International Journal of Multidisciplinary and Current Research

Research Article

ISSN: 2321-3124
Available at: http://ijmcr.com

A Study on the Adolescent Online Security Issues

V. Sithira and Yok-Yen Nguwi

Jame Cook University Singapore

Accepted 28 May 2014, Available online 01 June 2014, **Vol.2 (May/June 2014 issue)**

Abstract

Internet has great influence to most people. It has spread rapidly and one can spend endless hours on internet activities. Excessive internet usage is an emerging threat and has negative impacts towards the youth. This group of users involve in various harmful activities without knowing the risks associated with it. This research targets on this group of people and investigate their common online activities and their behaviour towards these activities. We designed a study to acquire information on the types of common online activities; students' reactions towards online activities; social networking interactions among students; students' online security perception and perception on most risky online activities. The outcome of this study shows that majority of the respondents identified giving out personal information including personal information as the most risky activity online. Students are more apprehension in misuse of information and money compared to a possibility of malware infected systems. The study also reveals that female students are bolder and more vocal online compared to male students. This finding is supported by the work by Gareth Walsh and John Elliott on women involvement in serious crime and the figure is growing compared to a drop in male involving in crime.

Keywords*: internet, threat, rootkits, internet cookies, spyware*

1. Introduction

The usage of internet has matured over the years. Activities on internet vary for different groups of people. People use internet for various activities such as e-mail, games, facebook, education etc. and the activities go on. Internet involvement among the youth is so common that it becomes part and parcel of their daily lives. Activities such as downloading/uploading, social networking, chatting are common among the youngsters. The growth of internet magnifies the issues associated with it. Internet threats have grown from just a simple virus to the current computer hacking, impersonation, scam, cyber bullying etc. Cyberbullying can occur between students in web chat rooms, email and texting, in blogs and especially on other social networking sites.(Kift, Campbell, & Butler, 2011)

Out of 75% of teenagers owning cell phones, 25% use them for social media, 24% use them for instant messaging and 54% use them for texting (Hinduja S. &Patchin J., 2007). Youths and teenagers are at some risk as they steer and experiment with social media because of their limited capacity for self-regulation and susceptibility to peer pressure. These groups of youths not only face risks on social networking sites, they may face other risks such as their personal and confidential information being stolen and face problems when this vital information being abused by others.

The parents of a 13-year-old girl who believe their daughter's October 2006 suicide was the result of a cruel cyber hoax. Megan Meier has an account on the social networking site, Myspace. Someone who used a fictitious account was sending cruel messages regarding Megan which made her upset and depressed and ultimately led her to death. Megan's parents are insisting on stricter measures to protect other children online ("Parents: Cyber Bullying Led to Teen's Suicide", 2007).

How vulnerable are this youth is a big question. They may not be equipped with the right knowledge. The chances of them learning the correct skills are very low and this group will not find it necessary to do so.

2. Literature Review

This section will review literatures from 4 areas of concern among youth; online fraud/scams, malware and social networking sites, online harassment and internet abuse at workplace.

2.1. Online fraud and scam

You might be giving out your confidential information online without knowing if it's the original web site. By following link and conforming your credit card information not knowing that you have been a victim to phishing attack. Phishing is a type of Internet fraud that

seeks to acquire a user's credentials by deception. It includes theft of passwords, credit card numbers, bank account details and other confidential information. These allow all credit card users bear the burden of fraud in the form of higher fees and interest rates. In addition you'll spend time cancelling credit card accounts, getting new cards issued, checking your credit card bill, and changing the numbers in various accounts if you use them for automatic payments(Andrew, 2009). Internet fraud is serious and affects an individual's trust on the Internet. Users who are not educated on the safety measures will fall victim to such activities. Interacting with spam mails can also lead to unwanted problems. Such dealings can put user's personal information at risks.

As youth spends more leisure time on the internet searching for their favorite stars and movies, they can also fall prey to malware which redirects their search results to fraudulent scam pages. According to cyberdefender, cyber criminals have increasingly focusing on youth realising their naivetés. They are the group that can easily fall victims to scams. Identity theft is creating more than $50 billion in consumer and corporate losses a year. Every login represents an opportunity for data and money to be stolen.("CyberDefender Warns Parents of Scams and Malware In Videos of Teen Favorite Celebrities, Movies," 2010)

Young adults are usually the group who fall victim to such fraud and scam. Some of these scams use some sort of malware that infects your computer files and system files. They convince the user to forward the e-mail to others thereby spreading the dangerous malware. Adolescents who are not aware of the harm of these activities will put their companies in great danger and unforeseen productivity loss and damages.

2.2.Malware and Social networking sites

Today's malicious software (malware) is written by professional hackers and criminals. In most cases, users are unwittingly tricked into executing a malicious program in the form of a Trojan horse. Users might think they are installing some needed software, which was "recommended" by a site they trust. The spread of malware through downloads or even accessing certain internet sites could lead to infected files and severe damages on computers. The impact to an individual personal computer would not be great compared to the impact of affected servers in an organization.

In 2009, 25 million unique malware programs were identified; this is definitely more compared to previous years. More than 4.6 million botnet infected computers which leaves the computers at danger and allow remote access without the user knowing. The anti-malware vendors have reported that 48% of computers they scan are infected (Roger, 2010). Recovery from malware spread in an organization is a time consuming process, loss of productivity and faces major challenges from customers. Are internet users aware of the danger of malware and its impact?

Social networking sites such as twitter and Facebook allows people to connect to each other and a platform for people to make new friends. This tools can also be misused that can raise a variety of legal issues concerning the right of publicity. This was the situation when the lawsuit filed by La Russa's claims that an unauthorized page that used La Russa's name to make light of drunken driving and two Cardinals pitchers, who died damaged La Russa's reputation and caused emotional distress. Tony La Russa filed a lawsuit against Twitter for unauthorized and offensive content that was posted in his name. ("Social networking sites can raise publicity legal issues," 2009)

Facebook, Twitter, MySpace and other social networking sites have become one of the favorite past times for young adults in the recent years. They share many experiences, views and thoughts. Sharing views has reached a point of harassment lately. People share their views and not realising that they are hurting and tarnishing the other party's reputation. This act causes emotional agony to the affected party.

2.3. Online harassment on Social networking sites

Online harassment is a form of cyberviolence and can be perceived as a type of violence that can lead victims to feel fear or distress in much the same manner as real-world stalking and harassment. Harassment most often involves threatening or sexual messages delivered via e-mail, instant messaging services, or posts in chatrooms. The popularity of social networking sites like Facebook and twitter among youth allows them to post cruel messages about other people for public to see. The impact of such activities is so great that some of the victims are led to suicidal acts ("Predicting Online Harassment Victimization Among a Juvenile Population," 2012). Some of the young adults, who engage in social networking sites, are unaware of the mannerism they should adopt when posting messages. The messages can be antagonizing and ruthlessly punishing the other party.

Base on the research by Jones, Mitchell and Finkelhor to explore the trends on youth reports on harassment and online sexual solicitation; they found that youth online harassment is increasing particularly girls. Another point discussed in their report is the lack of information for both parents and youth in terms of online harassment. Youth should know how to intervene effectively during online harassment (Jones, Mitchell, & Finkelhor, 2012).

2.4 Risks of Internet abuse at Workplace

Using Internet at workplace could benefit the organization in many ways. It's used for decision making, gathering information, comparing results and many more. However, employees can abuse the Internet at workplace. Base on Mark Griffiths, the typical Internet

abuse at workplace are online friendship/relationship abuse, online information abuse, criminal internet abuse and internet activity abuse. The most common of all is the internet activity abuse, which involves using the internet during work hours for non-work related activities. This includes online gambling, online shopping, online computer gaming etc. (G. Mark, 2010)

This kind of abuse can also lead to computer risks where the company's information systems are insufficiently protected against certain kinds of damages and loss. Internet abuse is a habit that can lead to addiction if it's not controlled and if no precautionary measures put in place. It is a serious issue in work productivity and the organization will suffer in the long run.

An exciting fact discussed by Bax Trent, youth use the internet to seek out the feeling of satisfaction, freedom, peace, equality and superiority which they can't in reality. The real world is full of discrimination and in this virtual world is the only place they look for such feelings (Bax, 2013). Therefore they tend to take it too lightly and easy when involve in internet activities. They do not put any boundaries around their internet activities which may be the problem when dealing with internet threats.

Internet activities described in the literature review can be considered to be some of the major problems faced by organizations today. Surfing the Internet has become one of the major tasks in organization and this could be for their own purpose and not work related internet use. It has reached a devastating level to many organizations and uses a time consuming approach in dealing with such incidents. Employees are trained to deal with such incidents with a well-defined incident response plan as well as the company's security education and training program. Another tool that can help solve this problem will be an effective employee handbook. (Danek, 2008)

However, younger adults and potential employees have lack of understanding on internet security. Base on Taylor and Shumba's work they have emphasized on the need for educating graduates on security including coding and development. Some schools do not put their security education as a top priority and the lack of security knowledge among this group (students) has serious consequences on the future systems they use and develop. (Taylor & Shumba).

Understanding students behavior on the internet and the risks on activities they are involve in internet allows the fact to be validated and understood. This research will provide the required statistics on youths' current security knowledge and skills on online activities, and to escalate the issue to the next level.

3. Design of Survey

The questions were decided base on the needed input which will substantiate the research question and the hypothesis.

The questions were structured in a manner to discover the interest and the current knowledge of youth (students) during online activities. Youth spend more time online and engages in diverse activities than adults. It is imperative to learn more about youth experience to diverse viewpoints and the factors that may shape that experience. ("Youth online activity and exposure to diverse perspectives," 2012)

The question starts with asking the type of activities that they engage in such as chat, social networking, e-banking, downloading and e-mail. The objective of these questions are to find the type of online activities they are involved. This will be a good start to recognize the type of activities mainly that youth is attracted to and common among this age group.

Risks involved in downloading materials are high. The next question emphasises on how often they download materials from the internet. The answer to this question will show the percentage of users who actively rely on internet for online resources. This can be considered dangerous due to infected online materials could be downloaded to their laptops or desktops.

The next question is to find how users' feel (which range from very uneasy to very confident) on several online activities such as, online banking (giving account information, transferring funds), e-commerce activities such as giving credit card information and purchasing products online, giving personal information to others met in chat room, downloading programs and music files onto personal computer and giving out e-mail address overall. This information is significant in understanding users' emotions on online activities.

In the recent years wireless access is common among internet users. Two related questions are to discover students' wireless access usage outside the university campus that is at hotspots. This question finds the type of activities they engage in using wireless access at these locations and does it pose any danger to their laptops.

Another segment of questions is to understand students' awareness on danger components related to Internet, such as Spyware, cookies and rootkits. These questions are relevant to recognize students' level of consciousness when involve in online activities.

This questionnaire also consists of open ended questions. The open ended questions are used to collect narrative responses and more in depth analysis. Two open ended questions are included to identify riskiest online activity that students' perceive. These questions vary from the rest of the questions so as to collect respondents' answers in their own words which will help in this quantitative research.

Survey questions are analyzed and chosen based on the requirements of the topic selected. This allows us to optimize the research tool used and to obtain the best response from the respondents to substantiate the hypothesis.

3.1. Design of Studies

The study of this topic will provide us with a detail understanding of the risks and problems faced by the young generations as well as finding the right skills needed for this group to engage in internet activities safely.

Questionnaire is chosen as the tool for this research. Questionnaire is decided so as to gather large number of inputs in a short span of time. An estimation of 50 participants is required to complete this survey. The participants are students from James Cook University from the School of Business and Psychology. The factors on selection of participants were on several areas including the field of study of the participants which must not be from Information Technology or Information Security group, so as not to impact the overall study of the topic and findings. The survey will identify the gender of participants. This will allow us to identify if any gender preferences in the internet activity habits.

The survey consists of 13 – 15 questions. Both close and open ended questions are included for a wide spectrum of inputs and answers which can help to analyse the problem in detail.

3.2. Design of survey

The questions were decided base on the needed input which will substantiate the research question and the hypothesis. The questions were structured in a manner to discover the interest and the current knowledge of youth (students) during online activities. Youth spend more time online and engages in diverse activities than adults. It is imperative to learn more about youth experience to diverse viewpoints and the factors that may shape that experience. ("Youth online activity and exposure to diverse perspectives," 2012)

The question starts with asking the type of activities that they engage in such as chat, social networking, e-banking, downloading and e-mail. The objective of these questions are to find the type of online activities they are involved. This will be a good start to recognize the type of activities mainly that youth is attracted to and common among this age group.

Risks involved in downloading materials are high. The next question emphasizes on how often they download materials from the internet. The answer to this question will show the percentage of users who actively rely on internet for online resources. This can be considered dangerous due to infected online materials could be downloaded to their laptops or desktops.

The next question is to find how users' feel (which range from very uneasy to very confident) on several online activities such as, online banking (giving account information, transferring funds), e-commerce activities such as giving credit card information and purchasing products online, giving personal information to others met in chat room, downloading programs and music files onto personal computer and giving out e-mail address overall. This information is significant in understanding users' emotions on online activities.

In the recent years wireless access is common among internet users. Two related questions are to discover students' wireless access usage outside the university campus that is at hotspots. This question finds the type of activities they engage in using wireless access at these locations and does it pose any danger to their laptops.

Another segment of questions is to understand students' awareness on danger components related to Internet, such as Spyware, cookies and rootkits. These questions are relevant to recognize students' level of consciousness when involve in online activities.

This questionnaire also consists of open ended questions. The open ended questions are used to collect narrative responses and more in depth analysis. Two open ended questions are included to identify riskiest online activity that students' perceive. These questions vary from the rest of the questions so as to collect respondents' answers in their own words which will help in this quantitative research.

Survey questions are analyzed and chosen based on the requirements of the topic selected. This allows us to optimize the research tool used and to obtain the best response from the respondents to substantiate the hypothesis.

4. Findings

Many teenagers do not safeguard sensitive information. This vulnerability sometimes rooted to the "naive" student culture that can be observed when sharing information on social networking sites, not protecting data on mobile devices and sharing password and identification numbers with friends (Ludwig & Parviz, 2012). The impact can be huge as confidential information can leak and this can tarnish their reputation and loss of resources. This section presents the data collected as described in previous section. Students from James Cook University are invited to take part in this study. The study was carried out for two groups of students from two different faculties: the business (IT) discipline and psychology discipline.

The details of the study are shown from Figure 1 to Figure 7. Figure 1 shows how the feelings of students towards writing offensive views on social networking sites. It shows that highest percentage of students is very comfortable with writing offensive views on social networking sites. Figure 2 denotes the frequency of downloading music, or other materials online. Figure 3 shows majority of students feel comfortable about carrying out online banking activity. Figure 4 shows that e-commerce is common and students are very comfortable with it. Figure 5 shows that major percentage of female students give out personal details

easily online. Figure 6 denotes that students generally feel that the materials the download online are safe especially female.

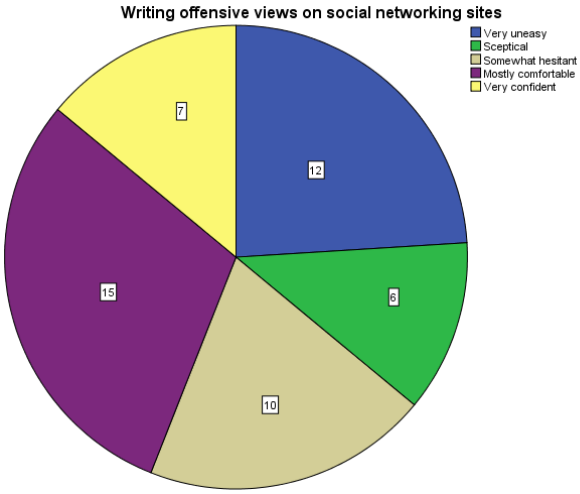

Figure 1 Writing offensive views online

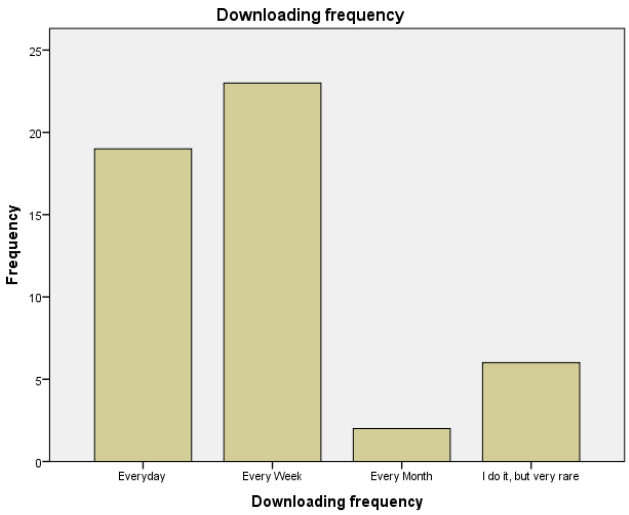

Figure 2 Downloading frequency

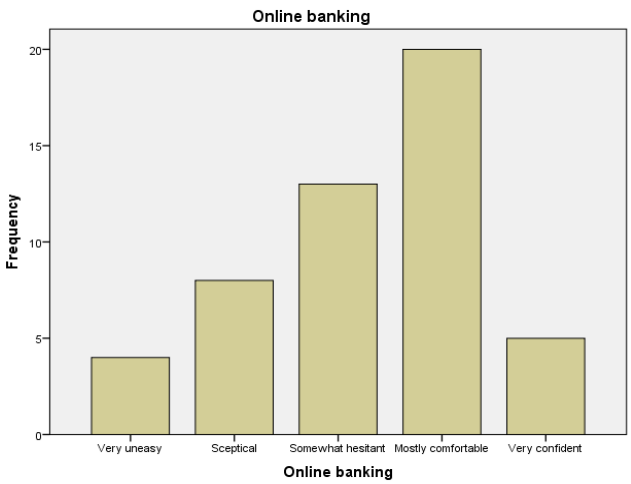

Figure 3 Online banking activities

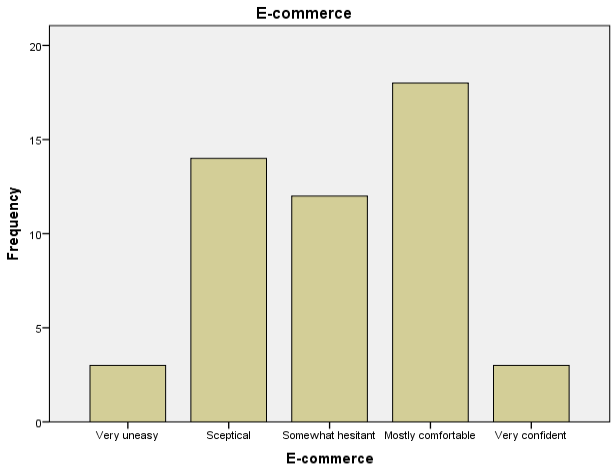

Figure 4 Students' emotion on e-commerce

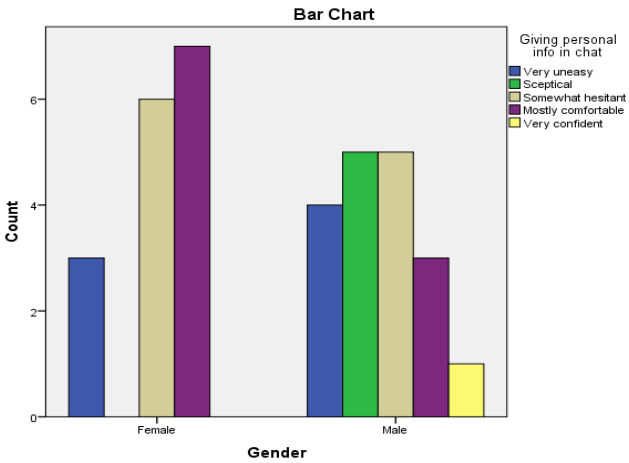

Figure 5 Giving personal info during online chat

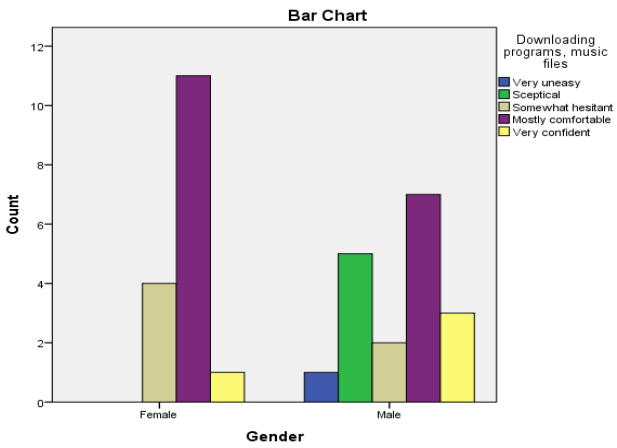

Figure 6 Downloading materials

In conclusion, the study shows that majority of the respondents identified giving out personal information including credit card details and personal information as the most risky activity online. Students are more apprehension in misuse of information and money compared to a possibility of malware infected systems. The above data shows that students are mostly not cautious when carry out internet activities. The study also

reveals that female students are bolder and more vocal online compared to male students. This finding is supported by the work by Gareth Walsh and John Elliott on women involvement in serious crime and the figure is growing compared to a drop in male involving in crime (Gareth & John, 2004). Another article that backs up this point is by Thelwall and Kousha that suggest females are more popular uses of social network sites than males (62% male and 71% female) (Thelwall & Kousha, 2014). These findings puts forward a strong point on internet security lapse among student community and that online security is secondary to them.

Proper guidance on security is recommended for this age group of users. The concept of educating this group of users is not new. In 2006, ISC2 and Childnet International launched an Internet security awareness program aimed at students in the age group from 11-13 years old with the goal of educating them to understand the danger of the internet and implement safe and secure online practices ("(ISC)2: (ISC)2 and Childnet International launch internet security public awareness programme for schools; UK security experts called to volunteer in new Internet safety education campaign," 2006). Security awareness is a must to educate the users on suitable conduct when they are involved on internet activities. The content of security training and awareness that will benefit and educate the students will be on password protection, latest malware/scam, spam, copyright infringement, social engineering, and identity protection and browser security. The lists of topics will vary time to time depending on the demands (Cooper, 2009). Students should also be given regular updates on internet threats and risks. The content of the training sessions should be carefully drafted so as to be accurate, interesting and beneficial to the audience. It has to meet the current needs and to resolve current security issues.

References

[1]. Andrew, B. (2009). High-Risk Security Threats. *PC World, 27*(3), 63.

[2]. Bax, T. (2013). *Youth and Internet Addiction in China*. Hoboken: Taylor and Francis.

[3]. Cooper, M. (2009). *Information security training: what will you communicate?*

[4]. CyberDefender Warns Parents of Scams and Malware In Videos of Teen Favorite Celebrities, Movies. (2010) (pp. 37): NewsRX.

[5]. Danek, S. K. (2008). Bad Behavior, *Las Vegas Business Press,* p. P24.

[6]. Gareth, W., & John, E. (2004). Serious female crime increases: Final 2 Edition, *Sunday Times*

[7]. (ISC)2: (ISC)2 and Childnet International launch internet security public awareness programme for schools; UK security experts called to volunteer in new Internet safety education campaign. (2006).

[8]. Hinduja S., Patchin J (2007), "Offline consequences of online victimization: school violence and delinquency", Journal of S. Violence. 2007;6(3):89–112

[9]. Jones, L. M., Mitchell, K. J., & Finkelhor, D. (2012). Trends in youth internet victimization: findings from three youth internet safety surveys 2000-2010. *The Journal of adolescent healt*

[10]. Kift, S., Campbell, M., & Butler, D. (2011). Cyberbullying in Social Networking Sites and Blogs: Legal Issues for Young People and Schools. *Journal of Law, Information and Science, 20*(2), 60-97.

[11]. Ludwig, S., & Parviz, P.-N. (2012). Students Information Security Practices and Awareness. *Journal of Information Privacy & Security, 8*(4), 3.

[12]. Mark, G. (2010). Internet abuse and internet addiction in the workplace. *The Journal of Workplace Learning, 22*(7), 463-472. doi: 10.1108/13665621011071127

[13]. Parents: Cyber Bullying Led to Teen's Suicide. (2007). Retrieved from http://abcnews.go.com

[14]. Predicting Online Harassment Victimization Among a Juvenile Population. (2012). *Youth & Society, 44*(4), 500-523. doi: 10.1177/0044118X1140752

[15]. Roger, A. G. (2010). Fighting today's malware. *InfoWorld.com*

[16]. Social networking sites can raise publicity legal issues. (2009). *The Hindustan Time*

[17]. Taylor, C., & Shumba, R. (2008). *Security education: a roadmap to the future*

[18]. Thelwall, M., & Kousha, K. (2014). Academia.edu: Social network or Academic Network? *Journal of the Association for Information Science and Technology, 65*(4), 721-731. doi: 10.1002/asi.23038

[19]. Youth online activity and exposure to diverse perspectives. (2012). *New Media & Society, 14*(3), 492-512