International Journal of Education and Science Research Review
E-ISSN 2348-6457
Volume-9, Issue-5 Sep - Oct – 2022
P-ISSN 2349-1817
www.ijesrr.org
Email- editor@ijesrr.org

TO STUDY MEASURE SUCCESS OF YOUR CYBER SECURITY AWARENESS AND TRAINING PROGRAM.

Rahul Saini
Research Scholar
Computer Science
CMJ University Meghalaya

Ajay Agarwal
Guide
Computer Science
CMJ University Meghalaya

ABSTRACT

Ineffective SETA systems may lead users to behave inappropriately, which can lead to legal ramifications, penalties, harm to their reputation, threats to national security, and even criminal activities. Executives in charge of information technology from four different companies in the Hampton Roads, Virginia area took part. Analysis of secondary data from SETA program materials (n = 31) and interviews with Organisation IT executives (n = 6), conducted by telephone and video conferencing were used to acquire the data. This study found that cyberattacks target small and medium-sized firms (SMEs) at a higher rate than large corporations (MEs). Perhaps the answer lies in the Swedish society's ongoing effort to foster a culture of information security. This might lead to a better grasp of security concerns, more education for the general public, and more active participation from home users in ensuring the safety about the information they collect.

keywords: Measure, Cyber, Security, Awareness, Training and Technology.

INTRODUCTION

Every piece of data that is stored, and sent is ever-increasing in today's information age. Every person and every community should be concerned about information security. It was hard to imagine a decade ago how much information society and individuals processed every day, and how much of an impact information technology had on people's daily lives now. Increased focus on information security is necessary for a development of this kind. Information technology is becoming something that the majority of us utilize on a regular basis, rather than just being a niche interest for techies. The rising number of scams, virus outbreaks, and hacking attacks highlights the growing dangers that society and people face due to their reliance on information technology.

Viruses and worms were the primary forms of security breaches in the early days of the Internet; they may display advertisements or messages on the screen but seldom physically damaged the machine or the data. On the other hand, there were very unusual instances when assaults may compromise data, such the Friday the 13th virus in the late 1980s, which aimed to delete all data on disc drives. With the passage of time, the attacks' potential to create issues grew. Dlamini, Eloff. J., & Eloff. M. (2009) found that security breaches had a significant detrimental effect on company reputation, profitability, and economic growth. Security breaches have far-reaching effects due to the linked nature of computer systems. According to Kumar, Mohan, and Holowczak (2008), a security compromise may lead to the deletion or corruption of personal information.

It is critical to emphasize the dangers that home users may face and create, according to Furnell (2005). Each user poses a risk to other users due to their careless actions. A person with a hacked computer, according to the author, might transmit the infection to other users online or even cause damage to organisations. People could endanger others if they don't have the necessary knowledge and awareness.

There is already written material about the topic of knowledge about information security and possible ways to increase end-user understanding. On the other hand, most of these studies have concentrated on information security awareness inside organisations and the measures made to increase the significance of this subject's awareness among workers. An integral part of any policy is the training and education of staff. for the protection of sensitive company data, together with education on the importance of being one of the primary concerns of the business. Both the Kriitzinger and Solms (2010) and the Talib, Clarke, and Furnell (2010) research stress the need of educating house users on the issue and providing them with the knowledge they need to make their homes safer. Among the little literature on the topic, only two studies— Both papers address the needs of home users. knowledge of information security risks. An example of a home user would be someone who uses their home computer to browse the Internet.

LITERATURE REVIEW

Borthwick and Hansen (2017) paper discussed on the present policy of OET and the National Educational Technology Plan with regard to the training of teachers in the United States. The article's central argument is that, in order to ensure that college instructors and students entering technologically advanced classrooms are adequately prepared to utilise technology in the classroom, there has to be a standardized set of expectations about students' technical competence.

Sincar (2021) Standards of digital citizenship behaviour among potential educators are examined in this research. Seventeen future educators who attended the University of Gaziantep's School of Education from 2009 to 2010 make up the sample. The study's data collecting and analysis processes were qualitative. According to the results, the majority of educators followed established standards for digital literacy and communication. Conversely, few educators modelled appropriate conduct in areas such as digital wellness, digital security, online etiquette, online commerce, rights and obligations, and digital law. As a result, Conclusions drawn from the research suggest that for digital citizenship be taught as an ancillary course during teacher training.

The study by Wilson (2021) on the structure of the curriculum for media and information literacy lays out the fundamental skills that educators should possess. To supplement the MIL curriculum, the framework includes nine mandatory courses, two optional modules, and three non-mandatory sections. Teachers and institutes of teacher education may modify the module's materials and activities to fit their own nations' needs. The curriculum framework includes media and information ethics as a significant piece of instruction.

As Genner (2017) points out in his essay "Socialisation as a Media Effect," younger generations are more likely to utilise digital media. Therefore, media literacy as not just a means to a goal, but also the goal itself should be adequately prioritised. To be media literate is to be able to utilise, comprehend, assess, and produce media. In addition, the paper highlights the significance of media literacy for proper socialisation, the dangers of problems with information overload, digital diversions in an ever-changing media environment and the "datafication" of society

Ala-Mukta (2021) As people's tools and behaviours evolve in their profession, education, and leisure time, it is necessary for them to achieve digital competence, according to the research report by. Consequently, there should be two tiers to digital competence development guidelines: 1) a conceptual level for identifying the core areas of digital competence, and 2) a level for more practical learning and

evaluation activities to be completed using current tools and protocols. The conceptual framework may be kept constant while being operationalized to adapt to group-specific situations on a regular basis. The conceptual level is the primary emphasis of this article.

RESEARCH METHODOLOGY

Following an overview of the research's credibility and validity, concerns about ethics, and final verdict, the study's methodology came under fire. The application of an interpretative philosophical framework in the study of information systems is becoming more popular among scholars (Myers and Avison, 2002). The social phenomena known as "the researcher seeks to establish the meaning of a phenomenon from the view of participants" is an example of an interpretive philosophical assumption that aims to explain human interactions and experiences. We may learn about analysis of the IT participants' experiences and knowledge to determine the decision-making processes underlying the security measures employed by six different SMEs and their operating environments. A detailed introduction to data collection is provided in the following portion. Qualitative research methods include using observation, focus groups, and interviews to gather data (Saunders et al., 2018). Qualitative research approaches, such as interviews, let researchers zero in on specific questions about the whys and hows of policy and strategy implementation, which quantitative methods miss (Lancaster, 2017). IT leaders in the hospitality industry as they applied SETA strategies to secure their organizations' information systems and data.

DATA ANALYSIS

Security education and best practices for protecting sensitive information

Results pertaining to the theoretical parts of information security awareness and baseline security practices will be provided in this section.

One awareness-related question in the data collection self-completion form requested respondents to define words pertaining to information security. The stated security word was used to gauge the respondents' perception of their own knowledge level. The fifth question asked how well you understood topics connected to information security. Trojan horse, worm, adware, spyware, phishing, hacker, firewall, and identity theft were among the phrases mentioned. Extremely low, medium, high, and very high were the possible rankings for the respondent's level of knowledge. The analytical approach did not include respondents who selected "average," but rather combined the extremely low and very high responses into one variable, low or high.

Table 1 displays the percentage of respondents that scored low or high on the security terminology quiz. It also shows how trained home users vary from unskilled ones. In contrast to trained respondents, a larger proportion of untrained respondents have reported a lack of familiarity with the defined security terminology, as seen in the table.

Table 1 - Distribution of groups' knowledge of security terminology

	Low		High	
Security Terms	**Trained**	**Untrained**	**Trained**	**Untrained**
Virus	3 (2,6%)	15 (13,1%)	65 (57%)	31 (27,2%)
Adware	22 (17,3%)	45 (35,4%)	46 (36,3%)	14 (11%)
Spyware	21 (15,9%)	44 (33,3%)	50 (37,9%)	17 (12,9%)
Phishing	18 (13,1%)	55 (40,1%)	52 (37,9%)	12 (8,7%)
Hacker	5 (4,3%)	22 (19,1%)	59 (51,3%)	29 (25,2%)

Firewall	5 (4%)	20 (16%)	63 (50,4%)	37 (29,6%)
Identity theft	11 (8,3%)	40 (30,5%)	57 (43,5%)	23 (17,5%)
Worm	20 (15,5%)	52 (40,3%)	46 (35,6%)	11 (8,5%)
Trojan Horse	6 (4,8%)	35 (28,2%)	59 (47,6%)	24 (19,3%)

We also asked them to judge how well they understood the various security measures and how much they thought they knew about them. Question 8 asked participants to rate their level of familiarity with various information technology security protocols. The many security procedures that were mentioned were firewalls, anti-spyware, anti-spam, software upgrades, safe password practices, backups, and mobile device protection. Extremely low, medium, high, and very high were the possible rankings for the respondent's level of knowledge. The analytical approach, however, did not include the respondents who selected "average" as their response. In addition, the very low and very high response groups were combined into low and high, respectively.

Table 2 shows the percentage of respondents who scored low or high on the security knowledge quiz. Also included are the distinctions between home users who have received training and those who have not. While trained respondents reported greater levels of awareness, the majority of untrained respondents reported lower levels, as seen in the table. In this table, the percentages indicate what proportion of the total number of responders each category represents.

Table 2 - Distribution of group awareness of security measures

	Low		**High**	
Security Measures	**Trained**	**Untrained**	**Trained**	**Untrained**
Anti-virus	6 (4,9%)	18 (14,8%)	66 (54,1%)	32 (26,2%)
Anti-spyware	19 (14,7%)	45 (34,9%)	50 (38,8%)	15 (11,6%)
Anti-spam	16 (15,2%)	41 (39%)	29 (27,6%)	19 (18,1%)
Firewall	6 (4,9%)	23 (18,7%)	63 (51,2%)	31 (25,2%)
Software updates	3 (2,4%)	19 (15,3%)	69 (55,6%)	33 (26,6%)
Secure password practices	3 (2,4%)	16 (12,6%)	69 (54,3%)	39 (31%)
Backups	7 (5,6%)	26 (12,9%)	64 (51,6%)	27 (22%)
Securing mobile devices	18 (17,1%)	29 (27,6%)	39 (37,1%)	19 (18,1%)

Observations about data protection

What follows is a presentation of the findings as they pertain to the theoretical parts of information security behaviour.

In addition, information security-related behavioural characteristics might be measured with the use of

the self-completion questionnaire. In that part of the survey, people were asked to rate their level of adherence to various home security measures, among other behavior-related items. Home security measures were listed, and respondents were asked to indicate whether they employed them. In question nine, we asked if anybody makes use of the information technology security best practices listed below. Security precautions on mobile devices, software updates, safe password practices, firewalls, anti-spyware, anti-spam, and antivirus software were all mentioned. Yes, no, and "I don't know" were the three options available to the responders. Nevertheless, the "No" and "I don't know" options were combined since being unaware of whether or not you have implemented a certain security precaution still suggests engaging in unsafe security behaviour, which is obviously associated with bad actions. Consequently, this group was included with others that have claimed not to use the particular security measure.

Those who responded "yes" are represented as applying the security measures in table 3, whereas those who replied "no" or "I don't know" are shown as not applying. As an added bonus, we also show you how trained home users vary from untrained ones. Table 1 shows that there is a significant difference in awareness between trained and untrained home users, but no such difference in responses. To better understand the distinctions between the two groups of home users, the percentages given in this table reflect the total number of respondents in each category: apply and don't apply.

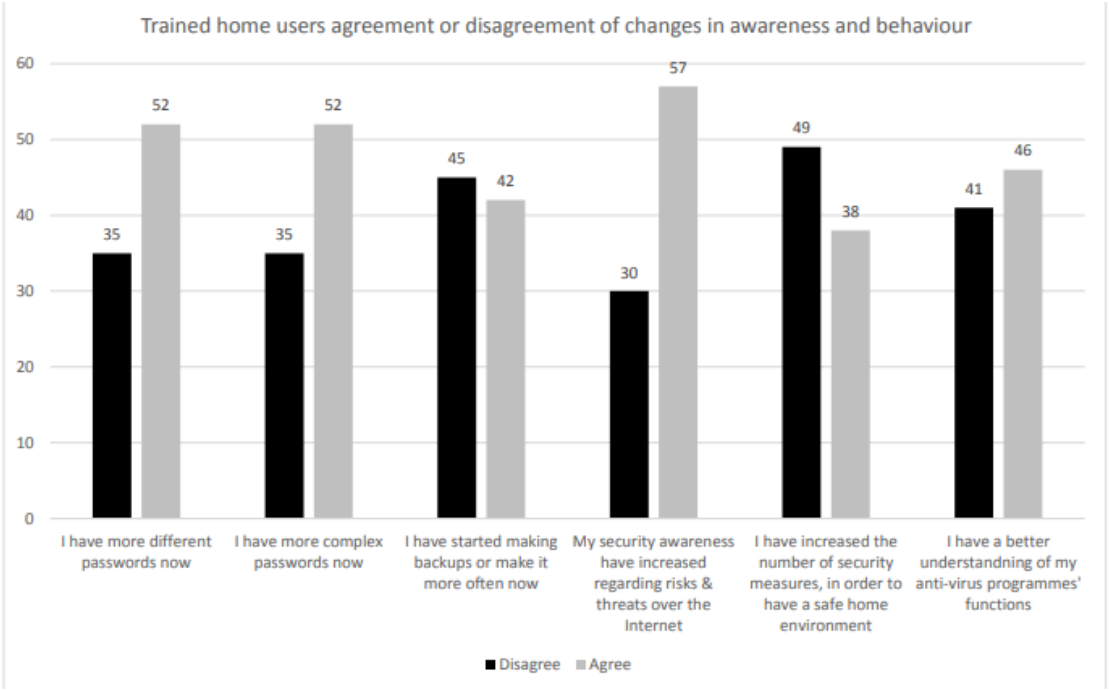
Behaviour and distribution of the groupings are shown in Table 3.

	Apply		**Don't apply**	
Security Measures	**Trained**	**Untrained**	**Trained**	**Untrained**
Anti-virus	69 (56%)	54 (43,9%)	18 (46,1%)	21 (53,8%)
Anti-spyware	43 (63,2%)	25 (36,7%)	44 (46,8%)	50 (53,2%)
Anti-spam	43 (58,9%)	30 (41%)	44 (49,4%)	45 (50,5%)
Firewall	77 (57,4%)	57 (42,5%)	10 (35,7%)	18 (64,2%)
Software updates	84 (57,1%)	63 (42,8%)	3 (20%)	12 (80%)
Secure password practices	61 (55,9%)	48 (44%)	26 (49%)	27 (50,9%)
Backups	61 (58%)	44 (41,9%)	26 (45,6%)	31 (54,3%)
Securing mobile devices	47 (55,9%)	37 (44%)	40 (51,2%)	38 (48,7%)

Additionally, we questioned those respondents who were also considered trained home users a separate question. Regarding their newfound information security vigilance and precautions, individuals were asked to indicate how much they agreed or disagreed with several assertions. Question 20 asked respondents to rate how much they agreed with statements on the ways in which their security awareness and behaviour had been impacted by their education in the areas of information security, informatics, or IT, both during and after completion of the course. Respondents might score their agreement of using the following options: completely disagree, somewhat disagree, somewhat agree, and agree.

See figure 1 for a breakdown of the trained respondents' opinions on the assertions made about their improved security awareness and conduct, including whether they agree or disagree. You can sum up the

categories that disagree and agree by looking at which one they lean towards. According to the graphic, there is a large discrepancy in the answers given by the trained home users to certain claims, while the discrepancy is low for other claims.



The perspective of trained responders about their altered consciousness and conduct is shown in Figure 1.

More sophisticated statistical analysis was required to infer the hypotheses, which allowed for the formulation of more robust scientific claims. You may see the analytical findings that were necessary to accept or reject the hypotheses to a certain extent in this chapter.

Making ensuring that the Likert scale items were extremely reliable—checking for high inter-item consistency—was a prerequisite to attempting to find a link between the many factors in the questions on the scale. In order to look at this specific need, Cronbach's Alpha was applied. The test was administered using three separate Likert scale questions, and the results are shown below.

CONCLUSIONS

With the overarching goal of making them less susceptible, the theoretical framework was developed with an emphasis on IT workers' decision-making processes about cyber security. technology is the tool for tackling cyber space. Second, the traits of IT professionals play a role in cyber security decisions. Third, organizational tasks address cyber security in three stages, as mentioned above. In support of this claim, consider that only 2 out of 6 IT experts met all requirements. Among the remaining IT experts, technical knowledge was at the highest degree of awareness This research did find some other causes, however. To begin, only two of the six companies completely adhere to all three standards of cyber security, and those two companies even hire people with formal training in cyber defence. Furthermore, these two workers are solely devoted to cyber security and have no other responsibilities.

REFERENCES

1. Arlene C. Borthwick & Randall Hansen (2017) Digital Literacy in Teacher Education: Are Teacher Educators Competent? Journal of Digital Learning in Teacher Education, 33(2), 46-48.

2. Ala-Mukta,K(2021)*Mapping Digital Competence*, Luxemburorg, Publication office of the European Union

3. Alwi, N. H. M., & Fan, I. S. (2020). E-learning and Information Security Management. International Journal of Digital Society (IJDS), 1(2), 148– 156.

4. Anastasiades, P. S., & Vitalaki, E. (2021). Promoting Internet Safety in Greek Primary Schools: The Teacher's Role. Educational Technology & Society, 14 (2), 71–80.

5. Andrea, K. (2021). Digital Literacy in Education. UNESCO IITE. Retrieved August 21, 2019, from https://iite.unesco.org/publications/3214688/

6. Arafat, Y., & Ibrahim, M. I. M. (2018). The Use of Measurements and Health Behavioral Models to Improve Medication Adherence. In M. I. M. Ibrahim, A. I. Wertheimer, Z. U. D. Babar (Eds.), Social and administrative aspects of pharmacy in low-and middle-income countries (pp. 53–69). Academic Press. https://doi.org/10.1016/B978-0-12-811228-1.00004-2

7. Arlene C. Borthwick & Randall Hansen (2017) Digital Literacy in Teacher Education: Are Teacher Educators Competent? Journal of Digital Learning in Teacher Education, 33(2), 46-48, https://doi.org/10.1080/21532974.2017.1291249

8. Arora, A., & Mendhekar, A. (2017) Information Security Education, Training and Awareness Initiatives by Government of India. International Journal of Research in Economics and Social Sciences (IJRESS), 7(5), 145–155.

9. Bairagi, V. & Munot, M.V., (2019) Research Methodology: A Practical and Scientific Approach, New York, Taylor & Francis.

10. Barbosa, A., O'Neill, B., Ponte, C., Simões, J.A., and Jereissati, T. (2023). Risks and safety on the internet: Comparing Brazilian and European children. LSE, London: EU Kids Online.

11. Barik, N., & Karforma, S. (2022). Risks and Remedies in E-Learning System. International Journal of Network Security & Its Applications (IJNSA), 4(1), 51–59.

12. Barros, M. J. Z. De, & Lazarek, H. (2018) A Cyber Safety Model for Schools in Mozambique. ICISSP, 251–258. https://doi.org/10.5220/0006573802510258

13. Bele, J. L., Dimc, M., Rozman, D., & Jemec, A. S. (2023, November 30). Raising Awareness of Cybercrime--The Use of Education as a Means of Prevention and Protection. Proceedings of the 10th International Conference Mobile, Spain, 281–284,

14. Bell J. (2020). Doing your Research Project: a Guide for First-Time Researchers in Education Health and Social Science (5th ed.). McGraw-Hill Open University Press. Retrieved August 30, 2019, from http://www.dawsonera.com/abstract/9780335239146.

15. Bhandari, P. (2021, August 13). A step-by-step guide to data collection. Retrieved August 23 ,2021 https://www.scribbr.com/methodology/data-collection/