Chalimbana University Multi-Disciplinary Journal of Research
ISSN: 2708-0471
http://www.journal.chalimbanauniversity.net/
Volume 1 Issue 2; January/February 2020

SOCIAL ENGINEERING, AN EMERGING CYBER CRIME THREAT IN HIGHER LEARNING INSTITUTIONS: A CRITICAL LITERATURE REVIEW OF THE PHISHING METHOD

William Phiri[1] & Edgar Zulu[2]
Department of Information, Communication, Educational Media and Technology, School of Education, Chalimbana University Lusaka, Zambia[1, 2]

Abstract

The paper is the critical literature review focusing on shattering methods that crackers use to gain access to the information that is deemed private in both Private and Public Higher Learning Institutions. The desk research addressed social engineering employing the phishing method that uses a fake login page of any website such as PayPal, Gmail, yahoo, Hotmail, twitter and Facebook. The point of departure of the paper will be proposed practical measures aimed at mitigating effects of hacking on data privacy, confidentiality, availability and integrity in Universities. It should be noted that hackers execute hacking for different motives, such as doing it for fun, educational purposes and more rampantly for financial gain. While there are other hacking methods that involves cracking passwords using different methods like the dictionary, hybrid and the brute force attacks, these take a relatively longer period of time in comparison to the phishing method has proved to be very effective and efficient from an attacker's view point as the attacker takes a very short time to execute the hacking process.

Keywords: Social engineering, information systems, hacking, reconnaissance, phishing.