

Information and Communication Technology Issues: A Case of Malaysian Primary School

¹Maslin Masrom, ²Nik Hasnaa Nik Mahmood, ³Othman Zainon,
⁴Hooi Lai Wan, ⁵Nadia Jamal

^{1,2,3,4,5}Human Capital and Knowledge Management Research Group
Universiti Teknologi Malaysia International Campus

Kuala Lumpur, Malaysia

¹maslin@ic.utm.my, ²nikhasna@ic.utm.my, ³othman08@ic.utm.my, ⁴hooilw@ic.utm.my, ⁵diyajamal@ic.utm.my

ABSTRACT

Over the past decade, technologies have seen unprecedented growth across the globe. Despite the advance in technology and the increase of internet use which provide numerous benefits to mankind, little is known about the problems and related issues of cyber ethics and behavior of using internet. It is urgent for researchers to study about ethics for cyber or computer and behavior of using internet. The aim of this study was to explore the information and communication technology (ICT) issues in Malaysian primary school. In this study, a review of past studies over a 10-years period that raises concern on issues related to cyber ethics and behavior of using internet is conducted, and the survey methodology has been adopted by distributing questionnaires among students. The results indicated that the students are able to comprehend the ethical issues in the use of ICT, and there were two major issues on cyber ethics that currently exist in the school environment, namely cyber bullying and cyber hacking.

Keywords: *Cyber Ethics, School, Internet Behavior, Information and Communication Technology, Malaysia, Primary School*

1. INTRODUCTION

Nowadays, there are several issues on ICTs occurred among primary school students. These scenarios have caused alarm among the parents who are concerned with their children specifically the primary school students. Several research studies have investigated issues related to ethical issues and behavior of using internet. In the previous study, Hope has raised his concerns about internet safety in primary schools at his country by stated that in New Zealand, one third of 7 to 10 years old and half 11 to 12 years primary students' use internet at home beside significance to the problem [1].

Willard stated in her book that a few of youngsters tend to rely on that the internet world as their personal playground and they do not need attention or guidance from their parents [2]. However while exploring the internet; students are opened to a wide world which is full of infinite possibilities and easy access to such vast amounts of information. There are huge chances for them especially to the primary school students to be exposed not to only the expanded unlimited information but also to the dangers of internet.

ICTs issues such as internet safety or cyber security, cyber bullying, internet addictive, hacking and cybercrime are becoming an advanced state of serious concern. Thurairasa asserted that three most serious of ICTs issues raised concern theft of copyright material, privacy and access to undesirable material on the Internet [3].

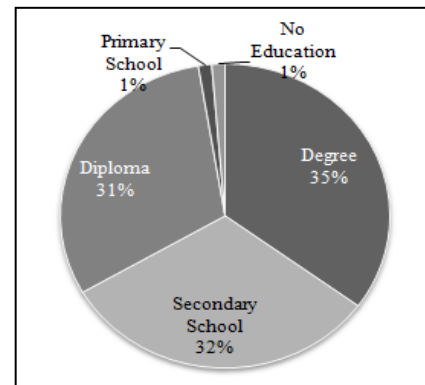


Fig 1: Malaysian Internet Users by Education

Based on the statistics as shown in Figure 1 retrieved from [4], the degree holders are the highest internet user by 35.1% followed by those with secondary school (31.5%) and diploma holders (30.9%). Primary students and users with no education show small percentage on using the internet in Malaysia (1.3%). Based on the statistics, there is already evidence that as education system in the country develops gradually; the numbers of internet users are expected to increase.

Cyber criminals always are preying on immature and undefended students through activities including online solicitation, cyber-bullying, obscenity and pedophilia as well being exposed to other peer pressure and improper activities [5]. Willard evaluated about the harm of internet to children such as risky sexual activities as they may expose to pornography or sexual materials, or become victims to the adult sexual predators [6]. Moreover, children could also involved in

<http://www.ejournalofscience.org>

cyber threats, gaming, gambling, hacking, plagiarism, copyright infringement, spam, scams or other technical security concerns.

The Malaysian Ministry of Education has given high priority for development of ICT among the students during the last decades. In 1996, Smart School Project (SSP) was presented as one of the programme integrating ICT in school as part of seven flagship under the Malaysia Super Corridor (MSC) program in order to achieve long term vision namely Vision 2020 [7].

However, this scenario does not only bring benefits but also flaws to the students. The Cyber Security Malaysia chief operating officer Zahri Yunos asserted that some 8,000 cases were reported in year 2010 and attributed this to the growth in Internet usage and broadband penetration that now stood at 55% [8]. This exponential rate in the statistics proves that ethics in cyber is not being implemented properly among its users. Figure 2 illustrated the Malaysian internet users by age groups in 2008.

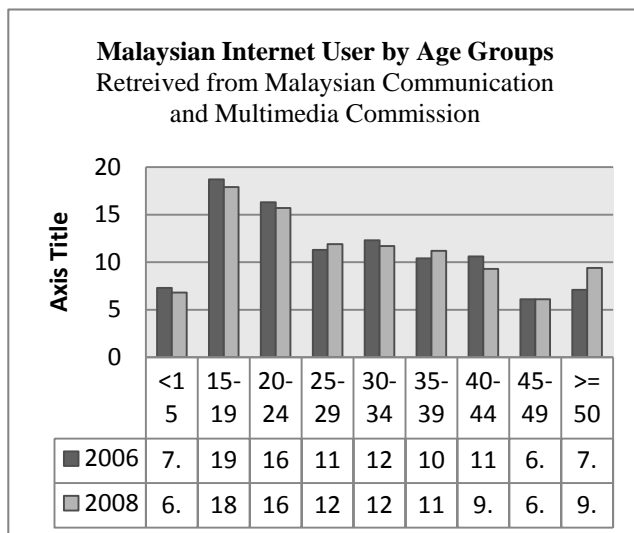


Fig 2: Malaysian Internet Users by Age Groups 2008

Based on the statistics retrieved from Malaysian Communication and Multimedia Commission (see Figure 2), there was a substantial hike in numbers from the below 15 years old age group to the 15 years till 19 years age bracket [4]. This statistics show that most Malaysian teenagers start using the Internet actively in upper secondary school (ninth year of formal education). Based on the statistics, there is already evidence that a large number of students are accessing into the Internet thus, exposed to cyber ethics issues.

The unethical use of internet is increasingly pervasive the lives of students. Parents and teachers are extremely worried on this issue because it can lead to more serious problem as stated before. So, it is crucial that every student practiced good cyber ethics in daily

lives. Positive behavior is developed at primary level so that it will be able to support the students' development to secondary level [1]. Therefore, this study will explore the cyber ethics issues and behavior of using internet in Malaysian school which focusing primary level.

The paper is organized as follows. This paper begins with an introduction of the study and follows by exploring the literature review of the study. Then it continues with methodology, and finally the results and conclusion are presented.

2. LITERATURE REVIEW

a. Definition of Cyber Ethics

Ethics is about directing peoples' actions in making decisions, derived from the differences between right and wrong or true or false. The authority of computer ethics as a separate subject of applied ethics has been and continues to be challenged and there are any rare or unique things about the moral difficulties measured by the computer ethic experts [9]. Computer ethics is the study of what people ought to do surrounding computers about the ethical issues escalated therein, grounded in ordinary moral principles, and perhaps an extension of these principles to situations created by computers [10]. Cyber ethics is ethics on computers and the internet and within the views of computers, technology and the Internet, cyber ethics is just a separate method of looking at ethics [11]. Another definition of cyber ethics are as the field of implemented ethical that inspect moral, legal, and social issues in the improvement and apply of cyber technology [12]. Other different terms were used to describe cyber ethics such as computer ethics, information ethics and internet ethics.

In the context of application on the internet, ethics or cyber ethics are the ethical rule for the users of computer world [13]. In earlier research cyber ethics referred as computer ethics and had been generally explained the theory of ethics which has been related with the analysis of person intentional action or the persons' character [14]. Computer ethics can also be described as the study of ethics which associated to computer use and as the ethical perception which describes a moral IT domain or area [15]. In our study, we defined cyber ethics as the behavior of human in internet world with provided rules or guidelines.

b. ICTs Issues in Malaysia

There are a lot of issues of ICTs occurred in Malaysia. According to the New Straits Times [16], based on the Norton Human Impact Cybercrime Report, 45% of Malaysian cyber crimes have never been resolved because it takes about 30 days and an average cost of RM7,323 (US\$2,270) to resolve each cases. The

<http://www.ejournalofscience.org>

Information, Communications and Culture Ministry have opened 20 investigation papers on cybercrimes in the first three months of this year. The crimes comprised dissemination of lies, misuse of information, defamation, sedition and pornography. Deputy Information, Communication and Culture Minister Datuk Joseph Salang Gandum said besides taking the culprits to court, the Malaysian Communication and Multimedia Commission (MCMC) will also block the access to phishing, fraud, illegal investment and pornography websites [17]. Figure 3 illustrates reported occurrence based on General Incident Classification Statistics 2011 organized by Malaysia Computer Emergency Response Team [18].

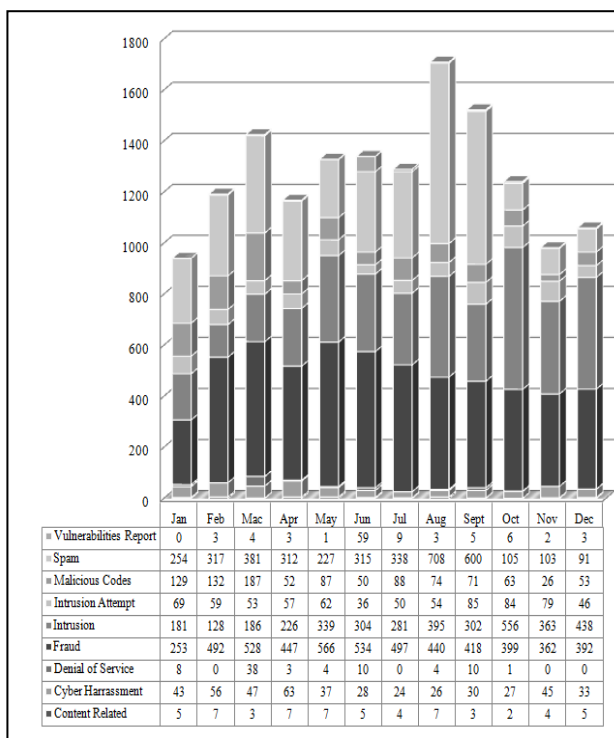


Fig 3: Reported Incidents Based On General Incident Classification Statistics 2011

The statistics show that the reported incidents rose rapidly from the first quarter of the year throughout to the end of the year 2011. Reported incidents such as vulnerabilities report, spam, malicious codes, intrusion attempt, intrusion, fraud, denial of service, cyber harassment and content related. Compared to the reported cases in 2010, the overall numbers of cases were increased around fifty percent more than last year. According to Cyber Security, 60 cases of cyber bullying in schools were reported in year 2007 and is expected to increase in the future.

It was reported that 41 government websites at different stage were disrupted by a group of hackers, calling themselves as 'Anonymous'. All of the hacking attacks were to dispute against the Government's act for restriction on the internet by blocking 10 file sharing

sites which were among the most visited by Malaysians to illegally download movies [19]. Federal Commercial Crime Investigation Department Datuk Syed Ismail Syed Azizan said police were working with the National Security Council and Cyber Security Malaysia for tracing and monitoring the hackers' group.

It is asserted that bullying is a form of offence that is based on an inequality or as a systematic imbalance of power [20]. Cyber bullying elaborated as an old problem in new disguise, referring cyber bullying as new way of bullying [21]. There are various medium that allows cyber bullying to occur such as email, instant messaging, mobile phones, websites, personal digital assistants, internet gaming, and others [22]. Although cyber bullying appear in a divided social perspective, a children who bully on the internet possible will involved in bully at school [23].

National Union of the Teaching Profession secretary-general Lok Yim Pheng, said emotional and cyber-bullying should not be taken carelessly even though they were relatively new in Malaysia and should be addressed before it become severe as there are tools for example Youtube as medium for exposing students' acts [24]. Cyber bully case involving a student in Malaysia went worst when the victim caught drinking her fathers' alcohol to avoid depression [25].

Meanwhile, in the world of computer programming in 1960s, the term 'hacker' was originated as a positive label to depict a person who has a great talent and very skillful in fixing computer problems by providing innovative and efficient solutions. However hackers were considered unethical and incompetent when they explore in others' computer systems which derived by curiosity, an aspiration to learn and discover, and distribute their findings with others, destructing systems while exploring intentionally or unintentionally. 'Hacking' and 'hackers' is term used to denote those persons who engage in such illegal activities related with computer infringement and manipulation [26]. In 2006, it is reported that 13 youths caught for internet phishing and scams in Malaysia. They managed to deceive at least 26 people and stealing RM36, 000 from their victims' accounts [27].

c. Cyber Ethics Issues in Other Countries

Researchers from other countries have also raised their concern about cyber ethics issues and behavior of using internet among students in schools. Cyber crimes explained as a common term of convenience and are acknowledge a subset of 'digital' or 'hi-tech' crime and as a generalization for criminal and undesirable or harmful behavior that is assisted or enabled by networked technology [28]. Cyber ethics issues occurred in other countries are summarized as follows.

Table 1: Cyber Ethics Issues in Other Countries

Year	Cyber Ethics Issues	Country	Source (s)
2003	Cyber Hacking	Poland	<u>Bannerman, 2011, When Genius Goes Bad, 19 June 2008, the Times.</u>
2005	Cyber Bullying	Australia	Marilyn A. Campbell, 2005, Cyber Bullying: An Old Problem in a New Guise? Australian Journal of Guidance & Counseling, 15(1), 68-76.
2006	Internet Fraud	United Kingdom	Teenage internet fraudster jailed, 7 July 2006, BBC News World Edition.
2007	Cyber Hacking	United Kingdom	Teen hacker held over £12.5m cyber crimes, 30 th November, 2007, the Metro Online (UK).
2007	Cyber Hacking	New Zealand	<u>Teenager 'Headed Cyber-Crime Network', 1 December 2007, the Times.</u>
2008	Cyber Crime	New Zealand	NZ teen convicted of cyber crime, 1 April 2008, BBC News World Edition.
2008	Hacking	United Kingdom	Alarm raised on teenage hackers, Mark Ward, 27 th October 2008, BBC News World Edition.
2008	Cyber Crime	<u>United Kingdom</u>	<u>Children 'turning to cyber crime', 27th October 2008, The Metro Online (UK).</u>
2008	Cyber Hacking	<u>United States of America</u>	Schoolboy hacker Omar Khan who upped his grades faces 38 years in jail, 19 June 2008, The Times (UK).
2011	Cyber Bullying	United Kingdom	Face book bully boy, 14, arrested for 'kill threats', 15 March 2011, The Metro Online (UK).

Most cases apparently reported mostly in developed country for example United Kingdom, United States of America and New Zealand. The above articles show the evidences of cyber crimes among students which were related to ICTs issues.

d. Use of ICT at Schools

In recent years, experimental studies have begun to examine the conditions under which young children will employ either an imitative or an emulative approach [29]. Meanwhile behavior is a statement or expressions of verbal or actions that are possibly available to careful observers using common sensory processes [30]. When kids exposes to unrated materials from the Internet, they will be tempted to emulate the actions from materials which they saw or learnt. It will create negative impact and severe psychology problems for the students.

Based on a survey study in Connecticut, one in every 25 teens reported to have inevitable desire to be on the Internet and they were tension when they weren't online, or said they had tried to quit or cut down on Internet time. According to the survey, students who has problematic internet issues have a tendency to be depressed and would usually involved in serious fights whereas the boys had higher tendency of smoking and drug use. Fundamental proof also proposes that problematic Internet use shares common features such as drug and alcohol abuse disorders, obsessive-compulsive disorders and impulse-control disorders [31].

3. METHODS

The research methods applied for this study is presented in this section.

Pilot study: The aim of executing this pilot study is to get feedback or comment from the respondents regarding the developed instrument. The questionnaires were distributed to 25 primary school students at a private primary school. It was found that no major changes were required on the questionnaire's layout or wordings. A response rate of 84% recorded.

Instrument: The instrument of the study, namely, questionnaire was structured based on the goal. The questionnaire was aimed to analyze the level of ethical awareness among the Malaysian primary schools' students. A set of questionnaire has been created in order to collect initial findings for this research. The questionnaire was divided into three parts.

For the first part of the questionnaire, profiles of the respondents are required. A set of demographic questions on respondents profile are included before the respondents proceed to the questions. Among of the

<http://www.ejournalofscience.org>

questions are the respondents' name, age, and schools' name

and class. The second part included the definition of ethics, cyber ethics and ethics in Islamic perspectives.

The third part consists of five IT-related scenarios in each four major ethical issues. All questions were distributed in close-ended format by providing a suitable list of responses to produce quantitative data. In this questionnaire, the questions were divided into four sections. There are consists of 20 set of questions in total.

Each question is divided into four different sections according to the ICTS issues which are accuracy, intellectual property, accessibility and privacy. The purpose of the study was to determine the significance people place on their information technology ethical issues (PAPA) as is relates to the given scenarios. The questions provide scenarios on anonymous individuals. Individuals are good. The four item questionnaire is presented in Table 2 as follows.

Table 2: PAPA Issues and Questionnaires Scenario

PAPA Issue	Specific Questionnaire Scenario
Privacy	Confidentiality of persons' information
Accuracy	Precision and legitimacy of persons' information
Property	Use by others of software or other intellectual property without the persons' consent
Accessibility	The right or privilege to obtain of persons' information or data

Each question consists of various situations on ethical and internet behaviour issues. The questionnaires are presented in close ended questions which the respondents' answers are limited to a fixed set of answers.

The scale used in the questionnaire is the three choices of answers which are 'Beretika' (ethical), 'Tidak Beretika' (non-ethical), and 'Tidak Pasti' (neutral). Table 3 display the distribution marks for each questions in the questionnaire. Each respondent were asked to mark or select one box for each question. Respondents answered the questionnaires during dedicated class hours. In order to collect total marks for the respondents, the marks are divided as follows. For each correct answer, five marks will be given. If their answer is wrong, no mark will be given and for indecisive answer, two marks will be given.

Table 3: Distribution Marks for Each Question

Results	Score
Correct	5
Indecisive	2.5
Wrong	0

Table 4 illustrates the marks distribution. The full marks for the whole quiz are 100 marks. Respondents who achieved 70 - 100 marks are considered to be excellent and possess higher ability to distinguish between the ethical or unethical behaviour. Respondents with 30 - 69 marks are considered as moderate while 0 - 29 marks are considered as weak.

Table 4: Number of Primary Schools by State

Marks	Grade
70 - 100	Excellent
30 - 69	Good
0 - 29	Weak

Once the questionnaires were allocated, the data was gathered from the respective primary school and later were examined to find any patterns available. This pattern will help to describe the data in appropriate way to assure the objectives of this research have been accomplished. Overall, a total of 25 questionnaires were allocated to obtain the result. Out of 25, 21 questionnaires were returned, yielding 84% response rate.

4. RESULT AND DATA ANALYSIS

In this study, we have reviewed articles in selected journal books and newspapers. Results indicated that cyber bullying and hacking are the most serious ICTs issues occurred in Malaysian primary schools. This section also summarizes the results of the quantitative survey research. A number of questionnaires were distributed in a selected primary school. The survey was conducted on April 2012 among Malaysian primary schools' students using a distributed questionnaire. Each respondent took approximately five to ten minutes to complete the questionnaire. Table 5 displays the gender demographics whereby 59 students who took part in the questionnaire consist of 61.0% (36) female and 39.0% (23) male.

Table 5: Gender Demographics

		Frequency (N)	Percent (%)
Valid	Female	36	61.0
	Male	23	39.0
Total		60	100.0

Based on the result in Figure 4 below, it reflects that students are able to understand the cyber ethics and internet behavior. The lowest marks achieved from the respondents are between 50-59 marks (3%), followed by 70-79 marks (9%), 80-89 marks (27%), and highest percentage of respondents obtained 90-100 marks (61%).

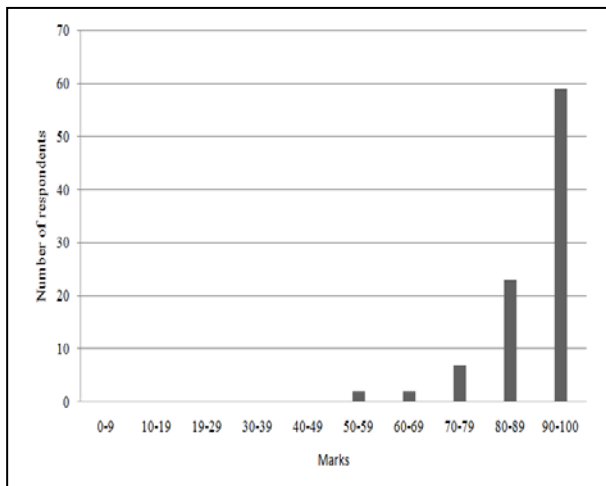


Fig 4: Percentage of Respondent in Total Scores

The result in Figure 5 also indicated that the most respondents answer correctly in the privacy section (93.38%), followed by accuracy (93.22%), accessibility (88.64%) and finally property (80.5%). From the results, it can be concluded that the respondents understand the use of ICT in an ethical manner.

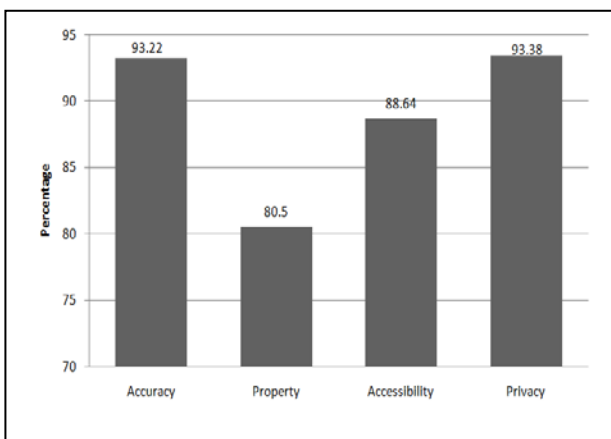


Fig 5: Level of Ethical Awareness

5. CONCLUSIONS

This study has presented the ethical issues in ICT in a Malaysian primary school. Although ethical standards and amount of cases in Malaysia may differ from those in Western and other countries, there are indeed common base and universal values that were shared together. Based on the pilot study, it is revealed that the students in the selected primary school were able to differ between the good and bad in making decision while using the internet or ICT. There are already some actions taken to control the issue of cyber ethics among the schools in developed country. In developed country, several websites had been created for teaching the students about the importance of cyber ethics. However, the same precautions were not taken seriously in developing countries. Thus, deeper and frequent follow-up as well as more analysis methods will be conducted to investigate in order to develop modules for teaching ethical issues and use of ICT in primary schools.

ACKNOWLEDGEMENT

The authors would like to acknowledge the support by Universiti Teknologi Malaysia. This research work is part of Research University Grant (Cost Center No. Q.K130000.7140.02H33).

REFERENCES

- [1] Hope, J. (2002). Internet Safety: Issues For New Zealand Primary Schools, Proceedings NetSafe: Society, Safety and the Internet. February, 59-68.
- [2] Willard, N. E. (2007). Cyber-Safe Kids, Cyber-Savvy Teens: Helping Young People Learn To Use the Internet Safely and Responsibly, John Wiley & Sons, Inc. ISBN 978-0-7879-9417.
- [3] Thurairasa, S., & Johnson, R. (2003). Is There a Need for Cyber ethics In The Middle School Curriculum. Educational Research, Risks and Dilemmas. 1-7.
- [4] Communication and Multimedia Commission (2012), My CERT. Retrieved from <http://comm215.wetpaint.com/page/Malaysia+Internet+Penetration> on 1 August 2011.
- [5] Byron, T. (2008). Safer Children in a Digital World, The Report of the Byron Review, available on the 25th September 2009 at, <http://publications.dcsf.gov.uk/eOrderingDownload/DCSF-00334-2008.pdf>.

<http://www.ejournalofscience.org>

- [6] Willard, N. E. (2007). *Cyber-Safe Kids, Cyber-Savvy Teens: Helping Young People Learn To Use the Internet Safely and Responsibly*, John Wiley & Sons, Inc.
- [7] Latif, R. A., & Sheard, J. (2009). Social Skills among Students while Playing Computer in Class: A Case Study in Malaysia. *International Conference on Future Computer and Communication*. 177-181, doi 10.1109/ICFCC.2009.9
- [8] The Star Online (2011). 28 April. Big Increase in Cyber Crimes. Retrieved from <http://thestar.com.my/news/story.asp?file=/2011/4/28/nation/8564427&sec=nation> on 1 August 2011.
- [9] Tavani, H. T., (2001). The State of Computer Ethics as a Philosophical Field of Inquiry: Some Contemporary Perspectives, Future Projections, and Current Resources. *Ethics and Information Technology*. 3(2), 97-108, doi: 10.1023/a:1011889808481.
- [10] Johnson, D. G. (2001). *Computer Ethical*. 3rd Edition (Upper Saddle River, NJ: Prentice-Hall).
- [11] Schwartau, W. (2001). *Cyber Ethics 101: What Are (Is) Ethics?* Retrieved 27 May, 2011, from <http://www.ed-u.com/cyber-ethics.htm>.
- [12] Spinello, R. A. & Tavani, H. T. (2004) *Readings in Cyber ethics*, Jones and Bartlett Publishers, Inc: Boston: 2, 1-10.
- [13] Whittier, D. (2006). *Cyber Ethics in the Googling Age*. *Journal of Education*. 187(2), 1-6. 00220574.
- [14] Johnstone, J. (2007). Technology as Empowerment: a Capability Approach to Computer Ethics. *Ethics and Information Technology*. 9 (1), 73-87, doi: 10.1007/S10676-006-9127-X.
- [15] Masrom, M., Ismail, Z, & Hussein, R. (2010). Exploring Computer Ethics in Malaysia. *Issues in Information Systems*. 11(1), 119-128.
- [16] Sani, R. (2011, February 28). *TRENDS: To Catch a Cyber-criminal*. *New Strait Times Online*. Retrieved from http://www.nst.com.my/nst/articles/TRENDS_To_catchacyber-criminal/Article/art_print on 10 June, 2011.
- [17] Bernama (2011, April 19). 20 Cyber crime Cases under Probe. *New Strait Times Online*. Retrieved from <http://www.nst.com.my/nst/articles/14sal/Article/> on 10 June, 2011.
- [18] MyCERT, (2011). Retrieved from <http://www.mycert.org.my/en/services/statistic/mycert/2011/main/detail/795/index.html> on 1 August 2011.
- [19] Camoens, A., & Aruna, P. (2011, June 16). Cops Probing Website Hackings. *The Star Online*. Retrieved 10 June, 2011, from <http://thestar.com.my/news/story.asp?sec=nation&file=/2011/6/16/nation/8913094>
- [20] Rigby, K. (2004). Addressing Bullying in Schools: Theoretical Perspectives and Their Implications. *School Psychology International*, 25(3), 287-300.
- [21] Campbell, M. A. (2005). Cyber Bullying: an Old Problem in New Guise? *Australian Journal of Guidance & Counseling*. 15(1), 68-76.
- [22] Bauman, S. (2007). Cyberbullying: a Virtual Menace. *National Coalition against Bullying National Conference*. November 2 – 4.
- [23] Wade, A. & Beran, T. (2011), Cyberbullying: the New Era of Bullying, *Canadian Journal of School Psychology*. 26(1), 44-61.
- [24] Bidin, B., & Tan, C. C. (2010, July 4). *Newsfocus: Ragging Bullies*, *New Strait Times Online*. Retrieved 10 June, 2010, from <http://www.nst.com.my/nst/articles/06BING/Article/>
- [25] D'Cruz, F. (2011). *The Malay Mail*. Being Frank: Teen Girl Cyber-bullied to Alcohol Abuse. Retrieved from http://www.mmail.com.my/content/79243-being-frank-teen-girl-cyberbullied-alcohol-abuse_on_30_August_2011.
- [26] Yar, M. (2005). *Computer Hacking: Just another Case of Juvenile Delinquency?* *The Howard Journal*. September. 44 (4), 387–39. ISSN 0265-5527.
- [27] Lee, S. L. (2006, October 11). 13 Youths Held for Online Theft. Retrieved 10 June, 2011, from http://www.cybersecurity.my/en/knowledge_bank/news/2006/main/detail/814/index.html
- [28] Hunton, P. (2009). *The Growing Phenomenon of Crime and the Internet: a Cybercrime Execution and Analysis Model*. *Computer Law & Security Review*. November 2009. 25 (6), 528-535.

<http://www.ejournalofscience.org>

- [29] Horner & Whiten, A. (2005). Causal Knowledge and Imitation/Emulation Switching in Chimpanzees (*Pan Troglodytes*) and Children (*Homo sapiens*), *Animal Cognition*. 164–181.
- [30] Furr, R. M. (2009). The Study of Behavior in Personality Psychology: Meaning, Importance and Measurement. *European Journal of Personality*. 23, 437–453.
- [31] Liu, T. C., Desai R.A., Krishnan-Sarin, S., Cavallo, D. A., & Potenza, M.N. (2011). Problematic Internet Use and Health in Adolescents: Data from a High School Survey in Connecticut, *J Clin Psychiatry*. PMID: 21536002.