BUSITEMA
UNIVERSITY
Pursuing Excellence

P.O. Box 236, Tororo, Uganda
Gen: +256 - 45 444 8838
Fax: +256 - 45 4436517
Email: info@adm.busitema.ac.ug

www.busitema.ac.ug

MITIGATION METHODS AND FACEBOOK USER ACCOUNT HACKS AMONG UNIVERSITY STUDENTS IN MBALE CITY

BY

OKWARE PHILIP

B.I.T Honors (CU)

REG NO, BU/GS18/MCF/5

STUDENT NO, 1800403970

SUPERVISORS

1. DR. NABIKORA IIDEPHONSE
2. MR. ODONGTOO GEOFFREY
3. MR. ALUNYO ANDREW

A DISSERTATION REPORT SUBMITTED TO THE FACULTY OF ENGINEERING IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF A DEGREE OF MASTER OF COMPUTER FORENSICS OF BUSITEMA UNIVERSITY

MAY, 2022

DECLARATION

I **Okware Philip** a student of Busitema University certify that;

a. The work in the thesis is unique and was completed by me under the supervision of my supervisor.

b. The work has not been submitted to any other Institute for the purpose of receiving a degree or diploma.

c. I followed the rules and principles outlined in the Ethical Code of Conduct.

d. I've used items (data, theoretical analysis, and writing) from other sources, I've cited them.

e. I have acknowledged their contributions by referencing them in the thesis text.

f. When I quote written items from other sources, I give acknowledgment to the original source.

g. The similarity index is determined by the plagiarism test.

Signature ………………………………… Date: ……………………………

Okware Philip

APPROVAL

This project that has been prepared by **Okware Philip,** has been carried out under our supervision, is now ready for submission to the school of postgraduate studies and research for the Award of the Degree of Master of Computer Forensics of Busitema University.

Signature: ………………………………… Date: ………………………………………

DR. NIBIKORA IIDEPHONSE

(SUPERVISOR)

Signature: ………………………………… Date: ………………………………………

MR. ODONGTOO GEOFREY

(SUPERVISOR)

Signature: ………………………………… Date: ………………………………………

MR. ALUNYU ANDREW

(SUPERVISOR)

ACKNOWLEDGEMENTS

I am profoundly grateful to my supervisors; Dr. Nibikora Iidephonse, Mr. Odongtoo Geoffrey, Mr. Alunyo Andrew for your tireless support and guidance to this project towards its completion and success, my research would have been impossible without the aid and support of you. The adequate time and reliability you exhibited made it possible for me to achieve this golden goal, May the Almighty Lord reward you abundantly for this wonderful service.

I would like to thank all my colleagues; Master of Computer Forensics (MCF) class 2018 for your cooperation.

Special thanks to my parents; Mr. Okitwi Bisansio and Late Athieno Anna Rose for resources and time you have always sacrificed towards achievement of this goal.

I am deeply grateful to Mr. Okemer Juventine for the good heart you rendered towards my education background, without you I wouldn’t have reached this far. God bless you

I sincerely appreciate Mr. Sempijja Emmanuel and Mr. Agama Philip for the encouragement and psychological support that you have always given me towards completion of this project

My honest gratitude to my family; Awor Judith, Okitwi Isaac Ernest, Atabong Curine Ruth, Okware Emillian Travis, and Okia Adrian Zane for being with me patient, encouraging, as regards to completion of this course

TABLE OF CONTENTS

List of Tables

ABSTRACT

The researcher carried out an inductive research that investigated the effect of Facebook user account security systems on preventing Facebook user account hacks among university students in Mbale City. The study objectives were to; investigate the effect of pass words, verification and log out on prevention of Facebook user account hacks among University students in Mbale City. A descriptive design was used by the researcher with both qualitative and quantitative approaches. The sample size was 92 respondents that included students from Universities in Mbale City and only 93.5% responded. Data was analyzed by the use of computer aided SPSS data analysis software. Presentation of data was done by the use of tables and percentages. Descriptive statistics and correlations were used to establish the contribution of mitigation mechanisms to prevention of Facebook user account hacking. Findings in this study indicate that; 75.6% recommend that Passwords are a good security mechanism against Facebook hacking but there has been laxity among Facebook account users on issues of strength of pass words, 77.9% say of use verification has been effective in mitigating Facebook user account hacks but it has not been embraced by a significant number of Facebook account users and that logout has been an effective ant-hacking mechanism but some users have not been effectively logging out timely or on other electronic gadgets hence opening a hole for hackers. The researcher recommends that; users to be educated to always have strong pass words that should be between 10-15 characters long, a mix of uppercase and lower case letters and include numbers or symbols; avoid sharing pass words and keep on changing pass words with the reminder by automated dates of password expiry dates; Verification is a helpful can be extended to ensure that it starts with user name apart from waiting at the point of pass word insertion; User account log out should be in such a way that users should always logout after every session and Automatic security alerts to be installed within the Facebook user account system

CHAPTER ONE

INTRODUCTION

1.0 Introduction

The exponential growth of social media (Facebook) has facilitated the development of many serious cybercrime and malicious activities or malicious Facebook Applications which pose a number of security threats to Facebook users. The study aimed at identifying mitigation framework for hacking of Facebook users. This chapter presents the background to the study, statement of the problem, the purpose of the study, Objectives of the study, the research questions, Scope of the study, justification of the study, the significance of the study, limitation of the study and definition of operational the terms.

1.1 Background of the study

Today the world of social networking media introduces a new set of experiences that range from quicker sophisticated and wider sharing of information to greater risk of misuse of information. Hacking threats to both individuals and organization's sensitive information have increased due to increased social networking as hackers are actively targeting individuals and organizations' to acquire secrets to undercut business or personal reputation of the victims (Margaret, 2008).

> A social networking service, often known as a social networking site, is an online platform that allows people to develop social networks or relationships with others who have similar personal or professional interests, activities, backgrounds, or real-life connections.

The type and amount of features offered by social networking sites differ. They can use a variety of modern information and communication tools on desktops and laptops, as well as mobile devices like tablets and smartphones. This could include online photo/video/sharing and diary writing (blogging). Developers and users occasionally mistake online community services for social-network services, but in a larger sense, a social-network service typically delivers an

REFERENCES

Alhazmi O. H. and Y. K. Malaiya, (2005) "*Modeling the Vulnerability Discovery Process*," 16th IEEE International Symposium on Software Reliability Engineering (ISSRE'05), pp. 129-138, 2005.

Aimeur, E, Gambs, S, Ho, A (2010) *Towards a privacy y-enhanced social networking site.* In: Conference paper, 5th international conference on availability, reliability and security, 15–18

Barracuda Labs (2011) "*Seven Annoying Attacks That Facebook Misses."* Barracuda Labs.

Benjamin Jensen, and Ryan C. Maness (2018) *Cyber Strategy*. Brandon Valeriaano,

Boyd, d, Hargittai, N (2010) *Facebook privacy settings: who cares? First Monday* 15(8): 22 pp.

Butler, E, McCann, E, Thomas, J (2011) *Privacy setting awareness on Facebook and its effect on user-posted content. Human Communication* 14(1): 39–55.

Chertov R., S. Fahmy, and N. B. Shroff, (2006) "*Emulation versus simulation: A case study of TCP-targeted denial of service attacks,"* in Testbeds and Research Infrastructures for the Development of Networks and Communities, 2006. TRIDENTCOM 2006. 2nd International Conference on, 2006, p. 10–pp

David. B. P. Pongsin, S. Dawn, and Z. Jiang (2008) *"Automatic patch-based exploit generation is possible: Techniques and implications,"* IEEE Symposium on Security and Privacy.

Debatin, B, Lovejoy, J, Horn, A. (2009) *Facebook and online privacy: attitudes, behaviors, and unintended consequences*. Journal of Computer-Mediated Communication 15(1): 83–108.

Deborah J. Bodeau and Richard Graubart (2011), Cyber Resiliency Engineering Framework, MITRE Technical Report MTR 110237, The MITRE Corporation, September 2011.

Erlingsson .U., (2007) "*Low-level Software Security : Attacks and Defenses Low-level Software Security : Attacks and Defenses,"* Redmond, WA, USA, 2007.

Fogel, J, Nehmad, E (2009) *Internet social network communities: risk taking, trust, and privacy concerns*. Computers in Human Behavior 25(1): 153–160.

Gerace T.and H. Cavusoglu, (2009) "*The critical elements of the patch management process,"* Communications of the ACM, vol. 52, no. 8, p. 117, Aug. 2009.

Greiner, L (2009) *Hacking social networks*. Networker 13(1): 9–11

Hoadley, C, Xu, H, Lee, J. (2010) *Privacy as information access and illusory control: the case of the Facebook News Feed privacy outcry*. Electronic Commerce Research and Applications 9(1): 50–60.

Hunter, P (2008) *Social networking: the focus for new threats-and old ones*. Computer Fraud & Security 2008(7): 17–18.

Jacobs. J.R, (2011). "*Measuring the Effectiveness of the USB Flash Drive as a Vector for Social Engineering Attacks on Commercial and Residential Computer Systems,"* Embry Riddle Aeronautical University, 2011.

Jansen W., (2009) "*Directions in security metrics research,"* DIANE Publishing, Gaithersburg, MD, 2009.

Lewis, K, Kaufman, J, Christakis, N (2008) *The taste for privacy: an analysis of college student privacy settings in an online social network*. Journal of Computer-Mediated Communication 14(1): 79.

Lippmann. R. et al., (1998) *"Evaluating intrusion detection systems: the 1998 DARPA off-line intrusion detection evaluation,"* Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00, pp. 12-26, 1998.

McQueen. M. A., T. A. McQueen, W. F. Boyer, and M. R. Chaffin, (2009) *"Empirical estimates and observations of 0day vulnerabilities," in System Sciences*, 2009. HICSS'09. 42nd Hawaii International Conference on, 2009, pp. 1–12.

Moullin (2004) *A Best Practices Guide for Mitigating Risk in the Use of Social Media* – (Alan Oxley 2011) University Technology. Malaysia

Neo. (2011) "*Configuring your Facebook Application Security Settings."* The Pizzy. N.p.

Nicole Perlroth (2021). "*How the U.S. Lost to Hackers*". The New York Times. Archived from the original on 28 December 2021

NIST Computer Security Resource Center (CSRC), (2011) "*National Vulnerability Database,"* 2011 Offensive Security, "Exploit Database," 2011.

Ozment A.. R, (2007) "Improving vulnerability discovery models," in Proceedings of the 2007 ACM workshop on Quality of protection, 2007, pp. 6–11.

Palilery, Jose (2014). "*What caused Sony hack: What we know now*". CNN Money. Archived from the original on 4 January 2015

Sagan S and M. Bunn, (2014) *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes* (Cambridge MA: American Academy of Sciences), 2014, ISBN 0-87724- 097-3.

Salah. K. and a. Kahtani,, (2009) "*Improving Snort performance under Linux*," IET Communications, vol. 3, no. 12, p. 1883, 2009.

Sommestad. T and A. Hunstad, (2012) "*Intrusion detection and the role of the system administrator,"* in Proceedings of International Symposium on Human Aspects of Information Security & Assurance, 2012.

Stevens, Tim (2018). *"Global Cybersecurity: New Directions in Theory and Methods"* (PDF). Politics and Governance. 6 (2): 1–4.

Stone burner, G.; Hayden, C.; Feringa, A., 2004). "*Engineering Principles for Information Technology Security"* (PDF). csrc.nist.gov. doi:

Wilander. J. and M. Kamkar, (2003) *"A comparison of publicly available tools for dynamic buffer overflow prevention,"* in Proceedings of the 10th Network and Distributed System Security Symposium, 2003, pp. 149–162.

Woo, S.-W. H. Joh, O. H. Alhazmi, and Y. K. Malaiya, (2017) *"Modeling vulnerability discovery process* in Apache and IIS HTTP servers," Computers & Security, vol. 30, no. 1, pp. 50-62, Jan. 2011.

Yost, Jeffrey R. (2015). "*The Origin and Early History of the Computer Security Software Products Industry*". IEEE Annals of the History of Computing. 37 (2): 46–58.