Available online at www.ijrp.org

IJRP.ORG
International Journal of Research Publications

International Journal of Research Publications

An Assessment On The Impact Of Ethical Hacking Training Towards Perceptions Among Information Technology Students'

JOHN KIOKO

Student, Department of Computer Science, Africa Nazarene University, P.O. Box 53067 – 00200, Nairobi, Kenya

Abstract

Many of the students undertaking IT programs in our universities possess the fundamental skills to carry out hacking in their future professional careers in the organizations in which they will be employed through the knowledge they have acquired as part of their training. Learning about networking, programming, coupled with hardware knowledge and exposure to various operating systems such as Unix, Linux, and Windows equips the average IT student with the skills and knowledge to infiltrate and manipulate systems, in essence making them hackers in the making. Accordingly, a black-hat hacker is a hacker who either ignores or intentionally defies legal or regulatory statutes with presumably little interest in ethical frameworks (Pike, 2013). Conversely, a white-hat hacker is defined as a hacker who is committed to full compliance with legal and regulatory statutes as well as published ethical frameworks that apply to the task at hand (Pike, 2013). One of the greatest challenges posed to business through recruitment of IT professionals is the risk of cybersecurity breaches to organizational systems as a result of the knowledge they possess. Many business organizations, as a result, have fallen victim to cyber-attacks. It was thus the focus of this research to explore why by training IT students in our University's, we are producing an increasing number of future hackers within Africa Nazarene University. The purpose of this study was to explore if ANU is a breeding ground for hackers of the future. The study explored if perceptions held of ethical hacking serve as deterrents to hacking through training achieved as IT students at ANU through the objectives of evaluating how the GoK codes of conduct and RoK ICT policy affect IT students, how ethical practices training has impacted IT students, when have the IT student's encountered ANU institutional policies, and what is the consequent level of awareness of ethical hacking. At its core was the theory that today's IT students are tomorrow's hackers with the target population being IT students undertaking undergraduate BCS, BBIT programs and graduate MIT studies at ANU. A sample size of 105 respondents, which was drawn using purposive sampling technique was used that targeted students who are part of the IT programs under study. Quantitative data was obtained from the respondents as collected using questionnaires and analyzed using SPSS through descriptive analysis that yielded correlations between the objectives under study as well as frequencies and percentages of the results of data. The results were presented in form of correlation tables, bar graphs, pie charts and a written report that detailed analysis of findings as well as evaluated the insights of the data analyzed. The study found that 61.9% respondents taking IT programs at ANU have no knowledge of the GoK code of conduct with 61.7% among the BBIT group indicating that they have not undergone hacking training. 95.8% indicated that coupled with having undergone hacking training they practice prudent online internet conduct through their ANU user accounts as well as 90.5% of the total respondents across all programs indicating that hacking sensitization would be an important part of their training. The study was able to conclude that ANU IT student’s curricula should be guided by the government master plan on the role out and implementation of ICT within Kenya, legal document added to exposure to the field, testing of skills, collaborations on projects as well as sharing of knowledge in line with sensitization on the latest trends should form part and parcel of the core training. Recommendations from the study include the establishment of an IT training policy, hacking and ethics training, and creation of hacking awareness programs on white hat and black hat hacking. The study sought to develop awareness among Africa Nazarene University IT students on ethical hacking and is intended to benefit ANU in particular as it will enable the institution to determine if the IT training programs have any shortfalls that may exist.

© 2018 Published by IJRP.ORG. Selection and/or peer-review under responsibility of International Journal of Research Publications (IJRP.ORG)

Keywords: Hacking; Black Hat Hacker; White Hat hacker; GoK digital laws; RoK ICT policy; Ethical hacking training; ANU institutional policies; Awareness.

1. Introduction

1.1 Background of the Study

The image of the individual termed as a “hacker” has evolved from that of one viewed as positive and complimentary in society, of a smart and eager computer programmer, to the negative and disdained cybercriminal. The term cybercriminal and hacker are today used synonymously. Hacker, as a term, is commonly used by the mass media to refer to an intruder breaking into computer systems to steal or destroy data. Police describe almost any crime committed through, with, by, or against a computer as “hacking” (Richet, 2013).

Conversely crackers use their computer security related skills to author viruses, trojans, etc., and illegally infiltrate secure systems with the intention of doing harm to the system or for criminal intent, as a means of differentiating them from the original and noncriminal hacker (Richet, 2013).

As shown by Suhasini (2014) the prevalence of internet connections and users has resulted in misgivings of the true intent of the users as it is hard to tell those with genuine intentions from those that don’t, particularly for ethical hackers whose real intent may not be able to be established as they breach vulnerable networks and information systems. This is evidenced by the technological base available marked by ever increasing tools that ease the lives of the general public being developed, but which if abused could encroach on our privacy, free will and respect.

As further highlighted by Suhasini (2014) media reports focus on 90% of cybercrime being perpetrated by people working within those organizations raising fears on how easy it is to exploit systems by employees. The aspect that arises is then, is ethical hacking the final solution to these challenges or is it in itself a problem. The security of networks and the protection of network resources are so vital to business operations, that when cyber-attacks do happen, business processes can literally come to a halt (McGregor, 2014). Furthermore, McGregor (2014), emphasizes that business professionals play a role in properly performing as a vital human resource in the business systems they help develop and use in their organization. As a manager or business professional, it will be your responsibility to make decisions about business activities and the use of information technologies, which may have an ethical dimension that must be considered.

However, Richet (2013) outlines that in this search by organizations, one of the best ways to evaluate the intruder threat to their interests would be to have independent computer security professionals attempt to break into their computer systems. A great number of hackers are self-taught geniuses and some organizations actually employ hackers as part of their information technology staff. These hackers use their skills to find vulnerabilities in the company’s information systems so that they can be fixed quickly. This type of hacker actually activity prevents serious cybercrimes.

A 2013 study by go-gulf on cybercrimes and statistics shows that cybercrimes are growing and by 2017, the global cyber security market is expected to skyrocket to $120.1 billion. The estimated annual cost of global cybercrime is $100 billion. Africaonline business (2015) states that in Africa, internet usage grew seven times faster than the global average between 2000 and 2012, clocking more than 3,600 percent growth to a total 167 million users. Yet the flipside of the rapid expansion of internet infrastructure is poor cybersecurity safeguards.

According to a 2015 article on the daily nation, there were 5.4 million cyber-attacks recorded last year alone in Kenya. That is almost three times the number recorded in 2013. Despite this large figure, though, communications authority of Kenya believes that a high number of cases are never reported, especially those involving banks. Pike (2013) outlines the argument for teaching ethical hacking focuses on the need to better understand attacks and attackers. Thus this study examined perceptions that influence IT students into committing criminal acts with the skills acquired in an ethical hacking course.

1.2 Problem of Research

One of the greatest challenges posed to business through recruitment of IT professionals is the risk of cybersecurity breaches to organizational systems as a result of the knowledge they possess. The impact of ethical hacking training on IT students perceptions is manifested in their individual points of view as regards ethicality of hacking. Many business organizations, as a result, have fallen victim to cyber-attacks. According to Abdulrahman (2015), ethical hackers must be network systems specialists and very familiar with computer networking, programming, and operating systems. Coupled with a comprehensive awareness of Windows, Unix, and Linux is considered as a necessity. “Patience, persistence, and immense perseverance are important qualities for ethical hackers because of the length of time and level of concentration required for most attacks to pay off. Networking, web programming, and database skills are all useful in performing ethical hacking and vulnerability testing”(Abdulrahman, 2015). Although many IT graduates will be charged with securing and testing of critical information systems in their future professional careers, there is no assurance that the ethical hacking training they have received will be a deterrent to engaging in black hat hacking activities as envisaged by the influence on their perceptions.

1.3 Objectives of the study

The general objective of this study was to determine what factors affect perceptions of ethical hacking.

1.3.1 Specific Objective

To assess the impact of ethical hacking training on perceptions among IT students

1.4 Hypothesis of the study

IT students of today are not the hackers of tomorrow. This is a null hypothesis that states there is no relationship between the variables under study.

H_0: There is no relationship between the level of IT students training and their level of hacking knowledge.

1.5 Scope of the study

This study covered students undertaking IT degree programs in Africa Nazarene University at the undergraduate and graduate levels i.e. BCS, BBIT, and MIT. The study was also limited to those students studying within main campus and Nairobi campus.

2.0 Literature Review

2.1 Ethical hacking training

Information Ethics is education and training on the responsible and accountable use of information on the one hand and of the technologies used to access and disseminate information in the private and public domain on the other, (Malan & Bester, 2014).

Alnatheer (2014), determines at the core of information ethics is an information security culture that defines the attitudes, assumptions, beliefs, values, and knowledge that employees/stakeholders use to interact with the organization's systems and procedures at any point in time. This interaction results in acceptable procedures that result in acceptable or unacceptable behavior evident in artifacts and creations that become part of the way things are done in an organization to protect its information assets.

Ried and Niekerk (2013), on the other hand, asserts that information security education provides the knowledge and skills needed to implement information security practices. Information security has however been mainly implemented in organizations and recently has come to target the general public.

According to Alhogail and Mirza (2014), information security culture develops as a result of employees' interaction with information security controls such as passwords, access cards or anti-virus software. Information security culture thus forms a natural aspect of employees' daily activities. This security culture is about the way things are done in the organization in order to protect information assets. It is created in the organization through embedding appropriate security practices to each employee to become a natural way of performing his/her daily job activities (Alhogail & Mirza, 2014).

Eloff (2015), further emphasize information security be incorporated into the everyday practices performed as part of an employee's job to make it a way of life and so cultivate an effective information security culture throughout the organization. However as portrayed by Veiga (2015), organizational vision and strategy are often depicted in organizational policies and procedures. Employee behavior becomes evident as guided by the vision, strategy, and policies. With time an organizational culture emerges, that encapsulates the vision and strategy, as well as the experiences employees, have had when implementing them. This culture is then incorporated into specific organizational behavior.

At the foundational educational level, the negative effects of lack of an IE culture have been witnessed through many primary schools in Africa that have embraced internet usage amongst their students having a great deficiency in online safety practices for students. Young students using the internet without proper guidance and knowledge of cyber conduct are vulnerable to predators and cyber criminals that are eager to take advantage of innocent minds (Solms, 2014). Further as portrayed by Solms (2014), this lack of knowledge of cyber code of conduct has also been witnessed among their teachers through a lack of requisite knowledge and skills on how to safely navigate through the web, how to tackle incidents of online harassment, prevent hackings and malware attacks, and through the lack of structured implementation of curricula on safe cyber practices for teachers as well as students.

In higher learning institutions the lack of an IE culture according to Amunga (2013), is manifest through the increasing evidence of cases of academic malpractices, especially plagiarism, in universities and it continues to be an everyday worry for universities, information creators and vendors in Kenya, this has brought about the need for information ethics training in university's in Africa.

3.0 Research Design and methodology

Burns and Grove (2003) define a research design as “a blueprint for conducting a study with maximum control over factors that may interfere with the validity of the findings”. Parahoo (1997) describes a research design as “a plan that describes how, when and where data are to be collected and analyzed”. Polit and Beck (2003) define a research design as “the researcher’s overall for answering the research question or testing the research hypothesis”. This study used quantitative research as conducted through a descriptive survey which presented a picture of the specific details of the research area. It sought to describe the characteristics of perceptions of ethical hacking. The descriptive research sought to determine the answer to who, what, where, and how questions. It offered the researcher a profile or description of relevant aspects of the research area. The study mainly concentrated on investigating the perceptions of ethical hacking.

3.1 Research site

The study was located in Africa Nazarene University both the main campus (Rongai) and the Nairobi campus (aghro house) that gave a good representation of a university that is training students in IT and that is likely to be subject to the vices of hacking. The ANU study, however, did not provide results that may be generalized, it sought to explore the issues of ethical practices as they impact IT students. The assumptions were that these results would provide a basis for future research to be conducted on the same subject as well as provide an insight of the situation in other similar higher learning institutions.

3.2 Target population

Parahoo (1997) defines population as “the total number of units from which data can be collected”, such as individuals, artifacts, events or organizations. Burns and Grove (2003) describe population as all the elements that meet the criteria for inclusion in a study. The target population for this study was Bachelor of Business and Information Technology (BBIT), Bachelor of Computer Science (BCS) and Master of Science in Information Technology (MIT) students in Africa Nazarene University.

3.3 Determination of study sample

Polit and Beck (2003) define a sample as “a proportion of a population”.

The formula below adopted from Kothari (2004) was used to determine the sample size.

$$N_c = \frac{Z^2 p \, . \, q \, . \, N}{d^2 (N-1) + Z^2 \, . \, p \, . \, q}$$

Where: N_c is the strater sample size

Z - is the confidence level (95%); that is, Z = 1.96

p - is the proportion of the of the strata population for the entire population (0.3)

q - (1-P) is the proportion to the total population of other clusters (0.7)

d - is the desired precision (0.05 level)

N - is the total number of population in the target population

Calculation

$$\text{Strata Sample size} = \frac{(1.96)^2\, 0.3*0.7*371}{0.05^2\,(371-1) + (1.96)^2*0.3*0.7}$$

$$= \frac{3.842\,(0.3*0.7*371)}{0.003\,(370) + 3.842*0.3*0.7}$$

$$= \frac{3.842 * 77.910}{0.925 + 0.807}$$

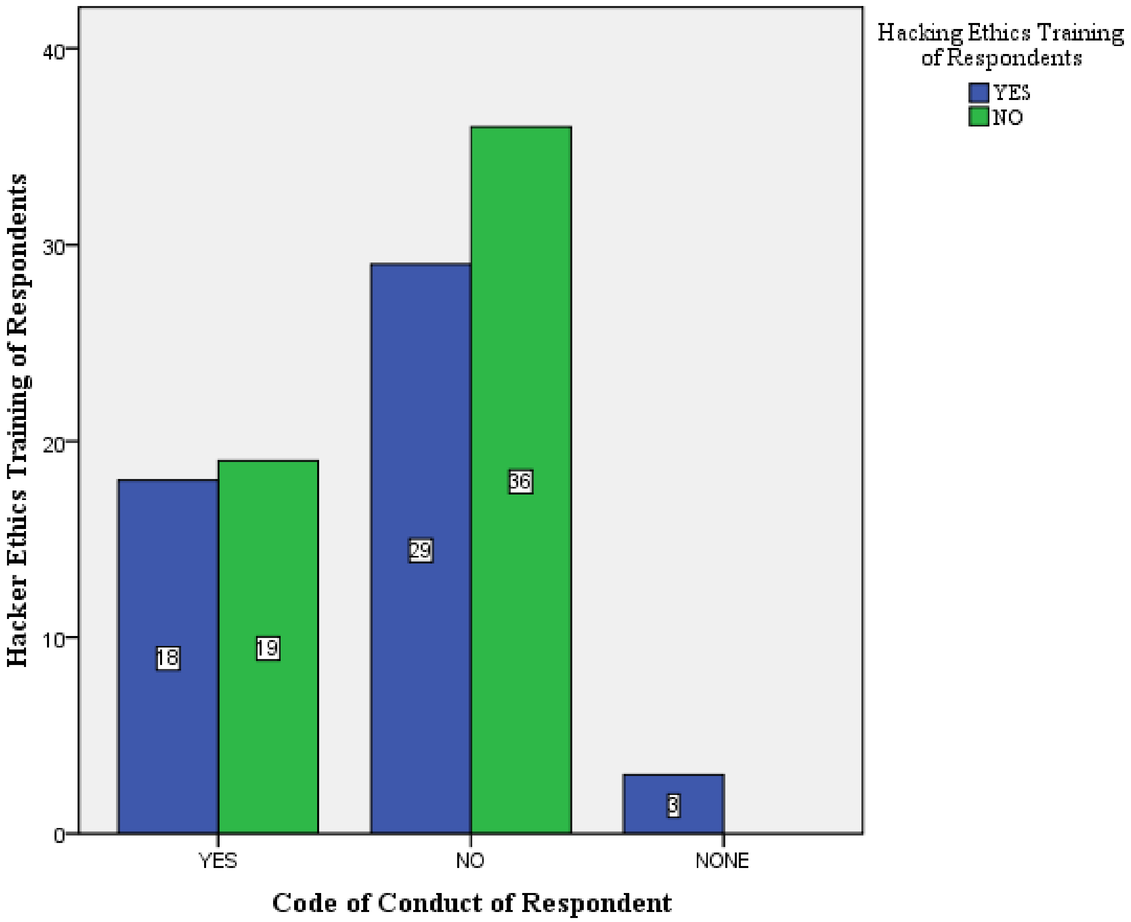
$$= \frac{299.330}{1.732} \Rightarrow \underline{\mathbf{172.823}}$$

Based on the above formula and the subsequent calculation, a sample size of 173 total population was arrived at. The size of the population that was targeted for the study was 173 respondents that provided a truly representative sample to give valid results.

3.4 Sampling procedure

The sampling the researcher undertook was a random selection of BCS, BBIT and MIT, Africa Nazarene Students where the study entailed selecting some of the elements in the population and drawing conclusions about the entire population from the sample. The population was the subject on which the measurement was being taken. Random sampling was chosen to be an appropriate sampling method as it was easy to administer as it requires only a random sample of the population and the sampling intervals were easy to compute. It only required the sample size and population size and as the elements were not organized in some kind of cycle or pattern as in systematic sampling, it gave a representative sample. This study made use of purposive sampling technique where a population that is specifically undertaking IT programs was being sampled.

4.0 Research findings and analysis



Source: SPSS 16.0

Figure 4-24: Trends on GoK Code of Conduct in relation to Hacker Ethics Training

A hypothesis test between the GoK code of conduct and hacking ethics training portrays that those that have no knowledge of the code of conduct and have not undergone hacking ethics training stands at 65.5%. In light of the objective of knowledge and familiarity with the GoK code of conduct, a hacking training program that is constituted of hacker ethics training and guided by the code of conduct is necessary in order to develop as an IT professional as per the respondents.

To assess what is the impact of Ethical Hacking training among IT students ?

In evaluating the impact of Ethical Hacking training among IT students noteworthy is the level at which hacking is taught at ANU. The views from the undergraduates greatly imply that this training has not been carried out at that level. Commensurate to this is an indication by many that they also have no exposure to ethics that goes along with hacking. However personal emotions are exposed even among those that have not gone through this process when posed with the question of whether hacking is right or wrong. Personal opinions greatly dictate how many view hacking. This should be taken positively because in order to become an effective hacker you need to explore both sides of black hat and white hat hacking and draw the line as to what one can do and what one can't do. Key to note however is that on the aspect of how they rated themselves, either as ethical hackers or unethical hackers, many respondents indicated they were unsure, which should be viewed positively as these are minds that should be molded, bounds set and then pointed in the right direction. Accordingly, Hall (2014) emphasizes, while the role of ethics is discussed in computing degree courses, there are inconsistent options in what should be taught to students to prepare them for their professional careers.

5.0 Discussion recommendation and conclusion

5.1 To assess what is the impact of Ethical Hacking training among IT students ?

Ethical hacking training among ANU IT students has had the impact of above all shaping perceptions in the field of hacking brought about by individual knowledge and exposure to this field. The impact of ethical hacking training is not evident that would otherwise dictate their actions and perceptions through prudent online conduct and established hacking training structures at ANU that cater to both students and trainers alike. Individual perceptions dictated by the ethical implications of hacking that are brought about by the impact of the actions of hackers are what is however evident. Rightly so, varied sentiments for and against hacking exist among the IT students which should be welcomed and exploited for in acquiring hacking training and skills students will be exposed to both aspects of what they would ordinarily do and would not do, in essence, their moral rights and wrongs. This should thus be above all be deemed as an opportunity to exploit, to educate, instill ethics, set bounds and above all, point in the right direction. For in hacking when you know just what the rogue elements are capable of and how far they would go, this is exactly what will make you very good at what you do and cause you to be a black hat hacker worst nightmare, with the dividing line being the moral aspect.

5.2 Recommendation

The inclusion of hacking training in the IT students curricula whether as part of the key learning curriculum or as extra curricula learning that seeks to educate and instill the various types of hacking training and skills sets that exist bolstered by ethics training to guide students learning and embed positive and constructive values that ultimately yield positive individuals.

5.3 Conclusion

Central to the training curriculum of IT students should be policies that lay out what should be taught and how it should be taught. The IT professional training program should be treated like other professions like law and medicine as in today’s world the responsibility of an IT steward in an organization is very weighty given the Security implications. Parallel to this is the role that ethics training should play in the administration of the training curriculum. Like other similar professions like in law and medicine, a code of ethics should guide the actions of IT professionals in their practice as the implications of their actions through malpractice have the same grave consequences that directly impact human life and livelihood. To guide the administration of these curricula should be the government master plan on the role out and implementation of ICT within Kenya, legal document. Exposure to the field, testing of skills, collaborations on projects as well as sharing of knowledge coupled with sensitization on the latest trends should be part and parcel of the core training of IT students. ICT security is the wave of the present and inextricably the future as we interconnect everything, and gadgets greatly take over the key roles in our lives, central to this should be the aspect of research and knowledge generation by ANU into cutting edge trends and practices in the IT field that spearhead its operations as opposed to being seen to be reactive in its approach. This, however, is only possible through an environment that fosters learning with an emphasis on exercising of individual talent as well as experimentation. In today’s world, collective effort and collaborations are the keys to the success of any institution, no one individual knows everything or has the skills to accomplish many tasks without others. The more information and knowledge you have, the better placed you are against your competitor and as such the more likely you are to lead in your field.

Acknowledgements

Author	**JOHN KIOKO-students name** MSc. Applied Information Technology. Student:-Africa Nazarene University E-mail: john_kioko@hotmail.com Website: http://www.anu.ac.ke
Co- Author	**DR.BONFACE NGARI-Supervisor 1** Dean and Lecturer, Department of Computer Science Africa Nazarene University E-mail: bnagri@anu.ac.ke Website: http://www.anu.ac.ke
Co- Author	**DR. KENDI MUCHUNGI- Supervisor 2** Lecturer, Department of Computer Science Africa Nazarene University E-mail: kmuchungi@anu.ac.ke Website: http://www.anu.ac.ke

6.0 References

Abdulrahman, M. S. (2015). Ethical Hackers. IT e-Magazine

Africa Nazarene University, (2016). Information Resource Use and Security Policy

Aggarwal, P., Arora, P., Neha & Poonam. (2014). Review on Cyber Crime and Security. IJREAS, Vol. 02, Issue 01

Ajayi, (2016). The impact of cybercrimes on global trade and commerce

AlHogail, A. & Mirza, A. (2014). Information Security Culture: A Definition and A Literature Review

Alnatheer, M.A. (2014). A Conceptual Model to Understand Information Security Culture. International Journal of Social Science and Humanity, Vol. 4, No. 2

Amunga, H.A. (2013). Introducing information ethics in the curriculum at Kenyatta university: views from lecturers and post graduate students. Innovation Journal of appropriate librarianship and innovation work in Southern Africa. No. 46, 12-43.

Briscoe, G. & Mulligan, C. (2014). Digital Innovation: The Hackathon Phenomenon

Brown, C. (2015). White or Black Hat? An Economic Analysis of Computer Hacking

Burns, N. and Grove, S.K. (2003). Understanding nursing research.

Calco, M. & Veeck, A. (2015). 'The Markathon: Adapting the Hackathon Model for an Introductory Marketing Class Project' Marketing Education Review 25(1) pp.33-38.

Carlin, A., Manson, D., & Zhu, J. (2008). Developing the cyber defenders of tomorrow with regional Collegiate Cyber Defense Competitions (CCDC). Proceedings of the 25th Information Systems Education Conference, ISECON 2008, November 6, 2008 –November 9, 2008, 25.

Cobb, S. (2016). Mind This Gap: Criminal Hacking And The Global Cybersecurity Skills Shortage, A Critical Analysis

Cohen, G. (2014). Best practices for network security management

Coleman, E . G. (2013). Coding Freedom: The Ethics and Aesthetics of Hacking. 41 William Street, Princeton, New Jersey 08540 : Princeton University Press.

Conklin, A. (2005). The use of a collegiate cyber defense competition in information security education. Proceedings of the 2005 Information Security Curriculum Development Conference, InfoSecCD *'05, September 23, 2005* – September 24, 2005 (pp. 16–18).

Cox, E. (2013). Ahmed Al-Khabaz expelled from Dawson College after finding security flaw. National Post.

Curbelo, A. M. & Cruz, A. (2013). Faculty Attitudes Toward Teaching Ethical Hacking to Computer and Information Systems Undergraduates Students. Eleventh LACCEI Latin American and Caribbean *Conference for Engineering and Technology (LACCEI'2013)"Innovation in Engineering,* Technology and Education for Competitive*ness and Prosperity" Cancun, Mexico.*

Maiga, I.M. (2015). Cyber Security: The subplot to Africa's connectivity boom. Africaonline Business, p. 1.

Drumwright, M. & Prentice, R. (2015). Behavioral Ethics and Teaching Ethical Decision Making. Decision Sciences Journal of Innovative Education Volume 13 Number 3

Eloff, J. H. P. (2015). An Information Security Governance Framework.

Eyong, K. (2014). "Recommendations for information security awareness training for college students ", Information Management and Computing Security , vol. 22(1) : 115-126

Falk, C. (2014). Gray hat hacking: Morally black and white. CERIAS Tech Report, 2004-20. Lafayette, IN: Center for Education and Research in Information Assurance and Security, Purdue University.

Garfinkel S. (2008). Database Nation. Cambridge, MA: O'Reilly & Associates.

Green, S & Salkiand (2003). Using SPSS for Windows and Macintosh: Analysis and understanding data. 3rd ed. NJ: Prentice Hall.

Hall, B. R. (2014). A synthesized definition of computer ethics. SIGCAS Comput. Soc., 44(3):21–35.

Hogg, M. A., & Terry, D. J. (2000). Social Identity and Self-Categorization Processes in Organizational Contexts. Academy of Management Review, 25(1), 121–140.

Cherono, S. (2015). It is a hackers' paradise out there as Kenyans bare their all online. Daily Nation, p. 1.

Jackson, E.S. (2015). Technology And Ethics. Journal of Information Technology Vol. 1 Art. 7, pp. 30-37

Ochieng', L. (2015). Kenya lost Sh15bn through cybercrime last year, the report says. Daily Nation, p. 2.

Kitheka, P.M. (2013). Information Security Management Systems In Public Universities In Kenya: A Gap Analysis Between Common Practices And Industry Best Practices

Kothari, C. R. (2004). Research Methodology: Methods and Techniques, (2nd ed.) New Age International Publishers: New Delhi.

Kortjan, N., & von Solms, R. (2013). "Cyber Security Education in Developing Countries: A South African Perspective," Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 119, pp. 289-297

Levy, S. (1994). Hackers: Heros of the Computer Revolution. New York: Penguin.

Malan, B. & Bester, C. (2014). Curriculum to teach Information Ethics at universities in Africa

McGregor, J. (2014). The top five most brutal cyber-attacks of 2014 so far.

Miles, M.B. & Huberman A.M. (1994). Qualitative Data Analysis. California 91320: SAGE Publications.

Mtsweni, J. & Abdullah, H. (2015). Stimulating and maintaining students' interest in Computer Science using the hackathon model. The Independent Journal of Teaching and Learning - Volume 10.

Mugenda, M. O. & Mugenda, A. (2008). Research Methods: Qualitative and Quantitative Approaches, African Centre for Technology Studies, Nairobi, Kenya.

Muthama, M.N. (2013). Regulation On Access To Internet: Problems And Solutions. Journal of Theoretical and Applied Information Technology.

Ongong'a, J. J. & Akaranga, S. I. (2013). Work Ethics For Lecturers: An Example Of Nairobi And Kenyatta Universities. International Journal of Arts and Commerce ISSN 1929-7106

Palmer, C.C. (2001). Ethical Hacking. IBM Systems Journal, Vol. 4:, No. 3

Parahoo, K. (1997). Nursing research: Principles, process and issues. London: MacMillan Press.

Pashel, B. A. (2007). Teaching students to hack: ethical implications in teaching students to hack at the university level. Proceedings of the 2006 Information Security Curriculum Development *Conference, InfoSecCD '06, September 22, 2006* – September 23, 2006, 197–200.

Perez, E. (2015). FBI: Hacker Chris Roberts claimed to hack into flights CNN (May 18).

Pike, R.E. (2013). "The "Ethics" of Teaching Ethical Hacking,". Journal of International Technology and Information Management: Vol. 22: Iss. 4, Article 4.

Pike, R.E. & Curl, S.S. (2013). *The "Ethics" of teaching Ethical Hacking.* California State Polytechnic University, Pomona, education Special Interest group of the AITP.

Polit, D.F. & Beck, C.T. (2003). Key Concepts and Terms in Qualitative and Quantitative Research. Nursing research: principles and research.

Pons, E. (2015). Social learning Theory and Ethical Hacking : Students Perspective on a Hacking Curriculum. Proceedings of the Information Systems education Conference Orlando, Florida.

Prasad, S. T. (2014). Ethical hacking and types of hackers. International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) 11, no. 2:24-27.

Radziwill, N., Romano, J., Shorter, D., & Benton, M. (2015). The Ethics of Hacking: Should It Be Taught?

Reid, R. & Niekerk, J.V. (2013). Snakes and ladders for digital natives: information security education for the youth. Institute of ICT Advancement, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa

Republic of Kenya - Computer and Cybercrimes Act, 2016., PART II OFFENCES on Unauthorised access.

Republic of South Africa, Cybercrime and Cybersecurity Bill (2015), Section 75 Chapter 2 – OFFENCES.

Richet, J.L. (2013). From Young Hackers to Crackers

Sterling, B. (1993). The Hacker Crackdown. New York: Bantam.

Suhasini, C. (2014). Ethical Hacking and its Vulnerabilities. International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE).

Solms, S.V., & Solms, R.V. (2014). Towards Cyber Safety Education in Primary Schools in Africa. Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA)

The Republic of Kenya - National Information and Communication Technology (ICT) Policy of 20Th June 2016, Part 15.

The South African National Integrated ICT Policy - White Paper of 28th September 2016, states on part 10 : A Digital Society, Pillar II : DIGITAL ACCESS.

Touray, A., Salminen, A. & Mursu, A. (2013). ICT barriers and critical success factors in developing countries. The Electronic Journal on Information Systems in Developing Countries, 56(7), 1-17.

Trabelsi, Z., & Ibrahim, W. (2013). Teaching Ethical Hacking in Information Security Curriculum: A Case Study. IEEE Global Engineering Education Conference (EDUCON)

Veiga, A. D. (2015). The Influence of Information Security Policies on Information Security Culture: Illustrated through a Case Study. Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance

Voiskounsky, A. E., & Smyslova, O. V. (2003). Flow-Based model of computer hackers' motivation. CyberPsychology & Behavior, 6(2), 171–180.

Wark, M. (2006). Hackers. Theory, Culture & Society, 23(2/3), 320–322.

White, G. B., Williams, D., & Harrison, K. (2010). The CyberPatriot national high school cyber defense competition. IEEE Security and Privacy, 8(5), 59–61.

Wiggins, A., Gurzick, D., Goggins, S. & Butler, B. (2014). 'Quality Hackathon' Proceedings of the 18th International Conference on Supporting Group Work - *GROUP '14* pp.321-323.

Xu, Zhengchuan, Qing H., & Chenghong Z. (2013). Why computer talents become computer hackers. Communications of the ACM 56, no. 4:64-74.

Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the minds of hackers. Information Systems Management, 24(4), 281–287.