Scale for Efficacy in the Safe Use of the Internet for Students

Nadire Cavus [a] *, Near East University, Department of Computer Information Systems, Nicosia, Cyprus
Alaa A. Mohammed [b], Near East University, North Cyprus

Abstract

College understudies are overwhelming clients of the İnternet contrasted with the overall public, and they assume a pivotal part in securing the Internet, and assurance of PCs is left to the activity of the clients. The main aim of the study is to investigate self-efficacy in the safe use of the internet for students. The volunteer participants used in this study consisted of a total of 99. The questionnaire is made up of 4 dimensions SNS, MS, WSS and CS which had 35 items altogether in total. The participants answered to items on 5 Likert Scale. The questionnaire reliability was calculated as 0.72. A questionnaire was used to collect data and was analysed and interpreted using SPSS. Frequency and percentage, Independent sample t-test, ANOVA, methods were used during the analysis process. According to the results of the study, students have good awareness of computer security on a general note, but specifically in terms of social networking sites, web security and malicious software, the majority of the students have little awareness of them. As a result, the study could help universities, government and even parents of students, in Cyprus and in other countries, to be able to access the Internet safely.

Keywords**:** Computer security; internet security; malicious software; social network sites; student perceptions

* ADDRESS FOR CORRESPONDENCE: **Nadire Cavus** *,* Near East University, Department of Computer Information Systems, Nicosia, Cyprus
E-mail address: *: nadire.cavus@neu.edu.tr* / Tel.: +90-322-3387101 - x16

1. Introduction

Computer users is frequently said to be the weakest join in computer security. Security and protection dangers, for example, Web cookies and phishing require some type of client complicity or passive consent (Shin & Shin, 2011). Sufficient security does not accompany the buy of the PC but rather requires extra programming watchful settings inside of utilizations, suitable decisions of passwords, standard overhauling of patches, and so forth (Hsiao et al., 2012). Additionally, as applications are turning out to be all the more fascinating/helpful and organizations are moving far from paper, home PC clients are performing more delicate undertakings online and putting away more private information on their PCs. Episodic proof, overviews, and studies figure out that home PC clients frequently don't sufficiently comprehend the dangers, or have room schedule-wise, longing and information to have the capacity to handle them (Liu & Yu, 2013). As substantial episodes of worms and infections have appeared, even systems managers are not sufficiently industrious in applying patches to enhance security (Kim & Lee, 2011).

1.1. Aim of the study

The main aim of the study is to investigate self-efficacy in the safe use of the internet for students from Near East University. To achieve this main aim, we need to achieve more sub aims like:

1. What is the university students' perception towards safe internet use?

2. Is there any gender based difference in university students' perception towards safe internet use?

3. Is there any age based difference in university students' perception towards safe internet use?

2. Theoritcal background

Aboud (2012) proclaimed that upgrading web security and defensive urgent information foundations are fundamental to each countrys security and monetary prosperity. Making the web more securely (and defensive web clients) has gotten to be fundamental to the occasion of late administrations also as government strategy. Hindering law-breaking is a necessary component of a national digital security and requesting information system insurance system. In particular, this incorporates the reception of material enactment against the abuse of ICTs for criminal or distinctive capacities and exercises expected to affect the trustworthiness of national vital systems. At the national level, this can be a mutual obligation requiring composed activity connected with bar, arrangement, reaction and recuperation from occurrences with respect to government powers, the individual part and voters. At the local and global level, this involves participation and coordination with significant accomplices.

Baaji (2012) proclaimed that utilization of the web is nowadays regular way of life see in modern nations. The vast majority of the general population can't envision an existence while not the ethics and prospects of web. However the fastest ascent and pervasive character of web conjointly made a few level headed discussions concerning wellbeing and security issues. With the development of web use, conjointly new dangers and threats went ahead. At present, web security is politically and socially a key issue. One among the courses by which governments endeavour to animate web security, is to create client mindfulness battles. Be that as it may, the adequacy of those crusades is addressed.

SNSs give clients with entertainment opportunities like recognition recordings, observing music, tuning in on-line recreations, and scanning the everyday news (Orchard et al., 2014; Shin & Shin, 2011). As a consequence of such a lot of youth have a place with SNSs these destinations can possibly significantly affect the social and mental improvement of youth who use them (e.g., relationship quality and prosperity; Kross et al., 2013; Kuss & Griffiths, 2011; Liu & Yu, 2013; Reinecke & Trepte, 2014) of the extra basic SNSs inside of the U.S. are Facebook and Twitter.

Shukla et al. (2014) reported that pernicious programs get transmitted into the PC system while not the information of its clients and are not good with the system. Once the PC programs are run, the infections get flowed along the edge of the programs and begin tainting related programs that acquire its contacts. There exists a potential risk of distinctive associated systems, acquiring contaminated as well. Malware will develop on a system just because of the interconnectivity of workstations. Such developments are frequently hazardous if the PCs have important data which may get undermined by infections as an after effect of all hubs inside of the system are in the end tainted. To clean the system, antivirus bundle is utilized to dispose of infections in a tainted system of hubs and safeguard distinctive hubs by diagnostic them, the insurance being administered by bundle with a steady rate that is generally blessing inside of the system (Hachman, 2012).

3. Methodology

3.1. Participants

The volunteer participants used in this study consisted of a total of 99. About 54% male and 45% female students participated in the survey study. The age group with 18-20 years old had 25.25%, 21-23 years old have 34.35%, 24-26 years old have 21.21% and 27+ years old have 19.19%. The demographic information about the students i s presented in Table 1.

Table 1: Demographic information of participants (N = 99)

Characteristic	Frequency	%
Gender		
Male	54	54.46
Female	45	45.45
Age		
18-20	25	25.25
21-23	34	34.35
24-26	21	21.21
27+	19	19.19

3.2 Instruments

The questionnaire used in this study was developed by Cavus and Ercag (2014), is made up of 4 dimensions Social Networking Site (SNS), Malicious Software (MS), Web Security and Social Engineering (WSS) and Computer Security (CS) which had 35 items altogether in total. In SNS, 12 items were assigned to it, in order to address the various security problems that arise or may arise from the use of social networking sites which had Cronbach alpha of 0.68. In MS, 9 items were assigned to it, in order to address the various malicious software issues that may arise from using the Internet or computer by students which had Cronbach alpha of 0.71. In WSS, 8 items were assigned to address the various web security and social engineering issues that may arise from the use of the Internet for emails, online shopping etc. by the students which had Cronbach alpha of 0.65. And finally, in CS 6 items were assigned to address the various computer security issues that may possible arise from the use of the computer by the students which had Cronbach alpha of 0.71. The participants answered to items on 5 Likert Scale from "Very Confident" (5 point), "Confident" (4 point), "Neutral" (3 point), "Not Confident" (2 point), and "Not Very Confident" (1 point). Selected items were revised based upon their comments and recommendations. The questionnaire reliability was calculated as 0.72. The result from this study show that the total items and coefficient of reliability of all groups are above 0.70, hence our findings shows that the scales are reliable (Sipahi et al., 2010).

3.3. Data Analysis

A questionnaire was used to collect data and was analysed and interpreted using SPSS 20.0 version. Frequency and percentage, Independent sample t-test, ANOVA, methods were used during the analysis process.

4. Result and discussion

4.1. Students' perception towards safe internet usage

In order to understand the opinions of the students' self-efficacy and their perceptions in the use of computer and Internet security descriptive analysis was employed. From the result shown in Table 1, CS had the highest mean total highest total mean value of M = 3.93; SD = 0.05, followed by SNS with mean value of M = 3.25; SD = 0.33, and WSS had M = 3.19; SD = 0.17. While MS had M = 3.11; SD = 0.16 which the lowest total mean value. This might be due to the fact that majority of the students have more technical ideas/knowledge about computer security than every other dimension and sub-items in the questionnaire.

According to Liang and Xue (2010) the generality of Internet and computer utilization and the thin line between home and work, damages can be caused not only to organization but also to individuals due to Internet security breaches. Also user can become victim to identify hacker if their information is lost. In-relation to that unsafe and uncontrollable attitude towards the use of Internet can lead to loop holes in the user's Internet and information security. Bagachi and Udo (2003) stated that Trojan can be used to steal user's login details of his or her company.

Table 1: Total mean and standard deviation of the question

Items	Mean	SD
Social Networking Sites (SNS)		
1. To be able to hide the information that İ share on social networking sites from people.	3.23	1.48
2. To be able to block requests from people İ don't know/want on social networking sites.	3.82	1.29
3. To be able to hide my profile information from people İ don't want on social networking sites.	3.52	1.43
4. To be able to protect personal information İ share with people on social networking sites.	3.93	1.19
5. To be able to contact the necessary people if my password is taken by someone on social networking sites	3.08	1.47
6. To be able to share videos and photos on social networking sites that will not harm my reputation.	3.05	1.46
7. To be able to share information about others on social networking sites that will not harm their reputation.	3.08	1.47
8. To be able to use social networking sites like Facebook and Twitter in a safe way.	3.07	1.47
9. To be able to protect myself from infected videos on social networking sites.	3.07	1.44
10. To be able to take necessary safety precautions against security breaches on social networking sites.	3.04	1.46
11. To be able to prevent theft of personal photo albums on social networking sites.	3.02	1.48
12. To be able to create a secure password on social networking sites.	3.07	1.47
Total	**3.25**	**0.33**

Malicious Software (MS)

13. To be able to prevent harmful software from infecting your computer.	3.17	1.43
14. To be able to protect my password from key loggers.	3.26	1.19
15. To be able to clean my computer when it has been infected with viruses.	2.91	1.21
16. To be able to prevent viruses from entering my computer.	3.19	1.41
17. To be able to take the necessary precautions to prevent Trojan horses from entering my computer.	3.25	1.19
18. To be able to protect my computer from worms.	2.90	1.20
19. To be able to protect myself from spyware software.	3.17	1.43
20. To be able to create a very secure password.	3.25	1.19
21. To be able to use Microsoft Security Essentials.	2.90	1.21
Total	**3.11**	**0.16**
Web Security & Social Engineering (WSS)		
22. To be able to do shopping in a secure way via Internet.	3.32	1.45
23. To be able to take the necessary security precautions against spam e-mails.	3.39	1.21
24. To be able to protect myself from built-in camera pens and glasses from social engineering attacks.	3.03	1.27
25. To be able to protect myself from social engineering attacks via e-mails.	3.03	1.27
26. To be able to use the necessary precautions while using interactive banking on the Internet.	3.29	1.43
27. To be able to use the necessary precautions against hoax e-mails.	3.40	1.20
28. To be able to protect myself from phishing e-mails.	3.04	1.27
29. To be able to show the difference between HTTP and HTTPS.	3.03	1.27
Total	**3.19**	**0.17**
Computer Security (CS)		
30. To be able to protect my personal files.	3.85	1.17
31. To be able to take the necessary security measures for logging on to my computer.	3.92	1.19
32. To be able to add a password to my operating Windows system.	4.01	1.18
33. To be able to update my security files.	3.95	1.19
34. To be able to add a password to my files.	3.95	1.23
35. To be able to create backup files in case of problems.	3.92	1.21
Total	**3.93**	**0.05**

4.2. Difference based on gender towards safe internet usage by students

In order to understand the students' self-efficacy and perceptions of Internet and computer use between both genders independent samples *t*-test was employed. According to the Table 3, concerning the self-efficacy and user's perception towards computer and Internet security, there are statistically significant differences between genders in this study (p<.05). This result is similar to that of Genis-gruber and Gonul (2012) who reported that significant different existed on gender in relation to internet usage. However, Suri and Sharma (2013) reported there is no significant difference between genders in relation to internet usage.

Table 3: Difference between genders

	Gender	N	Mean	SD	Mean Difference	T	p
SNS	Male	54	3.65	1.03	.175	2.038	**.042***
	Female	45	3.48	1.16			
MS	Male	54	3.48	1.13	.464	4.720	**.000***
	Female	45	3.01	1.23			
WSS	Male	54	3.53	1.11	.454	4.650	**.000***
	Female	45	3.07	1.19			
CS	Male	54	3.23	1.26	.079	.787	.431
	Female	45	3.15	1.35			

* p<0.05

4.3 Difference based on Age towards safe internet usage by students

In order to understand the students' self-efficacy and perceptions of computer and Internet use between different ages, one-way ANOVA was employed. As indicated in Table 4, in this study there are statistically significant differences between in all ages towards computer and Internet security ($p<0.05$). This study shows that is difference between different age groups in relation to internet usage, however Stephen et al. (2003) reported there is no difference in age groups in relation to internet usage.

Table 4: Differences between ages

Groups	Age	N	Mean	SD	Mean Square	F	p
SNS	18-20	25	3.664	.931	3.401	3.642	**.013***
	21-23	34	3.701	1.060			
	24-26	21	3.525	1.034			
	27+	19	4.000	.930			
	Total	99	3.687	.972			
MS	18-20	25	3.673	.873	11.997	14.668	**.000***
	21-23	34	3.462	.958			
	24-26	21	3.606	.998			
	27+	19	4.320	.872			
	Total	99	3.701	.930			
WSS	18-20	25	3.627	.835	4.636	5.946	**.001***
	21-23	34	3.443	.916			
	24-26	21	3.626	1.006			
	27+	19	3.920	.893			
	Total	99	3.629	.892			
CS	18-20	25	3.594	.885	2.475	2.753	**.042***
	21-23	34	3.528	1.035			
	24-26	21	3.455	1.023			
	27+	19	3.853	1.062			
	Total	99	3.592	.952			

* p<0.05

5. Conclusion

According to the results of the study, students have good awareness of computer security on a general note, but specifically in terms of social networking sites, web security and malicious software, the majority of the students have little awareness of them. The study could help universities, government and parents of students, in Cyprus and in other countries, to be able to access the Internet safely.

References

Aboud, S. J. (2012). An overview of cybercrime in Iraq. *The Research Bulletin of Jordan ACM*, *2* (2), 31-34.

Baaij, E. (2012). *Safe Internet Use How a Website Can Stimulate Internet Safety.* Master Thesis, Philosophy of Science, Technology and Society Science and Technology Studies.

Bagachi, K. & Udo G. (2003) An Analysis of the Growth of Computer and Internet security Breaches. *Communications of the AIS, 12*, 684-700.

Genis-Gruber, A., Gonul, M. S. & Tas, B. K. O. (2012). Obstacles to Online Shopping: Impact of Gender and Internet Security Issues. *Dokuz Eylul Universitesi İktisadi ve İdari Bilimler Fakultesi Dergisi*, *27* (2), 27-54.

Hachman, M. (2012). Anonymous: Symantec Offered $50K for Stolen Code, Plus a Lie, *PC Magazine.* Retrieved 12/2/2012, from http://www.pcmag.com/article2/0,2817,2399912,00.asp

Hsiao, H., Tu, Y. & Chung, H. (2012). Perceived Social Supports, Computer Self-Efficacy, and Computer Use Among High School Students. *The Turkish Online Journal of Educational Technology*, *11* (2), 167-177.

Kim, J. & Lee, J. E. R. (2011). The Facebook Paths to Happiness: Effects of the Number of Facebook Friends and Self-Presentation on Subjective Well-Being. *Cyberpsychology Behavior and Social Networking, 14* (6), 359–364.

Kross, E., Verduyn, P., Demiralp, E., Park, J., Lee, D. S. & Lin, N.(2013). Facebook Use Predicts Declines In Subjective Well-Being In Young Adults. *PLoS ONE, 8* (8), 12-24.

Kuss, D. J. & Griffiths, M. D. (2011). Online Social Networking and Addiction – A Review of the Psychological Literature. *International Journal of Environmental Research and Public Health*, *8* (9), 3528–3552.

Liang, H. & Xue, Y. (2010). East Carolina Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems,11* (7), 394-413.

Liu, C.-Y. & Yu, C.-P. (2013). Can Facebook Use Induce Well-Being? *Cyberpsychology, Behavior and Social Networking*, *16* (9), 674–678.

Orchard, L. J., Fullwood, C., Galbraith, N. & Morris, N. (2014). Individual Differences as Predictors of Social Networking. *Journal of Computer-Mediated Communication, 4*,12-19.

Reinecke, L. & Trepte, S. (2014). Authenticity and Well-Being on Social Network Sites: A Two-Wave Longitudinal Study on the Effects of Online Authenticity and the Positivity Bias in SNS Communication. *Computers in Human Behavior,30*, 95–102.

Shin, D. H. & Shin, Y. J. (2011). Why do People Play Social Network Games? *Computers in Human Behavior, 27* (2), 852–861.

Shukla, J. B., Singh, G., Shukla, P. & Tripathi, A. (2014). Modeling and Analysis of the Effects of Antivirus Software on an Infected Computer Network. *Applied Mathematics and Computation*, *227*, 11–18.

Sipahi, B., Yurtkoru, E.S. & Cinko, M. (2010). *Sosyal Bilimlerde SPSS'le Very Analizi*. Istanbul: Beta Yayinlari.

Stephen J. Cutler, Hendricks, J. & Guyer, A. (2003). Age Differences in Home Computer Availability and Use. *Journal of Gerontology*, *58* (5), 271–280.

Suri, G. & Sharma, S. (2013). The Impact of Gender on Attitude Towards Computer Technology and E-Learning: An Exploratory Study of Punjab University, India. *International Journal of Engineering Research, 2* (2), 132-136.