European Journal of Education Studies
ISSN: 2501 - 1111
ISSN-L: 2501 - 1111
Available on-line at: www.oapub.org/edu

DOI: 10.46827/ejes.v9i10.4501 Volume 9 │ Issue 10 │ 2022

IMPROVING DIGITAL SECURITY AND PRIVACY OF STUDENTS IN COLLEGES OF EDUCATION: AN ATTITUDINAL CHANGE FRAMEWORK BASED ON COMPETENCE LEARNING MATRIX

Azaabi Cletus[i]
St. John Boscos College of Education,
Navrongo, Ghana

Abstract:

The information revolution is affecting every aspect of society including education resulting in a concept known as digital learning or e-learning. One problem of digital learning environments and tools is the security and privacy of the learners. How to ensure the security and privacy of digital learners remains a major challenge leading to exposure among naive students. The objective of the study was to explore digital security and privacy culture among students and to propose a novel framework to enhance the security and privacy culture of students using a framework based on the competence learning theory. The Design Science Research (DSR) was adopted as a research paradigm with quantitative and qualitative data gathered from the implementation of the framework. 300 students from a college of education were purposively sampled for the study. A WhatsApp message was sent to the student requesting their confidential information under pretexting and impersonation to assess how security and privacy conscious they were. A framework was developed and implemented based on the theory of competence learning. The results showed high levels of vulnerabilities among students at 67.67% before the Implementation of the Framework in Round 1. This vulnerability reduced to 1.67% in after the implementation of the framework in Round 2 and further reduced to 0% in Round 3. The paper concluded that the lack of security and privacy awareness of the students made them Unconsciously Incompetent (UI). Exposure to the vulnerability made them consciously incompetent (CI), whiles further rounds of exposures led them to be consciously competent (CC). further exposure will eventually result in unconsciously competent (UC) as students become resistant and or immune to security and privacy attacks. The implication of this study is that, as more students converge in the digital space, the need to build their immunity and resistance against cyber-attacks is critical to avoid exposure. Learning to be security conscious should be consistent and routine to ensure that students have renewed behavior changes to become resistant and immune to online attacks.

[i] Correspondence: email cleinhim@yahoo.com

Copyright © The Author(s). All Rights Reserved.

Keywords: digital space, online learning, e-learning, competence model, digital security

1. Introduction

The words like 'digital', 'security' and 'privacy' are infiltrating everything; no part of society is exempted including students. Globally, students are adopting and integrating online content as supplementary or main material for learning such as Google, Microsoft and Apple Products to learn (Singer, 2017, Saidu et al. 2018, Al-hamadani, 2017). However, these technologies come with their attendant problem of cybersecurity and privacy issues.

According to Singer (2017), many schools in the USA are vigorously integrating technology such as Microsoft, Apple, Google and other platforms. These tools used in their classroom environments by teachers have little or no training on the implication of privacy and security such as how to monitor, the data gathered by device owners and how the schools use the gathered data (Smith, 2016; Giabrome, 2015). In addition, educators pay less attention to the digital privacy and security of the learners they are teaching (Hewell, 2018). This results in students having poor appreciation of the digital space(platforms) they are studying.

A lot of work is done by the developers and owners of these programs and platforms to ensure the confidentiality, integrity and availability of the information resources but such technical controls alone are not adequate to provide the needed security and preserve the privacy of digital students (Miguel et al., 2014, Seudu et al., 2015). According to Halawa, Ripeanu and Konsfantin (2020), online services are an integral part of our personal and professional lives. Thus, the personal information/ credential of the member is online and these attributes are attractive commodities for cybercriminals. Consequently, making them targets for cyber-attacks using unconventional attack methods such as social engineering, which targets the user instead of the technology (Alderwoods or Skinner, 2020). They indicated that social engineering is the use of psychology to manipulate either personally or in a virtual mode that influences a person leading to the disclosure of confidential information such as PINs, passwords and other personally identifiable information (PII). Thus, to ensure optimum security and privacy culture of digital learners, there is a need for a solution targeting the user of the information who is the target of this attack in the digital space (Albladi & Weir, 2020).

In recent times, the use of digital technology in teaching and learning and security has been explored. Kumar et al. (2019) studied privacy and security consideration for digital technology use in elementary schools and concluded that the use of technology has become an integral part of learning at the elementary level; educators are worried about the digital security and privacy of learners; but less effort at teaching digital security and privacy of learners. Again, it is common knowledge that tablets, connected toys, netbooks and other devices have become the common everyday tools of digital students (Mazmanian & Lannette, 2017). They concede that the security implications of these tools are dire as learners are exposed to the vagaries of cyberspace. Kumae et al., (2017) conducted a study and concluded that learners have little knowledge about privacy and security concerns and they need more and further training. They also suggested parental, school level and policy-level support for the improvement of digital security for learners.

Therefore, as the entire educational system migrates its activities online; more students are converging in the digital space with its danger of compromising of security and privacy, knowing the level of vulnerability of the learners would invariably lead to the development of efficient and effective tools to build the resistance, immunity and reflective behavior of students against digital attacks.

Thus, in this paper, the researcher explored the level of vulnerability of learners and proposed a model that assists in improving the digital security and privacy culture of digital learners.

To achieve this, we asked this broad research question "How can the security and privacy culture of digital learners be improved?" This was broken down into specific research questions as:

1) What is the level of vulnerability of learners to digital/online attacks?
2) How can the security and privacy culture of learners be ensured in the digital environment using an innovative framework?
3) How efficient is the model in improving the security and privacy culture of learners?

The achievement of these objectives contributed to knowledge in the following ways:

- Highlighted the level of student vulnerability to digital attacks; hence, sharing rich and practical insights into students' vulnerability studies in particular and cybersecurity in general.
- Proposed an approach (SSAM) for improving the digital security and privacy culture of students; thus, contributing to the theory and methodology of the study.
- The proposed model with its evaluated results reduced the vulnerability of digital learners by about 19 percentage points.

2. Theoretical Framework

2.1. Conscious Competency Model and Digital Learning Change

In learning, being able to understand your level of competency in an area or topic can boost the potential for effectiveness and efficiency. This is what the concept of the Competency Learning Model or theory is. It describes how a learner learns a skill from the stage of ignorance to full knowledge and awareness as explained by Kongsvit (2021). The approach shows the sequence of stages an individual follows from the time of unconsciousness to competency. There are four phases:

- Unconscious Incompetence,
- Conscious Incompetence,

- Conscious Competency, and
- Unconscious Competency (Chapman, 2019).

Figure 1 shows the competence matrix.

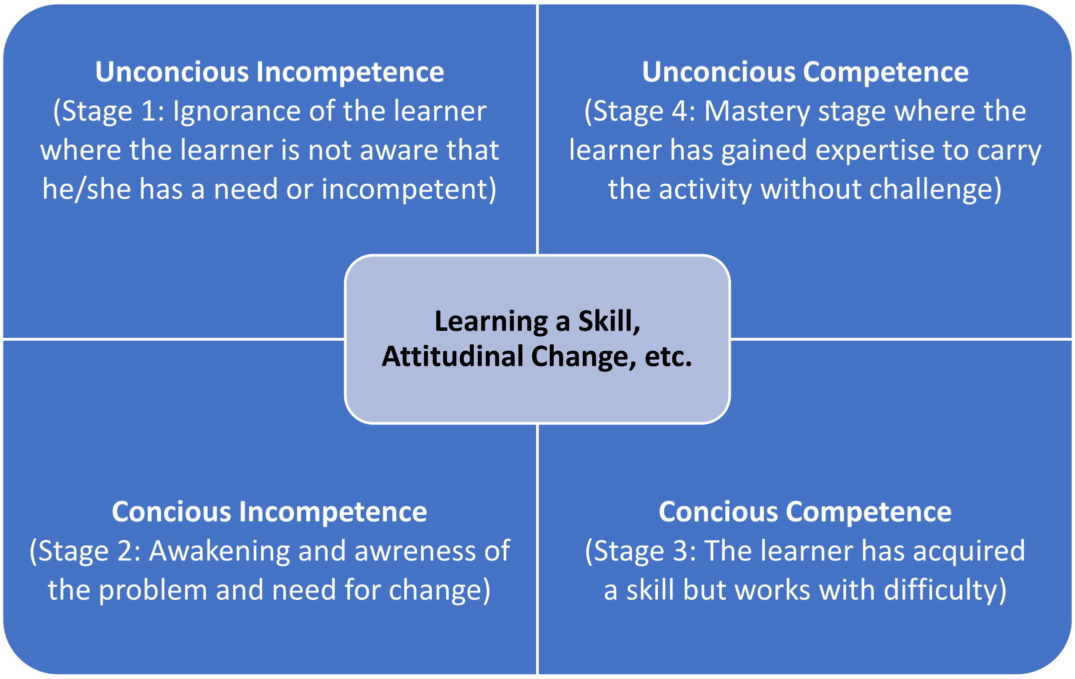
Unconcious Incompetence
(Stage 1: Ignorance of the learner where the learner is not aware that he/she has a need or incompetent)
Unconcious Competence
(Stage 4: Mastery stage where the learner has gained expertise to carry the activity without challenge)
Learning a Skill, Attitudinal Change, etc.
Concious Incompetence
(Stage 2: Awakening and awreness of the problem and need for change)
Concious Competence
(Stage 3: The learner has acquired a skill but works with difficulty)

Figure 1: The Competence Learning Matrix

As shown in Figure 1, the model starts with stage 1 where the learner is Unconsciously Incompetent (UI); i.e. the person is ignorant of the existence of the problem. This is where every learner starts. Sometimes, learners deny the existence of a lack of skill or a problem. (Manthey & Fitch, 2012). Creation of awareness is always required at this stage to create the need and desire to want to learn or change attitude as stated by Kongsvit (2021).

Conscious Incompetent (CI): At this stage, the person is aware of the problem, awoken, sees the need for change or to learn and commits to learning or changing the behavior or attitude.

Conscious Competent (CC): here the learner has made effort, learned the skill, and has gained some appreciable level of mastery. However, at this stage, he does the activity with some level of carefulness and consciousness.

Unconscious Competent (UC): At this stage, the learner has become a master of the trade (Skill, attitude) and can perform the action unconsciously without thinking. It is the level of mastery. Continuous use and practice over time lead to perfection in the skill or art.

Following this theory, we proposed a model for improving the privacy and security of digital learners and used the model to evaluate the performance of the learners. The next section describes the methodology of the study.

3. Materials and Methods

The study was about improving the digital security and privacy culture of students in Colleges of Education (COEs) using a model based on the competence learning theory and reflective behavioral theory.

The DSR approach or the Constructivist approach was adopted for this study. DSR is a research paradigm where novel artefacts are produced as solutions to identified real-world problem (Sonneberg et al., 2014; Venabel, 2016). Consequently, since the aim of the researcher was to explore and propose a novel model for improving privacy and security culture among learners, the most appropriate approach was the DSR. This is because the approach led to the development of an artefact of importance that solved a societal problem. This section describes the methodological procedure followed in solving the problem as detailed in the proceeding sections and subsections.

3.1 Population and Sampling

The universe of discourse for this study was all level 300 students who were out of the campus doing their out-program. However, the population that met the criteria were those with smartphones. Students who registered and were present in the WhatsApp group deemed to meet the criteria for selection. Thus, the students were purposively sampled which is one of the non-probabilistic methods.

3.2 Ethical Clearance

As a study involving humans and especially their privacy, there was the need to obtain clearance. This is relevant because the consent of the participants is of the essence since the study may infringe upon their privacy. To this end, we obtained clearance from the administrator of the group who was the only person aware of the study. In addition, we only counted the responses to get the tally and immediately delete the message so that, the details can and were not used for anything else apart from the purpose for which it was collected.

3.3 Data Collection

To collect data for analysis, the researcher impersonated a finance officer and sent a scam message onto the platform the students requesting confidential information for the processing of students' allowances.

The responses of the students were gathered, analyzed based on those who responded by providing their details, those who abstained and those who read the message and refused to respond by providing their details.

After the data was gathered, the students were debriefed and the implication of their actions relative to their privacy and security in the digital space or medium.

After a six-week period, after the student returned from their study, security awareness of online risk following the model was conducted. A similar scam message(2) with different content were this time administered to the same students this time with a link for them to sign in to watch their continuous assessment results. The results of this were gathered and analyzed. The level of vulnerability of the students in the experiments were compared. The architecture of the proposed system is shown in Figure 2.

3.4. The Proposed Framework and Description

The model called Student Security Awareness Framework (SSAF) was developed for the study as shown in the Figure 2 below:

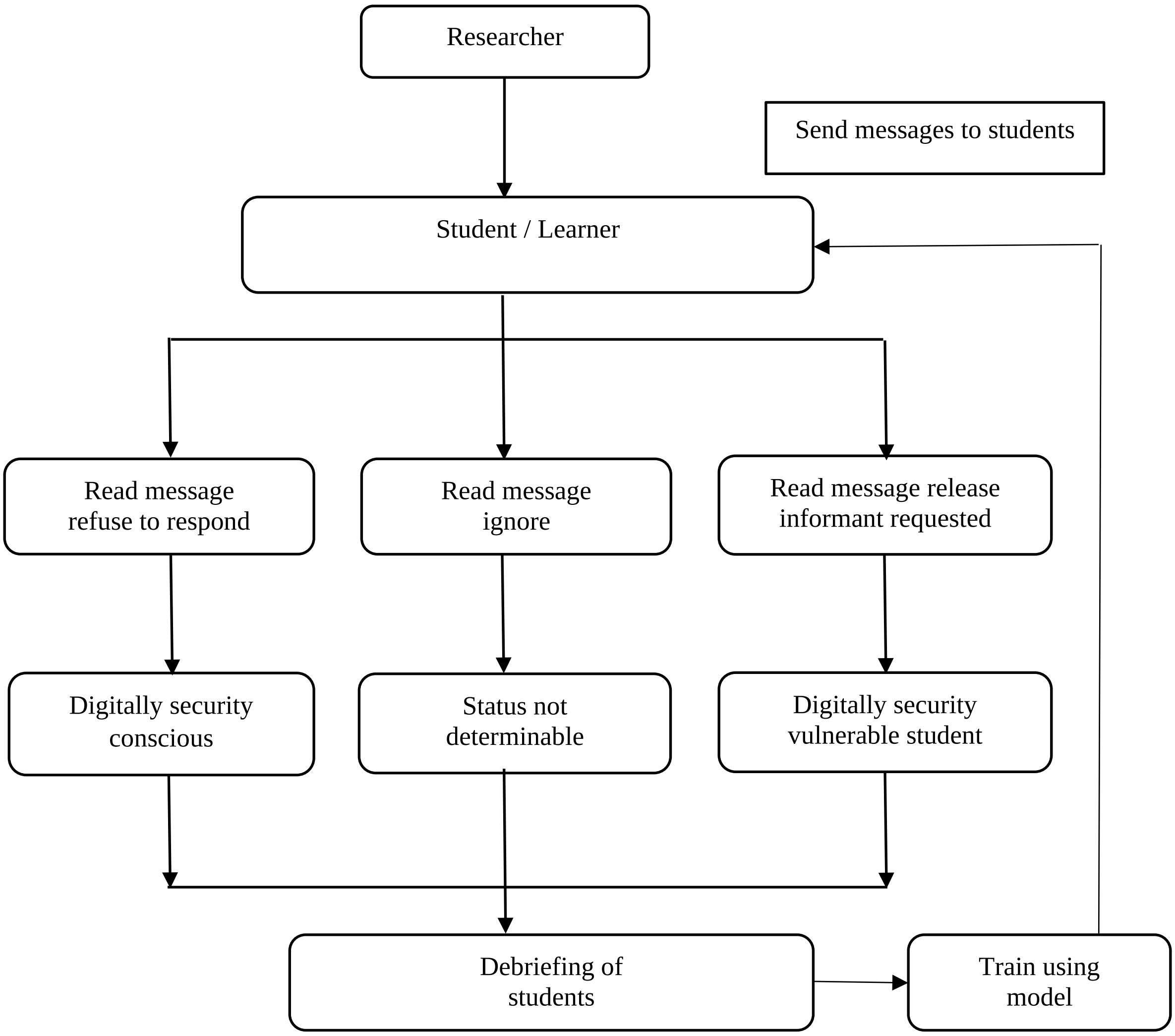
Researcher
Send messages to students
Student / Learner
Read message refuse to respond
Read message ignore
Read message release informant requested
Digitally security conscious
Status not determinable
Digitally security vulnerable student
Debriefing of students
Train using model

Figure 2: SSAF for Improving Security and Privacy of Students

3.4.1. How the Proposed Framework Works

The researcher impersonates and sends a message to participants (students). Students react in three ways to the message:

- Read and refuse to provide the requested information (assumed to be security and privacy-conscious);
- Ignore message/not delivered (assumed to be indeterminate);

- Read and provide the requested confidential data (assumed to be security and privacy susceptible).

After the first round, the students were debriefed and told the implication of their reaction to the message following the framework. The experiment is repeated after the first round an interval of 3-weeks. The result of the reactions to these messages can be analyzed to determine vulnerable users.

3.4.2 Implementation of the Framework

The researcher crafted an appealing scam text message and send it via WhatsApp to students (participants) such that the message appears real and urgent by adding deadlines.

When a student receives the message, it will be indicated that the said student has seen the message by a double check mark or by using the settings to check whether the recipient has seen and read the message. The participant has three options: Read the message and refuse to provide the right information requested – which suggests the student is online security conscious. Read the message and ignore it – indeterminate. Read the message and respond by providing the confidential informant requested – online security is unconscious and therefore vulnerable to exploitation. Based on the outcome, all students were debriefed about the implications of their actions and how that could exploit their privacy and security leading to exposure and breach of confidentiality, integrity and availability goals.

After the 3-week interval, a second and third similar scam mail was sent to the students and their responses to these new emails were evaluated based on their reactions. This was done to observe whether there is a change in behavior after the initial exposure The results of the respondent in Round 1, Round 2 and Round 3 of the experiment were analyzed using quantitative and qualitative data obtained from their reactions.

3.5 Data Analysis

The data gathered from the responses of the participants were analyzed using descriptive statistics, and inferential and qualitative formats.

4. Results of the Study

The study aimed at improving the security and privacy of digital students by evaluating the participants' susceptibility to online requests for private and confidential information. Based on the outcome, we proposed and implemented SSAF for improving the digital privacy of learners in COEs. This section presents the results of the study based on the research questions using graphs, tables, diagrams and illustrations.

4.1. Biodata of Respondents

In all, there were 300 subjects for the study. Out of this number, 168 of the respondents were male representing 56%, whiles 132 of the respondents were females and constituted

44% of the population of the study. This is consistent with the entire student population as there are more males than females as depicted in Figure 3.

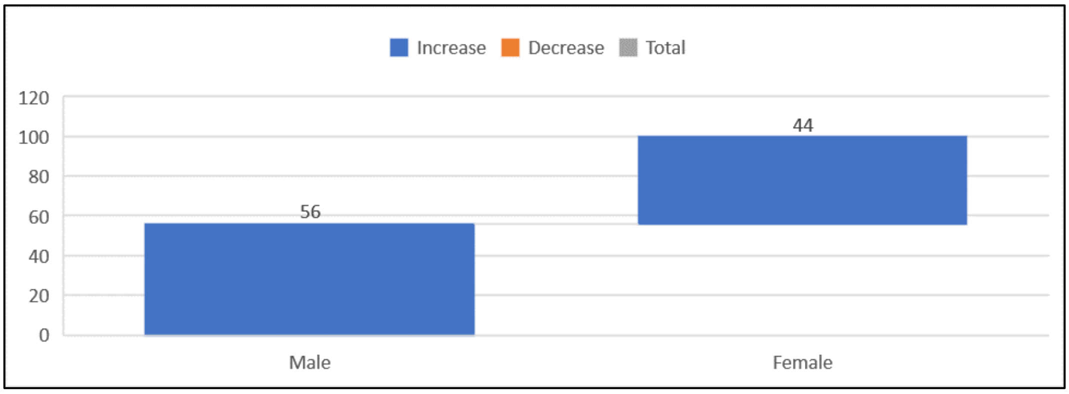

Figure 3: Participants by Gender

Regarding the students' classification by course, data suggest that there were more students from the general class compared to the others; science/maths, ICT and Technical students respectively. This statistic is consistent with the admission of students, as the institution seems to get more students applying from the general side more than the other courses. This result is shown in Figure 4.

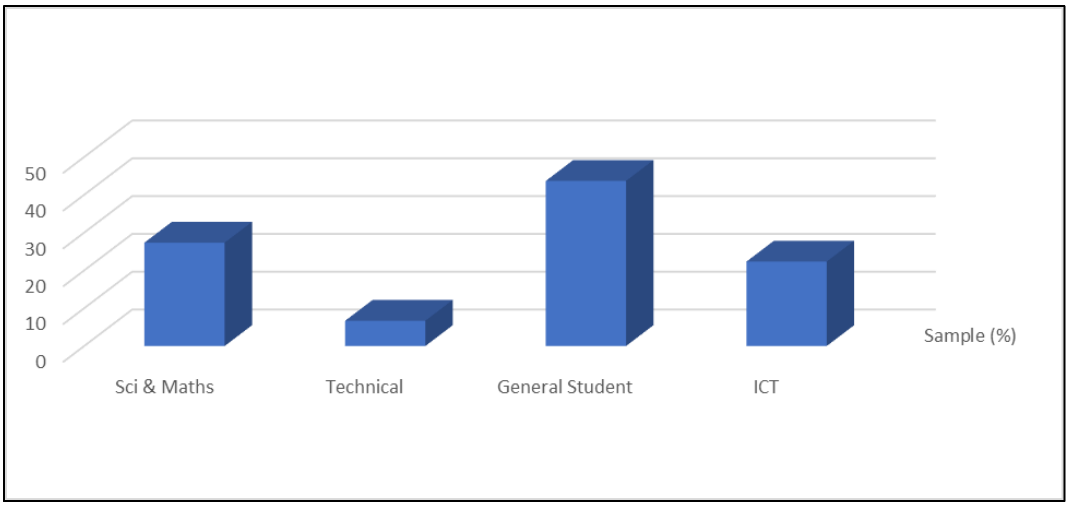

Figure 4: Participants by Courses

4.2. Vulnerability of Learners to Digital Attacks

To measure how vulnerable the students are to digital attacks, an experimental attack was conducted on the participants. They were sent a scam message and requested confidential information using pretexts and impersonation. Respondents were to ignore the message after reading, disclose the requested information or abstain after reading the message. We administered the exercise in three rounds. In Round 1, the exercise was administered without the framework, i.e., before the framework. In Round 2 and 3, the SDSAF was followed and the experiment was repeated using different scam mails. As depicted in Figure 5, 67.67% of the respondents disclosed their information before the use of the framework (Round 1); this was reduced to 1.67% in Round 2 and further reduced to 0% in Round 3. For those who abstained, 9% abstained in Round 1 before framework use, reduced to 7.33% and further reduced to 2.33% in round 3. Those who refused to disclose their information were 23.33%, which improved to 91% in Round 2 and further improved to 97.67. As indicated, the resistance of the participants to the scam improved consistently after the use of the framework.

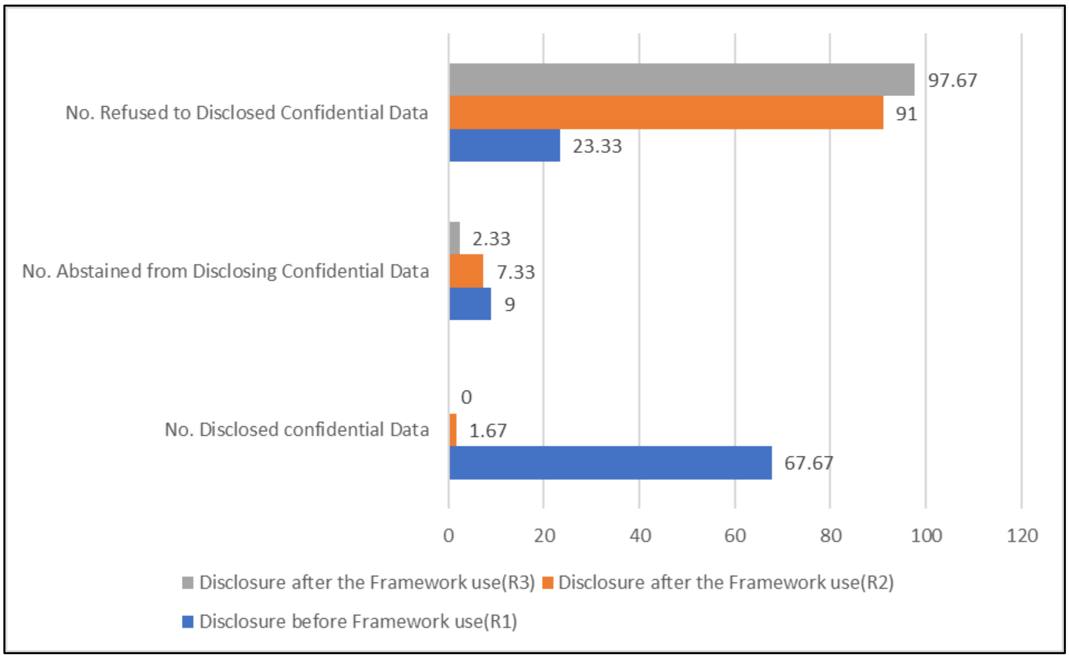

Figure 5: Disclosure of Confidential Data in Round 1, 2, 3

Regarding susceptibility to online attacks by gender, the result shows a slightly higher number of females than males. This is depicted in Table 1 below.

Table 1: Analysis of Vulnerability by Gender in Round 1

Gender	No. of students	Percentage (%)
Male	96	47.29
Female	107	52.71
Total	203	100

The data from the second experiment, however, showed that no female was a victim after the training with all 5 vulnerable users in this study being males as indicated in Table 2.

Table 2: Analysis of Vulnerability by Gender in Round 2

Gender	No. of students	Percentage (%)
Male	5	100
Female	0	0.00
Total	5	100

In Round 3 of the experiment, there was no disclosure of sensitive information by respondents.

To measure vulnerability according to courses studied by students, we analyzed the results according to the course studied by respondents. The result of this is as depicted in Table 3 below.

Table 3: Analysis of Vulnerability by Courses Before and After Use of Model

Course	Before the Model Use	After the Model Use
Science/Maths	70 (85.37%)	2 (40%)
Technical	16 (80.00%)	0 (0%)
General	93 (70.99%)	3 (60%)
ICT	24 (35.82%)	0 (0%)
Total of students	203 (100%)	100

4.3. Qualitative Analysis of the Responses

Some of the students responded by giving the following statements as depicted in table 6. Their questions and comments suggest some level of knowledge of online attacks. However, the numbers were very insignificant (only 3 respondents):

"why do you need my past word for?".

"this for be 419."

"I day come school come provide the information."

Figure 5: Qualitative Responses of Students

5. Discussion

The study was conducted to ascertain the level of vulnerability of students in the digital space and to propose a model for improving the security and privacy of students following a phenomenological approach by exposing students to the experience of digital attacks and measuring their vulnerability before and after the use of the model.

5.1. Susceptibility of Learners to Digital Attacks

Our findings show that 67.67% of the students are susceptible to security and privacy attacks with relatively more females than males at 52.71% and 47.29% respectively. This suggests that a good number of digital learners are likely to be exposed to the digital space should they encounter such attacks. This is consistent with Kumar et al., 2019 who suggested that the use of technology tools in education exposes learners to digital risks and who lacks the needed skills to evade such attacks leading to exposure at the personal and institutional levels. Regarding exposure by courses studied, the results showed a relatively low susceptibility of ICT students compared to the others that ranged from approximately 80% to 85.37%. This might be due to the fact that as ICT students, they might have had quite some level of experience with cyber-attacks using such schemes. The implication of this is that these attacks have the tendency to compromise the security and privacy of learners and expose them to cyberbullying, extortions, and indecent exposures. Again, according to the competency model, the learners are at the ignorant stage and are not aware of the risk of their behavior regarding cyber-attacks; Unconsciously Incompetent. This is why the level of vulnerability is high requiring some form of awareness creation among the students as depicted in stage 1 of the matrix. This finding is consistent with Bratina & Krasna (2017).

5.2. The Use of SDSAM Model Improved Susceptibility of Learners

The data suggest that students are vulnerable to online attacks. This digital vulnerability to online or digital attacks might be due to a lack of knowledge of digital security and privacy. Thus, requires education and awareness creation to expose the learners to the phenomenon. The result after learners we exposed to the security and privacy of being online showed that only 5% were victims from the male participants with 87.67% of the learners showing resistance to the attack. This result agrees with the position of Albladi and Weir (2020) and Aldawood and Skinner (2020) who suggested that user vulnerability to social engineering attacks can be improved by organizing training, awareness creation and educational activities to build resistance, immunity and reflective behaviors among digital users. This result means that, after the debriefing of the learners and exposing them to risk, they learned and became Consciously Incompetent i.e., they became aware and ready to learn and change their behavior. This continuous use led to them being consciously competent.

5.3. Measuring the Efficiency of the Proposed Approach

To determine the efficiency of the model, we compared the performance results of the learners. Susceptibility before the administration of the model with the result of the model after. The data suggest that, in Round 1 of the study, 203 participants representing 67.67% were susceptible, compared with Round 2 where 5 respondents representing 1.67% were susceptible with 273 participants, representing 91% showing resistance or immunity to the online attack. This suggests that, after the awareness created by the use of the model, learners were careful and changed their reaction to the attack this time. This is consistent with the competency learning theory proposed by Chapman (2019), which suggests that people learn through constant practice moving from being Unconscious Incompetence (Ignorance stage) to Conscious Competence (Awareness stage), Unconscious Competence (Learning stage) and finally to Conscious Competence (Mastery stage).

Thus, the continuous and regular use of the model will lead to the acquisition of relevant skill or attitudinal changes required to overcome digital attacks and exploitations leading to improvement in the privacy and security of learners. This is supported by Bandura and Lighsey (1999) on self-efficacy as people continuously carry out an activity which leads to perfection.

Therefore, as more digital learners converge in the digital ecosystem, privacy and security remain a challenge. This requires innovative approaches to improve learners' resistance and immunity to such attacks to avoid the compromise of personal confidential information and provide secure digital space for E-learning and other digital services.

6. Recommendation

The study aimed at evaluating the susceptibility of students to online attacks (security and privacy culture) and proposed a novel framework for improving security and privacy when in the digital space. The result demonstrates that students are susceptible to these attacks due to a lack of awareness. When awareness is created, it leads to immunity and resistance of students and promotes secure digital security culture. Thus, we recommend that:

- Teachers should routinely and regularly expose students to digital security and privacy risks through security and privacy awareness programs and other Social Engineering Awareness, Training, and Education (SEATE) programs.
- Developers of school curricula should involve digital security and privacy content to enable learners to imbibe the concepts and build reflective behaviour against online attacks
- The SSAF used should be adopted to teach security and privacy as it follows the competence-learning model and gradually leads the student to perfection and complete attitudinal change.

7. Conclusion and Future Works

The study explored the vulnerability of digital learners' security and privacy in virtual/digital learning environments and proposed an approach based on phenomenology as a means of improving their digital behaviors. The results showed high vulnerability among learners as they willingly provided confidential information in the experiment; the results after the training using the model showed an improvement as only 1.6% were still vulnerable thereafter. The paper concluded that as educational products, and services migrate to digital ecosystems, the privacy, and security of the learners remain a challenge requiring constant and consistent behavioral change techniques to build the resistance and immunity of learners against such attacks. Consequently, the use of our approach based on phenomenology presents good potential for improving learners' digital privacy and security. Even though the framework performed relatively well, it is inflexible. Future works will follow the framework and implement it using machine-learning to ensure adaptability.

Acknowledgement

The researcher acknowledge the participants for availing themselves for the study.

Conflict of Interest Statement

The author declares no conflict of interest.

About the Author

Mr. Azaabi is currently a Graduate Student at the University of Energy and Natural Resource, Sunyani, Ghana and a Tutor at St. John Boscos College of Education, Navrongo, Ghana. He holds a Master of Science Degree in Information Technology from the Kwame Nkrumah University of Science and Technology, Kumasi, Ghana. A Post-Graduate Diploma in Management Information Systems (MIS) from the Ghana Institute of Marketing and Public Administration (GIMPA), a Bachelor's Degree in Computer Science and Education, University of Cape Coast, and a Teacher's Certificate from the Pusiga Training College. He is a beginning Researcher with an interest in cybersecurity, green computing and adaptable learning systems.

References

Albladi, S., M., and George R. S. Skinner. A Conceptual model to Predict Social Engineering Victims. IEEE 12th international conference on global security, safety and sustainability, ICGS3-2019.

Al-hamdani, W. (2018). Secure E-learning and Cryptography. Kentucky State University.

Bandura, A., Freeman, W. H., & Lightsey, R. (1999). Self-Efficacy: the exercise of control. Journal of cognitive psychotherapy, 13(2), 158-166. https://doi.org/10.1891/0889-8391.13.2.158.

Bratina, T., and Krasna, M., (2017). Students' attitudes towards digital security. Faculty of Education, Koroska, Slovenia.

Chapman, A. (2019). The conscious competence model. https://www.businessballs.com/self.awareness/conscious-competence-learning-model.

Drew Harold (2018). The new lesson plan for elementary school: surviving the internet. Washington Post (April, 2021). https://www.washingtonpost.com/business/economy/the-newlesson-plan.

Giambrone, A., (2015). Can data improve education without compromising privacy? The Atlantic (June, 2015). Retrieved from https://www.theatlantic.com/education. (April, 2022).

Hussain Aldawood & Geoffrey Skinner (2019). An Academic Review of Current Industrial and Commercial Cyber Security Social Engineering Solutions, ICCSP

2019, January 19-21, 2019, Kuala Lumper, Malaysia DOI: https://doi.org/10.1145/3309074.3309083

Kongsvik, J., R. (2021). Using the competency matrix to support teacher change efficacy by boosting teacher efficacy when implementing new techniques from professional development workshops, PhD Thesis, retrieved from https://www.proquest.com/openview/c1b8c1ee8ab2d8d46854fa0f8a13ff9e/1?pq-origsite=gscholar&cbl=18750&diss=y

Kumar, M. Chaudhary, and N. Kumar (2015). Social engineering threats and awareness: a survey, European Journal of Advances in Engineering and Technology, vol.2, no.11, pp.15-19, 2015.

Lindsey Kalter and Erin Smith (2016). ACLU of Massachusetts. Encourage students to beef up student data privacy. Boston Herald. https://www.govtech.com/education/k-12/ACLU

Manthey, D., and Fitch, M. (2012). Stages of the competence for medical procedures. Clinical Teacher, 9(5).317-319. https://doi.org/10.1111/j.1743-498x.2012.00561.x

Mellissa Mazmanian and Simone Lannette (2017). An ethnography of parenting in the digital age. In Proceedings of the 2017 ACM Conference on computer-supported cooperative work on social computing (CSCW'17). ACM, New York, USA. https://doi.org/10.11145/2998181.2998218.

Miguel, J., Cabale, S., Xhafa, F., and Prieto, J. (2014). Security in online learning assessment towards an effective trustworthiness approach to support e-learning teams. In advanced information networking and applications (AINA), 2014 IEEE28TH Conference on (PP.123-130).

Natasha Singer (2017). How Google took over the classroom. The New York Times (May, 2022). Retrieved from https://nytimes.com/2017/05/13/technology/googl-educate-chromebooks-schools.html.

Saidu, A., Mohammed, A., C., Mohammed, M. (2018). E-learning security challenges, implementation and improvement in developing countries: A review, Retrieved from https://www.iiste.org/Journals/index.php/IKM/article/view/40633

Sonnenberg, C. and vom Brocke, J. (2014). Evaluations in the science of the artificial - reconsidering the build-evaluate pattern in design science research. Proc. of DESRIST 2012, Las Vegas, NV, pp. 381-397

Venable, J., Pries-Heje, J., and Baskerville, R. (2016). FEDS: A Framework for Evaluation in Design Science Research. European Journal of Information Systems 25(1): 77-89.

Creative Commons licensing terms
Author(s) will retain the copyright of their published articles agreeing that a Creative Commons Attribution 4.0 International License (CC BY 4.0) terms will be applied to their work. Under the terms of this license, no permission is required from the author(s) or publisher for members of the community to copy, distribute, transmit or adapt the article content, providing a proper, prominent and unambiguous attribution to the authors in a manner that makes clear that the materials are being reused under permission of a Creative Commons License. Views, opinions and conclusions expressed in this research article are views, opinions and conclusions of the author(s). Open Access Publishing Group and European Journal of Education Studies shall not be responsible or answerable for any loss, damage or liability caused in relation to/arising out of conflicts of interest, copyright violations and inappropriate or inaccurate use of any kind content related or integrated into the research work. All the published works are meeting the Open Access Publishing requirements and can be freely accessed, shared, modified, distributed and used in educational, commercial and non-commercial purposes under a Creative Commons Attribution 4.0 International License (CC BY 4.0).