Creating Mass Cyber Security Awareness Among Children, Parents and Teachers Through Appropriate Training And Campaign Mechanism

Dhuha Nasser Shamis Al-Nomani
Middle East College,
Muscat, Oman.
09F5675@mec.edu.om

Sumayia Abdullah Muhanna Al Nabhani
Middle East College,
Muscat, Oman.
snabhani@mec.edu.om

Syed Thoufeeq Ahmed
Middle East College,
Muscat, Oman.
thoufeeq@mec.edu.om

Abstract:

Nowadays, we are currently and completely living in an age where the use of internet has become the second nature of millions of people around the globe. With the continuous development and growth of the internet providing new services and applications to different users, many of them are also becoming more and more active in engaging with the internet and because of this they are more likely become vulnerable to different malicious threats and risks brought along by the Internet such malwares, viruses, cyber bullying, identity theft, unauthorized access, hacking and other malicious threats. Furthermore, these risks and attacks can greatly affect and threatened the safety and security of each users especially those that have limited knowledge and understanding about cyber space and are not aware of the threats that comes along with the Internet and the means on how to protect and secure themselves from these risks. This paper aims to provide essential information's to all users, by conducting a program about cyber security awareness for all stakeholders of different age groups. Moreover, the aim is to deliver message to the community to be aware from potential risks that occur from cyber security.

With the underlying consequences of having limited knowledge, understanding and relevant information regarding cyberspace or internet, this project study also will equip and empower as well as educate each users enough information and awareness through different cyber security awareness sessions and campaign mechanisms

Keywords: Cyber threats, Cyber security, Awareness

1. INTRODUCTION

we are currently living in age where the use of internet has become the second nature to millions of people around the globe [11]. However, according to many experts [12], [13], [14] and [15], the internet has now been continuously threatened by different malicious threats and numerous risks such as hacking, phishing, cyber-crimes, viruses and many other malicious attacks. Core to unethical activities on the internet is the exploitation of sensitive and confidential or private information's and violations of different policies or internet ethics. Thus, making the internet users at high risks of having their private information's compromised, misused, destroyed and modified.

[16] in his study found that many of the internet users lack awareness and knowledge and are ignorant of the need to protect their personal, sensitive and confidential information's. Moreover, their online behaviors and insecurities make them an easy target for destruction, exploitation and violations. The lack of knowledge about cyber security awareness amongst the adults bring negative impacts on their roles in protecting children, their own selves and even their families and their loved ones.

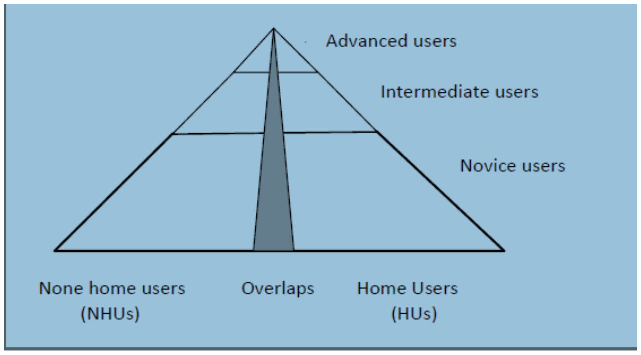
With the underlying consequences of lack of knowledge and relevant information's about the internet, cyber-security and awareness, it becomes an important fundamental issues faced by the most of the internet users. [17] found that promoting cyber-security awareness will greatly contribute to cyber security as a whole and can provide the users' ability to recognize and protect themselves from any threats and risks that they encounter or may appear online.

2. BACKGROUND AND RELATED WORK

Cyber Security focuses mainly on protecting computers, networks, programs and information's from unauthorized and unintended access, modification and destruction [18]. It is also commonly referred to as computer security that protects and secure different computer systems, from different hazards or unethical cyber space behaviors such theft, software and hardware damage or destruction and modification of information as well as the misdirection of services they provide [19]. Cyber security also allows every user or operator to control the physical access to the hardware as well as protect it against harmful factors brought by different network systems access, data and code injection and malpractice by both parties either intentional or accidental.

Cyber security awareness is a form of conducting actions to protect and secure important and confidential information's stored in a computer and accessible through the cyber by the authorized person only [20]. It is an act of raising realization of all the potential risks that may evolve from the rapid growth of different forms of information as well as the increasing growth of threats that comes with it. As data or information stored increases in value, threats from attackers also becomes highly unavoidable. These attackers increased and develops their capabilities to a new extent in order for them to create or design highly risk able and more attack methods that targets not only the cyber space itself but the lives of people as well. Cyber security awareness aims to make everyone understand that they also are at high levels of vulnerability from different malicious attacks circulating in the cyber world and help them be fully aware of their susceptibility from the opportunities and challenges in today's cyber space threats, changes in human risk behaviors and enhance a secured organizational group since there is a wide range and vast growth of development in information technology.

"The ability to protect or defend the use of cyberspace from cyber-attacks" [1]. Cyber space is defined "A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" [2]. Cyber security is the formal program that aims to train users of the different potential threats and risks to an organizations information's and the possible ways on how to avoid and prevent this threats and risks [3]. The study done [3] reflect on breaches portrays the large number of social engineers that took the advantage of exploiting humans. [4] in his book discusses the reinforcements of issues on security and collaborations between individuals and businesses as being a priority or important factors during the beginning of the twenty-first century. He also discusses the about the fast and rapid growth of the Internet from simple forms to larger forms that provides great impacts to the global world. [5] highlighted importance of educating people about cyber infrastructure since the world is now rapidly building this infrastructure. Aside from this, cyber ethics cyber security and cyber safety must be integrated within the educational process beginning at an early age to ensure the confidentiality, availability and integrity of information systems and protect them from different cyber security attacks. [6] point out that if implemented correctly, security awareness training becomes an important necessity to every organization. If the users are properly informed as what to watch for, possible ways of prevention and remediation procedures , can alone be a measure to prevent a lot of potential problems such as threats that can affect the infrastructure and the organization as well. It is often that awareness is the only key to prevention and protection. [8] highlighted Cyber situational awareness by conducting a systematic review of literature. [8] in their study focused on the establishment of necessary infrastructure in small businesses who lack extensive ICT support and services. [9] has done an Empirical Study of Cyber Security Perceptions. Their study clearly suggests that prior to security education, the users definitely agree that it is a very important process especially to businesses and home users. From their findings, the general awareness of the importance of cyber security awareness or education is relatively high which is caused probably by the consequence of the combination of media efforts and personal experiences in malware infection, identity theft or system compromise. [10] has done an campaign on creating the cyber security for home user by adopting the methodology given in figure1. [10] also proposed an E-Awareness Model that can help in empowering the users through a better understanding about the different security risks, issues possible threats and how to prevent and avoid them from incurring further damages to both users and their system.



3. METHODOLOGY ADOPTED

This research project primarily focus on creating mass cyber security awareness among children, parents and teachers in Sultanate of Oman. The primary stakeholders and data source for this project are given in figure 2.

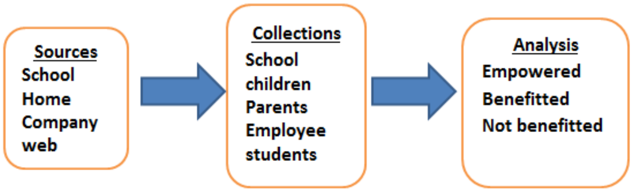


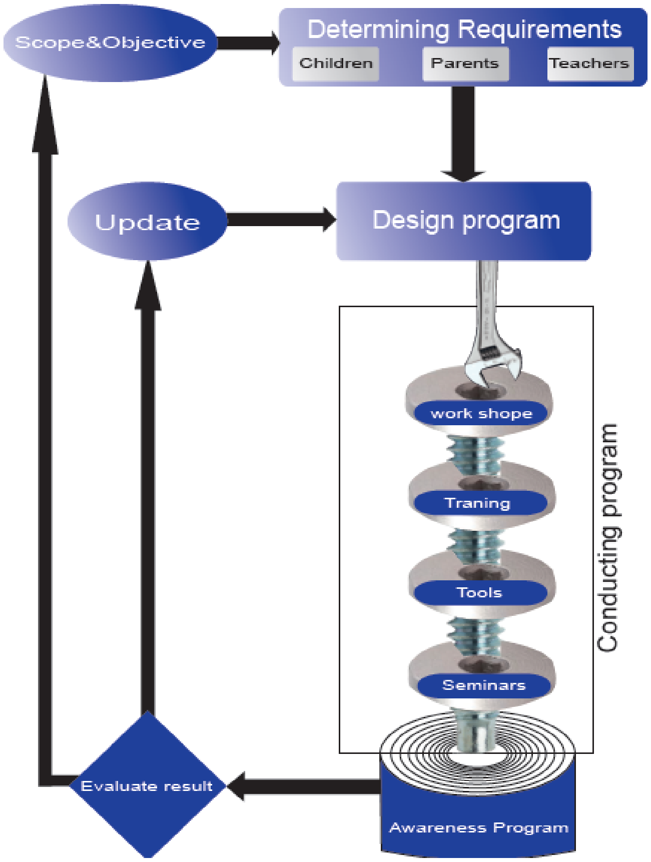
Figure 2: data sources for analytics for understanding of cyber security awareness.

The methodology adopted for this project is given in figure 3 and it consists of four stages:

- Phase1 – Determining the requirements of stakeholders
- Phase2 – Designing &developing the awareness program
- Phase3 – Conducting the awareness program
- Phase4 –Evaluating &revising

In the phase1 of this project the following tools have been used to capture the requirements of the stakeholders which is examining the present knowledge in the field of cyber security. The output of phase1 will help in developing the cyber security awareness material to be used in phase3 of this project.

- Surveys
- Questionaries'
- Social media
- Workshops



Phase 2 In this phase of the project, different contents that are needed to spread the awareness sessions are designed and developed. This includes trainings sessions, workshops, seminars, camping's and other contents such as games and videos. These contents will also be used during the conduction of the phase 3 of the project.

Phase 3Phase 3 is the actual conduction and implementation of the project study. Schools, organizations and societies will be identified to conduct the awareness sessions and spread the messages of cyber security awareness programs. From these phase, data are being gathered and collected for analyzation and result generation purposes.

Phase4. This phase is the final phase of the project wherein the results generated from phase 3 are being analyzed thoroughly and findings are being published using statistical tools such as SPSS in order to arrive to a concrete conclusion and determine the benefits of the project study for future works.

4. RESULTS & EVALUATION

Three sets of questionnaires were distributed among the parents, students and employees, each receiving different types of questions but has only one topic which is cyber security awareness. After getting permission from Office of Educational Supervision to let the public be part of my study, the respondents completed the questionnaires.

The three sets of questionnaires were completed by three different respondents and the results were being analyzed critically and were presented using a pie chart. The results are being studied well in order to determine in which area does these respondents need to be aware of in terms of cyber security awareness programs. The findings are also analyzed and discussed according to the sets of questionnaires given.

The sets of questionnaires include:

1.For parents

2.For employees

3.For kids/schoolchildren

Data Visualization has been used in analyzing the results in order to formulate the summary of the findings and since the results of the data gathering process has been presented using a graphical chart which is the pie chart.

Pre-Survey Results

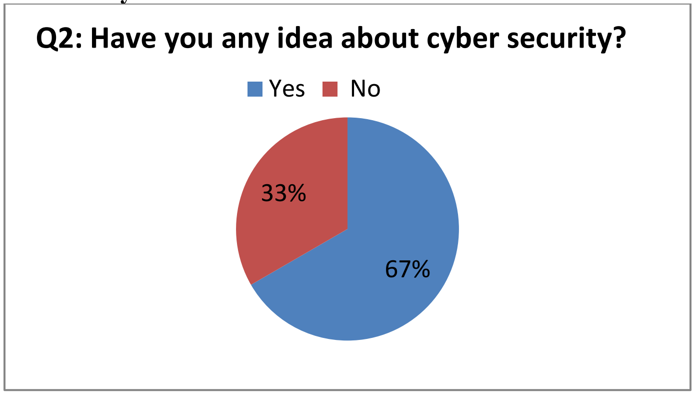


Figure 4. graph showing the percentage of employees having ideas about cyber security.

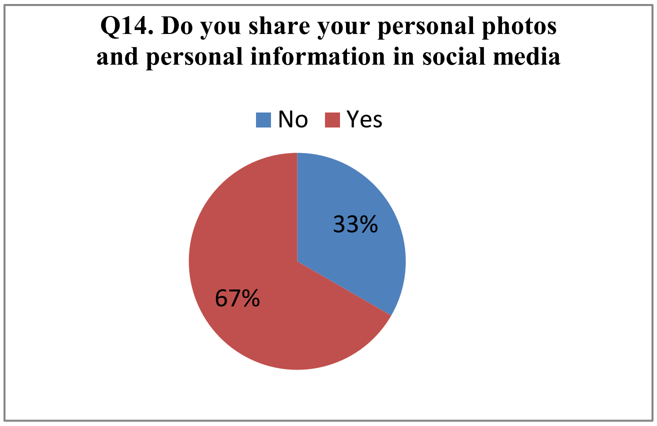


Figure 5. graph showing the results of question number 14 answered by schoolchildren

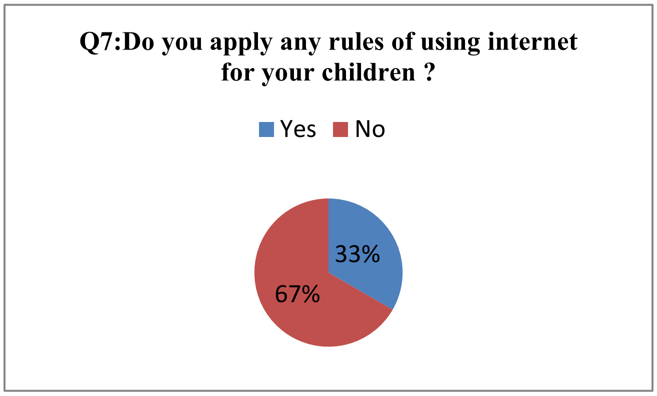


Figure 6. graph showing the result of question number 7 for parents.

Post-Survey Results

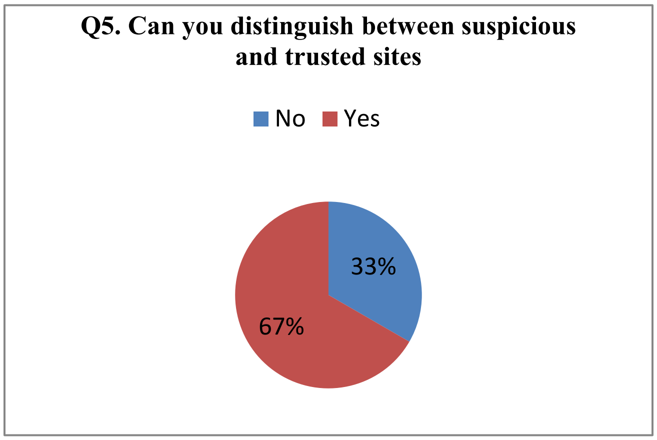


Figure 7. results derived during the post survey showing if the students can determine the difference between trusted and suspicious sites.

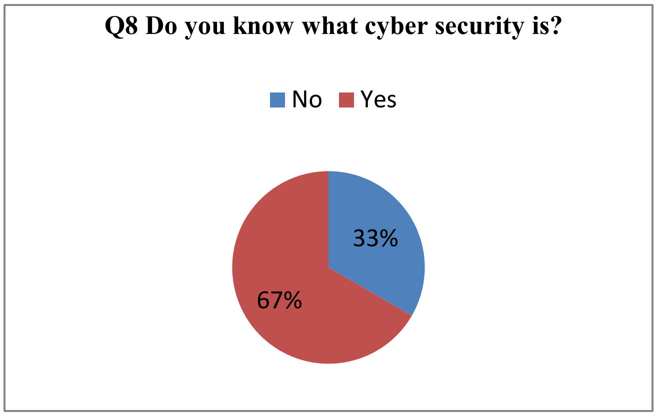


figure 8. graph showing the results of post survey from students about cyber security

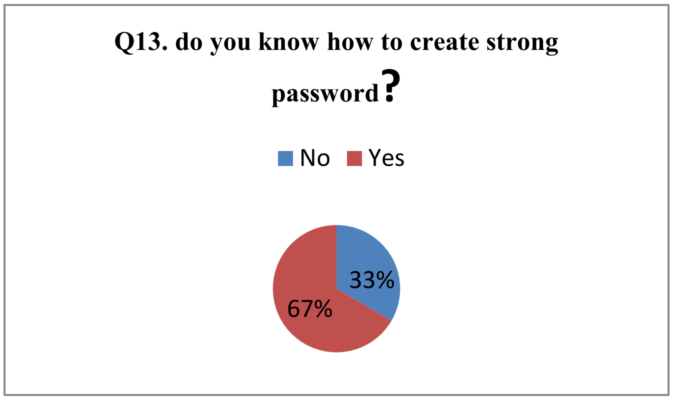


Figure 9. graph showing if each students knows how to create strong password during the post survey

5. CONCLUSION

As the world faces a millennium of continuous technological advancements, enhancements and improvements, the people become more and more dependent on its end products such as the cyber space or the Internet. Users are now becoming more engage on its applications and the comforts and benefits it gives to them.

Accessing the internet also means opening oneself to be a vulnerable and easy target of malicious attacks, threats and risks. Also new range of applications means new range of threats and risks arises. This study examined the effectiveness of conducting cyber security awareness programs to the public including employees, school children and parents using different program tools such as brochures, workshops, trainings and posters. The results and findings of the study reveals that although there are different methods of ensuring cyber security, the lack or limited knowledge and full understanding about its concept as well as unawareness of users is a very big hindrance in the effectiveness of this methods. As a result, malicious attacks and threats make their way to easily break in on the users' computers, systems, networks and devices causing damages and problems. this study will provide enough knowledge, better and clear understanding and full awareness about cyber space and cyber security is to conduct cyber security awareness programs using different awareness tools such as workshops, trainings, posters brochures and campaigns. This is so because in a world of continuous technological advancements and improvements everybody can be a target of malicious attacks, threats and risks that comes along with it and lack of awareness and knowledge about cyber security makes it a challenge for every user.

After a thorough analysis of the data gathered and the results gained, this project study highly recommends the inclusion of cyber security awareness programs in every aspect of life in order to be safe and protected from any malicious threats and risks that invades our cyberspace or technological devices.

6. REFERENCES

[1.] The National Institute of Standards and Technology U.S Department of Commerce

[2]. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[3.] Bulgurcu, B., Cavusoglu, H. and Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), pp.523-548.

[4]. Ben-Asher, N. and Gonzalez, C., 2015. Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, *48*, pp.51-61.

[5.] Cone, B.D., Irvine, C.E., Thompson, M.F. and Nguyen, T.D., 2007. A video game for cyber security training and awareness. computers & security, 26(1), pp.63-72.

[6.] Colwill, C., 2009. Human factors in information security: The insider threat–Who can you trust these days?. Information security technical report, 14(4), pp.186-196.

[7.] Franke, U. and Brynielsson, J., 2014. Cyber situational awareness–a systematic review of the literature. Computers & Security, 46, pp.18-31 .

[8.] Maqousi, Ali, Tatiana Balikhina, and Michael Mackay. "An effective method for information security awareness raising initiatives." International Journal of Computer Science & Information Technology 5.2 (2013): 63.

[9.] Zhang, Chen, and Janet J. Prichard. "AN EMPIRICAL STUDY OF CYBER SECURITY PERCEPTIONS, AWARENESS AND PRACTICE."

[10.] Kritzinger, Elmarie, and Sebastiaan H. von Solms. "Cyber security for home users: A new way of protection through awareness enforcement." Computers & Security 29.8 (2010): 840-847.

[11.] Castells, Manuel. The rise of the network society: The information age: Economy, society, and culture. Vol. 1. John Wiley & Sons, 2011.

[12.] Goyal, Mohit. "Ethics and Cyber Crime in India." International Journal of Engineering and Management Research 2 (2012): 2250-0758.

[13.] Carr, Jeffrey. Inside cyber warfare: Mapping the cyber underworld. " O'Reilly Media, Inc.", 2011.

[14.] Zhang, Yanping, et al. "A survey of cyber crimes." Security and Communication Networks 5.4 (2012): 422-437.

[15.] Dawson, Maurice, Jorja Wright, and Marwan Omar. "Mobile Devices: The Case for Cyber Security." New Threats and Countermeasures in Digital Crime and Cyber Terrorism (2015): 8.

[16.] Thomson, Kerry-Lynn, Rossouw von Solms, and Lynette Louw. "Cultivating an organizational information security culture." Computer Fraud & Security2006.10 (2006): 7-11.

[17.] Arachchilage, Nalin Asanka Gamagedara, and Steve Love. "Security awareness of computer users: A phishing threat avoidance perspective." Computers in Human Behavior 38 (2014): 304-312.

[18.] Peltier, Thomas R. Information Security Policies, Procedures, and Standards: guidelines for effective information security management. CRC Press, 2016.

[19]. Anderson, Ross J. Security engineering: a guide to building dependable distributed systems. John Wiley & Sons, 2010.

[20.] Newman, Robert C. Computer security: Protecting digital resources. Jones & Bartlett Publishers, 2009.