REFERENCES

Ahlan, A. R. and Lubis, M. 2011. "Information security awareness in university: Maintaining learnability, performance and adaptability through roles of responsibility". *In Information Assurance and Security (IAS),* 2011 7th *International Conference on* (pp. 246-250). IEEE.

Allen, J. H. and Westby, J. R. 2007. "Characteristics of Effective Security Governance". EDPAC: The EDP Audit, Control, and Security Newsletter, 35(5), PP. 1-17.

Albrechtsen, E. 2007. "A qualitative study of users' view on information security". *Computers & security*, 26(4), PP. 276-289.

Alnatheer, M., Chan, T. and Nelson, K. 2012. "Understanding And Measuring Information Security Culture". *PACIS. Pacific Asia Conference on Information Systems.*P. 144. 7-15-2012.

Alnatheer, M. A. 2012. "Understanding and measuring information security culture in developing countries: case of Saudi Arabia". PhD Thesis.

Aiman-Smith, L., and Markham, S. K. 2004. "What you should know about using surveys". *Journal of Research-Technology Management.* Vol 47(3), pp. 12-15.

Alshomrani, M. and Mehdim, M. 2012. "The Importance and Dilemmas of Education In Information System". WIAR 2012. *National Workshop on Information Assurance Research, Proceedings of.* VDE. PP. 1-5.

Alfawaz, S. Nelson, K. and Mohannak, K. 2010. "Information security culture: A behaviour Compliance Conceptual Framework". *Proceedings of the Eighth Australasian Conference on Information Security-Volume* 105. *Australian Computer Society, Inc.* PP. 47-55.

Bada, M., and Sasse, A. 2014. "Cyber Security Awareness Campaigns Why do they fail to change behaviour?". *Global Cyber Security Capacity Centre: Draft Working Paper.*

Bozic, G. 2012. "The role of a stress model in the development of information security culture". *In MIPRO, 2012 Proceedings of the 35th International Convention* (pp. 1555-1559). IEEE.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness". *MIS quarterly,* 34(3), PP. 523-548.

Bernard, H. R. 2011. "Research methods in anthropology: Qualitative and quantitative approaches". *Rowman Altamira*. ISBN. 978-0-7591-1243-8.

Brynjolfsson, E. (1994). "Information assets, technology and organisation". *Management Science*, 40(12), pp. 1645-1662.

Burn, R.B., 2000. "*Introduction to research method*". Australia: Longman

Chou, C. Y. 2013. "The Influence of Personality and Organisational Citizenship Behaviours on Information Security Awareness: A case study of District Office of New Taipei City Government". Shih Hsin University Department of Public Policy and Management. Master Thesis.

Chen, C. C., Medlin, D. B., and Shaw, R. S. 2008. "A cross-cultural investigation of situational information security awareness programs". *Information management & computer security,* 16(4), pp. 360-376.

Cone, B. D., Irvine, C. E., Thompson, M. F., and Nguyen, T. D. 2007. "A video game for cyber security training and awareness". *Computers & security*, 26(1), pp. 63-72.

Cortina, J. M. 1993."What is coefficient alpha? An examination of theory and applications". *Journal of applied psychology*, Vol 78(1), pp. 98-104.

Colwill, C. 2009. "Human factors in information security: The insider threat–Who can you trust these days?". *Information security technical report*. Vol. 14. pp. 186-196.

Chan, M., Woon, I., and Kankanhalli, A. 2005. "Perceptions of information security in the workplace: linking information security climate to compliant behaviour". *Journal of Information Privacy and Security*, 1(3), pp. 18-41.

Cavana, R., Delahaye, B. L., & Sekeran, U. 2001. "Applied business research: Qualitative and quantitative methods". John Wiley & Sons Australia. ISBN, 0471341266.

Da Veiga, A., Martins, N., and Eloff, J. H. 2007. "Information security culture-validation of an assessment instrument". *Southern African Business Review*, 11(1), pp. 147-166.

Darvishi, M. 2013. "An analysis on security awareness of social networks users". Universiti Teknologi Malaysia, Faculty of Computer Science and Information System. *Master thesis of Computer Science (Information Security)*.

Doherty, N. F., Anastasakis, L., and Fulford, H. 2009. "The information security policy unpacked: A critical study of the content of university policies". *International Journal of Information Management*, 29(6), pp. 449-457.

Da Veiga, A. and J. H. Eloff. 2010. "A framework and Assessment Instrument for Information Security Culture". *Computers & Security*. Vol. 29. pp. 196-207.

Furnell, S., and Evangelatos, K. 2007. "Public Awareness and Perceptions of Biometrics". *Computer Fraud & Security*, 2007, 1, pp. 8-13.

Fakeh, S. K. W., Zulhemay, M. N., Shahibi, M. S., Ali, J., and Zaini, M. K. 2012. "Information Security Awareness Amongst Academic Librarians". *Journal of Applied Sciences Research*, 8(3), pp. 1723-1735.

Furnell, S., and Thomson, K. L. 2009. "From culture to disobedience: Recognising the varying user acceptance of IT security". *Computer Fraud & Security*, 2009(2), pp. 5-10.

Field, A. 2009. "Discovering Statistics using SPSS". (3rd ed.). Third edition Thousand Oaks, CA: Sage Publishing. ISBN, 978-1-84787907-3.

Fowler, F. J., Jr. 2009. "Survey research methods". (4th ed.). Los Angeles, CA: Sage. ISBN, 979-1-4129-5841-7.

Gerber, S. B., & Finn, K. V. 2005. "Using SPSS for Windows: Data analysis and graphics". Springer Science & Business Media. ISBN. 0-387-40083-4

Grant, G. J. 2010." Ascertaining the relationship between security awareness and the security behaviour of individuals". *Nova Southeastern University*. ISBN. 978-1-124-23641-4.

Guttman, B., and Roback, E. 1995. "An introduction to computer security: the NIST handbook". DIANE Publishing. NIST Special Publication. 800 - 12.

Goel, S., and Chengalur-Smith, I. N. 2010. "Metrics for characterizing the form of security policies". *The Journal of Strategic Information Systems*, 19(4), pp. 281-295.

Guo, K. H. 2013. "Security-Related Behaviour in Using Information Systems in the Workplace: A review and Synthesis". *Computers & Security*. Vol. 32. pp. 242-251.

Gupta, M., and Sharman, R. 2012. "Determinants of Data Breaches: A Categorization Based Empirical Investigation". *Journal of Applied Security Research*, 7(3), pp. 375-395.

Halim, A. Abu Bakar, A. Hamid, H. and Alwi, N. 2008. "A Study of Information Security Awareness Among USIM Staff". Technical Report. USIM.

Huang, D. L., Patrick Rau, P. L., Salvendy, G., Gao, F., and Zhou, J. 2011. "Factors affecting perception of information security and their effects on IT adoption and security practices". *International Journal of Human-Computer Studies*, 69(12), pp. 870-883.

Hight, S. D. 2005. "The importance of a security, education, training and awareness program", November 2005. http://www.infosecwriters.com/text resources/pdf/SETA SHight.pdf.

Hussein, R., Lambensa, F and Anom, R. B. 2011. "Information security behaviour: a descriptive analysis on a Malaysian public university". *Symposium on Information & Computer Sciences* (ICS 2011). pp. 59-61.

Haeussinger, F. and Kranz, J. 2013. "Information security awareness: Its antecedents and mediating effects on security compliant behaviour", in Proceedings of 2013 *International Conference on Information Systems (ICIS), Italy, San Milan*. Paper 1149.

Hair, J. F., Money, A. H., Samouel, P. and Page, M. 2007. "Research methods for business". Education+ Training, Vol. 49 Iss: 4, pp.336 - 337.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. 2006. "Multivariate data analysis (Vol. 6)". Upper Saddle River, NJ: Pearson Prentice Hall. ISBN, 0130329290.

Hair, J. F., Anderson, R. E., Tatham, R. L., & William, C. 1998. Black 1998. "Multivariate data analysis". ISBN. 0139305874.

Hazari, S., Hargrave, W., & Clenney, B. 2008. "An empirical investigation of factors influencing information security behaviour". *Journal of Information Privacy and Security*, *4*(4), pp. 3-20.

Humaidi, N., and Balakrishnan, V. 2012. "The influence of security awareness and security technology on users' behaviour towards the implementation of health information system: a conceptual framework". *In Proceeding of international conference on management and artificial intelligence, Singapore*. Vol. 35, pp. 1-6.

Ishak, I.S., Ishak, I.S., Abu Hassan, R., Suradi, Z., and Mansor, Z. 2014. "Information Security Awareness and Practices In Malaysian IHLs: A Study at UNISEL". *DOI: 10.15224/978-1-63248-034-7-29 Conference: Second Intl. Conf. on Advances in Computing, Electronics and Electrical Technology - CEET 2014, At Kuala Lumpur.*

Ismail, Z., Masrom, M., Sidek, Z., and Hamzah, D. 2010. "Framework to Manage Information Security for Malaysian Academic Environment". *Information Assurance & Cybersecurity*, 2010, pp. 1-16.

Iles, J. 2014."Cyber Security in the UK: A critical analysis of the threat to the UK and the Government Response (National Cyber Security Strategy 2011)". *Technical Report RHUL–MA*–2014– 5 01 September 2014.

ISF. 2003. "The standard of good practice for information security". *Version 4.0. Information Security Forum.*

Jones, C. M., McCarthy, R. V., Halawi, L., and Mujtaba, B. 2010."Utilizing the technology acceptance model to assess the employee adoption of information systems security measures". *Journal of International Technology and Information Management Vol*, 19(2). pp. 43-56.

Jaw, G. Y., and Chen, J. Y. 2007. "Asian New Generation_s Perceptions Regarding Network Fraud". *In Innovative Computing, Information and Control*, 2007. ICICIC'07. Second International Conference on. pp. 278-278. IEEE.

Kvavik, R. B., and Voloudakis, J. 2003. "Information technology security: Governance, strategy, and practice in higher education". Educause.

Kreicberga, L. 2010. "Internal threat to information security: countermeasures and human factor within SME". Master Thesis, Administration and Social Sciences, Division of Information Systems Sciences. Luleå University of Technology.

Kaur, J., & Mustafa, N. 2013. "Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME". In *Research and Innovation in Information Systems (ICRIIS), 2013 International Conference on*, pp. 286-290. IEEE.

Kruger, H. A., Flowerday, S., Drevin, L., & Steyn, T. 2011. "An assessment of the role of cultural factors in information security awareness". In *Information Security South Africa (ISSA), 2011* .pp. 1-7. IEEE.

Kritzinger, E., and von Solms, S. H. 2010. "Cyber security for home users: A new way of protection through awareness enforcement". *Computers & Security*, 29(8), pp. 840-847.

Kruger, H. and W. Kearney. 2006. "A prototype for Assessing Information Security Awareness". *Computers & Security*. Vol. 25. PP. 289-296.

Kotrlik, J. Bartlett, J. & Higgins, C. 2001. "Organisational research: Determining appropriate sample size in survey research appropriate sample size in survey research". *Information technology, learning, and performance journal*, *19*(1), 43.

Lim, J. S., Chang, S., Maynard, S., and Ahmad, A. 2009. "Exploring the relationship between organisational culture and information security culture".In Australian *Information Security Management Conference* (p. 12). pp. 87-97.

Lewis, P., Thornhill, A., and Saunders, M. 2007." Research methods for business students". Pearson Education UK. ISBN. 978-0-273-71686-0.

Leech, N. L., Barrett, K. C., and Morgan, G. A. 2005. "SPSS for intermediate statistics: Use and interpretation". Psychology Press. ISBN. 0-8058-4790-1.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., and Giannakopoulos, G. 2014." The Human Factor of Information Security: Unintentional Damage Perspective". *Procedia-Social and Behavioural Sciences*, 147, pp. 424- 428.

MYCERT. 2010. "3RD Quarter 2010 Summary Report". Taken From. https://www.mycert.org.my/en/services/advisories/mycert/2015/main/detail/1074/index.html. (Accessed Date: 20 Aug, 2015).

Montesdioca, G. P. Z., and Maçada, A. C. G. 2015."Measuring user satisfaction with information security practices". *Computers & Security*, 48, pp. 267-280.

Malcolmson, J. 2009. "What is security culture? Does it Differ in Content From General Organisational Culture?". *Security Technology*, 2009. 43rd Annual 2009. *International Carnahan Conference on*. IEEE. pp. 361-366.

McIlwraith, A. 2006."Information security and employee behaviour. How to reduce risk through employee education, training and awareness". ISBN, 0566086476.

Newman, I. 1998. "Qualitative-quantitative research methodology: Exploring the interactive continuum". SIU Press. E- book. ISBN. 0-8093-2150-5.

O'BRIEN, J. E. S. S. I. C. A., Islam, S., Bao, S., Weng, F., Xiong, W., and Ma, A. 2013. "Information security culture: literature review". *Department of Computing & Information Systems. University of Melbourne*. Working Paper.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., and Jerram, C. 2014. "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)". *Computers & Security*, 42, pp.165-176.

Parsons, K., McCormac, A., Butavicius, M., and Ferguson, L. 2010. "Human factors and information security: individual, culture and security environment", (No. DSTO-TR-2484). *Defence Science and Technology Organisation Edinburgh (AUSTRALIA) Command Control Communications and Intelligence Div. Technical Report.*

Payne, S. 2003."Developing security education and awareness programs".*Educause Quarterly*, 26(4), pp. 49-53.

Pallant, J. 2013. "SPSS survival manual".McGraw-Hill International. ISBN. 9780335262595.

Quagliata, K. M. 2010. "Factors Related to Components of User Training on Perceived Security Effectiveness". Thesis Degree of Doctor of Philosophy, University of Fairfax

Rezgui, Y., and Marks, A. 2008. "Information security awareness in higher education: An exploratory study". *Computers & Security*, 27 (7), pp.241-253.

Richardson, R. 2008. "CSI computer crime and security survey". *Computer Security Institute*, 1, pp1-30.

Rhee, H. S., Kim, C., and Ryu, Y. U. 2009. "Self-efficacy in information security: Its influence on end users' information security practice behaviour". *Computers & Security*, 28 (8), pp. 816-826.

Rotvold, G. 2008. "How to Create a Security Culture in Your Organisation". *Information Management Journal*, 42 (6), pp. 32-38.

Roy Sarkar, K. 2010. "Assessing Insider Threats to Information Security Using Technical, Behavioural and Organisational Measures". *Information Security Technical Report*. Vol. 15, pp. 112-133.

Schneier, B. 2011. "Secrets and lies: digital security in a networked world". *John Wiley & Sons*. ISBN. 0-471-25311-1.

Schlienger, T., and Teufel, S. 2003. "Analyzing information security culture: increased trust by an appropriate information security culture". In Database and Expert Systems Applications, 2003. Proceedings. 14th *International Workshop on* (pp. 405-409). IEEE.

Soltanmohammadi, S., Asadi, S., and Ithnin, N. 2013. "Main human factors affecting information system security". *Interdisciplinary Journal of Contemporary Research in Business. Department of Computer Science. Faculty of Computing, Universiti Teknologi Malaysia*. 81310 Skudai, Johor. November 2013.VOL 5, NO 7. pp. 339-354.

Shahri, A. B., Ismail, Z., and Rahim, N. Z. A. 2013."Security Culture and Security Awareness as the Basic Factors for Security Effectiveness in Health Information Systems". Jurnal Teknologi, 64 (2).pp. 7-12.

Siponen, M., Mahmood, M. A., and Pahnila, S. 2014. "Employees' adherence to information security policies: An exploratory field study". *Information & Management*, 51 (2), pp. 217-224.

Siponen, M. T. 2000. "A conceptual foundation for organisational information security awareness". *Information Management & Computer Security*, *8*(1), PP. 31-41.

Schultz, E. 2004."Security Training and Awareness Fitting a Square peg in a Round Hole". *Computers & Security*, 23 (1), pp. 1-2.

Sekaran, U. 2006. "Research methods for business: A skill building approach Ed.: John Wiley & Sons. ISBN. 1428813462, 9781428813465

Sekaran, U. 2000. "Measurement: Scaling, reliability, validity Research Methods for Business". Vol. 3, PP. 196-218.

Scarfone, K., Souppaya, M., Cody, A., and Orebaugh, A. 2008. "Technical guide to information security testing and assessment". *NIST Special Publication*, *800*, 115.

Sabbagh, B. A., Ameen, M., Watterstam, T., & Kowalski, S. 2012. "A prototype For HI 2 Ping information security culture and awareness training". In *e-Learning and e-Technologies in Education (ICEEE), 2012 International Conference on* (pp. 32-36). IEEE.

Talib, S., Clarke, N. L., & Furnell, S. M. 2012. "Establishing A Personalized Information Security Culture". *International Journal of Mobile Computing and Multimedia Communications (IJMCMC)*, *3*(1), pp. 63-79.

Talib, S., Clarke, N. L., and Furnell, S. M. 2010. "An analysis of information security awareness within home and work environments". In Availability, Reliability, and Security, 2010. *ARES'10 International Conference* on (pp. 196-203). IEEE.

Tsohou, A., Kokolakis, S., Karyda, M., and Kiountouzis, E. 2008."Investigating information security awareness: research and practice gaps". *Information Security Journal: A Global Perspective*, 17(5-6), pp. 207-227.

Takemura, T. 2010."A quantitative study on Japanese workers' awareness to information security using the data collected by web-based survey. *American Journal of Economics and Business Administration*, 2(1), pp. 20- 26.

Tsohou, A., Karyda, M., Kokolakis, S., and Kiountouzis, E. 2010. "Analyzing information security awareness through networks of association". In Trust, Privacy and Security in Digital Business (pp. 227-237). Springer Berlin Heidelberg.

Vroom, C. and R. Von Solms. 2004. "Towards Information Security Behavioural Compliance". *Computers & Security*. Vol. 23. pp. 191-198.

Von Solms, R., and von Solms, S. B. 2006."Information security governance: Due care". *Computers & security*, 25(7), pp. 494-497.

Williams, A., and Ayobami, A. S. 2013."Relationship between Information Security Awareness and Information Security Threat". *International Journal of Research in Commerce, IT & Management*, VOL 3(8), pp. 115-119.

Woodhouse, S. 2007. "Information Security: End User Behaviour and Corporate Culture". Computer and Information Technology, 2007. CIT 2007. 7th IEEE *International Conference* on. IEEE. pp. 767-774.

Wilson, M., and Hash, J. 2003."Building an information technology security awareness and training program". NIST Special publication, 800, 50.

Wang, Z. and H. Zeng. 2010. "Study on the Risk Assessment Quantitative Method of Information Security". Advanced Computer Theory and Engineering (ICACTE), (2010) 3rd International Conference on. IEEE. pp. V6-529-533.

Yin, R. K. 2003. "Case Study Research, Design and Methods". Sage Publications, Newbury Park, 3rd edition. ISBN. 076192552X, 9780761925521.

Zanoon, N., and Gharaibeh, N. 2013. "The effect of customer knowledge on the security of e-banking". Vol. 7. pp. 81-92.

Zakaria, O. (2004, November). "Understanding Challenges of Information Security Culture: A Methodological Issue". In *AISM* (pp. 83-93).

APPENDIX: A
Pilot Study Questionnaire

COMPARING SECURITY PRACTICES OF WORKPLACE AND HOME: A CASE FOR USIM STAFF

1-Survey purpose:

This survey intent to elicit employee's information security awareness and practice besides their attitudes on information security issues. The use of this survey is to study the information security, behavioural content in general, and attitude and opinions of employees towards information security in particular. Thank you for agreeing to take part in this important survey measuring information security awareness and practice. Today we will be gaining your thoughts and opinions about information security. This survey should take 10 minutes to complete the answer. Be assured that all answers you provide will be kept in the strictest confidentiality.

2- Instruction:-

You are expected to answer all questions base on your knowledge with the options provided. Your contribution to this research is appreciated; thanks for being part of the study.

Contact address: hamida2013@yahoo.com

SECTION A: Personal information

1-Gender

○ Male ○ Female

2-Age

○ Below 19 ○20-24 ○ 25-29 ○30-34 ○35-39 ○40 and above

3-Ethnicity

○ Malay ○Indian ○Chinese ○ Others

4- **Highest Education level**

○ Certificate (ex, Spm, Stpm) ○Diploma ○Bachelor ○Master ○PhD

5- **Your job role is**

○ Academic staff ○Administration staff

SECTION B: INFORMATION SECURITY AWARENESS BACKGROUND

Q1:

How you rate yourself on the information security culture

1 Very Low	2 Low	3 Moderate	4 High	5 Very High

Q2: The following terms related to information security threats. For each one, please indicate whether:

1- I know it
2- I do not know it

Information Security terms	I know it	I do not know it
Virus / Worm		
Spam		
Social engineering (Phishing)		
Trojan horse		
Denial of service		
Identity theft		
Hackers		

Q3: Do you install both firewall and antivirus at home and work computer?

Option	Work computer	Home computer
Yes, I install both		
Antivirus only		
Firewall only		
I do not know what antivirus and firewall is.		

Q4:

My computer is not important to hackers, they do not target me

1 Strongly Disagree	2 Disagree	3 Neither disagree, agree	4 Agree	5 Strongly agree

Q5:

You receive an email from an unknown sender, which contains an attachment. This surely can cause threat to information security system

1 Strongly Disagree	2 Disagree	3 Neither disagree, agree	4 Agree	5 Strongly agree

Q6:

When you delete a file from your computer or USB stick, you cannot recover that information again.

1 Strongly Disagree	2 Disagree	3 Neither disagree, agree	4 Agree	5 Strongly agree

Q7:

I think it is ok to share your password with somebody else

1 Strongly Disagree	2 Disagree	3 Neither disagree, agree	4 Agree	5 Strongly agree

Q8: Are you using the same computer password at work and home?

- Yes
- No

Q9: Have you heard of the security team at USIM known as USIM CERT?

- Yes
- No
- I do not have an idea.

Q10: Have you attended security training course lately?

- Yes
- No

Q11: Can you use your own personal devices, such as home computer or mobile phone, to store or transfer confidential university information?

- Yes
- No

Q12: In your workplace, do you have policies on internet websites which you can visit?

- No
- Yes

SECTION C: INFORMATION SECURITY PRACTICESAT WORKPLACE AND HOME

Q13: To what extent do the following statements are applied to you (Each statement requires a response) (Always, Sometimes, Never) When using computer systems in my workplace

	Always	Sometimes	Never
I log off my computer whenever I leave a computer system			
I backup my data on disks or CDs			
I click on hyperlinks in unsolicited/spam email messages and unknown websites			
I report security incidents to the IT helpdesk as soon as possible			
I do download or install unauthorized copies of software			
I do not open and execute an executable file (.exe file) from an email attachment			
I use an encryption key to protect my wireless connection			
My password consists of at least 8 characters and uses the combination of letters (a-z), symbols (!@#$%) and numbers (0-9)			
I write down my password in order to remember it			
I keep my password secret, I do not share it with anyone			
I change my password regularly			
I normally use simple password for my work computer at home			
I allow a web browser (e.g. Internet Explorer(IE)/Mozilla Firefox) to save my user id(s) and passwords for faster access			
I make sure an antivirus software is enabled and updated			
I scan with antivirus any external disk/thumb drive /USB driver before plugging it into computer systems.			
I use the organisation's firewall protection			

Q14: To what extent do the following statements are applied to you (Each statement requires a response) (Always, Sometimes, Never) When using computer systems in my house

	Always	Sometimes	Never
I log off my computer whenever I leave a computer system			
I backup my data on disks or CDs			
I click on hyperlinks in unsolicited/spam email messages and unknown websites			
I report security incidents to the IT helpdesk as soon as possible			
I do download or install unauthorized copies of software			
I do not open and execute an executable file (.exe file) from an email attachment			
I use an encryption key to protect my wireless connection			
My password consists of at least 8 characters and uses the combination of letters (a-z), symbols (!@#$%) and numbers (0-9)			
I write down my password in order to remember it			
I keep my password secret, I do not share it with anyone			
I change my password regularly			
I normally use simple password for my work computer at home			
I allow a web browser (e.g. Internet Explorer(IE) /Mozilla Firefox) to save my user id(s) and passwords for faster access			
I make sure an antivirus software is enabled and updated			
I scan with antivirus any external disk/thumb drive /USB driver before plugging it into computer systems.			
I use the personal firewall protection			

Question End.

Thank you for your time answering the survey. God bless.

APPENDIX: B

RESEARCH SURVEY

COMPARING SECURITY PRACTICES OF WORKPLACE AND HOME: A CASE FOR USIM STAFF

Name: Hamida Omer Issa Asker

Faculty of Science and Technology

Master of Computer Science via Mixed Mode in Information Security and Assurance

My name is Hamida Omer and I am Masters Student at the Universitit Sains Islam Malaysia (USIM). For my research project, I am evaluating information security awareness and practices among USIM staff both on their workplace and home. Therefore, I am inviting you to participate on this research by completing the attached questionnaire. This questionnaire requires 10 minutes to complete. We will assure all provided answers you provided will be kept in the strictest confidentiality. This questionnaire consists of three main sections answer all provided questions.

Thank you for taking time to assist me in my educational endeavors

Contact details:

(0182042025)

(hamida2013@yahoo.com

Supervisor:

Dr. Mohd Zalisham Zali.

(Zalisham@usim.edu.my)

SECTION A: (About yourself)

1-Gender:

○Male ○ Female

2-Age:

○Below 20 ○ 20-24 ○ 25-29 ○ 30-34 ○ 35-39 ○ 40 and above

3-Race:

○ Malay ○ Indian ○ Chinese ○ Others

4- Highest Education Level:

○ Certificate (eg, SPM, STPM, etc) ○ Diploma ○ Bachelor ○ Master

○ PhD

5- Your Main Job Role:

○ Academic staff ○ Administration staff

SECTION B: (Information Security Awareness and Practice.)

These questions related to Security Awareness

	Security Awareness	Workplace			Home		
	Elements	No	Not Sure	Yes	No	Not Sure	Yes
1	I am aware with the vulnerabilities associated with sharing devices.						
2	I am aware with the encryption that can prevent unauthorized access to confidential information.						
3	I am aware that it is important to back up my files.						
4	I am aware that information security is necessary to protect my information.						
5	I am aware with virus protection software that requires frequent updates.						

These questions related to <u>Security Practice</u>

	Security Practice	Workplace			Home		
	Elements	No	Not Sure	Yes	No	Not Sure	Yes
1	I log off my computer whenever I leave it.						
2	I regularly backup my data.						
3	I do not download or install unauthorized copies of software.						
4	I make sure the antivirus software is enabled and updated.						
5	I use firewall protection						

<u>SECTION C:</u> (Factors effecting information security awareness and practice in the workplace and home.)

These questions related to <u>Policy Factor</u>

	Policy Factors	Workplace			Home		
	Elements	No	Not Sure	Yes	No	Not Sure	Yes
1	Team related to security is needed.						
2	I know who to contact if my computer is hacked or infected.						
3	The firewall on my computer is always enabled.						
4	My computer is configured to automatically update.						
5	I have policies on which websites I am allowed to visit.						

These questions related to <u>Behaviour Factor</u>

	Behaviour Factors	Workplace			Home		
	Elements	No	Not Sure	Yes	No	Not Sure	Yes
1	I'll make sure that when I delete a file from the computer or USB stick, that the information is totally removed.						
2	I feel that my PC is safe.						
3	I often take information from the office and use a computer at home to work on it.						
4	I do not share my password.						
5	I use the same password both for work and home accounts.						

These questions related to <u>Training factor</u>

	Training Factors			
	Elements	No	Not Sure	Yes
1	I attended security training course lately.			
2	I receive adequate information security training.			
3	Training make me more aware (increase my awareness).			
4	Training promotes security awareness.			
5	Training promotes security practices.			

These questions related to <u>Knowledge of IT Factor</u>

	Knowledge of IT Factors	Workplace			Home		
	Elements	No	Not Sure	Yes	No	Not Sure	Yes
1	I have installed, updated, and enabled, antivirus software on my computer.						
2	I know what the risk is when opening e-mails from unknown senders; especially if there is an attachment.						
3	I know what an email scam is and how to identify it.						
4	I know how to use antivirus software and how to scan for viruses.						

These questions related to <u>Education Factor</u>

	Education Factors	Workplace			Home		
	Elements	No	Not Sure	Yes	No	Not Sure	Yes
1	I know what social engineering (phishing) attack is.						
2	I know what to do if my computer is infected with a virus.						
3	I never found a virus or a Trojan on my computer.						
4	My computer has no value to hackers, they do not target me.						
5	I always download and install software on my computer.						

Question End.

Thank you for your time answering the survey. God bless

APPENDIX: C

Statistical Analysis

Security Awareness at workplace

Reliability Statistics

Cronbach's Alpha	N of Items
.758	5

Security practice at workplace

Reliability Statistics

Cronbach's Alpha	N of Items
.738	5

Policy factor at workplace

Reliability Statistics

Cronbach's Alpha	N of Items
.736	5

Behaviour factor at workplace

Reliability Statistics

Cronbach's Alpha	N of Items
.724	5

Training factor

Reliability Statistics

Cronbach's Alpha	N of Items
.704	5

Knowledge of IT factor workplace

Reliability Statistics

Cronbach's Alpha	N of Items
.810	4

Education factor workplace

Reliability Statistics

Cronbach's Alpha	N of Items
.715	5

Security Awareness at home

Reliability Statistics

Cronbach's Alpha	N of Items
.746	5

Security practice at home

Reliability Statistics

Cronbach's Alpha	N of Items
.702	5

Policy factor at home

Reliability Statistics

Cronbach's Alpha	N of Items
.702	5

Behaviour factor at home

Reliability Statistics

Cronbach's Alpha	N of Items
.712	5

Knowledge of IT factor at home

Reliability Statistics

Cronbach's Alpha	N of Items
.714	4

Education factor at home

Reliability Statistics

Cronbach's Alpha	N of Items
.723	5

• Regression analysis security awareness at workplace and factors (policy, behaviour, training, knowledge of technology and education)

Descriptive Statistics

	Mean	Std. Deviation	N
Awareness workplace	2.71	.430	285
Policy workplace	2.65	.443	285
Behaviour workplace	2.66	.427	285
Knowledge workplace	2.72	.469	285
Education workplace	2.63	.440	285
Training	2.43	.589	285

Correlations

		Awareness workplace	Policy workplace	Behaviour workplace	Knowledge workplace	Education workplace	Training
Pearson Correlation	Awareness workplace	1.000	.684	.593	.655	.677	.376
	Policy workplace	.684	1.000	.629	.666	.816	.526
	Behaviour workplace	.593	.629	1.000	.550	.619	.406
	Knowledge workplace	.655	.666	.550	1.000	.681	.435
	Education workplace	.677	.816	.619	.681	1.000	.571
	Training	.376	.526	.406	.435	.571	1.000
Sig. (1-tailed)	Awareness workplace		.000	.000	.000	.000	.000
	Policy workplace	.000	.	.000	.000	.000	.000
	Behaviour workplace	.000	.000	.	.000	.000	.000
	Knowledge workplace	.000	.000	.000	.	.000	.000
	Education workplace	.000	.000	.000	.000	.	.000
	Training	.000	.000	.000	.000	.000	.
N	Awareness workplace	285	285	285	285	285	285
	Policy workplace	285	285	285	285	285	285
	Behaviour workplace	285	285	285	285	285	285
	Knowledge workplace	285	285	285	285	285	285
	Education workplace	285	285	285	285	285	285
	Training	285	285	285	285	285	285

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.759[a]	.576	.569	.283

a. Predictors: (Constant), Training, Behaviour workplace, Knowledge workplace, Policy workplace, Education workplace

b. Dependent Variable: Awareness workplace

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	30.315	5	6.063	75.910	.000[b]
	Residual	22.284	279	.080		
	Total	52.600	284			

a. Dependent Variable: Awareness workplace

b. Predictors: (Constant), Training, Behaviour workplace, Knowledge workplace, Policy workplace, Education workplace

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta			Lower Bound	Upper Bound	Zero-order	Partial	Part
1	(Constant)	.467	.119		3.914	.000	.232	.702			
	Policy workplace	.242	.070	.249	3.452	.001	.104	.379	.684	.202	.135
	Behaviour workplace	.182	.053	.180	3.444	.001	.078	.285	.593	.202	.134
	Knowledge workplace	.251	.051	.274	4.899	.000	.150	.353	.655	.281	.191
	Education workplace	.211	.073	.216	2.895	.004	.068	.355	.677	.171	.113
	Training	-.052	.035	-.071	-1.471	.142	-.121	.017	.376	-.088	-.057

a. Dependent Variable: Awareness workplace

- Regression analysis security practice at workplace and factors (policy, behaviour, training, knowledge of technology and education)

Descriptive Statistics

	Mean	Std. Deviation	N
Practice workplace	2.65	.447	285
Policy workplace	2.65	.443	285
Behaviour workplace	2.66	.427	285
Training	2.43	.589	285
Knowledge workplace	2.72	.469	285
Education workplace	2.63	.440	285

Correlations

		Practice workplace	Policy workplace	Behaviour workplace	Training	Knowledge workplace	Education workplace
Pearson Correlation	Practice workplace	1.000	.696	.582	.484	.606	.682
	Policy workplace	.696	1.000	.629	.526	.666	.816
	Behaviour workplace	.582	.629	1.000	.406	.550	.619
	Training	.484	.526	.406	1.000	.435	.571
	Knowledge workplace	.606	.666	.550	.435	1.000	.681
	Education workplace	.682	.816	.619	.571	.681	1.000
Sig. (1-tailed)	Practice workplace	.	.000	.000	.000	.000	.000
	Policy workplace	.000	.	.000	.000	.000	.000
	Behaviour workplace	.000	.000	.	.000	.000	.000
	Training	.000	.000	.000	.	.000	.000
	Knowledge workplace	.000	.000	.000	.000	.	.000
	Education workplace	.000	.000	.000	.000	.000	.
N	Practice workplace	285	285	285	285	285	285
	Policy workplace	285	285	285	285	285	285
	Behaviour workplace	285	285	285	285	285	285
	Training	285	285	285	285	285	285
	Knowledge workplace	285	285	285	285	285	285
	Education workplace	285	285	285	285	285	285

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.750[a]	.562	.554	.298

a. Predictors: (Constant), Education workplace, Training, Behaviour workplace, Knowledge workplace, Policy workplace
b. Dependent Variable: Practice workplace

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	31.876	5	6.375	71.561	.000[b]
	Residual	24.856	279	.089		
	Total	56.732	284			

a. Dependent Variable: Practice workplace
b. Predictors: (Constant), Education workplace, Training, Behaviour workplace, Knowledge workplace, Policy workplace

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta			Lower Bound	Upper Bound	Zero-order	Partial	Part
1	(Constant)	.355	.126		2.812	.005	.106	.603			
	Policy workplace	.291	.074	.289	3.936	.000	.145	.437	.696	.229	.156
	Behaviour workplace	.168	.056	.160	3.009	.003	.058	.277	.582	.177	.119
	Training	.069	.037	.091	1.861	.064	-.004	.142	.484	.111	.074
	Knowledge workplace	.151	.054	.158	2.784	.006	.044	.258	.606	.164	.110
	Education workplace	.191	.077	.188	2.474	.014	.039	.343	.682	.147	.098

a. Dependent Variable: Practice workplace

- Regression analysis security awareness at home and factors (policy, behaviour, training, knowledge of technology and education)

Descriptive Statistics

	Mean	Std. Deviation	N
Home awareness	2.70	.424	285
Home Policy	2.45	.499	285
Home behaviour	2.62	.453	285
Training	2.43	.589	285
Home Knowledge	2.62	.475	285
Home Education	2.63	.443	285

Correlations

		Home awareness	Home Policy	Home behaviour	Training	Home Knowledge	Home Education
Pearson Correlation	Home awareness	1.000	.344	.479	.397	.448	.630
	Home Policy	.344	1.000	.213	.446	.035	.480
	Home behaviour	.479	.213	1.000	.352	.368	.548
	Training	.397	.446	.352	1.000	.130	.635
	Home Knowledge	.448	.035	.368	.130	1.000	.364
	Home Education	.630	.480	.548	.635	.364	1.000
Sig. (1-tailed)	Home awareness	.	.000	.000	.000	.000	.000
	Home Policy	.000	.	.000	.000	.277	.000
	Home behaviour	.000	.000	.	.000	.000	.000
	Training	.000	.000	.000	.	.014	.000
	Home Knowledge	.000	.277	.000	.014	.	.000
	Home Education	.000	.000	.000	.000	.000	.
N	Home awareness	285	285	285	285	285	285
	Home Policy	285	285	285	285	285	285
	Home behaviour	285	285	285	285	285	285
	Training	285	285	285	285	285	285
	Home Knowledge	285	285	285	285	285	285
	Home Education	285	285	285	285	285	285

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.688[a]	.473	.463	.310

a. Predictors: (Constant), Home Education, Home Knowledge, Home Policy, Home behaviour, Training

b. Dependent Variable: Home awareness

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	24.117	5	4.823	50.043	.000[b]
	Residual	26.892	279	.096		
	Total	51.010	284			

a. Dependent Variable: Home awareness

b. Predictors: (Constant), Home Education, Home Knowledge, Home Policy, Home behaviour, Training

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta			Lower Bound	Upper Bound	Zero-order	Partial	Part
1	(Constant)	.525	.148		3.560	.000	.235	.816			
	Home Policy	.090	.044	.106	2.062	.040	.004	.176	.344	.123	.090
	Home behaviour	.131	.050	.140	2.623	.009	.033	.229	.479	.155	.114
	Training	.008	.042	.011	.182	.855	-.075	.090	.397	.011	.008
	Home Knowledge	.217	.044	.243	4.995	.000	.132	.303	.448	.287	.217
	Home Education	.389	.066	.407	5.942	.000	.260	.518	.630	.335	.258

a. Dependent Variable: Home awareness

- Regression analysis security practice at home and factors (policy, behaviour, training, knowledge of technology and education)

Descriptive Statistics

	Mean	Std. Deviation	N
Home Practice	2.64	.444	285
Home Policy	2.45	.499	285
Home behaviour	2.62	.453	285
Training	2.43	.589	285
Home Knowledge	2.62	.475	285
Home Education	2.63	.443	285

Correlations

		Home Practice	Home Policy	Home behaviour	Training	Home Knowledge	Home Education
Pearson Correlation	Home Practice	1.000	.426	.512	.402	.447	.670
	Home Policy	.426	1.000	.213	.446	.035	.480
	Home behaviour	.512	.213	1.000	.352	.368	.548
	Training	.402	.446	.352	1.000	.130	.635
	Home Knowledge	.447	.035	.368	.130	1.000	.364
	Home Education	.670	.480	.548	.635	.364	1.000
Sig. (1-tailed)	Home Practice	.	.000	.000	.000	.000	.000
	Home Policy	.000	.	.000	.000	.277	.000
	Home behaviour	.000	.000	.	.000	.000	.000
	Training	.000	.000	.000	.	.014	.000
	Home Knowledge	.000	.277	.000	.014	.	.000
	Home Education	.000	.000	.000	.000	.000	.
N	Home Practice	285	285	285	285	285	285
	Home Policy	285	285	285	285	285	285
	Home behaviour	285	285	285	285	285	285
	Training	285	285	285	285	285	285
	Home Knowledge	285	285	285	285	285	285
	Home Education	285	285	285	285	285	285

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.736[a]	.541	.533	.303

a. Predictors: (Constant), Home Education, Home Knowledge, Home Policy, Home behaviour, Training
b. Dependent Variable: Home Practice

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	30.271	5	6.054	65.896	.000[b]
	Residual	25.633	279	.092		
	Total	55.904	284			

a. Dependent Variable: Home Practice

b. Predictors: (Constant), Home Education, Home Knowledge, Home Policy, Home behaviour, Training

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta			Lower Bound	Upper Bound	Zero-order	Partial	Part
1	(Constant)	.175	.144		1.216	.225	-.108	.459			
	Home Policy	.175	.043	.197	4.119	.000	.091	.259	.426	.239	.167
	Home behaviour	.163	.049	.166	3.334	.001	.067	.258	.512	.196	.135
	Training	-.037	.041	-.050	-.918	.359	-.118	.043	-.402	-.055	-.037
	Home Knowledge	.213	.043	.228	5.012	.000	.129	.297	.447	.287	.203
	Home Education	.434	.064	.434	6.792	.000	.308	.560	.670	.377	.275

a. Dependent Variable: Home Practice

Appendix D:

- Conference Letter of Acceptance
- IRED Conference Review Result

theIRED

Ref No: - IRED/14/CEET /138
Dated: 27-October -2014

Subject: Letter of Acceptance and Invitation

Dear Author (**Hamida Omer Issa Asker**),

We are pleased to inform you that after hard review process your paper entitled "**A Comparative Study on the Information Security Culture Related to Workplace and Home Practices**" with paper ID "CEET-14-245" has been accepted for Oral presentation and publication in Early Bird Round of "Second International Conference On Advances in Computing, Electronics and Electrical Technology - CEET 2014." The conference will be held at Kuala Lumpur, Malaysia during 20-21 December, 2014. We invite you to present your full research paper at the conference and please bring PPT slides of your paper for presentation at the conference as there are data projectors at the venue.

Benefits of Publication:-

- Your paper will be included in the Conference Proceedings which will be published online with ISBN and will be archived in SEEK Digital Library so that it will be universally accessed. Seek Digital Library is being accessed by thousands of Students, Researchers and Scientists over the globe. Seek Digital Library is an Open access library. You may visit the Library at www.seekdl.org.
- Each paper will be assigned Digital Object Identifier (DOI) from CROSSREF.
- Registered Papers will be published in various Issues of International Journals with ISSN Numbers.
- You will get the chance to attend the conference and to meet the researchers from the globe.

We have received more than 195 research articles for review in Early Bird Round from more than 12 countries and only 82 articles has been accepted for publication and oral presentation with acceptance ratio of 42.05%. The Review Process has gone through Peer Review Process. The Editorial Committee focused on quality research articles to maintain the credibility of the conference.

If your paper wins the 'best paper award', it would be appreciated at the closing ceremony. For more details, please visit our website http://acec.theired.org/. Please send us attached completed registration form along with payment Proof on or before 14 **November, 2014** to confirm your participation. We do not provide any assistance relating to Visa and accommodation other than this acceptance letter for Malaysia conference. We look forward to seeing you at the conference.

With Best Regards,

Elena Alikchkina
Conference Co-ordinator
IRED

IRED Conference Review Result

theIRED

CEET

Conference Name: "SECOND INTERNATIONAL CONFERENCE ON ADVANCES IN COMPUTING, ELECTRONICS AND ELECTRICAL TECHNOLOGY - CEET 2014"

Paper Title: "A COMPARATIVE STUDY ON THE INFORMATION SECURITY CULTURE RELATED TO WORKPLACE AND HOME PRACTICES."

Paper ID: "CEET-14-245"

Conference Date: 20-21 December, 2014

Official Conference Website: www.ceet.theired.org

Evaluation:

	Poor	Fair	Good	Very Good	Outstanding
Originality	○	○	○	○	○
Innovation	○	○	○	○	○
technical merit	○	○	○	○	○
applicability	○	○	○	○	○
Presentation and English	○	○	○	○	○
Match to Conference Topic	○	○	○	○	○

Recommendation to Editors

	Strongly Reject	Reject	Marginally Accept	Accept	Strong Accept
Recommendation	○	○	○	○	○

International Journal of Advances in Computer Networks and Its Security– IJCNS
Volume 5: Issue 1 [ISSN : 2250-3757]
Publication Date : 30 April, 2015

A Comparative Study on the Information Security Culture Related to Workplace and Home Practices

[Hamida Omer Issa Asker & Mohd Zalisham Jali]

Abstract— Security awareness can be practiced from various angle like within school, government-sponsored initiatives and security providers. The aim of present paper is however confined to investigating the behavior, practices and interactions at the organization level and within home environments. Therefore, the survey was conducted to assess the information security culture among workers in terms of their workplace and home practices; and to determine if a relationship exists between information security culture practices at the workplace and at home. The result demonstrated that the awareness at home and within the workplace appears to be of the same level, with negative practices are still practices insecure behavior.

Keywords— Security awareness, workplace practice, home practice.

I. Introduction

Information security threats have experienced significant evolution in terms of volume and nature, shifting from technical savvy hackers with unerring skills to organized and meticulous crackers aiming to gain financial benefits for their work [1]. Consequently, cybercrime activities have increased and end-users find themselves the recipient of threats. According to [2], more than half (52%) of firms have been threatened in 2007 alone while [3]reported that 64% of the study respondents admitted to encountering Phishing email, a threat that was not widespread 5 years ago. In this regard, user's protection has been proposed in a range of security countermeasures. These safeguarding tools constantly involve in terms of sophistication and in number to counter the evolving threats. Nevertheless, the successful operation of such tools depends upon their effective deployment, configuration and operation by end-users. More importantly, it is a well-known fact that the strength of security is only as effective as its weakest link, and the latter is, more often than not, the end user [4]. In an attempt to counter the threat experienced by end-users, increasing concentration has been directed towards information security awareness, education and information dissemination.

Hamida Omer Issa Asker
Universiti Sains Islam Malaysia (USIM)
Malaysia

Mohd Zalisham Jali
Universiti Sains Islam Malaysia (USIM)
Malaysia

In the context of the organization, efforts have been expended towards enhancing awareness among workers [2] as evidenced by the fact that 82% of enterprise firms provide training. This scenario is however not common for all companies [5] as in majority of small-to-medium companies only 40% reported to provide training. Several organizations possess the training resources if they intend to provide training but they only constitute 95% of Internet users. The remaining 5% are home-users or the general public. The concern lies on the fact that 95% of users are prone to threats and attacks [6]. On the other hand, home users have various resources to enhance their online threats awareness and they are provided with supporting information by anti-virus providers, operating system vendors, and government initiatives [1].

Moreover, despite the available training programs and initiatives at the workplace and at home respectively, research dedicated to understanding what is being relayed and where, the strategies effectiveness and the level of learning styles' role in realizing good information security practice is still few and far between. In this regard, security awareness can be viewed from various directions like within school, government-sponsored initiatives and security providers. The present paper is however confined to investigating the behavior, practices and interactions at the organization level and within home environments. The organization of this paper follows the following sequence; the current information security awareness and the security culture development are discussed in Section II, followed by the study methodology in Section III, and the presentation of study findings in Section IV. Section V provides a discussion of the main findings, while Section VI presents the conclusion and sets the direction for future studies.

II. Related Works

Both academic and commercial communities have given due attention to information security awareness in the past few years. Organizations are increasingly acknowledging the significance of their information assets and the development of effective strategies to enhance awareness within the company. This has been further supported by effective corporate governance regulation and legislation [7]. In addition, a considerable amount of studies have called for the need to develop an information security culture in the organization and to shift from surface learning to embedding good practice among workers [8, 9]. Researchers are convinced that establishing such culture in the organization, can lead to the maintenance of long-term security practice and promote awareness and education of security issues as it facilitates employee engagement of the practice.

With regards to home users, awareness raising initiatives have been proposed; for instance, [10] is a U.K. Government sponsored initiative that offers general information concerning risks and protection from threats. Such initiative offers information from guidelines to particular information concerning threats and is primarily text based information coupled with a few video files. The U.S. and other countries also have a similar national-based websites catering to awareness [11]. Several companies providing security software and operating systems also offers web-based access reading-based resources to educate and inform home users [12, 13]

Evidently, it is a challenging feat to motivate home users to employ security measures as security, although a requirement is not always the user's primary task. People often fail to understand that they need to follow security measures and those that do understand, have limited time to so. According to evidence, even when users think they are well-informed about security and self-protection, they often fall off the mark. According to a study conducted by [14], 75% of home users think they are protected from spam, but in actuality only 42% did. This gap between what they know and the actual reality demonstrates a significant gap in understanding. Good security awareness has been investigated by various studies in the hopes of creating learning mechanisms like face-to-face training sessions, email messages, online training, video game, intranet-based access and poster campaigns [15]. Studies primarily concentrated on what and how to educate workers in the organization and highlighted the significance of measuring security programs effectiveness to guarantee that education results in practice [16].

[1] identified that the majority of the learning about information security occurred in the workplace, where clear motivations, such as legislation and regulation, existed. It was also found that user's were more than willing to engage with such awareness raising initiatives. From a comparison of practice between work and home environments, it was found that this knowledge and practice obtained at the workplace was transferred to the home environment. Given this positive transferability of knowledge and the willingness to learn about how to remain secure, an opportunity exists to move away from specific organizational awareness programs and to move towards awareness raising strategies that, whilst deployed in the organization, will develop an all-round individual security culture for users independent of the environment within which they are operating.

[17] identified the ambiguous aspects of current security awareness approaches and the proposed classification provides a guide to identify the range of options available to researchers and practitioners when they design their research and practice on information security awareness.

III. Survey of End Users' Awareness and Practices

Due to the lack of literature focused on end-user awareness and practice, determining the awareness and assessing information security culture in both organization and home place is quite challenging. Additionally, it is possible to assume that most employees perceive information security culture from within the workplace and at home, but the issue lies in determining the level of the relationship between home and workplace practices that encourage a security culture. For this reason, a survey was developed for the assessment of such factors where data were collected and a quantitative method was followed. The survey's primary objectives is to conduct an assessment of the information security culture among workers in terms of workplace and home practices.

The survey is divided into three namely demographics, background of information security awareness, workplace practices and home practices. The workplace practices are geared towards examining the present practice of the workers within their place of work. The survey was distribution to random people who are employed and are regular computer uses at work and at home.

IV. Results & Findings

• Reliability Test

The reliability of the survey were measured by analyzing the questionnaire' results to obtain coefficient Cronbach alpha. The most popular test of inter item consistency reliability is the Cronbach's Coefficient Alpha. In general, reliabilities less than 0.60 are considered to be poor, those with above 0.60 ranges are acceptable, and those over 0.80 are good. The Cronbach's Alpha value of this survey is 0.759 that considered an acceptable value.

TABLE I. Reliability Statistics

Cronbach's Alpha	*N of Items*
.759	92

After analyzing the demographics, it was revealed that the majority of respondents were male workers with 76.5%, while the remaining 23.5% were female workers. Also, 41.2% of the respondents were from the age range 30-34 years and 35% of the total respondents had at least a degree level of education. This may be attributed to the author's personal contacts who were in the same age group and who have a tendency to be more IT literate or have at least an email account. Most respondents (40%) perceived themselves to be moderate in their awareness level of security culture as presented in Figure 1. It is believed that this proportion of users do not represent the general population and that this would not bias the survey results but it would provide a more informed and accurate response to the survey questions. Therefore, the results showed a positive perspective of the use and knowledge of information security existing within the population at large.

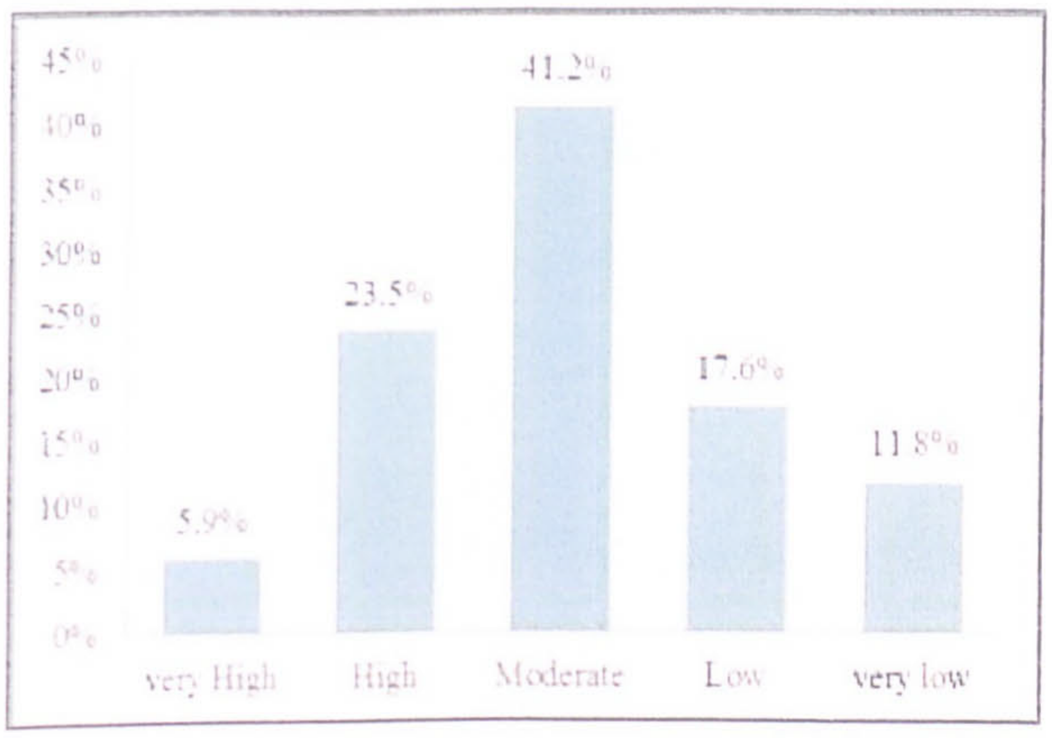

Figure 1. Level of information security awareness culture

• Information Security Awareness Background

The understanding of the information security culture of the workers entailed questions provided to them concerning the information security threats, particularly in question number 2 that is dedicated to Trojan, spam, social engineering (phishing), denial of service, identity theft and hackers. The entire respondents are aware of the virus and Trojan threat as evidenced in Figure 2.

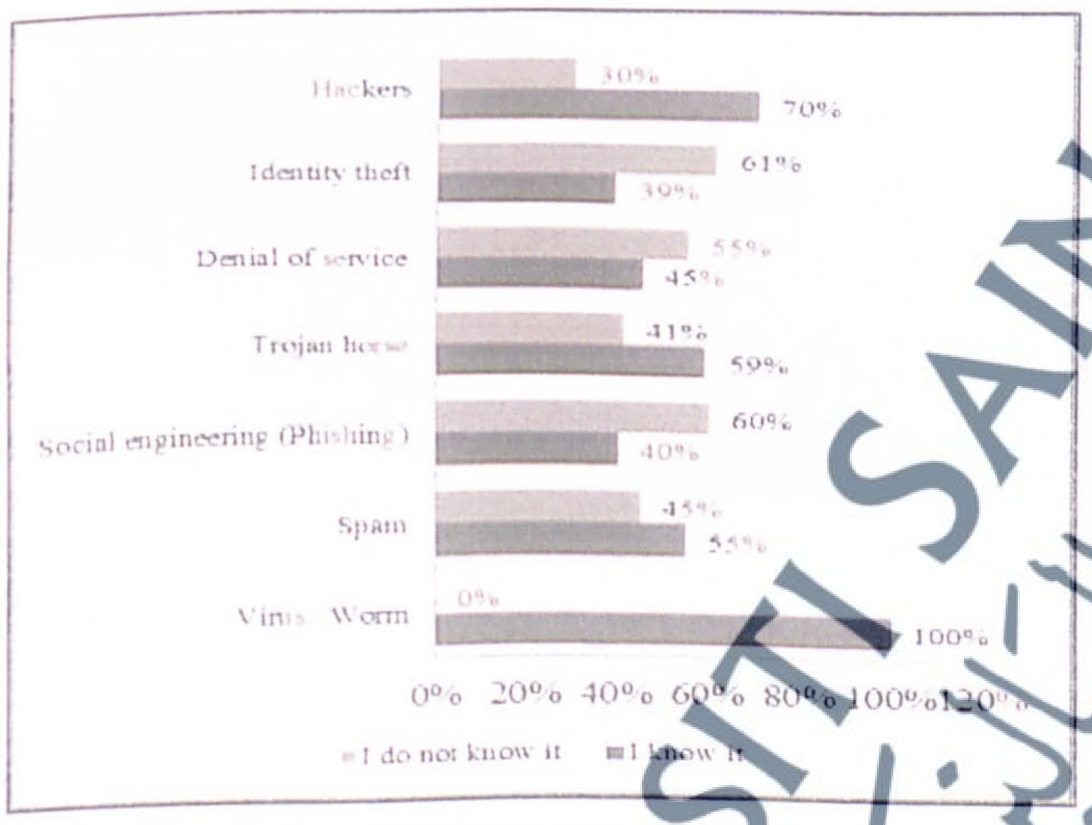

Figure 2. Security threats awareness

- Installing Antivirus

All the respondents (100%) have antivirus in their home computers, indicating that they are all aware of the virus/worm threats and they employ the required safeguard (installing antivirus).

TABLE II. USING ANTIVIRUS AT HOME

	Percent	*Valid Percent*	*Cumulative Percent*
Valid yes	100.0	100.0	100.0

• Information Security Practices at Workplace

With regards to the workplace, the respondents were requested to respond to several questions dedicated towards understanding common security practices. Questions pertaining to these practices are divided into general security practices, practices related to password and security practices related to antivirus and firewall the chosen for these practices it is the common simple practices that could be understood from the respondents.

- General Security Practices

This covers the practice of logging off computers whenever they are using a computer system where 71% of the respondents claim to do so, and steering clear of executable files received in their emails, a practice done by 77% of the respondents (see Figure 3).

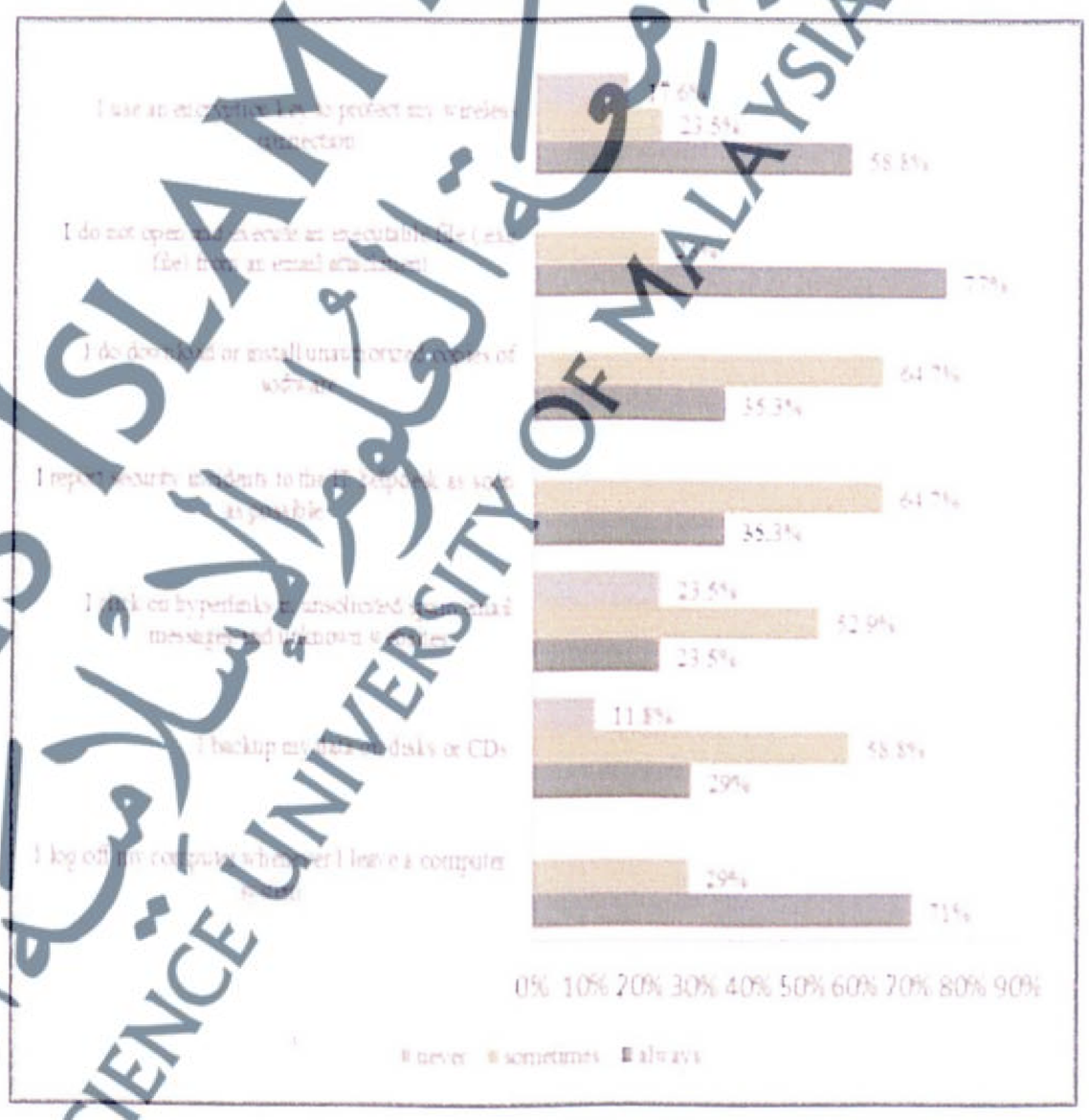

Figure 3. General security practices

- Practices Related To Password

These practices include the use of passwords comprising of at least 8 characters and the use of combined letter (a-z) symbols (!@#$%), where 64.7% of the respondents claim to do so, and keeping passwords confidential - a practice followed by 64.7% of the respondents (see Figure 4).

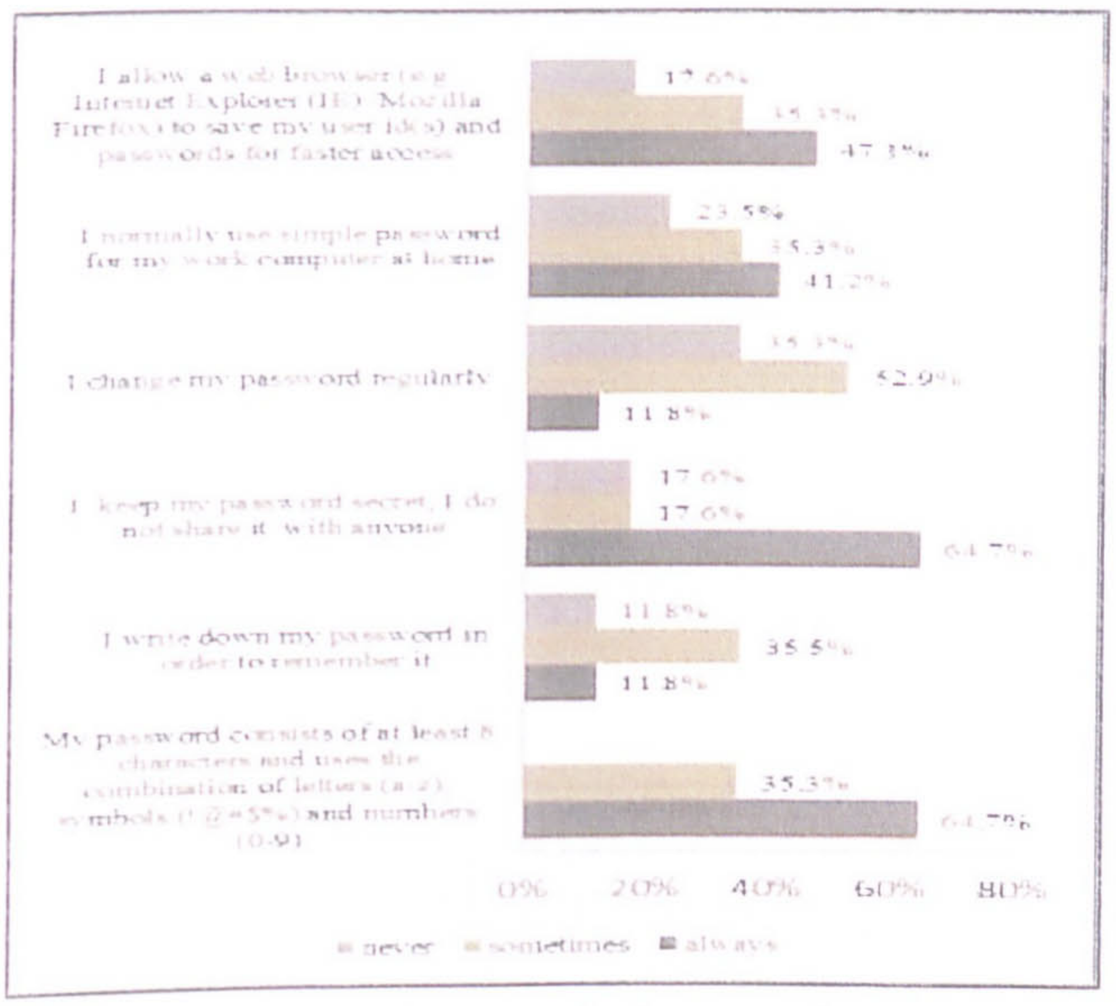

Figure 4. Practices related to password

- Security Practices Related to Antivirus and Firewall

This covers practices such as scanning external disk/thumb drive/USB driver with antivirus prior to reviewing the files within. As evident from Figure 5, 70.6% of the respondents claim to follow such practice (see Figure 5).

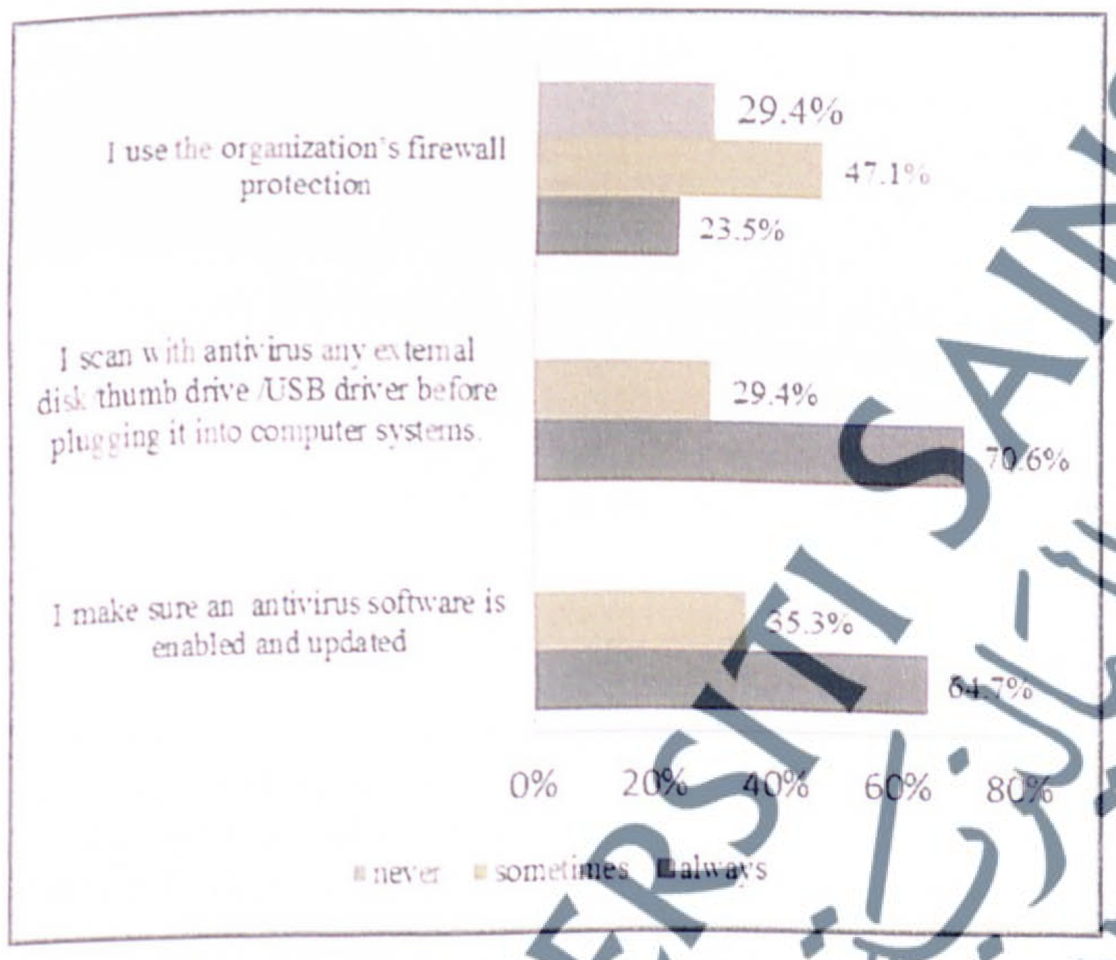

Figure 5. Security practices related to antivirus and firewall

- *Information Security Practices at Home*

With regards to their awareness at home, the respondents were asked questions pertaining to common security practices in three different categories, general security practices, practices related to password and security practices related to antivirus and firewall.

- General Security Practices

The majority of the respondents (82%) claimed to log off of their computers when they are done using the system (See Figure 6).

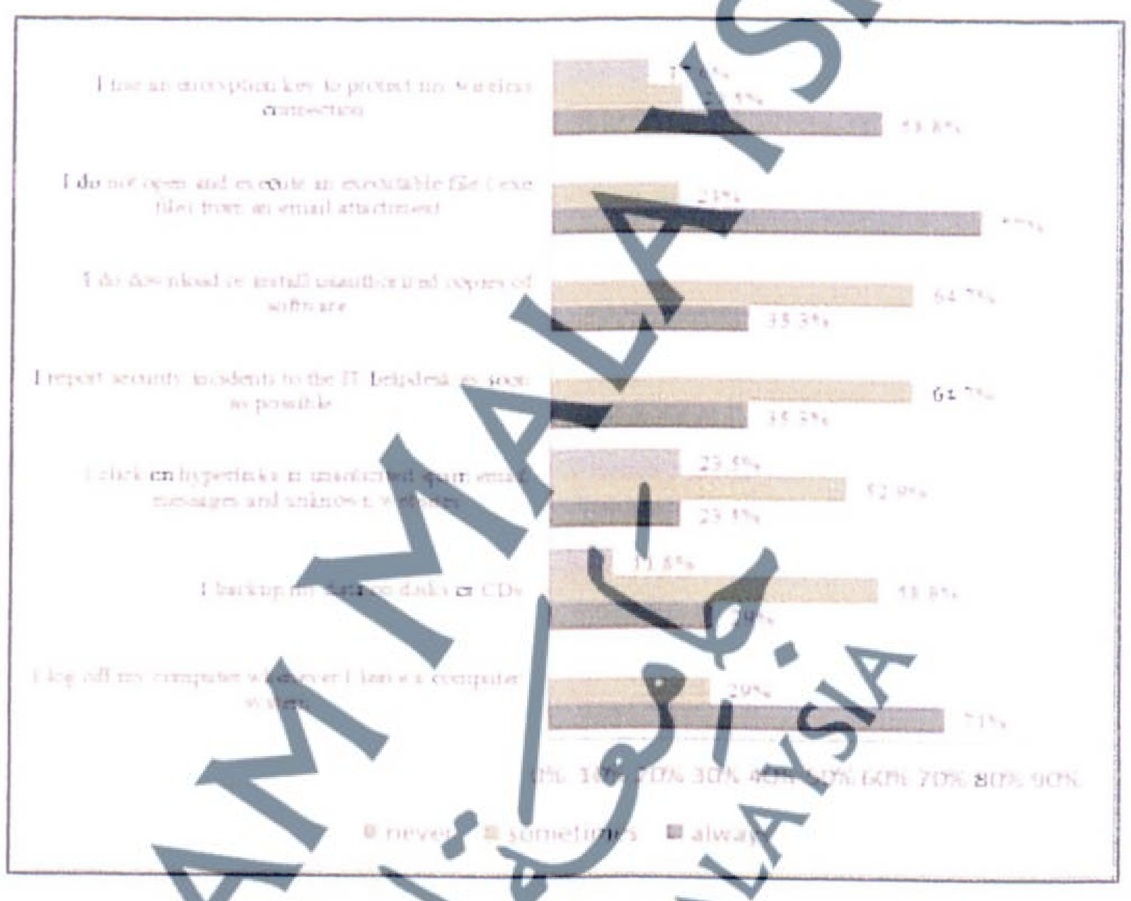

Figure 6. General security practices

- Practices related to password

The majority of the respondents (58.8%) change their passwords regularly as presented in Figure 7.

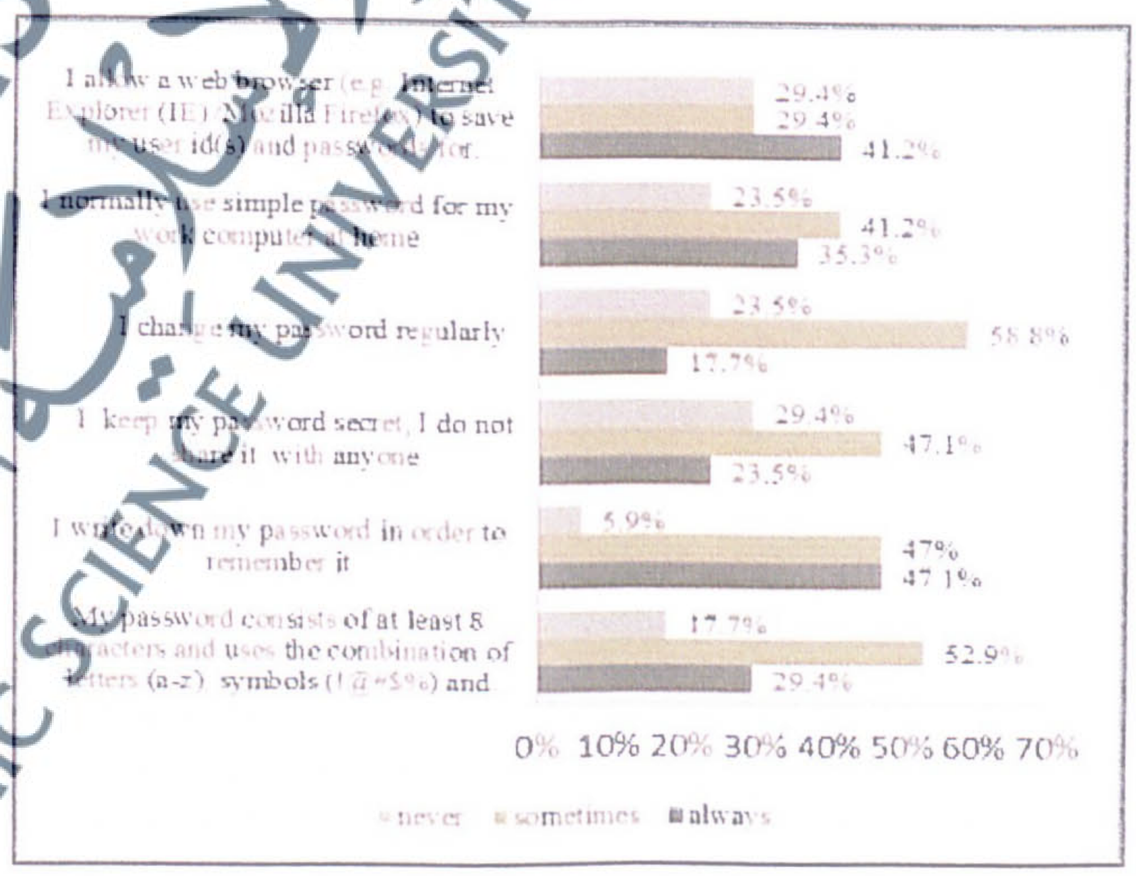

Figure 7. Practices related to password

- Security Practices related to antivirus and firewall

This covers the practice of scanning external disk/thumb drive/USB drivers prior to accessing it in computer systems and 71% of the respondents claimed to follow such practice (Figure 8).

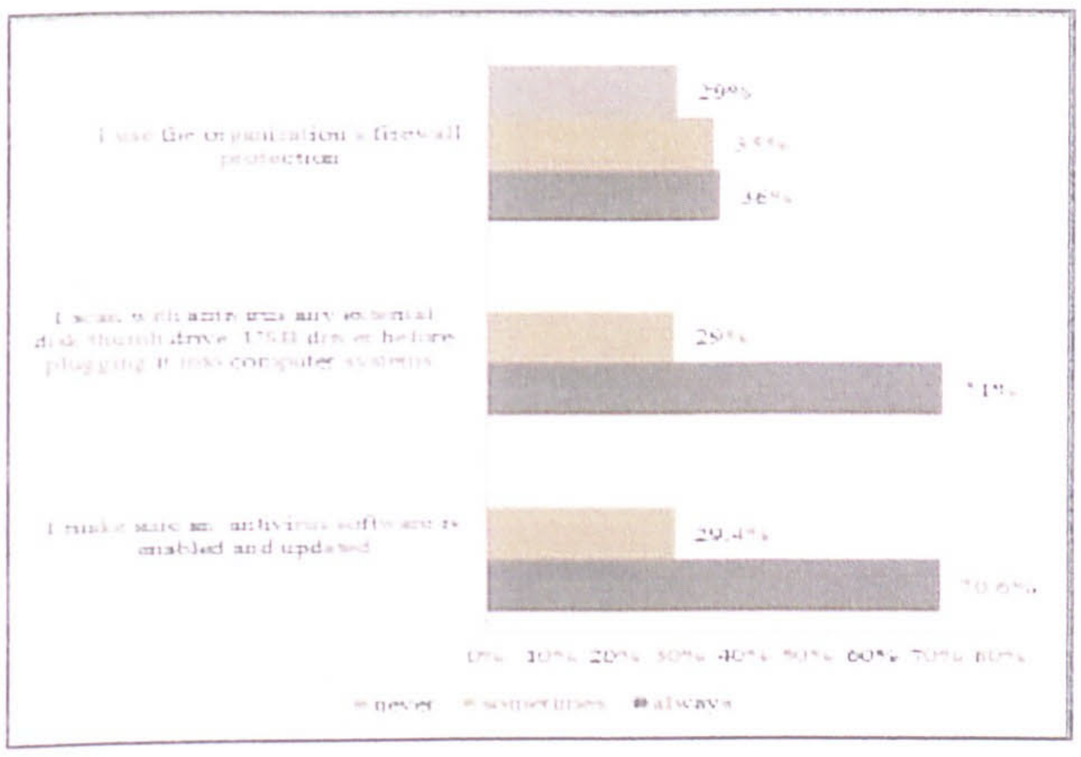

Figure 8. Security practices related to antivirus and firewall

V. Discussions

Overall, the respondents appeared to represent a knowledgeable group of individuals concerning the topic of IS, with majority of them possessing a good level of awareness and practice. However, generalizing the present study's findings to a wider population has to be done with caution as it is anticipated that the levels of IT and security awareness of the larger population is generally lower.

It is identified that practices for both workplace and home could resulted in danger for example downloading/install unauthorized copies of software and click on the hyperlinks in spam email/unknown website still for both practices participants were wrote down their password and use simple password . In addition, allowing browser to save user id and password could expose to insecure behavior if it is broken by hackers.

However, this does not affect the current study's results, although it is crucial to realize that the issue of information security awareness and practice still exists. On a brighter note, the respondents to the survey possess a good level of awareness and practice of IS security both at home and in the workplace.

VI. Conclusions

Good information security awareness should be achieved in the population of Internet users at large if users are to remain security and if e-business is to develop. Awareness at home and within the workplace appears to be of the same level as demonstrated by the survey findings pertaining to the scanning external disk/thumb drive/USB driver prior to accessing their contents, changing passwords on a regular basis and logging off of computers when done using the computer system.

On the other hand, it is identified that practices for both workplace and home could resulted in danger by considering to the survey finding in the following practices such as downloading/install unauthorized copies of software, click on the hyperlinks in spam email/unknown website and writing their password down to remember it.

Future research will focus upon the developing information security awareness framework and in particular look to incorporate other factors such as education background, training, and user behavior, as well as, to identify if there is transferability of the security practices from work place to home or from home to workplace, as well as targeting larger number participants with different backgrounds such as education background, ethnicity and religious.

References

[1] S. Talib, N. L. Clarke, and S. M. Furnell, "An Analysis of Information Security Awareness within Home and Work Environments," in *Availability, Reliability, and Security, 2010. ARES '10 International Conference on*, 2010, pp. 196-203.

[2] R. Richardson and C. Director, "CSI computer crime and security survey," *Computer Security Institute*, vol. 1, pp. 1-30, 2008.

[3] H. Interactive, "Online security and privacy study," 2009, [2, sep,2014].

[4] B. Schneier, *Secrets and lies: digital security in a networked world*: John Wiley & Sons, 2011.

[5] BERR. The 9th information security breaches survey [Online].[4,sep, 2014].

[6] E. Kritzinger and S. H. von Solms, "Cyber security for home users: A new way of protection through awareness enforcement," *Computers & Security*, vol. 29, pp. 840-847, 2010.

[7] R. von Solms and S. H. von Solms, "Information security governance: Due care," *Computers & Security*, vol. 25, pp. 494-497, 2006.

[8] S. Furnell and K.-L. Thomson, "From culture to disobedience: Recognising the varying user acceptance of IT security," *Computer Fraud & Security*, vol. 2009, pp. 5-10, 2009.

[9] T. Schlienger and S. Teufel, "Analyzing information security culture: increased trust by an appropriate information security culture," in *Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on*, 2003, pp. 405-409.

[10] GetSafeOnline. (2009). *Get safe online with free, expert advice*. [10, sep, 2014].

[11] StaySafeOnline. (2009). *Are your defenses up and your instincts honed?*.[12, sep, 2014].

[12] McAfee. (2009). *McAfee security tips - 13 ways to protect your system,[15,sep,2014]*.

[13] Microsoft. (2009). *Consumer online safety education*.[2, sep, 2014].

[14] NCSA and Symantec, "NCSA-Symantec national cyber security awareness study newsworthy analysis," ed, 2008.

[15] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, "A video game for cyber security training and awareness," *Computers & Security*, vol. 26, pp. 63-72, 2007.

[16] C. C. Chen, B. D. Medlin, and R. Shaw, "A cross-cultural investigation of situational information security awareness programs," *Information Management & Computer Security*, vol. 16, pp. 360-376, 2008.

[17] A. Tsohou, S. Kokolakis, M. Karyda, and E. Kiountouzis, "Investigating information security awareness: research and practice gaps," *Information Security Journal: A Global Perspective*, vol. 17, pp. 207-227, 2008

Appendix F:

- Copy of Certificate for conference presentation

theIRED

INSTITUTE OF RESEARCH ENGINEERS AND DOCTORS

2ND INTERNATIONAL CONFERENCE

ON

ADVANCES IN COMPUTING, ELECTRONICS AND ELECTRICAL TECHNOLOGY

CEET'14

20-21 DECEMBER (SATURDAY & SUNDAY), 2014

Certificate of Participation

This is to certify that Dr./Mr./Ms. **HAMIDA OMER ISSA ASKER** from **MALAYSIA** has presented a paper titled as **"A COMPARATIVE STUDY ON THE INFORMATION SECURITY CULTURE RELATED TO WORKPLACE AND HOME PRACTICES"** in the Second International Conference on **"ADVANCES IN COMPUTING, ELECTRONICS AND ELECTRICAL TECHNOLOGY"** Organized by **INSTITUTE OF RESEARCH ENGINEERS AND DOCTORS** at **HOTEL G TOWER, KUALA LUMPUR, MALAYSIA.**

Organizing Secretary

Chairman