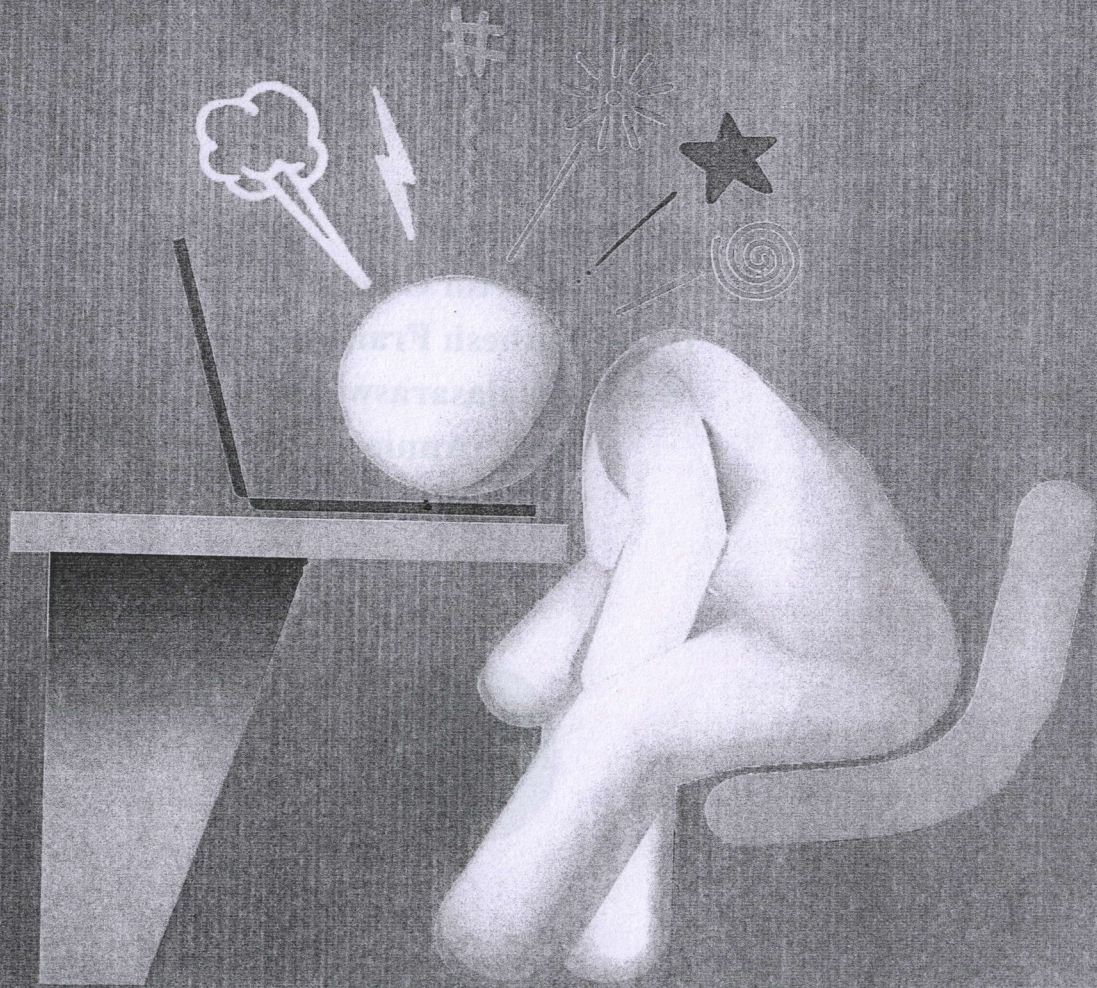


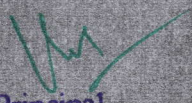
Bala - 9

SOCIAL MEDIA INFLUENCE ON YOUTH IN THEIR PSYCHO-SOCIAL BEHAVIOURAL FUNCTIONS

2017



Chief Editor
Dr. D. Thomas Alexander


Principal
St. Xavier's College of Education
(Autonomous)
Palayamkottai - 627 002

Social Media: Influence on Youth in their Psycho-Social Behavioural Functions ISBN: 978-93-84192-09-9

Published by

St. Xavier's College of Education (Autonomous)

(Re-accredited (3rd Cycle) by NAAC at 'A' Grade with CGPA: 3.67)

Palayamkottai-627002

Ph : 0462 – 2577630 Fax : 0462-2577631

e-mail : sxcebed@yahoo.com

Website: www.stxaviersbedcollege.org

First Edition: April, 2017

© All Rights Reserved

St. Xavier's College of Education (Autonomous) – Palayamkottai -2

ISBN : 978-93-84192-09-9

©All rights reserved. No part of this book may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher.

Printed at

Creative Printers

Murugankuruchi

Palayamkottai – 627 002.

S.No.	CONTENT	Page No.
29.	Positive and Negative Aspects of Using Social Networks <i>S. Shummuga Narayanan & Dr. H. Deepa</i>	109
30.	Social Media Overshadowing Newspaper <i>R. Wingling Paula Fari & Dr. S. Amaladoss Xavier</i>	114
31.	Impact of Social Media on Children, Adolescents <i>R. Esakki Durai & R. Rajendran</i>	117
32.	Does Social Media Impinge upon our Health? <i>S. Kiruba Malar & A. Metilda Jasmine Shanthi</i>	121
33.	Impact of Social Media on Face-to-Face Interaction <i>A. Maria Charlie</i>	126
34.	Influence of Social Media in Education on the Present Scenario <i>T. Josephine & C. Peter Alphonse</i>	130
35.	Impact of Social Networking Sites on Academic Performance of Students <i>G. Ponselvakumar</i>	134
36.	Influence of Social Media on Youth <i>R. Selvaganapathy & T. Ganesh</i>	137
CHAPTER- III SOCIAL MEDIA AND EDUCATION		139-230
37.	Study of Problematic Whatsapp Use Among Adolescents in Relation to Academic Achievement <i>A. Sasikala & Sr. Marthal</i>	139
38.	Social Media in Education: Pros and Cons on Students <i>S. Augustin Bens Raj & Dr H. Deepa</i>	144
39.	Social Media Enabled Learning <i>K. Denny John & Dr. P. S. Sreedevi</i>	148
40.	Dissemination of Educational Information through Social Media <i>Dr. M. Vasimalairaja</i>	152
41.	Use of Social Media in Education: Positive and Negative Impact on the Students <i>Dr. S. Arockiasamy</i>	155
42.	Teaching Ethical Hacking Pedagogy to Students <i>M. Balasaraswathi & M. Amalorpavam</i>	159
43.	Utilization of Social Media in Higher Education <i>G. Kokila Selva Kumari</i>	163

TEACHING ETHICAL HACKING PEDAGOGY TO STUDENTS

M. Balasaraswathi, Assistant Professor in English Education,

St. Xavier's College of Education, Palayamkottai

M. Amalorpovam, Assistant Professor in Tamil Education,

St. Justin's College of Education, Madurai

INTRODUCTION

The prominence of information technologies and increasing dependence on technological infrastructures continues to infiltrate the whole society. The Internet has provided vast opportunities in a wide array of areas that are unimaginable in the past. But today, we are able to access massive amounts of information, and connect in unprecedented ways. Along with the positive capabilities provided by the Internet and networking, unpleasant aspects also cherish in unexpected ways. Criminals of today, have a new platform for conducting activities that are unaccepted in the society. Such behavior must be cautioned from the initial stage and preventive measures have to be implemented. The very root of such act should be sensed and fired by the authority on constant basis for which monitoring becomes the foundation lodged by the Government. The purpose of this article is to analyze the use of an ethical hacking pedagogical approach to improve information security instruction.

A hacking methodology appears to be a more offensive and proactive approach for information security instruction. This approach may be effective to better prepare future information security professionals to combat unethical hacker intrusions associated with the Internet and computer networks. Future information security professionals would be better equipped to combat intrusions if equipped with the knowledge and skill sets currently used by attackers. In order to equip those professionals, students must be prepared to fight the ever-growing challenges associated with effectively securing computer networks.

ETHICAL HACKING

Ethical hacking may be thought of as a methodology for assisting computer professionals and administrators in their efforts to secure networks. As such this topic will be reviewed in light of its effectiveness for instructing proactive offensive measures to students in computer security courses. The basic assumption associated with ethical hacking is merely that of a different approach to security. Ethical hacking is primarily penetration testing and includes penetrating the "system like a hacker but for benign purposes" (Oriyano, 2014). It is felt by many that students need to experience firsthand what the attacker will be doing and what tools will be used (Ethical Hacking: Student courseware). They maintain that students must have opportunities to "experiment and practice with security technologies" in order to be equipped for contributions in the field of computer security.

Ethical hacking and ethical hacker are terms used to describe hacking performed by a company or individual to help identify potential threats on a computer or network. An ethical hacker attempts to bypass system security and search for any weak points that could be exploited by malicious hackers. This information is then used by the individual or an organization to improve the system security, in an effort to minimize or eliminate any potential attacks.

An ethical hacker is an individual hired to hack into a system to identify and repair potential vulnerabilities, effectively preventing exploitation by malicious hackers. They are security experts

Principal
St. Xavier's College of Education
(Autonomous)
Palayamkottai - 627 002

that specialize in the penetration testing (pen-testing) of computer and software systems for the purpose of evaluating, strengthening and improving security. An ethical hacker is also known as a white hat hacker, red team, tiger team or sneaker. Techopedia explains Ethical Hacker as a software or hardware vendor who achieves greater profitability by hiring ethical hackers, versus being subjected to other types of vulnerabilities and exploitations.

NEED FOR ETHICAL HACKING EDUCATION

Teaching students how to hack ethically may be seen as a worthy endeavor, and most educationists agree that it is critical for security professionals. Pashel (2006) proposes that the ability to determine weaknesses in computer systems can assist security professionals in preventing attacks. He goes on to offer that ethical hacking may be deemed a crucial element in a security program (Pashel, 2006). It is important to determine what skill sets are needed by security professionals and help educate those skills (Logan, & Clarkson, 2005).

Many of the skills used in ethical hacking may be viewed as more proactive rather than reactive in nature. Security educators feel that teaching "offensive methods" produces better security professionals than teaching "defensive techniques". A number of researchers and educators agree that practicing ethical hacking skills are crucial in developing necessary skill sets for computer security professionals. He goes on to propose, "One cannot perfectly design or build defenses for attacks that one has not truly experienced, first-hand" (Trabelsi, 2011). In another study, Trabelsi (2012) argues that by not providing information and knowledge gleaned from hacking, computer security professionals are not adequately being prepared for their career. He goes on to suggest that teaching attacks is considered a necessary element of security education. Finally, Trabelsi and Alketbi (2013) state that techniques of ethical hacking should be included in a curriculum to better prepare security professionals.

POLICY FOR USING COMPUTERS

One major step in deterring unwanted behavior in the instruction of ethical hacking instruction is the use of a computer ethics policy. Many argue that institutions must have a policy to assist in the process of instilling ethical behavior relating to new hacking skills. Greene (2004) argues that educational institutions need a policy to encourage ethical actions and to "dissuade students with weak ethics." While policies are only one component, they are crucial in assisting institutions with creating an environment of ethical behavior. Greene (2004) goes on to offer that computer use policies can help regulate a sense of ethics and permitted behavior. He concludes by suggesting that educators must stress legal implications and information concerning the punishment for crimes.

It is hoped that once students understand the legal aspects of unwanted behavior relating to ethical hacking instruction, that they will have second thoughts about acting unethically. Logan and Clarkson (2005) also contend with the importance of computer use policies in institutions of higher education. They further recommend that, "Computer Science departments should consider creating course-level AUPs to augment the university's general use policies" (Logan & Clarkson, 2005). They go on to offer that the tools and techniques used within the classroom be combined with instruction in ethics and legal issues (Logan & Clarkson, 2005). While the use of a computer ethics policy contributes in reduction of unethical behavior by students in ethical hacking preparation, it is critical that they know of its existence and content.

BEST PRACTICES IN ETHICAL HACKING EDUCATION

With the ethical and legal implications of ethical hacking being addressed, the attention will be placed upon the best practices currently being offered to prepare future security professionals. Some of the best practices emphasize a hands-on approach and the incorporation of soft skills. The curriculum for teaching ethical hacking techniques should adequately prepare students for a career in security. Trabelsi (2014) states that "a security education curriculum that does not give the students the opportunity to experiment in practice with security techniques" could potentially cause students to be inadequately prepared for a future career. He goes on to offer that students need to have the skills to feel confident in their ability to combat an attacker.

Lancor and Workman (2007) suggest that a "good defense" begins with understanding the opponent's offense. The educators offered Google hacking as a tool within a web security course. Students were exposed to a powerful approach in defending networks by using Google to perform attacks. The educators felt it critical to teach students how to protect against such Google attacks by intruders.

HANDS ON APPROACH

Logan and Clarkson (2005) argue that training in ethical hacking should be conducted with a "hands-on" approach. The educationists suggest that a "book and lecture-based instruction is not always as effective in demonstrating concepts as hands-on experience". Most agree that the quality of the instruction is critical to the success of the educational offering. Along with the importance of actually performing the hacking, the tools should be the effective in conducting the assignment. Students need to see that ethical hacking is only one component in a security plan. In addition to hacking, there should be the vulnerability assessments that continue to monitor the network. The goal would be to perform the process as an ongoing basis to improve the overall security of the network. When students were anonymously surveyed concerning the hands-on lab instruction, 85% felt that the applications were useful and helped them to understand the theoretical concepts in the class. Moreover, 87% of the students indicated that they would like further hands-on lab instruction, and 86% felt they would recommend the lab activities to others (Trabelsi, &McCoey, 2016).

SOFT SKILLS

A second area of best practices indicates that soft skills should not be overlooked in ethical hacking education. Dimkov, Pieters, and Hartel (2011) propose that "teaching students only the technical side of information security leads to a generation of students that emphasize digital solutions, but ignore the physical and social aspects of security." It was argued that often, when examining computer systems, a practice or instruction lacks the human component. Some researchers favor soft skills that enhance awareness of a potential security threat in the form of social engineering. For personal grooming, heightening privacy safeguards and for enhancing computer security there comes a necessity to be trained in soft skills incorporated with technopedagogy. Such awareness should be created among the students who get immersed in social media sites. Dealing with computers and with human has a lasting difference as both are not one and the same. Machines could not replace human as it could not frame and fix itself in soft skills.

CONCLUSION

The prominence of information technologies and networking permeate all aspects of our lives and society. Security concerns relating to attackers and intruders are causing many security

professionals to examine and explore more proactive approaches to securing networks. This article throws light on ethical hacking pedagogy, suggests ethical hacking as a computer security instruction methodology, and illustrates the ethical and legal consequences of teaching students to hack. Best practices in ethical hacking pedagogy were highlighted as well as suggestions and recommendations for ethical hacking instruction, effective role of instruction and preparation of future information security professionals are exposed.

This article demonstrates that not only future information security professionals need to be equipped with skill sets currently used by attackers, but students will also need skill sets to combat the persistent future advances and challenges imposed by attackers. In addition, future information security professionals will need similar hacker mindsets and skill sets to effectively secure networks from intruders. It also suggests that instruction in information security utilizing an ethical hacking methodology creates a better learning model to combat the destructive issues associated with the activities of attackers on the Internet and computer networks.

REFERENCE

1. Dimkov, T., Pieters, W., &Hartel, P. (2011). Training students to steal: A practical assignment in computer security education. Proceedings of the 42nd ACM Technical Symposium on Computer Science Education – SIGCSE '11.
2. Ethical Hacking: Student courseware. Ec-Council. (2005, March). Retrieved from www.eccouncil.org.
3. Greene, Tim (2004, July 22). Training ethical hackers: Training the enemy? Retrieved from https://defcon.org/html/links/dc_press/archives/12/ebcvg_training_ethical_hackers. Html.
4. Logan, P., & Clarkson, A. (2005). Teaching students to hack. SIGCSE Bull. ACM SIGCSE Bulletin, 157-157.
5. Trabelsi, Z. (2014). Enhancing the comprehension of network sniffing attack in information security education using a hands-on lab approach. Proceedings of the 15th Annual Conference on Information Technology Education – SIGITE '14.
6. Trabelsi, Z., &McCoey, M. (2016). Ethical hacking in Information Security curricula. International Journal of Information and Communication Technology Education, 12(1), 1-10
