Chapter 2

Awareness and Knowledge of Cyber Ethical Behaviour by Students in Higher Education Institutions in South Africa

Tlou Maggie Masenya
Durban University of Technology, South Africa

ABSTRACT

Students in Higher Education Institutions (HEIs) rely on cyber technologies almost daily to perform a wide variety of tasks related to their studies. However, there are ethical guidelines that govern the use of these technologies that also guard against ethical violations. The study examined the level of awareness and knowledge on the cyber ethical behaviour of students in HEIs in South Africa. The factors influencing unethical cyber behaviour and cyber security measures to prevent cyber unethical behaviour among students in HEIs in South Africa were also investigated in this study, using content analysis method. The study was also guided by ethical theories, namely consequentialism, deontology, virtue ethics, and Kohlberg's theory of moral development. Although most of the students in HEIs are aware of unethical cyber behaviours such as cyber bullying, fraud, hacking, pornography, etc., it appears as if there is no collaborative approach for best practices in computer security and training on cyber ethical behaviour for the students within these institutions.

INTRODUCTION

The use of cyber technologies and the Internet is prevalent in the digital world, and has become indispensable resources for exchanging information among users, devices and organizations. Therefore, every society is heavily dependent on technological-mediated communication in this digital transformation era, whereby physical borders are no longer boundaries to information and communication flow (Mohiuddin, 2006). Although digital transformation improves critical business operations and economic growth through the use of digital and cyber technologies, however, as noted by Tiirmaa-Klaar (2016),

the application of these technologies poses ethical challenges to the society. As also noted by Gunarto (2015) cyber technologies have problematic implications as they create some cyber ethical issues such as personal privacy, access right and harmful actions. The excessive use of cyber technologies and Internet thus brings with it many social and cyber ethics-related issues affecting HEIs students. The students are operating in a new world with unlimited access to the information which could affect either learning habits positively or negatively, when interacting with cyber technologies. The unethical cyber practices have thus become a common feature among students in HEIs. As also noted by Khasawneh (2012) the majority of university students have engaged in cyber technology unethical acts such as copyright violations and digital piracy.

Cyber technologies thus expose HEIs students to myriad cyber-attacks and unethical cyber practices that may result in devastating outcomes or profound impact if appropriate measures are not implemented to mitigate the risks. These students and other internet users thus encounter a wide variety of unethical cyber behaviours on social media platforms, including cyberbullying, hacking, privacy violations, cyber-sex, fraud, pornography, digital piracy, cyber plagiarism, cybercrime etc. However, as indicated by Moor (2005) the students in HEIs lack the understanding and awareness of the ethical use of cyber technologies, leading to decisions taken without foreknowledge about ethical responsibilities and consequences. Unethical cyber behaviours have thus been prominent in many countries, in this digital world, whereby countermeasures and preventive measures against these behaviours need to be formulated. HEIs and other private institutions are under immense pressure as they are required to monitor unethical behaviours or acts closely as they may have implications on students' professional life and society at large

It is therefore vital to make the students aware of the proper usage of cyber technologies and cyber spaces, to understand cyber ethics or computer ethics related to security, privacy issues and major negative impacts of these technologies. It is thus crucial for HEIs to create and adopt code of cyber ethics outlining the principles that will govern the use of cyber technologies and how students should behave in cyber spaces. The students should also adhere to cyber ethics while interacting with others and that will also allow them to make ethical decisions. Cyber ethics is a set of moral rules or a code of behaviour applied to the online environment, and any responsible citizen should therefore observe these rules to help make cyberspace a safe place (Tavani, 2013). It is the study of the ethics that are relevant to computer networks which is supposed to cover the user's behaviour and its impacts on individuals and society (Asma, Amber, Muhammad & Madiha, 2015). For the past years, increasing number of higher institutions and governments have enacted cyber ethics policies and regulations. For example, in 2002, Pakistan government has enacted the legal framework called the Electronic Transaction Ordinance (ETO) to address cyber ethics and cyber-crimes issues, with the objectives of identifying, recognizing and facilitating credentials, records, important information, communications and to support secure electronic transactions (Daudpota, 2017). This legal framework also aimed at providing for human resource development in electronic transactions, preventing abuse of information systems as well as encouraging the use of e-government services (Daudpota, 2017). Furthermore, other legal frameworks such as the Electronic Crime Act 2004, the National Response Center, the Accreditation Council were also established to address the issues related to cyber-crime, to stop internet misuse, to ensure strict licensing criteria in a variety of aspects such as personal integrity, security and procedures.

Related Content

Managing Enterprise IT Risks through Automated Security Metrics
Aristeidis Chatzipoulidis, Dimitrios Michalopoulosand Ioannis Mavridis (2016). *Automated Enterprise
Systems for Maximizing Business Performance (pp. 215-243).*
www.irma-international.org/chapter/managing-enterprise-it-risks-through-automated-security-metrics/138675

Personalized Web Service Provisioning to Mobile Users USING Policy-based Profile and QoS
Management
Elarbi Badidiand Larbi Esmahi (2011). *E-Strategies for Resource Management Systems: Planning and
Implementation (pp. 172-184).*
www.irma-international.org/chapter/personalized-web-service-provisioning-mobile/45104

Enterprise Systems in Small and Medium-Sized Enterprises
Sanjay Mathrani, Mohammad A. Rashidand Dennis Viehland (2010). *Business Information Systems:
Concepts, Methodologies, Tools and Applications (pp. 277-291).*
www.irma-international.org/chapter/enterprise-systems-small-medium-sized/44078

Management's Contribution to Internet Commerce Benefit - Experiences of Online Small
Businesses
Simpson Poon (2003). *Creating Business Value with Information Technology: Challenges and Solutions
(pp. 277-296).*
www.irma-international.org/chapter/management-contribution-internet-commerce-benefit/7205

Delivering the Whole Product: Business Model Impacts and Agility Challenges in a Network of
Open Source Firms
Joseph Feller, Patrick Finneganand Jeremy Hayes (2010). *Business Information Systems: Concepts,
Methodologies, Tools and Applications (pp. 978-992).*
www.irma-international.org/chapter/delivering-whole-product/44117