THE EFFECTS IN HACKING OF SOCIAL MEDIA AMONG COLLEGE STUDENTS IN MALAYSIA

RANJINI SHANMUGAM

A project reported submitted in partial fulfillment of the requirements
for the award of degree Master of Science (Information Assurance)

Advanced Informatics School
Universiti Teknologi Malaysia

DECEMBER 2014

DEDICATION

To my late father Mr.A.Shanmugam

ACKNOWLEDGEMENTS

I would thank all those who have helped me in finishing this research. I would like to thank my supervisor Pn. HafizaAbas. She has assisted me with her guidance. Next, I would like to acknowledge Dr.Shahidan who has assisted me during the completion part of the report.

I also like to thank all my family members mainly my sister Ms. S.Sumathi for their support. Thank you all.

ABSTRACT

The research aims to explore the influences or effects of hacking social media among private college students. The Social Learning and Low Self Control theories and nationality factor were used as a foundation to create the research model which use a survey design and interviews. Around 20 questionnaires were distributed to students at a private college in Malaysia. Five interviews were conducted where the first was a semi-structured and followed by another four unstructured interviews. Results show most of the hacker students are foreigners. The results also show how most of the students gain influences. Monetary rewards were not significant as opposing to past findings which is used in the Social Learning and Low Self Control theories. This research shows the existence of all the Social learning theory notions unlike the past research which found the absence of the Social Learning theory's notions Imitation and Differential Reinforcement. Thus, this research explain the effects of hacking social media among college students thus creating awareness for the public.

ABSTRAK

Penyelidikan ini bertujuan mengkaji siasat akan kesan pencerobohan media sosial di kalangan pelajar kolej swasta. Teori Pembelajaran Sosial dan Teori Kawalan Diri yang rendah serta faktor kenegaraan telah pun digunakan sebagai asas untuk membina model penyelidikan yang menggunakan kaedah-kaedah meninjauan dan menemu ramah. Sebanyak 20 borang soal selidik telah diedarkan kepada pelajar-pelajar sebuah kolej swasta di Malaysia. Lima temu ramah telah pun diadakan di mana, temu ramah yang pertama adalah berjenis separa-berstruktur manakala yang empat yang lain adalah berjenis bukan berstruktur. Hasil kajian menunjukkan bagaimana pelajar-pelajar terpengaruh. Penyelidikan ini menunjukkan faktor kewangan bukannya menggalakkan para pelajar di mana ini adalah bercanggah dengan hasil kajian yang lama. Penemuan dalam kajian ini menunjukkan kehadiran semua aspek Teori Pembelajaran Sosial bagi dalam menentukan faktor-faktor yang mempengaruhnya. Ini adalah berlainan dengan hasil kajian lama yang tidak menunjukkan kehadiran dua aspek Teori Pembelajaran Sosial, iaitu Peniruaan dan Pemberangsangan. Kajian ini telah pun menunjukkan kesan-kesan pencerobohan media social di kalangan penuntut kolej dan meyedarkan masyarakat supaya berwas-was.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Background of the Study

Internet's advancement whether the physical build or application is considered rapid as many innovations tend to come up meeting the world population's interest or needs. Almost in many fields of works ,Internet has been utilized to cover their business' functions. Internet have completely changed our way of interaction with our friends or family members. Changes at work are really prominent because of the online communication. Now everybody are turning to information technology for solutions as their business routines has been incorporated using latest technical expertise with heavy Internet usage. The usage of information communication technology is so prevalent that users worldwide spreading around it's advantages that even it can transform one's own live. The abilities of online sharing has promoted the Internet much more as it enhance communication's efficiency. The electronic mails have gained popularity replacing traditional post communication. Online interactions such as social media are rapidly increasing compared to other communication services because Internet gives variety of necessary routine function for everyone worldwide.

Having intruding other people or organization's account in Internet is something worrying many people around the world. This is done by criminals who tend to manipulates the users confidential data for their very own personal benefits. Since online communication methods are provided at no cost, many criminals are also seeking their ways of robbery in the Internet. Many people with poor wages too can easily afford to use the Internet as it's provided at cheaper rates. Thus, monetary difficulties are no longer an issue for many from stop using the Internet.

Online correspondence is a leading form communication where it's also much important in schools and colleges as the Internet's contribution in knowledge distribution is remarkably excellent. Teachers and learners see online links to knowledge as more effective done by manual search. The thriving quest for knowledge makes the Internet a very popular choice for the students at large. Many students tend to make it a main interaction medium too, where they use it to communicate with one and another as for economical reasons and efficiency. Many students have opted social media for online communication as the social media includes wide range of features which attracts them. The intense use of social media has risen up sharing and interaction activities done online. Many users get connected to each other and this promotes sharing of information sought online (Cheung et al., 2011).

Youngsters are actively using social media for various reasons as it bring adventures and fun to them. They have been using social media for more than a decade ever since it was launched. It has become their favorite interaction mode as it helps them to keep in touch with their associates and relatives (Sponcil et al., 2013).Online interaction still keep it's level at top as a main communication mode when it comes to business , educational, professional or even administration organizations. Therefore, the employers of such organization seek contenders with immense online interaction skills such as much social media exposure. Bloggers get them exposed to public by writing blogs in the Internet and this in a way promote

themselves as good communicators to meet their upcoming job prospects. Facebook positions the users in the virtual world where they can show off the world Internet users how they appear in form with including their comments and status updates. This kind of details provide facts regarding other people's lives and activities. Many people send invitations and wishes for events such as birthday via social media. It has replaced the sending of cards through the postal service for years. The widespread of social media usage has developed possibilities of it being exploited by the youngsters (Valenzuela. S, 2008).There are many online forums, chats or meetings that provide advice or guidelines to conduct unlawful activities such as hacking.

Online users across the world comprise of a huge population. The price of technical gadgets such smartphones, tablets or laptops are getting cheaper alongside the computers. The Internet transmission rate are also coming up to much better speed with the value many can afford. Many public places such cafes provide free wireless access to their customers. Globally, the population of Internet users are growing in size. Thus, cyber criminal activities are also seen escalating despite innovations in cyber security. There are many criminals activities operated using the Internet as the base and it's indeed tough in finding out about those who are being involve in such activities with their numbers. It is possible for a very small group of criminals to launch attacks on millions of computers located within any distance in the world. This shows the ratio between the offenders and victims could be vastly different. The rapidly growing online users also create troubles for the lawfully authorized organization to take action as it's obviously intricate to track down the criminals online.

Crimes which are committed via online are considered hazardous and pose greater impact on nations overall. The hackers too accumulate in many parts of the world, where offences are committed everyday. Many online users tend to get cheated via the Internet and they lose huge sum of money to the criminals. A decade

ago, losses were predicted more than thirty billion. Money generated via the Internet raked into billions, thus outshining other unlawful trades such cocaine distribution or smuggling. More than half of the trades operating in US implicate online crimes are much more expensive than other real live robberies. The Internet users such as hackers are wrongly using it for criminal purpose and this causes worries for many, thus debating it in many platforms. There are resolutions instigated towards this matter done globally. The cybercriminal activities are often executed with a variety of ways in using the technical expertise (Gercke,2012).

Everyone has heard of hacking since decades of years ago. The history of hacking returns to the 60's era where firstly it was used where "hacking" means breaking into systems illegally. Technical expertise was misused to obtain details which are not to be received and this issue became a major menace for the information technology world (Kirwan et al., 2012). Criminals do have also seized online users' interaction to derive important messages (Gercke,2012).

Criminals constantly hunt feeble characteristics in information technology field. Online users who use Internet without line connections are tremendously rising where this cause public centers to provide such online usage without any charges. But this has shown the delicate part of the technology where it can easily penetrated by unwanted intrusions, especially when users lack concern regarding existing safety methods (Gercke,2012).

Reliability of information with their services are equally important as the users' work functions. Untimely loss of Internet connection can bring major problems and monetary loss to organizations. This is because criminals can infringe online connections thus manipulate important information seized online. Those criminals even go to extent of disseminating hazardous small applications online to destroy computers thus running down the whole network system. There many reasons for the wide spread of such activities. The existing protection tools in the

market are not sufficient to address this problem . Now everybody are entitled to have them own websites and publish whatever they want others to read online. Even contents books that banned by some countries are being uploaded in the Internet for public to read. Photos are even displayed in the Internet for general view may cause problems as many youngsters or even kids are using the Internet. Fastness of the Internet is also taken into account as it dampen down the authorities' effort in curbing online criminal activities. This is because criminals promptly commit offences online and it's difficult for the police to track them online (Gercke,2012).

There many criminal activities done using the Internet which are still remain unknown to the public. Lack of evidences are found for such crimes, compared to robberies involving physical weapons like revolvers. Victims, especially commercial organizations hardly report any damages done to them via Internet as they fear it may bring bad images to them. Many even fail to make statements to the police as of being victimized through the Internet by the criminals. This is because they think it's useless as no cases were successfully solved that came into the public limelight. Furthermore they need to allocate their time the most for reporting such events. But there are also some online frauds are being reported when such crimes are being linked to high profile people or public at large (Gercke,2012).

Existing safety methods don't really pave problems faced by billions Internet users. The leading authorities in the cyber security must really take stern actions for the peril that worries everyone. What matter the most is that online criminals should be brought down to justice. Many realized that the critical issues that the Internet users are facing are often condoned by law-enforcement agencies. Although it's difficult handling such kind of task, it would be rather better having things resolved earlier than when it is too late. Cyber criminals are more dynamic where they aptly produced highly advanced tools which they circulate within them. Security programs also equally becoming better technically. Many nations find it tough to employ such technical security measures as of financial constrains and other

limitations. Those countries also suffer in this matter as they have poor legal control over it. Security features should had been integrated into Internet much earlier in order to cut down the online criminal activities. As financial barriers can never be used to impede the necessary procedures needed to overcome the problem. The losses estimated after the online attacks as far much higher compared to the price of available security tools. But having unnecessary or feeble security tools neither help much in fighting cyber crime. Safety of online users is crucial to ensure secured online interactions that contribute much to the growth of global industries (Gercke,2012).

The research done here concentrates mainly on the effects of hacking in social media within Kuala Lumpur Metropolitan University College students. Malaysian Police Force raided a bunch of college students in a housing area found at a close vicinity of Kuala Lumpur Metropolitan University College for engaging in online frauds. (Bernama,2014). All wrong doings linked to Internet are deemed to be illegal as well as any other crimes. A massive number of online users could be contacted at a split of seconds, thus it make the extent illegal activities done online much wider.

Presently, information technology is being utilized in various forms for illegal activities where stipulations are made that only serious cases are illegal. As for certain cases it mentioned that even for very first step done in the act gaining illegal entry into another account is being wrongful. There are certain cases when only hackers has made major changes such deletion or alteration are being accused illegal. The probe of hacking social media is categorized beneath PDRM's authority where it can lead to prosecution in regards to Computer Crimes Act 1997. Victims can easily make statements to the police.

1.2 Problem Statement

Social media is being abused for many reasons. Malaysia is also has been facing much problems such as its hacking that result worries and other serious issues (Gercke,2012). Unlawful intrusion is done to benefit hackers at large. Mastery of technical knowledge in hacking also lends much to the spread of hacking. The increase in online criminal activities especially social media's hacking doubt the appropriateness of existing Malaysian Internet 's rules and regulation. The hacking in social media has damaged one's public life with bad postings or vulgar word or images . It's one way of getting into other people's life to see their links and seek information. Its also a way of intimidating users and rob their privacy. Hacking of social media is seen as rising rapidly despite the usage of online security tools. The social media users tend to be anxious, worrying the kind of problems it can lead. Many users even lost their savings when their social media account got manipulates by hackers from different locations worldwide. Past researches has shown college students as active users the social media because they constantly engage themselves using different kind of gadgets. Their addiction towards social media has also tempted them for other acts which includes hacking. This has also have resulted poor grades for their education achievement. With a strategic location, Malaysia is becoming an educational site for many students worldwide where it's leading universities or colleges provide variety of courses (Malaysian Statistics Department, 2014). The international students who gained entrance to this country are not only limited to their role as students but also playing other significant parts in some destructive acts such as hacking. This is because of their much wider exposure of connection associates or links in the world.

1.3 Research Questions

The study on research works done earlier reveal that the demographic measure was used as a variable to research upon influence regarding hacking of the social media. (APPENDIX B). The research questions are seen in the Table 1.1.

Table1.1: Research Questions

Research Questions	Type of research	Source
i. What are the aspects in hacking social media among college students?	Qualitative	Literature review Interviews
ii. What are the ways the students acquire the influences?	Qualitative	Questionnaire Literature review Interviews
iii. Why most of the hacker students are foreigners?	Qualitative	Literature review Interviews Questionnaire

1.4 Objectives of the Research

i. To figure out the aspects of hacking social media among college students

ii. To recognize the causes of for the effects

iii. To know the reasons if most of the hackers are foreigners

1.5 Research Scope

The research was done in one of Malaysia's private university college, Kuala Lumpur Metropolitan University College (KLMUC), that's situated in Menara Tun Ismail Mohamed Ali, No.25 Jalan Raja Laut, 50350 Kuala Lumpur. The total of respondents for the survey are twenty . It includes the diploma and degree students, local and foreign students of different age groups. Five students have been interviewed. The first interview which the semi-structured interview is recorded using a Sony sound recorder. The rest of the four interviews are the unstructured interviews. It was difficult to many hacker students for interviews because many feared by tracked by others. As for this matter the interviews were done in a highly confidential way. Personal details of the hacker students were not revealed in order to maintain secrecy. Facebook and emails were used as the components of social media in this research.

1.6 Research Significance

Much exploration is done here in regards to investigate the effects of hacking social among college students. It is expected the people of Malaysia learn whatever being spread through social media cannot be exactly genuine. Thus, it would ridiculous to accept those messages or images circulated via social media are the actual messages or images from the correct source. The awareness about social media's safety concern all types of people from the old to the young ones, the professionals to the workers, the rich and the poor ones. The plight of those who became victims because of hacking seem to gain coverage from newspapers but with

no proper follow-ups from law enforcement agencies. Many people have experienced wonderful events such as marriages as because of social media usage but many have also experience bad events such as meetings which lead to cheat or even death. Many negative aspects of the social media surface as the result of illegal acts like hacking.

1.7 Purpose of the Research

The way of gaining knowledge is made easy via social media (Cheung et al., 2011). The main aim here is that to analyze the reasons that add up to the factors in hacking in regards to college students. Thus, this promotes consciousness about the bad sides of social media which are less known among many people. The hacking in social media tend to create more problems for society as it may used to fake documents or images. SKMM (Suruhanjaya Komunikasi Multimedia Malaysia), a law enforcement agency in Malaysia was started to address the problem where it also assure the users regarding the safety of social media. Globally, cyber safety professionals are facing challenges in guiding companies which are seeking security solutions for their woes (B.Still, 2005).

REFERENCE

Akers, R. L. (1991). Self-control as a general theory of crime.*Journal of Quantitative Criminology*.doi:10.1007/BF01268629

Arce, E., &Santisteban, C. (2006). Impulsivity: a review. *Psicothema*, *18*, 213–220.

Atkins, B., & Huang, W. (2013).A Study of Social Engineering in Online Frauds.*Open Journal of Social Sciences*, *01*(03), 23–32. doi:10.4236/jss.2013.13004

Balduf, M. (2009). Underachievement Among College Students. *Journal of Advanced Academics*.doi:10.1177/1932202X0902000204

Bandura, A. (1971). Social learning theory.In *Social Learning Theory* (pp. 1–46).

Carter, D. L. (2005).The Law Enforcement Intelligence Function.*FBI Law Enforcement Bulletin*, *74*, 1–9. doi:Article

Cheung, C. M. K., Chiu, P.-Y., & Lee, M. K. O. (2011). Online social networks: Why do students use facebook? *Computers in Human Behavior*. doi:10.1016/j.chb.2010.07.028

Collector, D., & Module, F. G. (2011).Qualitative Research Methods Overview.*Qualitative Research Methods A Data Collectors Field Guide*, *2005*, 1–12. doi:10.2307/3172595

Conti, G. (2006). Hacking and innovation.*Communications of the ACM*, *49*, 33–36. doi:10.1145/1132469.1132497.

Conway, M. (2006). Terrorism and the Internet: New media - New threat? *Parliamentary Affairs*. doi:10.1093/pa/gsl009

Cooper, R. (2004). Why Hacking is wrong about human kinds. *British Journal for the Philosophy of Science*, *55*, 73–85. doi:10.1093/bjps/55.1.73

Correa, T., Hinsley, A. W., & de Zúñiga, H. G. (2010). Who interacts on the Web?: The intersection of users' personality and social media use. *Computers in Human Behavior*, *26*, 247–253. doi:10.1016/j.chb.2009.09.003

Criado, J. I., Sandoval-Almazan, R., & Gil-Garcia, J. R. (2013).Government innovation through social media.*Government Information Quarterly*, *30*, 319–326. doi:10.1016/j.giq.2013.10.003

Crowe, A. (2011). The social media manifesto: a comprehensive review of the impact of social media on emergency management. *Journal of Business Continuity & Emergency Planning*, *5*, 409–420.

Curtis, L., Edwards, C., Fraser, K. L., Gudelsky, S., Holmquist, J., Thornton, K., &Sweetser, K. D. (2010).Adoption of social media for public relations by nonprofit organizations.*Public Relations Review*, *36*, 90–92. doi:10.1016/j.pubrev.2009.10.003

Cusumano, M. A. (2011). Platform wars come to social media. *Communications of the ACM*. doi:10.1145/1924421.1924433

Dana, J., Dawes, R., & Peterson, N. (2013). Belief in the unstructured interview: The persistence of an illusion. *Judgment and Decision Making*, *8*, 512–520.

DeLisi, M. (2011). Self-control theory: The Tyrannosaurus rex of criminology is poised to devour criminal justice. *Journal of Criminal Justice*, *39*, 103–105. doi:10.1016/j.jcrimjus.2011.02.012

Denzin, N. K., & Lincoln, Y. S. (2000).The discipline and practice of qualitative research.In *Handbook of Qualitative Research* (pp. 1–28).

Ellison, N. B., Ellison,Nicole B., Steinfield, C., Lampe, C., Steinfield,Charles, &Lampe,Cliff. (2007). The Benefits of Facebook "Friends:" Social Capital and College Students Use of Online Social Network Sites. *Journal of Computer-Mediated Communication*, *12*, 1143–1168. doi:10.1111/j.1083-6101.2007.00367.x

Everett, C. (2010). Social media: Opportunity or risk? *Computer Fraud and Security*.doi:10.1016/S1361-3723(10)70066-X

Fanning, E. (2005). Formatting a paper-based survey questionnaire: Best practices.*Practical Assessment, Research & Evaluation*, *10*, 1–14. Retrieved from http://parkdatabase.org/files/documents/2005_Formatting-a-paper-based-Survey-Questionnaire_E-Fanning.pdf

Flinders, D. J. (1997).InterViews: An introduction to qualitative research interviewing. *Evaluation and Program Planning*.doi:10.1016/S0149-7189(97)89858-8

Gercke, M. (2012), Understanding Cybercrime, ITU

Gold, S. (2013).Hacking the Internet.*Engineering & Technology (17509637)*, *8*, 34–37.

Gunkel, D. J. (2005). Editorial: introduction to hacking and hacktivism. *New Media & Society*.doi:10.1177/1461444805056007

Hadnagy, C. (2010). *Social Engineering: The Art of Human Hacking*. *The Art of Human Hacking* (p. 408). doi:10.1093/cid/cir583

Hammersley, B. (2006). *Hacking Gmail*.*ACM SIGCAS Computers and Society* (Vol. 33, p. 310). doi:10.1145/968358.968360

Higgins, G. E., & Makin, D. A. (2004). Does Social Learning Theory Condition the Effects of Low Self-Control on College Students ' Software Piracy ?, *2*(2), 1–22.

Hoath, P., &Mulhall, T. (1998). Hacking: Motivation and deterrence, part II. *Computer Fraud & Security*.doi:10.1016/S1361-3723(98)80094-8

Hoepfl, M. C. (1997). Choosing Qualitative Research : A Primer for Technology Education Researchers.*Journal of Technology Education*, *9*, 47–63. Retrieved from http://scholar.lib.vt.edu/ejournals/JTE/v9n1/hoepfl.html

Holt, K., Shehata, A., Strömbäck, J., &Ljungberg, E. (2013). Age and the effects of news media attention and social media use on political interest and participation: Do social media function as leveller? *European Journal of Communication*, *28*, 19–34. doi:10.1177/0267323112465369

Holt, T. J., Bossler, A. M., & May, D. C. (2011). Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance.*American Journal of Criminal Justice*, *37*(3), 378–395. doi:10.1007/s12103-011-9117-3

Holt, T. J., Strumsky, D., Smirnova, O., &Kilger, M. (2012).Examining the Social Networks of Malware Writers and Hackers, *6*(1), 891–903.

Knox, S., & Burkard, A. W. (2009).Qualitative research interviews.*Psychotherapy Research : Journal of the Society for Psychotherapy Research*, *19*, 566–575. doi:10.1080/10503300802702105

Lagrange, T. C., & Silverman, R. A. (1999). Low Self-Control and Opportunity: Testing the General Theory of Crime As an Explanation for Gender Differences in Delinquency. *Criminology*, *37*, 41–72. doi:10.1111/j.1745-9125.1999.tb00479.x

Lin, J.-H., Peng, W., Kim, M., Kim, S. Y., &LaRose, R. (2012).Social networking and adjustments among international students.*New Media & Society*.doi:10.1177/1461444811418627

MacDonald, C. D., & Roberts-Pittman, B. (2010). Cyberbullying among college students: Prevalence and demographic differences. In *Procedia - Social and Behavioral Sciences* (Vol. 9, pp. 2003–2009). doi:10.1016/j.sbspro.2010.12.436

Mansfield-Devine, S. (2009). Hacking the hackers.*Computer Fraud and Security*, *2009*, 10–13. doi:10.1016/S1361-3723(09)70073-9

Marshall, M. N. (1996). Sampling for qualitative research.*Family Practice*, *13*, 522–525. doi:10.1093/fampra/13.6.522

Matusitz, J. A. (2006). Cyberterrorism: A postmodern view of networks of terror and how computer security experts and law enforcement officials fight them. *ProQuest Dissertations and Theses*, 493.doi:1095467151

McClure, S., Scambray, J., Kurtz, G., & Kurtz. (2009). *Hacking exposed: network security secrets and solutions*. *Network* (pp. 1–249). doi:10.1036/0072192143

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, *28*(6), 2366–2375. doi:10.1016/j.chb.2012.07.008

Morse, J. M., Barrett, M., Mayan, M., Olson, K., &Spiers, J. (2008).Verification Strategies for Establishing Reliability and Validity in Qualitative Research.*International Journal of Qualitative Methods*. doi:10.1063/1.2011328

Ollmann, G. (2008). Hacking as a service.*Computer Fraud and Security*, *2008*, 12–15. doi:10.1016/S1361-3723(08)70177-5

Palen, L. (2008). Online Social Media in Crisis Events.*Educause Quarterly*, *31*, 76–78.

Paradiso, J. A., Heidemann, J., & Zimmerman, T. G. (2008). Hacking is pervasive. *IEEE Pervasive Computing*, *7*, 13–15. doi:10.1109/MPRV.2008.52

Passmore, C., Dobbie, A. E., Parchman, M., &Tysinger, J. (2002).Guidelines for constructing a survey.*Family Medicine*.

Pempek, T. A., Yermolayeva, Y. A., & Calvert, S. L. (2009). College students' social networking experiences on Facebook. *Journal of Applied Developmental Psychology*, *30*, 227–238. doi:10.1016/j.appdev.2008.12.010

Picazo-Vela, S., Guti??rrez-Mart??nez, I., & Luna-Reyes, L. F. (2012). Understanding risks, benefits, and strategic alternatives of social media applications in the public sector. *Government Information Quarterly*, *29*, 504–511. doi:10.1016/j.giq.2012.07.002

Qu, S. Q., &Dumay, J. (2011).The qualitative research interview.*Qualitative Research in Accounting and Management*, *8*, 238–264. doi:http://dx.doi.org/10.1108/11766091111162070

Roberts, P. (2001). Hacking Cyberspace.*ACM SIGCAS Computers and Society*. doi:10.1145/572306.572314

Rogers, M. K. (2001). A Social Learning Theory and Moral Disengagement of Criminal Computer Behaviour, (C).

Romero, D. M., Galuba, W., Asur, S., &Huberman, B. A. (2011).Influence and passivity in social media. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 6913 LNAI, pp. 18–33). doi:10.1007/978-3-642-23808-6_2

Ross, A. (1990). Hacking Away at the Counterculture.*Postmodern Culture*. doi:10.1353/pmc.1990.0011

Russo, A., Watkins, J., & Groundwater-Smith, S. (2009). The impact of social media on informal learning in museums.*Educational Media International*.doi:10.1080/09523980902933532

Salman, A., Saad, S., & Ali, M. N. S. (2013). Dealing with ethical issues among Internet users: do we need legal enforcement? *Asian Social Science*, *9*, 3–8. doi:10.5539/ass.v9n8p3

Saw, G., Abbott, W., Donaghey, J., & McDonald, C. (2013). Social media for international students – it's not all about Facebook. *Library Management*, *34*, 156–174. doi:10.1108/01435121311310860

Schoonmaker, S. (2012).HACKING THE GLOBAL.*Information, Communication & Society*. doi:10.1080/1369118X.2012.665938

Shafique, F., Anwar, M., &Bushra, M. Exploitation of social media among university students: A case study., 7 Webology 1–13 (2010). Retrieved from

http://search.ebscohost.com/login.aspx?direct=true&db=lih&AN=62640214&site=ehost-live

Shoemaker, D. J., Bailey, C. A., Bryant, C. D., Hughes, M., &Mcmullen, J. C. (1999). A Test of Self-control Theory Using General Patterns of Deviance John C . McMullen Dissertation submitted to the Faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirement for the degree of Doctor of Philo.

Silva, C. N. (2008).Designing Qualitative Research.*Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, *9*. doi:10.1057/omj.2011.23

Socialnomics.(2009). Social Media Revolution.*Think Magazine*. Retrieved from http://www.youtube.com/watch?v=sIFYPQjYhv8

Software, R. L. (2007).Hacking for Dummies.*Nature*, *465*, 1–74. doi:10.1038/nature09041

Soghoian, C. (2011). The Law Enforcement Surveillance Reporting Gap.*Social Science Research Network*, 1–26. doi:10.2139/ssrn.1806628

Sommer, P. (2006a).Criminalising hacking tools.*Digital Investigation*, *3*, 68–72. doi:10.1016/j.diin.2006.04.005

Sommer, P. (2006b).Criminalising hacking tools.*Digital Investigation*, *3*, 68–72. doi:10.1016/j.diin.2006.04.005

Sponcil, M., &Gitimu, P. (2013). Use of social media by college students : Relationship to communication and self-concept. *Journal of Technology Research*, *4*, 1–14. Retrieved from http://ehis.ebscohost.com/eds/detail?vid=7&sid=8495b59a-fe1d-473c-bc7b-3d7edb9b78b1@sessionmgr113&hid=4102&bdata=#db=a9h&AN=90440151

Steimel, B., Halemba, C., &Dimitrova, T. (2011).Social Media Monitoring.*Mind*, *7*, 1–87. doi:10.1007/978-3-658-00035-6_10

Steinfield, C., Ellison, N. B., & Lampe, C. (2008). Social capital, self-esteem, and use of online social network sites: A longitudinal analysis. *Journal of Applied Developmental Psychology*, *29*, 434–445. doi:10.1016/j.appdev.2008.07.002

Still, B. (2005).Hacking for a cause.*First Monday*, *10*, 1–8. Retrieved from firstmonday.org/ojs/index.php/fm/rt/printerFriendly/1274/1194

Stollak, M., Vandenberg, A., Burklund, A., & Weiss, S. (2011). GETTING SOCIAL : THE IMPACT OF SOCIAL NETWORKING USAGE ON

GRADES AMONG COLLEGE STUDENTS.*Proceedings of ASBBS*, *18*, 859–865.

Strayhorn, J. M. (2002). Self-control: theory and research. *Journal of the American Academy of Child and Adolescent Psychiatry*, *41*, 7–16. doi:10.1097/00004583-200201000-00006

Svensson, M., & Larsson, S. (2012). Intellectual property law compliance in Europe: Illegal file sharing and the role of social norms. *New Media & Society*.doi:10.1177/1461444812439553

Tenopir, C. (2013). Social media and scholarly reading.*Online Information Review*, *37*, 193–216. doi:10.1108/OIR-04-2012-0062

Tess, P. a. (2013).The role of social media in higher education classes (real and virtual) – A literature review.*Computers in Human Behavior*, *29*, A60–A68. doi:10.1016/j.chb.2012.12.032

The Nielsen Company. (2011). The state of media: The social media report 2011. *http://blog.nielsen.com/nielsenwire/social/2011/*. Retrieved from http://blog.nielsen.com/nielsenwire/social/2011/the-media-the-social-media-report-2012.html

Thomas, J. (2005). The moral ambiguity of social control in cyberspace: a retro-assessment of the "golden age" of hacking. *New Media & Society*.doi:10.1177/1461444805056008

Thompson, P. (2004). Cognitive hacking and intelligence and security informatics.In *Proceedings of SPIE - The International Society for Optical Engineering* (Vol. 5423, pp. 142–151). doi:10.1117/12.554454

Turgeman-Goldschmidt, O. (2005). Hackers' Accounts: Hacking as a Social Entertainment. *Social Science Computer Review*.doi:10.1177/0894439304271529

Valenzuela, S. (2008). Lessons from Facebook: The Effect of Social Network Sites on College Students' Social Capital. *Communication*, 39. Retrieved from http://online.journalism.utexas.edu/2008/papers/Valenzuela.pdf

Vegh, S. (2005).The media's portrayal of hacking, hackers, and hacktivism before and after Sept 11.*First Monday*, *10*, 1–18.

Von Hippel, E., &Paradiso, J. A. (2008).User innovation and hacking.*IEEE Pervasive Computing*, *7*, 66–69. doi:10.1109/MPRV.2008.62

Wagner, R. (2011a). Social Media Tools for Teaching and Learning.*Athletic Training Education Journal*, *6*, 51–52. Retrieved from http://csaweb109v.csa.com.ezproxy.lib.vt.edu:8080/ids70/view_record.php?id=4&recnum=41&log=from_res&SID=75pketf4eo60ftu6gurarhq7h4

Wagner, R. (2011b). Social Media Tools for Teaching and Learning.*Athletic Training Education Journal*, *6*, 51–52. Retrieved from http://csaweb109v.csa.com.ezproxy.lib.vt.edu:8080/ids70/view_record.php?id=4&recnum=41&log=from_res&SID=75pketf4eo60ftu6gurarhq7h4

Walls, D. M., Schopieray, S., &DeVoss, D. N. (2009). Hacking Spaces: Place as Interface. *Computers and Composition*, *26*, 269–287. doi:10.1016/j.compcom.2009.09.003

Weinberg, B. D., &Pehlivan, E. (2011). Social spending: Managing the social media mix. *Business Horizons*, *54*, 275–282. doi:10.1016/j.bushor.2011.01.008

Wilhelm, T. (2013).Hacking as a Career.In *Professional Penetration Testing* (pp. 389–434).doi:http://dx.doi.org/10.1016/B978-1-59749-993-4.00015-X

Williams, C. (2007). Research Methods, *5*(3), 65–72.

Wilson, C. (2014). Unstructured Interview. In *Interview Techniques for Ux Practitioners A User-Centered Design Method* (pp. 43–62). doi:10.4135/9781412950589.n1059

Wilson, H. J., Guinan, P., Parise, S., & Weinberg, B. D. (2011). What's your social media strategy? *Harvard Business Review*, *89*, 17.

Wolfson, M., Wagenaar, A. C., &Hornseth, G. W. (1995). Law officers' views on enforcement of the minimum drinking age: a four-state study. *Public Health Reports*, *110*, 428–438.

Xiang, Z., &Gretzel, U. (2010).Role of social media in online travel information search.*Tourism Management*, *31*, 179–188. doi:10.1016/j.tourman.2009.02.016

Yang, C. C., & Ng, T. D. (2007). Terrorism and Crime Related Weblog Social Network: Link, Content Analysis and Information Visualization. *2007 IEEE Intelligence and Security Informatics*. doi:10.1109/ISI.2007.379533

Yar, M. (2005). Computer Hacking: Just Another Case of Juvenile Delinquency? *Howard Journal of Criminal Justice*, *44*, 387–399. doi:10.1111/j.1468-2311.2005.00383.x

Youn, S. J., Trinh, N.-H., Shyu, I., Chang, T., Fava, M., Kvedar, J., & Yeung, A. (2013). *Using online social media, Facebook, in screening for major depressive*

disorder among college students.*International Journal of Clinical and Health Psychology* (Vol. 13, pp. 74–80).doi:http://dx.doi.org/10.1016/S1697-2600(13)70010-3

Young, R., Zhang, L., &Prybutok, V. R. (2007).Hacking into the Minds of Hackers.*Information Systems Management*.doi:10.1080/10580530701585823

Zhang, Y., &Wildemuth, B. M. (2005).by, (1998), 1–10.

Zhang, Y., &Wildemuth, B. M. (2009).Unstructured interviews.In *Applications of Social Research Methods to Questions in Information and Library Science* (pp. 222–231). Retrieved from http://hsmi.psu.ac.th/upload/forum/Unstructured_interviews.pdf