

DO MODERN TECHNOLOGIES ENCOURAGE CYBERCRIMES? A STUDY AMONG MALAYSIAN YOUTH

Saidatulakmal Mohd, Abdelhak Senadjki, Siti Rohaya Mat Rahim, Thurai Murugan Nathan, Chin-Yu Lee & Mahmud Abd Wahab

The easy access to modern technologies had resulted in many socio-cultural changes especially among young people. Technology changes the way youths interact and communicate with each other that may easily influences their way of life. Youth of different skills, backgrounds and educational levels develop different capacities dealing with technology in a new virtual world. There is no doubt that modern technology has brought both positive and negative sides to our societies (Bakar & Bidin 2014; Goggin, 2010; Goggin, 2013; Jonsson et al., 2014; Lenhart 2009; Lim, 2013; Shade & Shepherd, 2013; Shank & Cotten, 2014; Tsukayama, 2013; Wells & Mitchell, 2008; Ybarra & Mitchell, 2004; Yusop & Sumari, 2013).

While the positive sides of modern technologies could be the motives in obtaining and facilitating such technologies to youths, there are also many voices that warn us on the negative sides of modern technologies that could be detrimental, harmful and change one's social behaviour. Longe et al., (2009) claim that majority of youths are involved in various cybercrimes related activities including e-mail scam, cyber bullying and intimidations, lying, internet pornography, child and drug trafficking, examination fraud and sabotaging internet network providers. Igbo et al., (2013) point out that although the positive impact of modern technologies benefits education, economy and society, cautions must be taken when providing and investing in such technologies, both at individuals and the national levels. They emphasize that parents, school guidance, counsellors and professionals outside the school need to play their roles in directing and protecting youth against the negative consequences of modern technologies that may cause youth behaviour problems.

The easy access to modern technologies may influence youth's ways of thinking and behaving due to the absorption of foreign culture and behaviour that are incompatible with the nature of our societies, hence creating a gap between youths and their communities. Abrupt behaviour include involvement in cybercrime activities. To that extent, many researchers such as Baturay and Toker (2015); Passey et al., (2004); Al-Zahrani (2015); Mareschal et al., (2007) are calling for efficient and strict legal actions to be taken against youth founds guilty of practicing and involving in such demeaning activities. Other researchers, practitioners and policymakers call (Jonsson et al., 2014; Quayle & Taylor, 2011; Blinka & Smahel, 2012; Gupta & Parvesh, 2014) for the imposition of concrete and efficient mechanisms to control the use of modern technologies to reduce their negative effects on youths.

It is clear that misuse of modern technologies may bring unbearable consequences to society particularly youths. Although the misuse of modern technologies among Malaysian youths shows an increasing trend (The Star Online, 2014) there is no significant effort to investigate this. To the best of our knowledge there is no formal empirical evidences that investigate the possible danger of modern technologies (cybercrime) on Malaysian youths. The available case studies on Malaysia investigate the positive impacts of technology usage on students and youths. Yusop and Sumari (2013) examine the role of technology in assisting students to achieve their academic goals. They find that students are actively engaged in social media sites for information sharing and educational purposes.

Shade and Shepherd (2013) and Tsukayama (2013) call for effective strategies that promote “digital policy literacy,” to be directed to youths to help them understand communication policy process, the political economy of media, and the technological infrastructure of media institutions. Such policies may contribute to a more effective children development and empower youths in the digital economy. This study argues that control over technology era has passed and bring no result. This study envisages that designing and developing proper mechanisms enabling youth to attain the maximum benefit from technology revolution could be an appropriate solution. These mechanisms should be developed in ways that enable youths to be shareholders in the development of this technology rather than being recipients of it.

RESEARCH PROBLEM

There are serious debates on the impact of Internet and modern technologies on youths in recent years. Many researchers, practitioners and policymakers voice up for the need to tackle and solve the negative impacts of modern technologies on youths to protect the future generations. As such, Malaysia is not exempted. In fact, the Sophos Security Threat Report 2013 lists Malaysia as the sixth most vulnerable to cybercrime along with several countries such as Hong Kong, Taiwan, Thailand, China, India and Indonesia. Deputy Communication and Multimedia Minister Datuk Jailani Johari said Malaysians are also facing threats from international criminal organizations that abuse the Internet for illegal activities such as drugs, human trafficking, financial fraud and money laundering (Theantdaily, 2014). He points out that “Incidents of cyber harassment, fraud and spam have shown a slight increase with the highest reduction in intrusion incidents”. The Star Online (2009) raises an issue on the fact that Malaysian teenagers are exposed to the misuse of modern technologies. The Star Online (2009) claims that society may benefit from the millions of ringgit investment from organizations that promote their latest technology and at the same time being exposed to the negative sides of such technologies. A question arises on who is responsible to educate people and make them aware of the negative sides that come along with the advancement in technology? Keeping this unchecked, many young Malaysians will be exposed to serious threats that may put them in danger. At the same time, youths are also exposed to other types of digital technology that is prominent in threatening and destroying their behaviour. Youth is always at risk not only due to cybercrime activities, but also due to other destructive physical and psychological problems that could be developed from the engagement of youths with advanced modern technology.

LITERATURE REVIEW

Technologies have become an essential element of our daily lives. Technologies have boosted up the social ability of users. Technological advancement is constantly observed at almost every stage of our lives. Although technologies create a lot of benefits, if used without discretion.

Cell phones, laptops, tablets or any other devices that are able to connect to Internet are now every part of our daily lives, hence creating new and easy opportunities for crime. Individuals are now easy targets of borderless crime; location identifier through Twitter, personal information through online transactions, credit card fraud through online banking and identity theft through Facebook. What used to be traditional ways of committing crimes are now made advanced, simpler and easier via many creative and new ways of technologies. To make the situation worse, identity of these lawbreakers or delinquents remain anonymous through the many tricks and identity fraud assisted by the misused of technologies. This makes their presence and actions difficult to be detected and tracked. As such, the lawbreakers or delinquents remain free on the streets and on the social media, providing them even more opportunities to pursue their reckless behaviour. Youths with sufficient knowledge on information technology (IT) who are in need or greed of money could easily be enticed onto many online illegal activities.

The amazing capability of modern day Internet simplifies life of the many, especially teenagers, by providing easy way to share knowledge promptly. It is certainly possible to transmit pictures, videos, papers, proposals, and others alike with just a click of a button. And the transfer takes place within seconds. According to Shrivastav and Ekta (2013) as well as Nandhini and Sheeba (2015), most cybercrime accomplice and targets are the youths. Cyber bullying, one element of cybercrime activities, often target teenagers engaging with online activities such as Facebook and Online Gaming. Smith et al., (2008) finds that today's youth believes that cyber bullies are part of entertainment and fun. This motivates youth to use technology instead of face-to-face interactions. The study reveals that boys are often the aggressors but there is negligible gender difference in being a victim. Boys predominate in physical bullying while girls are at least relatively more involved in indirect and relational bullying. Girls typically display positive disposition for television and cellular phones, while boys have a greater predilection for computers, console games and computer games (Savahl et al., 2008).

According to the "Second Annual Cost of Cyber Crime Study – Benchmark Study of U.S. Companies" published by the Ponemon Institute (2012), a study consisting of 50 large-sized organizations in various industries, cybercrime has serious financial consequences for businesses and government institutions despite the high level of awareness of the cyber threat. The report shows that the median annualized cost of cybercrime for 50 organizations is \$5.9 million USD per year, with a range of \$1.5 million to \$36.5 million USD each year per company.

Cyber attacking are criminal activities on the Internet that include create and distribute viruses to infect victims, cyber espionage, post confidential business information on the internet, disrupt a country's critical national infrastructure and hack online bank accounts. Srivastava and Boey (2012) reveal that bullies are able to forward or post personal information or any other offensive materials in the form of writing, picture or video for the public to view that could potentially embarrass, harass, intimidate, threaten or ridicule victims. One of the most distinct features of cyber-bullying is its ability to reach a wider audience as compared to traditional schoolyard bullying. Anonymity and cyber-bullying attitudes are both significant risk factors for cyber-bullying. In fact, anonymity is a positive predictor of cyber-bullying behaviour (Wright, 2013).

Another major element of cybercrime is piracy; illegal copying of software, games, music, movies and others. Piracy is relatively easy to do, quite often requiring not more than a DVD or CD drive, which is able to replicate the original. Music, games, and applications either on computers, laptops or mobile phones can also be simply copied onto the internet to be downloaded anywhere and anytime with Internet. Yar (2016) finds that cyber-harassment and cyber-stalking are the persistent and targeted harassment of an individual using electronic communication channels such as emails and social applications. Cyber-stalking, also known as online victimising, has a very similar characteristic with offline stalking. Most of the victims are women and most stalkers are men. Majority of cases involve stalking by former friends, although stranger stalking sometimes occurs in the real world and in cyberspace. Stalkers are motivated by the desire to control victims or desire to dominate victims (Yar, 2016). Robert and Doyle (2003), point out that cyber-stalking is defined as repeated uses of Internet, social applications, email or related digital electronic communication devices to disturb, alarm, or threaten specific individual.

Cybercrime offenders are more likely to share a broader range of social characteristics and are likely to be young, smart, often without prior criminal records, possess expert knowledge and often motivated by a variety of financial and non-financial goals (Boateng et al., 2011). Controlling the upsurge of cybercrime in resource-poor country is particularly important if the promise of the Internet is yet to reach its full potential and if businesses and consumers are to face significant losses as a result of criminal activities. Youth find modern technologies as alternative to easy access of various illegal activities. This includes online drugs purchase than traditional method from a street dealer. Websites such as Silk Road provide exclusive alternative to purchasing drugs online rather than from traditional

methods from a street dealer which is more dangerous (Phelps & Watt, 2014). Such websites offer a simplified and anonymous service appealing to drug addicts, especially those living in rural areas (Phelps & Watt, 2014). The websites also provide variety of products at low prices and could be purchased in bulk. Not only that such activity pose further threat to the drug issue, it also increases youth exposure and involvement in drugs addiction and cybercrime activities of illegally trading drugs online.

Wiener-Bronner (2014) shows that experienced hackers can easily hack into users social media accounts and later use the gathered information to venture into one's personal email account, work email account and bank information. In 2012, there have been a few cases of a cybercrime activity called 'hacktivism', defined as the act of hacking for political or social reason (Francisco et al., 2015). Hackers are taking their activities to the next level and attempting to reach websites with a large number of visitors. This allows better access of information to affect as many victims as possible. Large websites and companies are at a higher online security risk for these types of acts. Francisco et al., (2015) finds that students underrated their involvements in cyber-bullying, a predicament that one's involvement in cyber-bullying could in fact, part and parcels of college students' life. College students seem to interpret cyber-bullying as one only construct, including both direct and indirect forms of aggression. A group of girls are more likely to harm others than a group of boys. Lim (2013) shows that youth who is associated with delinquent peers and who do not associate with adults are more likely to be drawn into delinquency.

METHODOLOGY

The data analysis procedure used in this study involves the following categories with clear steps.

Category One – Scoring Method

Given that the questions on the direct and indirect involvement in technology related activities are measured using Likert-Scale, the appropriate method is scoring method. Each individual/respondent is then assigned a particular score of each activity. In explaining the scoring method, the following example is employed.

Example for Cybercrime activity with two elements

B1: Cybercrime

B11: Piracy

B111.	Download song/video/picture/software without paying	0	1	2	3	④	5
B112.	Distribute or sell song/video/picture/software that has been downloaded	0	1	2	3	④	5
B113.	Cheating through online interactions	0	①	2	3	4	5

B13: High-Return Investment Scheme

B131.	Promote get-rich-quick scheme	0	1	2	3	4	⑤
B132.	Participate in get-rich-quick scheme	0	1	2	③	4	5
B133.	Involve in online gambling	0	①	2	3	4	5

Step 1: Score of each element for an activity is added to obtain the total score of the activity

$$\text{Score Piracy} = B111+B112+B113 = 9$$

$$\text{Score High-Return Investment Scheme} = B131+B132+B133 = 6$$

This process continues for all elements of the activity.

Step 2: Score of each activity is then added together
 Score Cybercrime = Score Piracy + Score High-Return Investment Scheme = 9 + 6 = 15

Step 3: The score is then recoded to comply with the original 6-point Likert-Scale, following below:

Maximum Total Point of original Likert-Scale	Range	New Likert-Scale	
0	0	0	Not applicable
6	1 – 6	1	Never
12	7 – 12	2	Seldom
18	13 – 18	3	Sometimes
24	19 – 24	4	Often
30	25 – 30	5	Always

The maximum total point of original Likert-Scale is calculated by multiplying the total number of question with the Likert-Scale. For example, there are 6 questions altogether and the maximum score obtained is 30 (6 x 5 = 30).

The above example on cybercrime shows a score of 15 and this provides a new Likert-Scale point of 3. This implies that this particular individual / respondent is ‘sometimes’ involved in cybercrime activity.

Step 4: Using STATA, the mean value of cybercrime for the whole sample is then estimated. Let’s assume that the mean value for cybercrime activity is 4.3. This assumes that youth engagement in cybercrime activity is ‘often’.

Category Two – Categorizing type of technologies

Section A1 is categorized into two types of technologies: New Technology and Old Technology

Old Technology is Laptop / Desktop

New Technology is among others listed in that section (Smart Phone, Tablet/Tab/IPad, iPod)

The calculation on the usage of such technologies follows the scoring method as explained earlier.

Category Three– Regression Analysis

A simple OLS is estimated to investigate the factors influencing youth involvement in Cybercrime activity. The following regression analysis is estimated.

Where

Y is the score for each activity

X is the independent variables to be measured (age, gender, education level, etc.)

u is the error term

Multiple regression analysis are performed with each regression focusing on each activity i.e. Cybercrime, Prior to the further explaining on data analysis, simple descriptive analysis to identify the basic information of respondents is first explained.

RESULTS

The Impact of Access and Usage of Technology on Piracy

Table 1 illustrates the results of the impact of the usage of modern technology on youth involvement in piracy activities. The results indicate that the score of involvement in committing piracy activities of youth who spends less than 3 hours on emails as compared with those who do not use emails would increase by 1.43 points. The score of involvement in committing piracy activities for youth who spends 4-8 hours on emails as compared with those who do not use emails would increase by 1.58 points. The score of involvement in committing piracy activities for youth who spends 9-14 hours on emails as compared with those who do not use emails would increase by 1.32 points. The score of involvement in committing piracy activities for youth who spends 15-23 hours on emails as compared with those who do not use emails would increase by 3.02 points and the score of involvement in committing piracy activities for youth who spends 24 hours on emails as compared to those who do not use emails would increase by 2.88 points. It is noted that the increase in the number of hours spent on emails increases the score of involvement in piracy activities. In other words, more hours spent on emails result in higher score of involvement in piracy activities.

Table 4.1: The Impact of Access and Usage of Modern Technology on Piracy

	Coefficient	Standard Error	t-statistics	Probability
Email				
Less than 3 hours	1.435373	0.311327	4.61	0.000
4 - 8 hours	1.580556	0.35058	4.51	0.000
9 - 14 hours	1.32673	0.373632	3.55	0.000
15 - 23 hours	3.02904	0.481089	6.3	0.000
24 hours	2.888889	0.592588	4.88	0.000
constant	4.402778	0.296294	14.86	0.000
F(5, 1128)	9.99			
Prob> F	0.000			
Instant Messaging				
Less than 3 hours	0.780367	0.501302	1.56	0.120
4 - 8 hours	1.147231	0.499014	2.3	0.022
9 - 14 hours	0.874153	0.499815	1.75	0.081
15 - 23 hours	1.284634	0.500539	2.57	0.010
24 hours	1.836973	0.508014	3.62	0.000
constant	4.724138	0.471454	10.02	0.000
F(5, 1128)	5.43			
Prob> F	0.0001			
Chat Rooms				
Less than 3 hours	0.699828	0.25181	2.78	0.006
4 - 8 hours	0.936872	0.284166	3.3	0.001
9 - 14 hours	0.731685	0.304147	2.41	0.016
15 - 23 hours	1.325815	0.368799	3.59	0.000
24 hours	2.227343	0.509084	4.38	0.000
constant	5.095238	0.226215	22.52	0.000
F(5, 1128)	5.36			
Prob> F	0.0001			

Create blog				
Less than 3 hours	0.899094	0.195959	4.59	0.000
4 - 8 hours	1.648352	0.358156	4.6	0.000
9 - 14 hours	1.349206	0.414502	3.26	0.001
15 - 23 hours	1.596429	0.654421	2.44	0.015
24 hours	3.071429	0.816722	3.76	0.000
constant	5.028571	0.174126	28.88	0.000
F(5, 1128)	8.28			
Prob> F	0.0000			
Social network				
Less than 3 hours	0.431746	0.333215	1.3	0.195
4 - 8 hours	0.867247	0.325252	2.67	0.008
9 - 14 hours	1.25582	0.345897	3.63	0.000
15 - 23 hours	1.716124	0.391137	4.39	0.000
24 hours	2.623502	0.542589	4.84	0.000
constant	4.957143	0.300601	16.49	0.000
F(5, 1128)	9.83			
Prob> F	0.0000			
Old Technology				
Less than 3 hours	0.2113	0.3388	0.62	0.533
4 - 8 hours	0.2742	0.3503	0.78	0.434
9 - 14 hours	0.1880	0.4179	0.45	0.653
15 and above	0.4017	0.6088	0.66	0.510
New Technology				
Less than 3 hours	1.0271	0.4015	2.56	0.011
4 - 8 hours	1.1284	0.4089	2.76	0.006
9 - 14 hours	1.3308	0.5356	2.48	0.013
15 and above	4.6659	0.9040	5.16	0.000
constant	4.5547	0.5100	8.93	0.000
F(5, 1128)	4.44			
Prob> F	0.0000			

Spending less than 3 hours in instant messaging does not significantly increase the score of involvement in piracy. The score of involvement in committing piracy activities for youth who spends 4-8 hours, 9-14 hours and 15-23 hours on instant messaging as compared with those who do not use instant messaging would increase by 1.14 points, 0.87 points and 1.29 points, respectively. The score of involvement in committing piracy activities is the highest at 1.84 points among youth who spends 24 hours on instant messaging as compared with those who do not use instant messaging.

The score of involvement in committing piracy activities for youth who spends less than 3 hours per day on chat rooms as compared with those who do not use chat rooms would increase 0.7 points while the score of youth who spends 4-8 hours per day on chat rooms as compared with those who do not use chat rooms to chat would have a higher score of 0.94 points. The score of involvement in committing piracy activities for youth who spends 9-14 hours per day on chat rooms as compared with those who do not use chat rooms would increase by 0.73 points. The score of involvement in committing piracy activities for youth who spends 15-23 hours per day on chat rooms as compared with those who do not use chat rooms to chat would increase by 1.33 points while the score of involvement in committing piracy activities for youth who spends 24 hours per day on chat rooms as compared with those who do not use chat rooms to chat would increase by 2.23 points.

The study finds that youth who spends less than 3 hours per day creating online blogs as compared with those who do not create blogs would have a higher score of involvement in committing piracy activities by 0.9 points while youth who spends 4-8 hours per day creating online blogs as compared with those who do not create blogs would have score of involvement in committing piracy activities higher by 1.65 points. Youth who spends 9-14 hours per day on creating blogs online as compared with those who do not create blogs would have score of involvement in committing piracy activities higher by 1.35 points while youth who spends 15-23 hours per day creating blogs online as compared to those who do not create blogs would have score of involvement in committing piracy activities higher by 1.6 points. It is found that spending 24 hours creating online blogs as compared with those who do not create blogs significantly increase the score of involvement in committing piracy activities by 3.07 points. It can be concluded that longer time spent on creating online blogs increases youth involvement on piracy.

Spending less than 3 hours on social network does not statistically significantly increases the score of involvement in piracy. Youth who spends 4-8 hours on social network as compared with those who are not involve in social networking would have an increase in the score of involvement in committing piracy activities by 0.87 points. Youth who spends 9-14 hours on social network as compared with those who do not involve in social networking would increase the score of involvement in committing piracy activities by 1.26 points while youth who spends 15-23 hours on social network as compared to those who do not involve in social networking would increase the score of involvement in committing piracy activities by 1.72 points. Spending 24 hours on social networking would gradually increase the involvement of youth in piracy activities by 2.62 points. Spending more hours on social networking significantly increase youth's involvement on piracy activities as proved by the data above.

Old technology is found not to be statistically significant in influencing youth involvement in piracy. On the other hand, youth who spends less than 3 hours using new technologies as compared with those who do not use new technologies would increase the score of involvement in committing piracy activities by 1.03 points. Youth who spends 4-8 hours using new technologies as compared with those who do not use new technologies would increase the score of involvement in committing piracy by 1.13 points and youth who spends 9-14 hours using new technologies as compared with those who do not use new technologies would increase the score of involvement in committing piracy activities by 1.33 points. Spending over 15 hours using new technologies will significantly increase the involvement of youths in piracy activities, which is by 4.67 points. This indicates that youth who are exposed to new technologies for long hours positively affect their involvements on piracy.

The Impact of Access and Usage of Modern Technology on Fraud Online Business

Table 2 illustrates the results of the impact of access and usage of modern technology on fraud online business. The results indicate that youth who spends less than 3 hours on online transaction as compared with those who do not use online transaction would increase the score of involvement in fraud online business by 0.56 points. Youth who spends 9-14 hours using online transaction as compared with those who do not use online transaction would increase the score of involvement in fraud online business by 1.06 points while youth who spends 15-23 hours on online transaction as compared with those who do not use online transaction would increase the score of involvement in fraud business by 2.4 points. Spending 24 hours on online transaction results in 3.04 points increase of youth involvement in fraud online business. This indicates that the longer the youths transact online, the higher is their engagement in fraud online business.

Spending less than 14 hours on social network does not significantly influence the score of involvement on fraud online business. Youth who spends 15-23 hours on social network as compared with those who are not involve in social networking would increase the score of involvement in fraud online business by 1.03 points. Youth who spends 24 hours on social network as compared with those who are not involve in social networking would increase the score of involvement in fraud online business by 2.6 points. Spending more hours on social networking increases the involvement in fraud online business but the effect is minimum.

Youth who spends less than 3 hours per day creating online blogs as compared with those who do not create blogs would increase the score of involvement in fraud online business by 0.63 points. Youth who spends 4-8 hours per day creating online blogs as compared with those who do not create blogs would increase the score of involvement in fraud online business by 1.1 points. Youth who spends 9-14 hours per day creating online blogs as compared with those who do not create blogs would increase the score of involvement in fraud online business by 1.57 points. Youth who spends 15-23 hours per day creating online blogs as compared with those who do not create blogs would increase the score of involvement in fraud online business by 2.57 points. Spending 24 hours creating online blogs as compared with those who do not create blogs would increase the score of involvement in fraud online business by 4.69 points. It can be concluded that the more time spent on creating blogs would increase youth involvement in fraud online business.

Youth who spends less than 3 hours per day on email as compared with those who do not use email would increase the score of involvement in fraud online business by 0.94 points. Youth who spends 4-8 hours per day on email as compared with those who do not use email would increase the score of involvement in fraud online business by 1.23 points. Youth who spends 9-14 hours per day on email as compared with those who do not use email would increase the score of involvement on fraud online business by 0.9 points. Youth who spends 15-23 hours per day on email as compared with those who do not use email would increase the score of involvement in fraud online business by 2.72 points. Youth who spends 24 hours per day on email as compared with those who do not use email would increase the score of involvement in fraud online business by 2.24 points. It is noted that the prolonged number of hours spend on emails increases the score of involvement in fraud online business.

The study found that spending less than 3 hours on instant messaging is statistically insignificant in influencing involvement in fraud online business. Youth who spends 4-8 hours on instant messaging as compared with those who do not spend time on instant messaging would increase the score of fraud online business by 1.12 points. Youth who spends 15-23 hours on instant messaging compared with those who do not spend time on instant messaging would increase the score of involvement in fraud online business by 1.06 points. Youth who spends 24 hours on instant messaging as compared with those who do not spend time on instant messaging would increase the score of involvement in fraud online business by 1.78 points. This indicates that more time spend on instant messaging increases the score of involvement in fraud online business.

Youth who spends less than 3 hours per day on chat rooms as compared with those who do not use chat rooms would increase the score of involvement in fraud online business by 0.49 points. Spending 4-8 hours per day on chat rooms is statistically insignificant in influencing involvement in fraud online business. Youth who spends 9-14 hours per day on chat rooms as compared with those who do not use chat rooms would increase the score of involvement on fraud online business by 0.65 points Youth who spends 15-23 hours per day on chat rooms as compared with those who do not use chat rooms would increase the score of involvement in fraud online business by 0.99 points. Youth who spends 24 hours per day on chat rooms as compared with those who do not use chat rooms would increase the score of involvement in fraud online business by 2.27 points.

Spending less than 8 hours on new technologies does not have a significant effect on youth involvement in fraud online business as compared with those who do not use new technologies. Youth who spends 9-14 hours per day on new technologies as compared with those who do use new technologies would increase the involvement score in fraud online business by 1.27 points. Youth who spends more than 15 hours on new technologies as compared with those who do not use new technologies would increase the score involvement in fraud online business by 5.18 points.

Table 4.2: The impact of access and usage of modern technology on Fraud Online Business

	Coefficient	Standard Error	t-statistics	Probability
Online transaction				
Less than 3 hours	0.56174	0.3003	1.87	0.062
4 - 8 hours	0.528289	0.32198	1.64	0.101
9 - 14 hours	1.057456	0.409181	2.58	0.010
15 - 23 hours	2.396212	0.485172	4.94	0.000
24 hours	3.041667	0.792989	3.84	0.000
constant	4.458333	0.271993	16.39	0.000
F(5, 1127)	7.53			
Prob> F	0.0000			
Social Network				
Less than 3 hours	0.210458	0.397247	0.53	0.596
4 - 8 hours	0.543902	0.387754	1.4	0.161
9 - 14 hours	0.534259	0.412367	1.3	0.195
15 - 23 hours	1.03	0.467253	2.2	0.028
24 hours	2.593548	0.646856	4.01	0.000
constant	4.6	0.358367	12.84	0.000
F(5, 1127)	4.62			
Prob> F	0.0004			
Web2				
Less than 3 hours	0.634216	0.243048	2.61	0.009
4 - 8 hours	1.096845	0.368718	2.97	0.003
9 - 14 hours	1.566845	0.441597	3.55	0.000
15 - 23 hours	2.566845	0.684976	3.75	0.000
24 hours	4.691845	1.074548	4.37	0.000
constant	4.433155	0.217647	20.37	0.000
F(5, 1127)	8.04			
Prob> F	0.0000			
Email				
Less than 3 hours	0.941795	0.370479	2.54	0.011
4 - 8 hours	1.230556	0.41719	2.95	0.003
9 - 14 hours	0.902778	0.445304	2.03	0.043
15 - 23 hours	2.72096	0.572497	4.75	0.000
24 hours	2.236111	0.70518	3.17	0.002
constant	4.097222	0.35259	11.62	0.000
F(5, 1127)	5.62			
Prob> F	0.0000			
Instant Messaging				
Less than 3 hours	0.737341	0.59338	1.24	0.214
4 - 8 hours	1.117756	0.590671	1.89	0.059
9 - 14 hours	0.832744	0.59162	1.41	0.160
15 - 23 hours	1.058227	0.592477	1.79	0.074
24 hours	1.780196	0.601558	2.96	0.003
constant	4.068966	0.558049	7.29	0.000
F(5, 1127)	3.57			
Prob> F	0.0033			

Chat Rooms				
Less than 3 hours	0.493088	0.298215	1.65	0.099
4 - 8 hours	0.515727	0.336535	1.53	0.126
9 - 14 hours	0.65293	0.360198	1.81	0.070
15 - 23 hours	0.988571	0.438577	2.25	0.024
24 hours	2.267281	0.602904	3.76	0.000
constant	4.571429	0.267904	17.06	0.000
F(5, 1127)	3.26			
Prob> F	0.0062			
Old Technology				
Less than 3 hours	0.202261	0.398065	0.51	0.611
4 - 8 hours	0.183562	0.411562	0.45	0.656
9 - 14 hours	0.325132	0.491743	0.66	0.509
15 and above	1.095983	0.715183	1.53	0.126
New Technology				
Less than 3 hours	0.656268	0.471624	1.39	0.164
4 - 8 hours	0.664752	0.480431	1.38	0.167
9 - 14 hours	1.266432	0.629117	2.01	0.044
15 and above	5.183785	1.061884	4.88	0.000
constant	4.18654	0.599112	6.99	0.000
F(5, 1128)	5.49			
Prob> F	0.0000			

The Impact of Access and Usage of Modern Technology on High Return Investment

Table 3 shows the result of the impact of access and usage of modern technology on high return investment. Result shows that instant messaging and new technologies involvement do not affect youth involvement in high return investment. Only youth who spends 15-23 hours per day using emails are said to be have higher score of involvement in high return investment as compared with those who do not use email by 1.42 points.

Youth who spends 15-23 hours using chat rooms as compared with those who do not use chat rooms would increase score of involvement in high return investment by 0.76 points. Youth who spends 24 hours on chat rooms as compared with those who do not use chat rooms would increase the score of involvement in high return investment by 1.45 points. This shows that chat rooms do have an effect on youth involvement in high return investment when time spends on chat rooms increases.

Youth who spends 24 hours on social networking as compared with those who are not involved in social networking would increase the score of involvement in high return investment by 1.26 points. Youth who spends 15-23 hours on online transaction as compared with those who do not spend time on online transaction would increase the involvement in high return investment by 1.31 points. Youth who spends 24 hours on social networking as compared with those who do not spend time on social networking would increase the score of involvement score in high return investment by 1.44 points.

Spending less than 8 hours creating online blogs is found to be insignificant in influencing involvement in high return investment. Youth who spends 9-14 hours on creating online blogs as compared with those youth who do not create blogs would increase the involvement in high return investment by 1.36 points. Youth who spends 15-23 hours creating online blogs as compared with those who do not create blogs would increase the score of involvement in high return investment by 1.38 points. Youth who spends 24 hours creating online blogs as compared with those who do not create

blogs would increase the score of involvement in high return investment by 5.3 points. This result concludes that time spent creating online blogs is significant in influencing the score of involvement in high return investment.

Interestingly, youth who spends 15 hours and more on old technologies positively impact their involvement in high return investment by 1.68 points.

Table 4.6: The impact of access and usage of modern technology on High Return Investment

	Coefficient	Standard Error	t-statistics	Probability
Email				
Less than 3 hours	-0.06439	0.268926	-0.24	0.811
4 - 8 hours	0.122222	0.302833	0.4	0.687
9 - 14 hours	0.264572	0.322745	0.82	0.413
15 - 23 hours	1.419192	0.415567	3.42	0.001
24 hours	0.638889	0.51188	1.25	0.212
constant	4.694444	0.25594	18.34	0.000
F(8, 1125)	4.48			
Prob> F	0.005			
Instant Messaging				
Less than 3 hours	-0.73998	0.429792	-1.72	0.085
4 - 8 hours	-0.34669	0.42783	-0.81	0.418
9 - 14 hours	-0.62541	0.428517	-1.46	0.145
15 - 23 hours	-0.30399	0.429138	-0.71	0.479
24 hours	0.049808	0.435547	0.11	0.909
constant	5.172414	0.404202	12.8	0.000
F(8, 1125)	3.44			
Prob> F	0.0044			
Chat Rooms				
Less than 3 hours	-0.22319	0.214747	-1.04	0.299
Less than 3 hours	-0.11686	0.242341	-0.48	0.630
4 - 8 hours	-0.01465	0.259381	-0.06	0.955
9 - 14 hours	0.756266	0.314517	2.4	0.016
24 hours	1.448541	0.434155	3.34	0.001
constant	4.809524	0.192919	24.93	0.000
F(8, 1125)	5.81			
Prob> F	0.000			
Social Network				
Less than 3 hours	-0.60458	0.286656	-2.11	0.035
4 - 8 hours	-0.22683	0.279805	-0.81	0.418
9 - 14 hours	-0.24074	0.297566	-0.81	0.419
15 - 23 hours	0.316832	0.336484	0.94	0.347
24 hours	1.258065	0.466775	2.7	0.007
constant	5	0.258599	19.33	0
F(8, 1125)	6.22			
Prob> F	0.000			

Online Transaction				
Less than 3 hours	-0.07605	0.218034	-0.35	0.727
4 - 8 hours	-0.17809	0.233813	-0.76	0.446
9 - 14 hours	0.260526	0.297135	0.88	0.381
15 - 23 hours	1.304545	0.352318	3.7	0.000
24 hours	1.4375	0.575846	2.5	0.013
constant	4.75	0.197513	24.05	0.000
F(8, 1125)	6.21			
Prob> F	0.000			
Web				
Less than 3 hours	0.070217	0.173417	0.4	0.686
4 - 8 hours	0.14246	0.263119	0.54	0.588
9 - 14 hours	1.355793	0.315126	4.3	0.000
15 - 23 hours	1.374841	0.488802	2.81	0.005
24 hours	5.29746	0.766802	6.91	0.000
constant	4.57754	0.155314	29.47	0.000
F(8, 1125)	14.97			
Prob> F	0.000			
Old Technology				
Less than 3 hours	0.133687	0.285649	0.47	0.640
4 - 8 hours	0.160414	0.295334	0.54	0.587
9 - 14 hours	0.310688	0.352285	0.88	0.378
15 and above	1.681556	0.513208	3.28	0.001
New Technology				
Less than 3 hours	-0.13543	0.338426	-0.4	0.689
4 - 8 hours	-0.15033	0.344718	-0.44	0.663
9 - 14 hours	0.051432	0.451446	0.11	0.909
15 and above	3.101022	0.762	4.07	0.000
constant	4.668518	0.429908	10.86	0.000
F(8, 1125)	8.16			
Prob> F	0.0000			

The Impact of Access and Usage of Modern Technology on Falsifying Information

Table 1 illustrates the results of the impact of the usage of modern technology on falsifying information. The result indicates that youth who spends less than 3 hours on emails as compared with those who do not use emails would increase the score of exposure to fake information by 1.14 point. Youth who spends 4-8 hours, 9-14 hours, 15-23 hours and 24 hours on emails as compared with those who do not use emails would increase the score of involvement on falsifying information by 1.3, 0.86, 2.39 and 2.15 points, respectively. It is noted that the increase number of hours spent on emails increase the score of involvement on falsifying information.

Spending less than 14 hours on instant messaging does not statistically significantly affect the score of involvement on falsifying information. Youth who spends 15-23 hours and 24 hours on instant messaging as compared with those who do not use instant messaging would increase the score of involvement on falsifying information by 1.18 and 1.86 points, respectively.

Spending less than 8 hours on chat rooms does not statistically influence the score of involvement on falsifying information. Youth who spends 9-14 hours, 15-23 hours and 24 hours on chat rooms as

compared with those who do not use chat rooms would increase the score of involvement on falsifying information by 0.71, 0.96 and 2.08 points. It is noted that the increase number of hours spent on chat rooms increases the score of involvement on falsifying information.

Spending less than 14 hours on social networking does not statistically significantly affect the score of involvement on falsifying information. Youth who spends 15-23 hours and 24 hours on social networking as compared with those who do not spend time on social networking would increase the score of involvement on falsifying information by 0.66 and 1.63 points, respectively.

Spending less than 3 hours using online transaction as compared with those who do not make any online transaction would increase the score of involvement on falsifying information by 0.5 points. Youth who spends 15-23 hours and 24 hours on online transaction as compared with those who do not spend time on online transaction would increase the score of involvement on falsifying information by 1.96 and 2.46 points.

Youth who spends less than 3 hours, 4-8 hours, 9-14 hours and 24 hours creating blogs as compared with those who do not create blogs would increase the score of involvement on falsifying information by 0.56, 0.68, 1.13 and 3.43 points, respectively.

Spending less than 8 hours on social networking with new friends does not significantly influence the score of involvement on falsifying information. Youth who spends 9-14 hours, 15-23 hours and 24 hours on social networking with new friends as compared with those who do not spend time on social networking would increase the score of involvement on falsifying information by 0.68, 0.9 and 2.28 points. Based on the results, spending 24 hours on online business would increase the score of score of involvement on falsifying information by 1.41 points.

Spending less than 8 hours on new technology does not significantly influence the score of involvement on falsifying information. Youth who spends 9-14 hours and over 15 hours on new technology as compared with those who do not spend time on new technology would increase the score of involvement on falsifying information by 1.23 and 4.84 points.

Table 4.8: The impact of access and usage of modern technology on Fake Information

	Coefficient	Standard Error	t-statistics	Probability
Email				
Less than 3 hours	1.139049	0.359167	3.17	0.002
4 - 8 hours	1.3	0.404451	3.21	0.001
9 - 14 hours	0.863843	0.431046	2	0.045
15 - 23 hours	2.391414	0.555015	4.31	0.000
24 hours	2.152778	0.683648	3.15	0.002
constant	3.972222	0.341824	11.62	0.000
F(5, 1128)	4.78			
Prob> F	0.0003			
Instant messaging				
Less than 3 hours	0.783784	0.573472	1.37	0.172
4 - 8 hours	1.141079	0.570854	2	0.046
9 - 14 hours	0.858974	0.571771	1.5	0.133
15 - 23 hours	1.179825	0.5726	2.06	0.040
24 hours	1.855556	0.581151	3.19	0.001
constant	4	0.539327	7.42	0.000

F(5, 1128)	4.16			
Prob> F	0.0009			
Chat rooms				
Less than 3 hours	0.275022	0.288321	0.95	0.340
4 - 8 hours	0.315349	0.325369	0.97	0.333
9 - 14 hours	0.705434	0.348247	2.03	0.043
15 - 23 hours	0.959482	0.422274	2.27	0.023
24 hours	2.075781	0.5829	3.56	0.000
constant	4.698413	0.259015	18.14	0.000
F(5, 1128)	3.67			
Prob> F	0.0027			
Social networking				
Less than 3 hours	-0.12951	0.385907	-0.34	0.737
4 - 8 hours	0.072822	0.376685	0.19	0.847
9 - 14 hours	0.130027	0.400595	0.32	0.746
15 - 23 hours	0.65785	0.452988	1.45	0.147
24 hours	1.627189	0.628391	2.59	0.010
constant	4.985714	0.348137	14.32	0.000
F(5, 1128)	2.84			
Prob> F	0.0147			
Online transaction				
Less than 3 hours	0.503825	0.291957	1.73	0.085
4 - 8 hours	0.30301	0.313085	0.97	0.333
9 - 14 hours	0.610526	0.397877	1.53	0.125
15 - 23 hours	1.963636	0.471769	4.16	0.000
24 hours	2.4625	0.771083	3.19	0.001
constant	4.6	0.264479	17.39	0.000
F(5, 1128)	5.29			
Prob> F	0.0001			
Web				
Less than 3 hours	0.558485	0.237442	2.35	0.019
4 - 8 hours	0.683155	0.360261	1.9	0.058
9 - 14 hours	1.133155	0.431469	2.63	0.009
15 - 23 hours	1.099822	0.669266	1.64	0.101
24 hours	3.433155	1.049902	3.27	0.001
constant	4.566845	0.212656	21.48	0.000
F(5, 1128)	3.58			
Prob> F	0.0032			
Social networking with new friends				
Less than 3 hours	0.380715	0.255769	1.49	0.137
4 - 8 hours	0.427907	0.297886	1.44	0.151
9 - 14 hours	0.681746	0.327681	2.08	0.038
15 - 23 hours	0.899656	0.454225	1.98	0.048
24 hours	2.277962	0.673105	3.38	0.001
constant	4.674419	0.222031	21.05	0.000
F(5, 1128)	2.97			
Prob> F	0.0114			

Online Business				
Less than 3 hours	0.114505	0.31191	0.37	0.714
4 - 8 hours	-0.03623	0.323521	-0.11	0.911
9 - 14 hours	0.434179	0.336477	1.29	0.197
15 - 23 hours	0.2	0.3844	0.52	0.603
24 hours	1.413487	0.49727	2.84	0.005
constant	4.913043	0.271812	18.08	0.000
F(5, 1128)	2.51			
Prob> F	0.0286			
Old Technology				
Less than 3 hours	-0.01965	0.388039	-0.05	0.960
4 - 8 hours	-0.06949	0.401196	-0.17	0.863
9 - 14 hours	0.393277	0.478561	0.82	0.411
15 and above	-0.4727	0.697166	-0.68	0.498
New Technology				
Less than 3 hours	-0.01965	0.388039	-0.05	0.960
4 - 8 hours	-0.06949	0.401196	-0.17	0.863
9 - 14 hours	0.393277	0.478561	0.82	0.411
15 and above	-0.4727	0.697166	-0.68	0.498
constant	4.323756	0.584009	7.4	0.000
F(8, 1125)	3.37			
Prob> F	0.008			

The Impact of Access and Usage of Modern Technology on Virus Distribution

Table 5 shows the result of impact of access and usage of modern technology on virus distribution. Based on the result, youth who spends less than 3 hours, 4-8 hours, 9-14 hours, 15-23 hours and 24 hours per day on email as compared with those who do not spend time on email would increase the score of involvement in virus distribution by 0.99, 1.25, 0.85, 2.2 and 2.04 points, respectively.

Spending less than 14 hours per day on instant messaging does not significantly influence their involvement in virus distribution. Youth who spends 15-23 hours and 24 hours per day on instant messaging as compared with those who do not spend any time on instant messaging would increase the score of involvement in virus distribution by 1.2 and 1.6 points, respectively. This indicates that youth who spend more time on instant messaging will have higher score of involvement in virus distribution as compared to those who did not.

Youth who spends less than 3 hours per day using smart phone as compared with those who did not use smart phone would increase the score of involvement in virus distribution by 0.95 points. Spending more than 3 hours per day using smart phone does not significantly influence youth involvement in virus distribution.

Spending less than 8 hours per day on chat rooms does not significantly affect youth involvement in virus distribution. Youth who spends 9-14 hours, 15-23 hours and 24 hours on chat rooms as compared with those who do not spend time on chat rooms would increase the score of involvement in virus distribution by 0.72, 0.84 and 2.03 points, respectively.

Spending less than 14 hours on online transaction does not significantly influence the score of involvement in virus distribution. Youth who spends 15-23 hours and 24 hours on online transaction as compared with those who do not spend time on online transaction would increase the score of involvement in virus distribution by 2.1 and 1.83 points, respectively.

The result indicates that engagement on social networking does not significantly influence youth involvement in virus distribution.

Youth who spends less than 3 hours, 4-8 hours, 9-14 hours, 15-23 hour and 24 hours per day creating blogs as compared with those who do not do create blog would increase the score of involvement in virus distribution by 0.49, 0.87, 1.31, 1.16 and 3.17 points, respectively.

The result also indicates that youth who spends less than 3 hours, 4-8 hours, 9-14 hours, 15-23 hours and 24 hours per day on new technology as compared with those do not spend time on new technology would increase the score of involvement in virus distribution by 0.91, 0.81, 1.21 and 4.28 points, respectively. Involvement on old technology does not significantly influence youth engagement in virus distribution.

Table 4.10: The impact of access and usage of modern technology on Virus Distribution

	Coefficient	Standard Error	t-statistics	Probability
Email				
Less than 3 hours	0.988199	0.370081	2.67	0.008
4 - 8 hours	1.252778	0.416741	3.01	0.003
9 - 14 hours	0.844945	0.444144	1.9	0.057
15 - 23 hours	2.200758	0.57188	3.85	0.000
24 hours	2.041667	0.704422	2.9	0.004
constant	3.958333	0.352211	11.24	0.000
F(5, 1128)	3.93			
Prob> F	0.0015			
Instant Messaging				
Less than 3 hours	0.749146	0.591905	1.27	0.206
4 - 8 hours	1.006725	0.589203	1.71	0.088
9 - 14 hours	0.94076	0.590149	1.59	0.111
15 - 23 hours	1.196158	0.591004	2.02	0.043
24 hours	1.596743	0.59983	2.66	0.008
constant	3.931034	0.556662	7.06	0.000
F(5, 1128)	2.54			
Prob> F	0.0271			
Smartphone				
Less than 3 hours	0.946863	0.398985	2.37	0.018
4 - 8 hours	0.516241	0.361943	1.43	0.154
9 - 14 hours	0.535507	0.39969	1.34	0.181
15 - 23 hours	0.673634	0.507601	1.33	0.185
24 hours	1.102372	0.927504	1.19	0.235
constant	3.452853	0.606003	5.7	0
F(10, 1123)	1.91			
Prob> F	0.0407			
Chat Rooms				
Less than 3 hours	0.306783	0.296849	1.03	0.302
4 - 8 hours	0.246323	0.334992	0.74	0.462
9 - 14 hours	0.715507	0.358547	2	0.046

15 - 23 hours	0.841688	0.434763	1.94	0.053
24 hours	2.033538	0.60014	3.39	0.001
constant	4.579365	0.266676	17.17	0.000
F(5, 1128)	3.19			
Prob> F	0.0072			

Online Transaction

Less than 3 hours	0.491166	0.300696	1.63	0.103
4 - 8 hours	0.336065	0.322457	1.04	0.298
9 - 14 hours	0.50614	0.409787	1.24	0.217
15 - 23 hours	2.098485	0.485891	4.32	0.000
24 hours	1.829167	0.794164	2.3	0.021
constant	4.483333	0.272396	16.46	0.000
F(5, 1128)	4.65			
Prob> F	0.0003			

Social Networking

Less than 3 hours	-0.04099	0.398116	-0.1	0.918
4 - 8 hours	0.120209	0.388602	0.31	0.757
9 - 14 hours	0.15291	0.413268	0.37	0.711
15 - 23 hours	0.706082	0.467319	1.51	0.131
24 hours	0.97788	0.64827	1.51	0.132
constant	4.828571	0.35915	13.44	0.000
F(5, 1128)	1.45			
Prob> F	0.2027			

Web

Less than 3 hours	0.493933	0.244149	2.02	0.043
4 - 8 hours	0.870107	0.370437	2.35	0.019
9 - 14 hours	1.306774	0.443656	2.95	0.003
15 - 23 hours	1.159155	0.68817	1.68	0.092
24 hours	3.165107	1.079557	2.93	0.003
constant	4.459893	0.218662	20.4	0.000
F(5, 1128)	3.69			
Prob> F	0.0026			

Old Technology

Less than 3 hours	-0.10295	0.400325	-0.26	0.797
4 - 8 hours	-0.09432	0.413898	-0.23	0.820
9 - 14 hours	0.208587	0.493713	0.42	0.673
15 and above	-0.25201	0.719239	-0.35	0.726

New Technology

Less than 3 hours	0.912345	0.474289	1.92	0.055
4 - 8 hours	0.81352	0.483107	1.68	0.092
9 - 14 hours	1.204767	0.632683	1.9	0.057
15 and above	4.280516	1.067911	4.01	0.000
constant	4.156829	0.602499	6.9	0.000
F(8, 1125)	2.49			
Prob> F	0.0113			

DISCUSSION

The impact of access and usage of technology on involvement in cybercrime

The increase usage of Internet and modern technologies has resulted in the increase of electronic piracy. Results indicate that increased number of hours using Internet lead to an increase in the score of involvement in cybercrime. Youth use various ways and tools for cybercrime activities. The use of emails, instant messaging, chat rooms, blogs, social networking and smart devices are significant medium that increases the score of involvement in piracy activities. Piracy activities include downloading videos, songs and software without paying, distributing pirated materials and cheating people through online interactions. Studies have proved that youth who are frequently using online chatting are more engaged in piracy activities. They use online chatting as a tool to target new victims (Khajehnoori, 2010; Ybarra & Mitchell, 2004). One of the important reasons that lead to software piracy is the expensive original software or licensed copies. This is coupled with the advancement of technology providing easy access to recording via personal computers and distributing materials via the Internet. As such, copying and distributing of software or materials are made easy either manually to peers or electronically via blogs and other websites. While statistics have indicated that piracy rates in Malaysia have been slightly reduced from 56% in 2010 to 55% in 2011 (DNA, 2012), our study indicates that almost 80% of Malaysian youths admit that they have involved in piracy activities at least one time. This finding is similar to the findings of Digital News Asia that 78% of internet users admit that they have acquired pirated software (DNA, 2012).

In addition, youth uses emails, instant messaging, blogs, social network, online transactions, chat rooms and smart devices to commit fraud online business, involve in high return investment scheme and falsify information. Results indicate that 17% of the respondents advertised and sold goods and services that are not theirs at least one time. 15% admit that they have sold illegal goods and services, 14% cheated in online shopping and 15% online purchased illegal goods and services. 13% of youths promoted get-rich-quick schemes, 14% participated in such schemes and another 7% were involved in online gambling. These percentages may seem low but could be worse and may affect the whole online industry if proper measures to curb such behaviours are not implemented. It is clear that youths are investing in advanced and sophisticated technologies available today and develop highly and advance levels of fraud strategies (McFadden, 2007). There are several reasons that could motivate youths to engage in online fraud. Material acquisition is a key factor that leads to online fraud involvement (Atwai, 2011; Holt, 2011; Burton et al., 1999). Youths nowadays have sophisticated lifestyles; they want and crave for expensive things, devices, gadgets and fashions. Since the youths in this study are still pursuing their education and not many are working, it is understood that the income they received from loans, scholarships or parents may be inadequate to cover their expenses. Thus, few of them choose to engage in illegal activities to earn easy money and therefore buy what they want and like. This situation is supported by the findings of Al-Zahrani (2015) who indicates that single students are more inclined to be involved in cyber bullying as compared with married students. As most single students rely on their parents to finance their daily expenses, those who realized inadequate financing would revert to online fraud in attempt to gain more income. In contrast, most married students have some secure source of income that deters them from such involvement. Youths use and implement various ways and methods to commit online fraud. This includes fake website to gain profit (13%), distribute false news (15%), use third party information for personal gains (15%) and forge and plagiarise online documents and materials (19%). Studies have proven that most fraud activities are committed by youths aged between 17 and 30 years old (Rogers, Siegfried & Tidke, 2006). This is consistent with our findings as the results indicate that age is a significant factor that determines youth involvement in cybercrime activities. Our results illustrate that a one (1) year increase in age would decrease the score of involving in cybercrime activities by 0.08 points. This means that younger youth have more tendencies to involve in cybercrime activities as compared to older youth. Male is more likely to engage in cybercrime

activities as compared to female. This is consistent with other studies by Wong et al., (2014), Al-Zahrani (2015) and Barlett (2015). Furthermore, the higher the level of education the youth acquires, the more is youth's involvement in cybercrime. This is due to the fact that education helps youth to learn and master various ways and tools of cybercrime and online fraud activities. This statement is in line with the findings of Francisco et al., (2015).

RECOMMENDATIONS

Our proposed recommendations are divided into two main sections. The first section of recommendations is based on direct findings of the study while the second section of recommendations is more of a general recommendation to curb negative influence of technology on youths.

1. Specific recommendations from study findings

- a. The study finds that the longer hours spent on Internet or technology related activities promote negative behaviours such as cybercrime, behaviour problems, sexual activities and truancy. From the regression analysis, the study finds that the common medium or channel use to engage in negative Internet or Technology related activities is emails, blog creation, online transactions and new technology. The regression analysis also finds that age (younger youth), gender (male), ethnicity (Malay), accommodation (Flat/Apartment/Condominium) and region (Klang Valley) are the significant socio demographic variables influencing youth involvement in Internet and Technology related activities.
- b. As such, the followings are proposed.
 - i. We propose that two set of rules/policies are imposed on two different age categories. Youth aged 21 years old and below is subject to a 'control/educate' policy while youth above 21 years old is not subject to such policy but provided with proper avenue to practice their technology skills.
 - ii. 'Control/Educate' Policy for youth aged 21 years old and below
 1. This study reveals that higher score of involvement on negative technology related activities start at 9 – 14 hours.
 2. As such, youth aged 21 years old and below is only allowed to use the Internet for a maximum of 8 hours per day.
 3. This policy can only be implemented through the cooperation with all stakeholders such as the government and Internet providers (Unifi, ASTRO, Maxis, and all private internet providers such as Starbucks, Coffee Bean and McDonald).
 4. This policy requires all individuals (regardless of age) to register for Internet, similar to what is currently adopted that requires all individual to registering prepaid card before being allowed to use it. (PUT INFORMATION ON YEAR AND HOW THIS WORK) Incidentally, all Internet users need to register their details prior to be allowed accessed to Internet. Adult, guardian or parent has to register for minors. Once registered, the system will detect the number of hours spent on the Internet, regardless where youth use the Internet. The system will cut itself once the daily quota of usage has been met.

5. This is similar to many Internet applications for children that require adult / parent approval via parent's email address or parent login consent. (PUT EXAMPLE OF APPLICATION).
- iii. Proper Avenue to practice skills on Internet or technology related activities by youth over 21 years old.
 1. Youth over 21 years old want to be treated as adult. (PUT SOURCE). Any attempt to control them would only lead to more rebellious act (PUT SOURCE).
 2. Therefore, the study recommends that a centre named 'innovation centre' is set up in every municipal area.
 3. Youth can come to this centre to practice or execute their creative and innovative ideas on technology.
 4. For example – one centre could allow youth to be involved in anti-piracy innovation. One project could be designing ways to hack an ATM machine. The most effective ways in solving the issue would be rewarded.
 5. To minimize cost, new centre need not be built. As it is there are a lot of community areas that have not been fully utilized and these centre could be used for such engagement. (PUT SOURCE).
 6. The current Jawatankuasa Kemajuan Kampung (JKK) scope of responsibility could be expanded to monitor youth at this centre. Volunteers among university students or any member of the public could also be recruited to do community work at the centre.
 7. The centre could provide prizes and cash for youth involved in such engagement; identify Internet threats and provide solutions for these threats such as malicious programs, spam and phishing.
 8. Competitions could also be arranged that involved youth all over Malaysia. But, this requires sponsorship from various organizations. For example – for innovation on hacking ATM Machine, sponsors could be among financial institutions as the technology could definitely benefit them.
 9. This strategy is a similar solution adopted by Google and Apple. (PUT SOURCE & EXAMPLE).
 - iv. This policy is a holistic approach that cut across various dimensions of socio demographic profiles of youth and the use of various Internet and Technology related activities such as emails, blog creation and online transactions. Effective control of such dimensions and effective use of creative idea could be enhanced to maximise the great potential of technology.
2. General recommendation to curb negative influence of technology on youth.
 - i. We propose a development of a three-stage construct (Awareness – Knowledge – Culture) to encourage positive behaviour and attitude towards technology.

- ii. The important element is Awareness that need to be inculcated in youth. Knowledge and Culture are the by-products or outcome of Awareness that are achieved upon the success of awareness. As we can be observed that citizens in many developed countries have the culture of abiding rules and regulations due to the strict implementation of the rules and regulations. Over time, such practise has become a culture and normal behaviour.
- iii. We follow the guidelines of 'Safe and Responsible Use' (SERU) of Internet a guide for educators as outlined by the United Nations. This has been successfully implemented in schools of some countries such as Scotland, Australia, Denmark and Thailand. The guidelines include:-
 - a. Set-up of wide network of national awareness-raising centres that promote safe and responsible use of online technology particularly among children and young people.
 - b. The avenue proposed in 1 (b) (iii) above could also be used to execute this activity. All centres are linked with network Internet to ease communication with all youth around Malaysia and around the globe.
 - c. With advised from the government and other stakeholders, the awareness-raising centres would develop mechanisms and programs to promote safe and responsible use of technology among youth. Among the programs (as practised by other countries) are:
 - i. Tackling unwanted and harmful content by promoting parental control tools and testing the effectiveness of available filters (European Union Safer Internet Programme).
 - ii. Supporting information exchange on safer Internet use particularly for personalised interactive and mobile applications (European Union Safer Internet Programme).
 - iii. Teaching Internet safety via video discussions where anyone can view and discuss videos used to teach Internet safety (Education Scotland Foghlam Alba)
 - iv. Providing teachers and authorised staff certain powers when they have reasonable grounds to believe that a student has digital information stored on their digital device or technology that is endangering the emotional or physical safety of other students or detrimentally affecting the learning environment (Ministry of Education, New Zealand).

REFERENCES

- Al-Zahrani, A.M. 2015. Cyberbullying among Saudi's Higher-Education Students: Implications for Educators and Policymakers. *World Journal of Education*, 5(3), 15-26.
- Atwai. 2011. Youth cybercrime influenced by peers youth today. University of Liverpool. <http://www.youthtoday.org/viewarticle.cfm?article id=4859>
- Bakar, M.S.A., & Bidin, R. 2014. Technology acceptance and purchase intention towards movie mobile advertising among youth in Malaysia. *Procedia-Social and Behavioral Sciences*, 130, 558-567.
- Barlett, C.P. 2015. Predicting adolescent's cyberbullying behavior: A longitudinal risk analysis. *Journal of Adolescence*, 41, 86-95.
- Baturay, M.H., & Toker, S. 2015. An investigation of the impact of demographics on cyberloafing from an educational setting angle. *Computers in Human Behavior*, 50, 358-366.
- Blinka, L. & Smahel, D. 2012. Predictors of adolescents' excessive Internet use: A comparison across European countries. *Proceedings of the 15th European Conference on Developmental Psychology* (pp. 337-342) . Bologna, Italy, Mediamond.
- Boateng, R., Olumide, L., Isabalija, R.S., & Budu, J. 2011. Sakawa–cybercrime and criminality in Ghana. *Journal of Information Technology Impact*, 11(2), 85-100.
- Burton, V.S. Jr., Evans, TD. Cullen, G.T Olivares, K.M. & Dunaway. 1999. Age, self-control, operationalization theories and adult criminality. *Journal of Qualitative Criminology*, 10, 213-239.
- DNA. 2012. Piracy rate dips, but Malaysians think illegal software is okay. *Digital News Asia*, May 15, 2012, <https://www.digitalnewsasia.com/node/105>
- Francisco, S.M., Simão, A.M.V., Ferreira, P. C., & das Dores Martins, M.J. 2015. Cyberbullying: The hidden side of college students. *Computers in Human Behavior*, 43, 167-182.
- Goggin, G. 2010. Official and unofficial mobile media in Australia: Youth, panics, innovation. In S. H. Donald, T. D. Anderson, & D. Spry (Eds.), *Youth, society and mobile media in Asia* (pp. 120–134). London, UK: Routledge.
- Goggin, G. 2013. Youth culture and mobiles. *Mobile Media & Communication*, 1(1), 83-88.
- Gupta, M., & Lata, P. 2014. Absenteeism in schools: A chronic problem in the present time. *Educational Confab*, 3(1), 11-16.
- Holt, T.J. 2011. Low self-control, deviant peer associations, and juvenile cybercrime. *American Journal of Criminal Justice*, News.msu.edu/medial/06/963e40c7-08ff-411d-af1-fe7563496f89.pdf
- Igbo, H.I., Egbe-Okpenge, E.G., & Awopetu, R.G. 2013. Influence of information and communication technology on behavior problems of nigerian youths. *Procedia-Social and Behavioral Sciences*, 84, 97-106.
- Jonsson, L.S., Priebe, G., Bladh, M., & Svedin, C.G. 2014. Voluntary sexual exposure online among Swedish youth–social background, Internet behavior and psychosocial health. *Computers in Human Behavior*, 30, 181-190.

Khajehnoori, B. 2010. The relationship between ict's and adolescents' delinquencies case study: Students in Abadeh County. *Journal of Applied Sociology*, 39(3), 113-134.

Lenhart, A. 2009. Teens and sexting. How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging. December 15, 2009. Washington, DC: PEW Research Centre. Retrieved from http://www.pewinternet.org/_/media//Files/Reports/2009/PIP_Teens_and_Sexting.pdf. Accessed on 13 September 2015.

Lim, S.S. 2013. On mobile communication and youth "deviance": Beyond moral, media and mobile panics. *Mobile Media & Communication*, 1(1), 96-101.

Longe, O., Ngwa, F., Wada, F. & Mbarika, V. 2009. Criminal uses of ICT in sub-Saharan Africa: Trends, concerns and perspectives. *Journal of Information Impact*. 9(3), 155-172.

Mareschal, P.M., McKee, W.L., Jackson, S.E., & Hanson, K.L. 2007. Technology-based approaches to preventing youth violence: A formative evaluation of program development and implementation in four communities. *Youth violence and juvenile justice*, 5(2), 168-187.

McFadden, L. 2007. Detecting synthetic identity fraud. *Bankrate.com*. pp. 1-2. Archived from the original on 2012-07-18. Retrieved 2008-09-21.

Nandhini, B.S., & Sheeba, J.I. 2015. Online social network bullying detection using intelligence techniques. *Procedia Computer Science*, 45, 485-492.

Passey, D., Rogers, C., Machell, J., & McHugh, G. 2004. The Motivational Effect of ICT on Pupils. Research Report 523. Department of Educational Research Lancaster University. Accessed on 10 August 2015 via: http://downloads01.smarttech.com/media/research/international_research/uk/lancaster_report.pdf

Phelps, A., & Watt, A. 2014. I shop online—recreationally! Internet anonymity and Silk Road enabling drug use in Australia. *Digital Investigation*, 11(4), 261-272.

Ponemon Institute. 2012. Cost of cybercrime study: United States. Retrieved from http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

Quayle, E., & Taylor, M. 2011. Social networking as a nexus for engagement and exploitation of young people. *Information Security Technical Report*, 16(2), 44-50.

Robert, D., & Doyle, J. 2003. Study on cyberstalking: Understanding investigative hurdles. *FBI Law Enforcement Bulletin*, 72(3), 10-17.

Rogers, MSeigfried, K. & Tidke, K. 2006. Self-reported computer criminal behavior: A psychological analysis. *Proceedings of the Digital Forensics Workshop*. Elsevier, 116-120.

Savahl, S., September, R., Odendaal, W., & Moos, A. 2008. Information and communication technology: a descriptive study of children's communication patterns. *South African Journal of Psychology*, 38(3), 515-525.

Shade, Leslie Regan & Shepherd, Tamara 2013. Viewing youth and mobile privacy through a digital policy literacy framework. *First Monday*, 18 (12), <http://firstmonday.org/ojs/index.php/fm/article/view/4807>; viewed 21.02.15.

- Shank, D.B., & Cotten, S.R. 2014. Does technology empower urban youth? The relationship of technology use to self-efficacy. *Computers & Education*, 70, 184-193.
- Shrivastav, A. K., & Ekta, D. 2013. ICT Penetration and Cybercrime in India: A Review. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(7), 414-419.
- Smith, P.K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. 2008. Cyberbullying: Its nature and impact in secondary school pupils. *Journal of child psychology and psychiatry*, 49(4), 376-385.
- Srivastava, A., & Boey, J. 2012. Online bullying and harassment: An Australian perspective. *Masaryk University Journal of Law and Technology*, 6(2), 299-320.
- The Star Online. 2009. The effect of modern technology on Malaysian youth. Visited on 24/02/2015 via. <http://www.thestar.com.my/Story/?file=%2F2009%2F5%2F15%2Ffocus%2F3898698&sec=focus>
- The Star Online. 2014. Malaysia is sixth most vulnerable to cybercrime. <http://www.thestar.com.my/news/nation/2014/09/23/cyber-crime-malaysians-sixth-most-vulnerable/>
- Theantdaily. 2014. Yet another high profile cyberspace fraud for netizens to ponder. Accessed on 22/02/2015 via: <http://www.theantdaily.com/Main/Yet-another-high-profile-cyberspace-fraud-for-netizens-to-ponder>
- Tsukayama, Hayley. 2013. Facebook: Teens can now post publicly, but posts are friends-only by default. *Washington Post*, 16.10.13. http://www.washingtonpost.com/business/technology/facebook-teens-can-now-post-publicly-but-posts-are-friends-only-by-default/2013/10/16/57d5051c3682-11e3-be86-6a6aa439845b_story.html; viewed 25.02.15.
- Wells, M., & Mitchell, K.J. 2008. How do high-risk youth use the Internet? Characteristics and implications for prevention. *Child Maltreatment*, 13(3), 227-234.
- Wiener-Bronner, D. 2014. Syrian electronic army seems more interested in hacking than Syria. *The wire, News from Atlantic*. <http://www.thewire.com/technology/2014/01/syrian-electronic-army-hacks-skype/356627/>
- Wong, D.S., Chan, H.C.O., & Cheng, C.H. 2014. Cyberbullying perpetration and victimization among adolescents in Hong Kong. *Children and Youth Services Review*, 36, 133-140.
- Wright, M.F. 2013. The relationship between young adults' beliefs about anonymity and subsequent cyber aggression. *Cyber psychology, Behavior, and Social Networking*, 16(12), 858-862.
- Yar, M. 2013. *Cybercrime and society*. Sage.
- Ybarra, M. L., & Mitchell, K. J. 2004. Online aggressor/targets, aggressors, and targets: A comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry*, 45, 1308-1316.
- Yusop, F.D., & Sumari, M. 2013, January. The use of social media technologies among Malaysian youth. In: *International Educational Technology Conference (IETC)*, Kuala Lumpur, Malaysia.