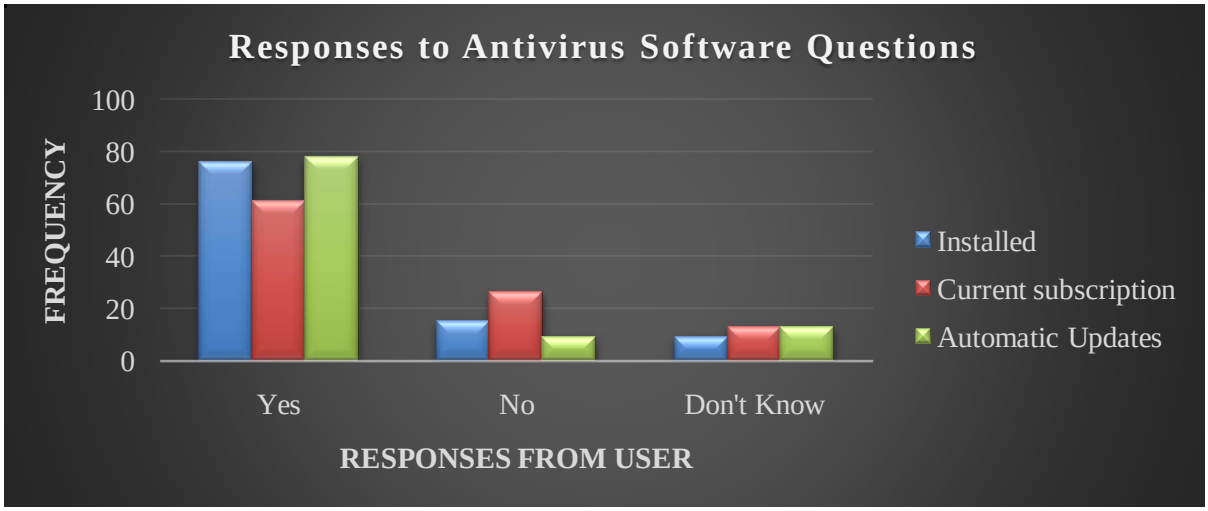
ISSN 2454-8596
www.MyVedant.com

An International Multidisciplinary Research E-Journal

Table 3: Frequency of responses to Antivirus Software questions

	Yes	No	Don't Know
Installed	76%	15%	9%
Current subscription	61%	26%	13%
Automatic Updates	78%	9%	13%

Figure 3: **Frequency of responses to Antivirus Software question**



Participants were asked: When do you scan e-mail attachments before opening? Always, If not expected, If suspicious looking, Occasionally, Never, Other (specify). The most frequently selected response was Always, 48%, followed by Never, 29%. Table 2 shows the percentage and frequency of responses.

	Always	If not expected	If suspicious looking	Occasionally	Never	Other
Percent	48	6	3	10	29	4
Frequency	15	2	1	3	9	1

ISSN 2454-8596
www.MyVedant.com

Table 4: E-mail attachments scanned before opening

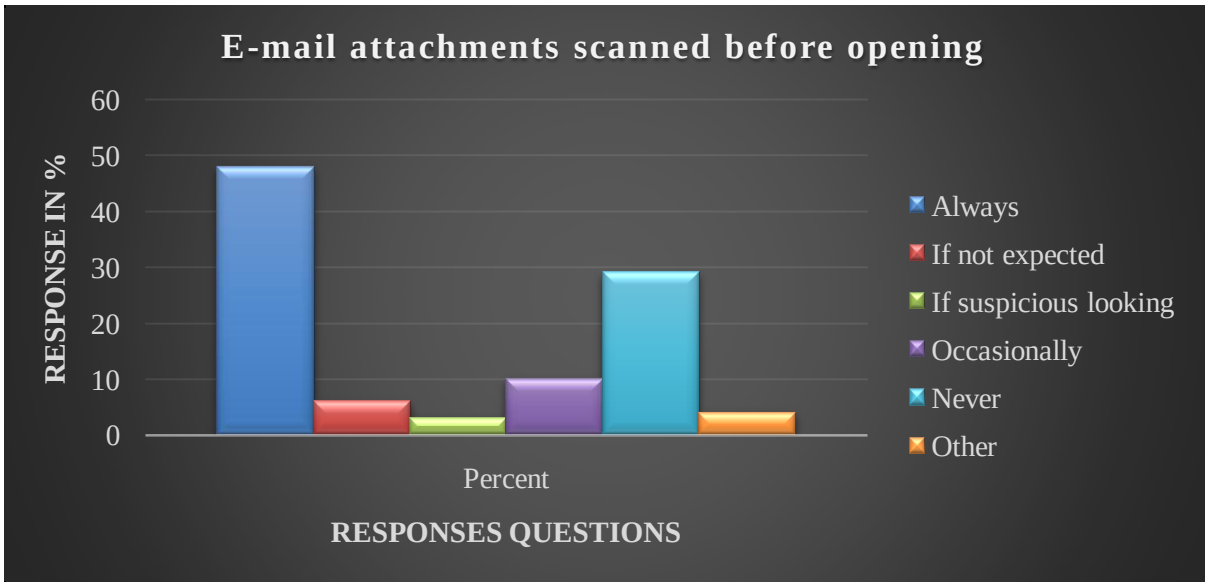


Figure 4: E-Mail attachment scanned before opening

Firewall, Spyware, and Popups

56%, indicted they had a firewall. 30% had not firewall and 14% don't know about it. Almost 27% of students knows about spyware, 65% students don't know about it and 8% students don't know about spyware. Moreover 72% students know about popup, 23% students don't know about the popup and 5% students are not awareness for popup.

	Yes	No	Don't Know
Firewall	56	30	14
Spyware	27	65	8
Popup	72	23	5

Table5: Frequency (percent) of responsesbyproduct

ISSN 2454-8596
www.MyVedant.com

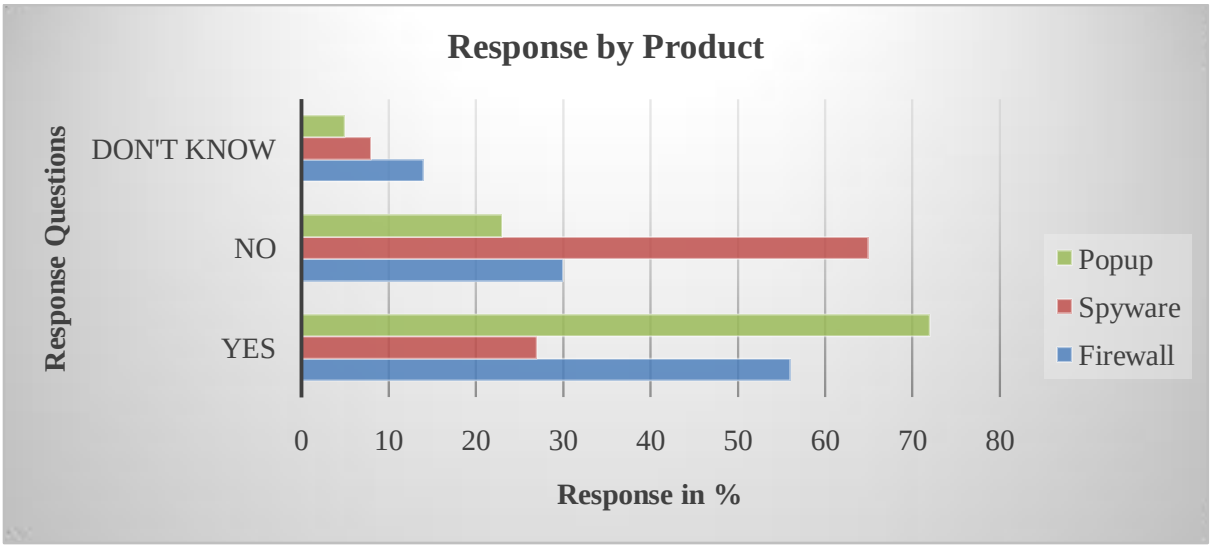


Figure 5: Frequency in % of responses by Product

CONCLUSION

The results of this study indicate that accounting students may not be sufficiently prepared to help safeguard sensitive data and resources as they become practicing accountants. Though some results are positive, security is an area that requires safeguards from multiple directions to be effective. The damage caused by viruses has received much media attention. The need to protect against viruses seems to be well known; 72% of the students indicated they hadantivirus software and 68% did some e-mail scans prior to opening an attachment. However, all the students with antivirus software did not have a current subscription or perform automatic updates. Interestingly the majority of the students that indicated they never scan e-mail attachments before opening them have antivirus software. This could mean the antivirus product is set to do automatic scans or the students with antivirus software have a false sense of security. Results for passwords were also mixed. 72%, said their password was not easy to guess and 68% indicated they did not write them down. However, an overwhelming 64% said they never change their password. In the critical area of software patches and updates, just 30 % of students were current.Results also expose weaknesses in the computer security knowledge of the students. In five different areas the percentage of students that selected Don't Know was at least15%:

As universities focus on preparing accountants to succeed in using technology, the area of computer security should not be ignored. Forced compliance measures that help protect the campus network do not ensure students are conversant in computer security. The potential damage to clients and businesses only continues to increase as attackers devise new ways to take advantage of vulnerabilities that exist in software and people. In addition to concerns about identity theft, viruses, and loss data, Richmond (2004) reports that Symantec identified an average of over 10,000 programs a day that allow an attacker to remotely control a victim's PC. The person who is capable of using technology must also be security conscious.

REFERENCES

1. American Accounting Association. (1990). Position Statement Number One Objectives of Education for Accountants September 1990. Position and Issues Statements of the Accounting Education Change Commission; Retrieved December 7, 2005 from http://aaahq.org/AECC/PositionsandIssues/pos1.html
2. American Institute of Certified Public Accountants. (n.d.). Personal Competencies. Retrieved December 7, 2005 from http://www.aicpa.org/edu/pers.html
3. Association to Advance Collegiate Schools of Business. (2005). Eligibility Procedures and Standards for Accounting Accreditation, p18. Retrieved December 7, 2005 from http://www.aacsb.edu/accreditation/accounting/ACCOUNTINGSTANDARDS-APRIL- 22-2005.pdf
4. Datacentrick. (n.d.). Why Use Data Loss Prevention / Disaster Recovery Planning? Retrieved December7,2005from http://64.233.187.104/search?q=cache:o8sSQt4NKogJ:www.datacentrik.com/images/DataCentrikDataLossPreventionFlyer.pdf+site:www.datacentrik.com+National+Archives+an d+Records+Administration&hl=en
5. Federal Trade Commission. (2005). Take Charge: Fighting Back Against Identity Theft. Retrieved December 7, 2005 from

http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm#Introduction

6. Foster, A. (2004). Insecure and Unaware, The Chronicle of Higher Education, 50(35), 33-35.Retrieved December 7, 2005 from Academic Search Premier database.
7. Internet Security Alliance. (2004). *Common Sense Guide to Cyber Security for Small* Businesses(1st Edition). Retrieved December 7, 2005 from http://www.isalliance.org/
8. Krebs, B. (2003, September 4). Universities Rush to Protect Networks; Area Schools Adopt Strict Policies Aimed at Getting Student to Upgrade Computer Security. *Washingtonpost.com.* Retrieved December 7, 2005 from InfoTrac OneFiledatabase.
9. Nathans, A. & Welch, L. (2003, August 21). 2,200 UW computers hit by virus; E-Mail networks slowed. *The Capital Times*, 1A. Retrieved December 7, 2005 from Custom Newspapers (InfoTrac-Gale) database.
10. Richmond, R. (2005, September 19). Huge Numbers of Spammers Hack Away at PCs. *Dow Jones Newswires*, B4. Retrieved September 23, 2005 from :

    http://online.wsj.com/article/0,,SB112709853807444600,00.html
11. Wikipedia**.** (n.d.). Retrieved December 7, 2005 fromhttp://en.wikipedia.org/wiki/Spyware