An Exploratory Study of the Security Management Practices of Hispanic Students

Yi-Chia Wu *ywu@utpa.edu*
College of Business Administration
Department of Marketing
University of Texas-Pan American
Edinburg, 78539, USA

Francis Kofi Andoh-Baidoo *andohbaidoof@utpa.edu*
College of Business Administration
Department of Computer Information Systems & Quantitative Methods
University of Texas-Pan American
Edinburg, 78539, USA

Robert Crossler *recrossler@utpa.edu*
College of Business Administration
Department of Computer Information Systems & Quantitative Methods
University of Texas-Pan American
Edinburg, 78539, USA

Jesus Tanguma *tangumaj@utpa.edu*
College of Business Administration
Department of Computer Information Systems & Quantitative Methods
University of Texas-Pan American
Edinburg, 78539, USA

Abstract

The growing Internet and mobile technologies create opportunities for efficient communication and coordination among individuals and institutions. However, these technologies also pose security challenges. Although users' understanding and behavior towards security solutions have been recognized as critical to ensuring effective security solutions, few research articles have examined user security management practices. The literature lacks empirical research that examines users' everyday behavior and practices to managing security. In an effort to bridge the gap in user security management practices, this paper presents an exploratory study of how Hispanic college students manage the security of their computer systems. Specifically, we examine how ethnicity, gender, and age influence users' behavior towards updating their operating systems, non-operating system software and antivirus definitions. The results reveal that gender influences the frequency of updating operating systems, antivirus definitions and non-operating system software, whereas ethnicity and age influence only frequency of update of operating systems but not the frequency of update of non-operating system software and antivirus definitions.

Keywords: Non-operating System Software, Antivirus Software, Security Practices, Software Update, Users' Security Management, Hispanic.

1. INTRODUCTION

Even as the Internet and mobile technologies facilitate electronic commerce and effective global coordination and communication, users' security management practices can hinder the benefits that such technologies promise [1]. Studies show that users' security management is a problem [2] [3] [4] [5]. Other studies have noted that people tend to delegate computer security responsibilities to technology, trusted individuals or trusted institutions [1] [2]. When an individual

delegates his or her security responsibilities, they somehow believe that their system's security is guaranteed by the trustee (such as a family member or a roommate, even when for instance the roommate moved out). Hence the individual or computer user who has delegated his or her security responsibilities may lack information on the security safeguards that are available and what needs to be done to secure their computer systems.

One specific group of users that is of concern in this paper is the Hispanic population. The rapidly growing Hispanic population has formalized a new target audience for marketers. The differences of the demographic distribution of the Hispanic population not only enforce the necessity of localization but also the modification of Hispanic online users. Even with the emerging market of Hispanic consumers, socio-economic factors such as education, income, and language barrier impede Hispanic consumers from the acceptance of online information. Among the Latino population in the United States, Mexicans are the largest national origin group. A U.S. study shows that 52% of Latinos of Mexican origins have a lower probability of online usage. Holding the socio-economic factors, such as age, income, language, generation, and nativity, constant, the Mexican population tends to have lower chances to adopt the Internet [6].

Thus, the understanding of the security behavior of the Hispanic population is useful in the design of software that may be adopted by this particular target. However, there is a lack of research on this population. This study seeks to contribute to the understanding of the security practices of the Hispanic community. Specifically, this paper examines the behavior of undergraduate students in a Hispanic serving institution with respect to how often they update operating systems, non-operating system software (hereafter referred to as non-OS) and antivirus definitions. We also examine how ethnicity (Hispanic vs. Non-Hispanic), gender, and age influence individual's frequency or likelihood of updating operating systems, non-OS and antivirus definitions. The rest of the paper is organized as follows. We present a related background study of the topic in the next section. Here, we discuss prior related studies and present our research hypotheses. Following, we discuss the research methodology. We then present the results and discussion. Finally, we conclude the paper where we suggest some future research directions.

2. BACKGROUND AND HYPOTHESES

Dourish and Grinter [1] found that users in general had a neutral to negative attitude toward security technologies. Our definition of security practices is based on Dourish and Grinter's [1] work where they define security practices as "…actions, and what practices and patterns people adopt to manage their security needs and accommodate them into their work" (p. 393).

2.1 Operating Systems and Non-Operating Systems Vulnerabilities

Unlike operating systems, the updates of non-OS are not normally set up automatically in computers [7]. End users have to regularly update the systems to enhance Internet security for the latest patch. The term patch in this paper indicates "any type of update to a piece of software, whether technically a patch, update, or upgrade" [8]. A patch file allows modified changes with a patching utility in a form of source code or as binary code to current files. The purpose is to replace file content with either the line- or byte-level code [8]. Users who are aware of the necessity of updating the non-OS tend to be more knowledgeable and sensitive to security vulnerabilities. The failure of updating non-OS will threaten clients' stored information. Non-operating systems include: instant messaging (Yahoo, AOL, MSN), accounting software, PDF viewers (Adobe Acrobat, Ghostview), Microsoft Office (Windows and Mac), music players (iTunes, Winamp, RealPlayer, Windows Media Player) and email clients (Mozilla, Eudora, Outlook, Lotus Notes) [9]. Many operating systems provide automated notifications for end users to update the patches. Operating systems are a lucid target for patch management because the usage is prevalent. Network applications are easy targets for attacks from outsiders since the damage can influence a work station or the entire organization [10]. The problem is, particularly for non-technical end users, not all of the non-OS automatically notify users about the availability of update packages [8]. The risks for end users, individual or organizations, of not updating a non-OS increase when the patch is not applied [11]. The longer the delay is for updating the

patches, the more vulnerable the computer is to outside attacks. It is increasingly dangerous when the end users fail to update a patch within days of it being made available [8].

2.2 Factors That May Influence Security Behavior

One of the major demographic variables that may influence security practices is gender. Furnell, Bryant and Phippen [12] conducted research on the awareness of security issues and respondents' attitude on the use of safeguard tools of 415 personal internet users in the UK. The findings indicated that male respondents tend to be more confident in considering themselves as advanced in IT experience. Similarly, Dourish and Grinter's [1] study noted that age influences users' attitude towards security.

In this study, we use students from a higher education institution for our study. This is very important especially for the group of users that is the target of this study. Education levels influence Internet usage [13]. Ten percent of Latinos have a college degree, and of that small group, 89% go online. By comparison, 28% of whites have college degrees, and 91% of them use the Internet. Twenty percent of African Americans have college degrees, and 93% report using the Internet [14]. According to previous studies, higher education may lead to higher confidence and the adoption of self-service technology [13].

According to the 2010 United States census data, Hispanics make up the fastest growing ethnic group in the population [15]. Also, Latinos are a young population with approximately twice as large a share of adults under age 40 than that among the white non-Hispanic population. Sixty-seven percent of Latinos age 18-29 go online, whereas 77% of African Americans and 86% whites in the same age range go online [14]. For ages 30-41, 61% of Latinos, 77% African Americans, and 85% whites go online. Fifty-eight percent of Latinos, 69% of African Americans, and 80% of whites age 42-51 use the internet. Finally 46% of Latinos, 49% of African Americans, and 75% of whites age 52-60 go online [14].

Based on the extant literature discussed in this section, we present a set of hypotheses that are tested in this exploratory study (see Table 1). Our dependent variables are frequency of updates of operating systems, non-OS and antivirus definitions whereas the independent variables are Ethnicity (Hispanic vs. Non-Hispanic), Age (< 21 years vs. >= 21 years) and Gender (Male vs. Female).

H1	Non-Hispanics are more likely to update their operating systems software than Hispanics.
H2	Non-Hispanics are more likely to update their non-operating system software than Hispanics.
H3	Non-Hispanics are more likely to update their antivirus definitions than Hispanics.
H4	Males are more likely to update their operating systems than Females.
H5	Males are more likely to update their non-operating systems than Females.
H6	Males are more likely to update their antivirus software than Females.
H7	Students less than 21 years of age are more likely to update their operating systems than those older than 21 years.
H8	Students less than 21 years of age are more likely to update their non-operating systems than those older than 21 years.
H9	Students less than 21 years of age are more likely are to update their antivirus software than those older than 21 years.

TABLE 1: Set of Hypotheses tested in this study.

3. METHODOLOGY

Dourish and Grinter [1] found that users in general had a neutral to negative attitude toward security technologies. Our definition of security practices is based on Dourish and Grinter's [1] work where they define security practices as "…actions, and what practices and patterns people adopt to manage their security needs and accommodate them into their work" (p. 393).

Data Collection

A survey was conducted to gather information regarding students' behavior to security practices. The sample consisted of 315 students taking an entry level Computer Information Systems class in a Hispanic serving university in the South Eastern region of the United States. This study allowed students to have abundant time to answer the survey questions and guaranteed the anonymity of the responses. Students were permitted to opt out anytime during the administration of the survey. There were no identifying questions enclosed in the survey. The survey included demographic questions based on the 2010 United States Census form.

This study uses the chi-square statistical test to examine the percentage of students' responses that fit into the various categories of the frequency of updates ("automatic", "weekly", "monthly", "rarely", "never", and "I don't know") for the different values of the independent variables. The independent variables are gender, ethnicity, and age.

4. RESULTS AND DISCUSSION

According to 2000 census Overview of Race and Hispanic Origin guideline, Hispanics can be categorized as any race. Hispanic groups such as Mexican, Puerto Rican, or Cuban, are classified as Some other race category [6]. Therefore, students who self-identify themselves as Hispanic may contain Hispanic origin as well as with at least one other race. In order to examine different levels of demographic variables affecting the frequency of updating the operating systems, non-OS and antivirus definitions among students, this study splits race into two categories: Hispanics/Latinos and Non-Hispanics/Latinos. Table 2 presents the Chi-square analysis for the % distribution of students' responses within the different categories within the independent variables.

		Operating System					Non-Operating System				Antivirus Update			
		Auto	W	N	?	X^2	W	M	R	X^2	W	M	R	X^2
Gender	Male	69.5	16.1	7.6	6.8	15.88	18	17.1	65	9.959	39.4	24	36.5	6.777
	Female	70.4	5	7.5	17.1		9.1	10.1	80.8		25.7	24	50.3	
Ethnicity	Hispanic	70.7	8.7	6.3	14.3	10.56				2.827				0.285
	Non-Hispanic	62.1	13.8	21	3.4									
Age	< 21	71	6.7	8	14.3	7.545				0.734				1.026
	>=21	66.2	16.9	6.5	10.4									

Note: All the numbers are in the unit of percentage except for Chi-Square.
Auto = Automatic update, W = Weekly, M = Monthly, N = Never, ? = I don't know,
R = Rarely, X^2 = Pearson Chi-Square.

TABLE 2: Chi-Square Analysis-User Response Percentage Distribution

Prior to discussing the statistically significant differences in our results, it is interesting to note the low overall level of security practices. Operating system updates is the behavior that is most regularly performed automatically. However, this is a setting that is generally set by default and taken care of by the operating system vendor. When it comes to updating non-Operating System software and antivirus definitions there is very poor performance. While this in itself presents useful information for the overall population of interest, we also demonstrate in the following section that there are differences in behavior based on demographic variables.

Hypothesis		Pearson Chi-Square	P-Value	Hypothesis supported?
H1	Males are more likely to update their operating systems than Females	15.881	0.001***	Yes
H2	Males are more likely to update their non-operating systems than Females	9.959	0.007***	Yes
H3	Males are more likely to update their antivirus software than Females	6.777	0.034**	Yes
H4	Non-Hispanics are more likely to update their operating systems software than Hispanics	10.56	0.014***	Yes
H5	Non-Hispanics are more likely to update their non-operating system software than Hispanics.	2.827	0.243	No
H6	Non-Hispanics are more likely to update their antivirus definitions than Hispanics	0.285	0.867	No
H7	Students less than 21 years of age are more likely to update their operating systems than those older than 21 years	7.545	0.056*	Yes
H8	Students less than 21 years of age are more likely to update their non-operating systems than those older than 21 years	0.734	0.693	No
H9	Students less than 21 years of age are more likely are to update their antivirus software than those older than 21 years	1.026	0.599	No

Note: *** Significance at 0.01, ** Significance at 0.05, * Significance at 0.1

TABLE 3: Results of the Hypotheses tests

Table 3 shows that gender is the only independent variable that significantly influences the frequency of update of all the three dependent variables (operating systems, non-OS and antivirus definitions). The Ethnicity and Age variables only significantly influence the frequency of update of operating systems but not non-OS and antivirus definitions.

4.1 Gender and Frequency of Update of Operating System

The calculated Pearson Chi-Square (χ^2 = 15.881, d.f. = 3) and its corresponding p-value ($p < .05$) for the relationship between frequency of update of operating system and gender indicate that hypothesis 1 is supported at the 5% significance level. Our research shows that males are more likely to update their operating systems frequently than females. While the difference in the number of students who set up their operating system to automatic update is low between males and females (69.5% v. 70.4%), there are differences for the "weekly" and "I don't know" categories. This observation can be explained by Durish and Grinter's [1] observation that individual users are likely to rely on a set of guarantees such as technology, family member, friends or institutions and delegate their security responsibilities to the guarantee. As we can see from our data, the female users were more dependent on the guarantee than the males as we see that more males updated their antivirus on a weekly basis. Further, the percentage of those who responded "I don't know" was far higher for females (17.1%) compared to 6.8% for males. This suggests that females are more likely to exhibit a security behavior whereby once they delegate their security management responsibility do not even worry about what security guards are available on their systems and do nothing to enhance the security of their systems.

4.2 Gender and Frequency of Update of Non-OS

Once again our data reveals that males are more likely to update their non-OS than females. Hence hypothesis 2 that states that males would update their non-OS more frequently than females is supported. Although both hypotheses 1 and 2 are supported, there is a sharp distinction concerning gender and frequency of update between operating systems and non-OS. Unlike the operating systems where a great majority of both males and females set their systems to automatic, here a great majority report that they rarely update their non-OS (80.8% females to 65.0% males). Both females and males feel that they are at disadvantage in comparison with hackers and others who can undo all what they could do to protect their security and would rather prefer to delegate their security management practice to a tool or trusted person or institution and not be bothered by the mundane of managing non-operating systems.

4.3 Gender and Frequency of Update of Antivirus Definitions

Hypothesis 3 is supported as the Pearson Chi-Square was significant at the 5% level. Specifically, about 39.4% males compared to 25.7% females update their antivirus definitions on a weekly basis. In addition, while 50.3% of females update their antivirus definitions rarely, only 36.5% of males do so. This suggests that males are less likely to delegate their responsibility to update their antivirus definitions to others and take time to frequently update their antivirus definitions in comparison to females.

4.4 Ethnicity and Frequency of Update of Operating System

The literature suggests that Non-Hispanics are more likely to have experience with computers than Hispanics. Dourish and Grinter [1] suggest that experience with technology influences users' behavior towards security management practice. Thus as we observe from the data, Non-Hispanics are more likely to update their operating systems more frequently than Hispanics because the former have more experience with technologies such as operating systems. Hence hypothesis 4 is supported. We also observe from our data that Hispanics are more likely to delegate their security management practice to the technology as observed in 70.7% of Hispanics compared to 62.1% setting their operating systems to automatic update. However, more Non-Hispanics update their operating systems on a weekly basis with higher percentage of Hispanics responding that they do not know whether their operating systems are being updated or not.

4.5 Ethnicity and Frequency of Update of Non-OS

The Pearson Chi-Square value ($\chi^2 = 2.827$, d.f. = 2, $p = 0.243 > \alpha = 0.05$) for hypothesis 5 that tests the relationship between ethnicity and frequency of update of non-OS demonstrates that the hypothesis was not supported by our data. A plausible reason for this observation is that most users may have negative attitudes towards non-OS systems in terms of how they may hinder how they use their systems [1]. Similarly, others have observed that users sometimes believe that hackers have more technological skills than they do and that whatever they do to protect their computers against viruses and other attacks, hackers can overdo and so make no effort to work towards protecting the security of their computer systems [1] [5]. Dourish and Grinter [1] also note that users see security as a barrier. They observed from their study that users could not distinguish between security and spam. To the users, security and spam were different aspects of security and so feel that a single technology can address all kinds of problems. Hence they are less interested in addressing issues of non-OS. Thus, users' lackadaisical attitudes towards updating non-operating systems may not differ between ethnicities (here Hispanics and Non-Hispanics).

4.6 Ethnicity and Frequency of Update of Antivirus Definitions

Similar to the relationship between ethnicity and frequency of update of antivirus definitions, the relationship between ethnicity and frequency of update of antivirus definition is not significant. Thus, hypothesis 6 is not supported by our data. Once again, users may rely on technology and may not see the importance of worrying about updating antivirus definitions. Dourish and Grinter [1] observe that users may look at an antivirus definition as complete solution to security problems.

4.7 Age and Frequency of Update of Operating Systems

Our results reveal that young people (ages < 21) delegate their responsibility to update operating systems to technology than people older than 21 years (71% vs. 66.2%). At the same high percentage of people older than 21 update their operating systems on a more regular weekly basis than those who are younger than 21. The situation is different when it comes to those who report that they never update their operating systems or do not know whether their operating systems are updated or not. The results suggest that those young people who have experience with operating systems would typically set their systems to automatic update while those who may have less experience may not care about the update of the operating systems. However, in general gender influences the frequency of update of operating systems supporting other studies

that suggest that gender influence security practice. Thus hypothesis 7 is supported by our data at the 10% significance level.

4.8 Age and Frequency of Update of Non-OS

For the relationship between age and frequency of updating the non-OS, the calculated Pearson Chi-Square value ($\chi^2 = 0.734$, d.f. = 2, $p > .05$) indicates that hypothesis 8 is not supported by our data. The explanation that was offered for relationship between ethnicity and frequency of update of non-OS may be relevant in this relationship as well. While Dourish and Gritner [1] observe that young people have confidence in what they can do with computer systems, they generally are unhappy with security technologies that hinder their abilities to work efficiently and may therefore choose not to worry about updating non-OS which they may feel would hinder their overall productivity and experience with their computer systems.

4.9 Age and frequency of update of antivirus definition

Age was not found to influence the frequency of update of antivirus definitions. Hence our data did not support hypothesis 9. Once again, users irrespective of age would rather delegate responsibility of updates of antivirus definitions or may not be bothered.

5. CONCLUSION

The study examined security management practices of Hispanic college students. Specifically, we examine how ethnicity, gender, and age influence users' behavior towards updating their operating systems, non-OS and antivirus definitions. The results reveal that gender influences the frequency of updating operating systems, non-OS and antivirus definitions, whereas ethnicity and age influence only frequency of update of operating systems but not the frequency of update of non-OS and antivirus definitions. In particular, we observe that non-Hispanic students rarely update their systems. Second, male students tend to update their system more frequently. Our research supports other study that demonstrates that male users in a primarily Hispanic institution not only update non-OS more frequently than females, but also update Anti-Virus software more frequently as well [17]. Our results also support prior research that shows that users typically delegate their security management responsibilities to technology, trusted individuals and institutions [1].

6. SUGGESTIONS FOR FUTURE RESEARCH

The fundamental question that derives from this research is: what are the implications for end users in regard to updates of operating systems, non-OS and antivirus definitions. It is arguable that certain non-operating systems would not endanger individual's information security when the software is not exploited frequently. Without the updates of the new patches, the original files are still protected and performed with no technical issues. The non-OS such as iTunes can function without the new updates based on the end user's purposes. However, the lack of new updates of anti-virus software will imperil the end user's information security if the new patches are not updated in time exposing the user to threats from outside attacks.

This empirical study concludes that race (Hispanic versus non-Hispanic students) and age are not significant indicators for non-OS and antivirus definition update. For further research, this study suggests that the range of the non-OS should be narrowed down to several specific categories in order to detect participants' awareness of non-OS updates. Additionally, future research could conduct a similar survey at a non-primarily Hispanic serving institution and compare the results. The results would provide insight to the differences in security practices between the groups of students served at each of these universities. Further research could also be conducted that utilizes theories, as opposed to demographics to hypothesize differences in security practices at primarily Hispanic serving institutions.

7. REFERENCES

[1] P. Dourish, R.E. Grinter, J.D.D.L Flor, and M. Joseph. "Security in the wild: user strategies for managing security as an everyday, practical problem." *Personal Ubiquitous Computing*, vol. 8, pp. 391–401, 2004.

[2] B. Friedman, D. Hurley, D. Howe, E. Felten, and H. Nissenbaum. "Users' Conceptions of Web Security: A Comparative Study," Short paper presented at ACM Conf. Human Factors in Computing Systems CHI, Minneapolis, MN, USA, 2002.

[3] J. Rimmer, I. Wakeman, L. Sheeran and M.A. Sasse. "Examining users' repertoire of internet applications," In Sasse and Johnson (eds), Human-Computer Interaction: Proc. of Interact'99, 1999.

[4] L. Sheeran, M.A. Sasse, J. Rimmer and I. Wakeman. (2002). "How Web browsers shape users' understanding of networks." *Electronic Library, The*. [On-line]. 20(1), pp. 35-42. Available: http://www.emeraldinsight.com/journals.htm?articleid=861950 [Jan. 31, 2011].

[5] D. Weirich and M.A. Sasse. "Pretty good persuasion: a first step towards effective password security for the real world," In: Proc. of the ACM new security paradigms workshop (NSPW 2001), Cloudcroft, New Mexico, ACM Press, New York, 2001, pp. 137–143.

[6] S. Fox and G. Livingston. "Latinos Online: Hispanics with Lower Levels of Education and English Proficiency Remain Largely Disconnected from the Internet." Internet: http://www.eric.ed.gov/PDFS/ED495954.pdf, Mar. 14, 2007 [Jan. 22, 2011].

[7] "Home network security." United States Computer Emergency Readiness Team. Internet: http://www.us-cert.gov/reading_room/home-network-security/#IV-A-7, Dec. 5, 2001 [Jan. 25, 2011].

[8] J. Antman. "Patch Management: An Overview." Internet: http://rutgerswork.jasonantman.com/antman-patchManagement.pdf, Dec. 10, 2008, [January 21, 2011]

[9] Updating non-operating system software, "Updating non-operating system software to prevent security compromises." Internet: UCSF ITS, University of California, San Francisco: http://security.ucsf.edu/EIS/BestPractices/Staff/StaffUpdatingSoftware.html, 2010 [Jan. 25, 2011]

[10] D. Brandl. (2008). "'DONA' forget about security." *Control Engineering*. 55 (12), pp.14.

[11] C. Higby and M. Bailey. "Wireless security patch management system," in Proc. of the 5th conference on Information technology education, Salt Lake City, UT, USA: ACM, 2004.

[12] S.M. Furnell, P. Bryant, and A.D. Phippen. (2007). "Assessing the security perceptions of personal Internet users." *Computers & Security*. [On-line] 26 (5), pp. 410-417. Available: http://www.sciencedirect.com/science/article/B6V8G-4N6NJTT-1/2/492a40cf1c60d7fbf02f0bdc01c3f609 [Jan. 25, 2011].

[13] M.L. Meuter, M.J. Bitner, A.L. Ostrom and S.W. Brown. "Choosing among alternative service delivery modes: An investigation of customer trial of self-service technologies." *Journal of Marketing*, vol. 69(2), pp. 61-83, 2005.

[14] S. Fox and G. Livingston."Latinos Online: 2006-2008: Narrowing the Gap." Internet: http://pewhispanic.org/reports/report.php?ReportID=119, Dec. 22, 2009 [Jan. 22, 2011].

[15] K. Humes, N. A. Jones and R.R. Ramirez. "Overview of Race and Hispanic Origin: 2010, 2010 Census Briefs." Internet: http://www.census.gov/prod/cen2010/briefs/c2010br-02.pdf, Mar. 2011 [Jan. 22, 2011]

[16] E.M. Grieco and R.C. Cassidy. "United State Overview of Race and Hispanic Origin: Census 2000 Brief." Internet: http://www.census.gov/prod/2001pubs/cenbr01-1.pdf, Mar., 2001 [Jan. 22, 2011].

[17] R. Crossler, M. A. Villarreal, and F. K. Andoh-Baidoo. "A Preliminary Study Examining the Security Practices of Hispanic College Students." *SouthWest Decision Science Institute*, 2011.