The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities

F B Fatokun1, S Hamid1, A Norman1,3, J O Fatokun2,4

1Department of Information Systems, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia
2Department of Mathematical Sciences, Faculty of Natural and Applied Sciences, Anchor University, Lagos, Nigeria

Abstract. A lot of cybersecurity breaches occur due to human errors. Tertiary institutions need to enhance students’ cybersecurity awareness and capabilities, hence promoting safe cybersecurity behaviors. Socio-psychological factors affects students’ cybersecurity behaviors. We explore to what extent age, gender and educational level, plays a role in mediating the factors affecting tertiary institution students’ cybersecurity behaviors. A cross-sectional survey was conducted among 340 students and Structural Equation Modelling was employed for evaluating impacts. Data analysis was conducted via SPSS (V.25). Results show that students cybersecurity behaviors varies based on Age for factors such as: Perceived Severity, Peer Behavior, Familiarity with Cyber Threats, Response Efficacy and Perceived Vulnerability. Gender effects existed in Security Self Efficacy, Computer Skills, Cybersecurity Behaviors, Perceived Severity, and little effects in Prior Experiences with Computer Security Practices. Educational level differences existed in Cues to Action and Familiarity with Cyber-Threats. Age, gender and educational level are important factors in mediating students’ cybersecurity behaviors. Practically, our findings can instigate the need for specific/focused cybersecurity training and interventions for students in the tertiary institutions. It can also help cybersecurity training units in the tertiary institutions to target very vital components of cybersecurity behavior model, hence improving the cybersecurity behaviors of the students.

1. Background Information
As a result of the swift escalation of the internet across the globe, vis-à-vis the expansion of larger connectedness across individuals, finance, and business, building necessary safeguards against privacy and security will only be of more importance. However, inappropriate behaviors of humans on the internet is one of the common issues regarding their cybersecurity assurance. In fact, some studies have referred to humans as the major weak link in cybersecurity [1], due to the common mistakes they usually make online. Some of these mistakes could be simple actions like the opening of suspicious email attachments (which could even be in executable file formats), consciously making use of a virus-infected pen drive, or even clicking a bad phishing link sent to Social media groups due to want of gain.

Furthermore, the understanding as to how the personal differences of internet users affects their cybersecurity behaviors, is of criticality to assisting organizations, institutions, security practitioners as well as
Researchers, to identify such users that have higher susceptibility to security practices that are poor and dangerous. Students of tertiary institution are a group of intellectuals who regularly make use of the internet due to their explorative nature of study. According to the study of [2], these students have been however reported to be vulnerable to cyber-threats. It has also been found out that similar age groups, gender and educational level is being shared among students in tertiary institutions [3], which makes it reasonable to conduct investigations among such factors with regards to their cybersecurity behaviors. Hence investigation on how age, gender, and educational level impact their cybersecurity behaviors would be of much importance to be able to understand how to create specific interventions with regards to their cybersecurity assurance. Previous studies have shown lower age group students in higher institutions to be more prone to cyber-attacks [4]. In another recent study, gender has also been found to have a moderating effect on the cybersecurity behaviors of employees [5]. The factor of educational level is not left out totally, as it has been discovered to have some differences with regards to the impact of online user’s security behaviors [6]. Furthermore, in a study that investigated on the familiarity of undergraduate students with cyber threats, it was found out that the students were less familiar with cyber threats [7]. Kearney and Kruger [8], argued that the perceptual alignment of diverse groups in an organization is a prerequisite and critical necessity to reach the information security congruence amongst such group of people. This could imply that different individuals could have distinct perceptions with respect to their cybersecurity behaviors.

With regards to how individual differences could affect relationships between perceived severity and cybersecurity behaviors, a study by Chakraborty, Lee [9], on online shopping intentions with regards to data breaches was conducted on younger and older adults. From this study, it was discovered that younger adults had a marginal significance with regards to a hacking incidence perceptions of severity, also they found out that gender had some significant differences with regards to perceived severity of online shopping security intentions [9]. Moreover, in another study which focused on how gender could mediate the cybersecurity behaviors of employees in an organization, it was discovered that gender importantly mediated the cybersecurity behaviors of the employees in diverse perspectives [5]. For example, still from Anwar’s study, their results revealed that statistical significant differences in gender was prominent in the employees cues-to-action, computer skills, prior experience, security self-efficacy as well as their self-reported cybersecurity behaviors. It was also discovered that women had a lower self-efficacy than the men with regards to their cybersecurity, hence indicating that their self-efficacy could be a target for further interventions.

Another work on the individual differences in Cybersecurity behaviors, which focused on the risky practices of sharing passwords based on some factors such as age, among others, found out that age was a significant predictor of password sharing among the individuals [10]. Younger persons were more likely to share passwords as to when compared with the older ones, hence this could be due to reason being that younger persons have more opportunities to share passwords since they might always be active online more than the older persons. In a phishing experiment conducted by Moheszada, El Zarka [2], we were informed that age and gender had some effects on the results from the phishing exercise, even though the correlations were not very strong. From their study, younger students between the age of 18 and 21 years were of less susceptibility to phishing than the senior students, which contradicts some other studies [11-13] that states that the younger the age, the higher the susceptibility to phishing.

From all the previous studies so far, it has been revealed that in one way or the other, individual differences of age, gender and educational experiences could have some mediating effects on the cybersecurity behaviors of various persons. However, not much has been done with regards to how such factors of age, gender, and educational level can have mediating effects on the cybersecurity of students in the tertiary institution. It is in this vein that the current paper presents results based on investigations carried out to find out as to what extent age, gender and educational level mediate the cybersecurity behaviors and beliefs of tertiary institution students.

2. Theoretical Framework
The current study is based on two theories of which are: The Health Belief Model by Becker, [14] and Protection Motivation Theory by Maddux, [15]. These theories have been majorly used by researchers to explain the intentions of users with regards to employing security technologies, and also describe the
when and how of the adoption of maladaptive or adaptive behaviors by a user when he/she gets informed about a threatening security occurrence.

Furthermore, the Health Belief Model (HBM), is a conceptual model that was developed to provide insights on reasons regarding the participation of individuals in health behaviors. The HBM consists of the following components of: Perceived Severity, Perceived Benefits, Perceived Susceptibility, Cues to Action, and Perceived Barriers. On the other hand, the Protection Motivation Theory (PMT), refers to a reworking and an extended version of the HBM. Thus, the consideration of PMT lies on the intention for self-protection in determining health behavior, and this intention has its dependence based on components such as Perceived Severity, Perceived Susceptibility, Response Efficacy, and Self-Efficacy.

Being guided by the aforementioned theories, previous empirical studies [5, 16-19] from information and cybersecurity fields, have discovered that there is a correlation between security behaviors and perceived susceptibility, perceived benefits, self-efficacy, and perceived severity. Additionally, some other scholars [20, 21] have revealed that Cues to Action, Perceived Barriers, Peer Behaviors (i.e., those triggers or experiences by which a user can be activated and motivated to practice computer security), previous security compliance habits as well as personal factors (such as, educational level and gender), also have some impacts on the security behavior of users. More so, other scholars found out that information seeking skills, prior experience with computer security practices, and computer skills can be predictors of the security behavior of an individual [6, 17, 22].

Investigation has also been conducted on familiarity with cyber-threats and how it relates to cybersecurity behaviors, however not much have been revealed about it. Yet in a study that found out if individuals vary in their familiarity level with cyber-threats, it was discovered that the younger group of students had less familiarity with cyber-threats unlike the older ones [7], which shows that people differ in their familiarity with cyber-threats based on age.

Hence, following the previous studies, it can be stated that the need for more research with respect to examining the differences and similarities in the cybersecurity beliefs and behaviors of individuals based on personal factors such as gender, age, and educational level, most especially among students in the tertiary institution which is a lacking area in literature.

This research has investigated the association between age, gender and educational level and the components of the proposed cybersecurity behavior model for students in the tertiary institutions (Fig. 1), which is based on the Protection Motivation Theory and the Health Belief Model.

In this study, we have studied the following constructs as being guided by our foundational theories explained previously. The constructs are summarized in Table 1 below:

| CONSTRUCT          | DEFINITION IN TERMS OF CYBERSECURITY                                      | REFERENCES |
|--------------------|---------------------------------------------------------------------------|------------|
| Perceived Vulnerability | Used to measure users belief on their risk to cyber threat.               | [16, 17, 23]|
| Perceived Severity  | Used to measure users perceptions on consequences of risky cybersecurity behaviors serious. | [16, 17, 23, 24]|
| Security Self-efficacy | Used to measure the confidence level of handling cyber-threats issues.     | [17, 19, 25]|
| Perceived Barriers  | Used to measure inconvenience levels in checking for cybersecurity issues. | [17]        |
| Response Efficacy   | Used to measure response level with regards to cybersecurity policies adherence. | [20]        |
Cues to Action  Used to measure the level of promoting good cybersecurity behavior in an organization. [17]

Peer Behavior  Used to measure level of users belief about their friends security behavior. [21, 26, 27]

Computer Skills  Used to measure the basic computer competency level of a user. [28]

Internet Skills  Used to measure competency level of a user with the Internet. [28, 29]

Prior Experience with computer security practices  Used to measure experience level of a user with regards to good cybersecurity practices. [17, 30]

Perceived Benefits  Used to measure the perception of a user with regards to benefits of good cybersecurity practices. [17]

Self-reported cybersecurity behavior  Use to measure actual cybersecurity behaviors of users. [17, 20, 31, 32]

Familiarity with Cyber-Threats (New)  Used to measure the users’ level of familiarity of some defined common cyber-threats. [7, 33, 34]

The aim of our study is to investigate into the mediating effects of age, gender and educational level in terms of the above-stated constructs affecting the cybersecurity beliefs and behaviors of students in the tertiary institutions. The research question sought to be answered is the exploration as to whether differences in cybersecurity beliefs and behaviors of tertiary institution students existed based on age, gender, and educational level. In such direction, leading to the test of the following hypothesis:

H1: Age has a mediating effect on the cybersecurity behaviors and beliefs of Tertiary Institution Students;

H2: Gender has a mediating effect on the cybersecurity behaviors and beliefs of Tertiary Institution Students;

H3: Educational level has a mediating effect on the cybersecurity behaviors and beliefs of Tertiary Institution Students.

To test our hypothesis, we conducted an online survey based experiment amongst students in tertiary institutions across Klang Valley, Malaysia. The students were asked questions regarding the perceptions of several crucial constructs of our cybersecurity behavioral model. Likert items were made use of in measuring the survey participants’ perceptions/behaviors to a specific question. Furthermore, the responses were coded in a reverse order from 1(Strongly Disagree)-5(Strongly Agree). Our findings offered additional fine-grained comprehension of the users as well as their motivations and how this would aid the designing of appropriate and fantastic interventions.

Our proposed Cybersecurity Behavioral Model based on the mediating effect of Age, Gender and Educational level is given in figure 1 below:
3. Methodology

3.1. Participants & Approach
We sent out an online survey from January 2019 to undergraduate and postgraduate students in tertiary institutions within Klang valley, Malaysia. Selection of the students wasn’t based on their fields of study, as the survey was randomly sent via online mediums such as central university emailing systems, institutions Facebook Pages, and Student WhatsApp groups, among others.

A total of 340 respondents were gathered, however only 336 were eventually used for the final analysis. This was due to issues of redundant and double entry as this was detected via our online system. The distribution among the participants in respect to gender, age groups and educational level was normal. Among the 336 valid respondents, 186 were females while 150 were males; for the age distribution, 220 of the students were below the age of 30, while the remaining 116 were above the age of 30; In respect of their educational levels, 131 of the students were undergraduates while the remaining 205 were postgraduate students. This will be displayed more expressly in the result section.

All the participants were given adequate information regarding the essence as well as the procedure to contribute in this study. They were also informed about the identifying information (a fake email address), which was collected for purposes of data validity and management purposes. Sensitive information such as names, full date of birth was not attached to the survey. All participants for this study had the change to exclude themselves from the survey at any time they felt like, as this was a voluntary exercise. Also it is important to note that the Internal Review Board (IRB) of investigators gave approval for the study.

3.2. Measurement
Having carried out a critical review of literature relating to scholarly articles of behavioral information security, cybersecurity behavioral studies, and our proposed model, we proceeded to design a survey which was used for data collection in this study. Although most of the items on our survey were adopted
from a related study’s questionnaire, however the questions were modified to suit the student population; for example, questions regarding business organizations were modified to tertiary institutions. A Pilot study of 50 students was used to test the survey instruments around December 2018 at a particular university in Kuala Lumpur, Malaysia. The result from the pilot study was employed to confirm if the wordings were easy to understand and if the items were appropriate for the level of the students. The scales used in the final version of the survey were assessed based on a five-point Likert scale, which ranged from Strongly Disagree (1) to Strongly Agree (5), for most of the items. However, this was not the case in some other scales; for example, the item that measured students comfort level with regards to their computer skills made use of five point Likert Scale ranging from Very Uncomfortable (1) to Very Comfortable (5). Same was the case of the Familiarity with Cyber Threat scale, which ranged from: Very Unfamiliar (1) to Very Familiar (5). The final survey comprised of 83 Likert items collecting data that measured the student’s security self-efficacy, perceived vulnerability, among other elements as depicted in the proposed model. Items used for measuring the individual latent variables in the research model were developed via adoption or modifying of questionnaires from existing/related literature. For example, the measures used for testing the cybersecurity belief scales were adapted and adopted from [5], who also depended on other studies such as [17, 19, 20, 32]. While the measure used for the familiarity with cyber-threat scale, which is a new construct we added into the existing model, was adapted/adopted from [7, 35].

3.3. Data Analysis

Structural Equation Modeling (SEM) was used for analyzing the gathered data. In our analysis, the goal was to evaluate the impacts of age, gender and educational level as moderator variables in the association between psychosocial factors as well as reported cybersecurity behaviors. The Point Biserial Correlation was used with inclusion of the Spearman rho for finding the differences among the moderating factors and the Cybersecurity Behaviors and perceptions, while the comparing of means was used to further detect more specifically which of the component of each groups had higher impacts (for example, whether males or females, younger students or older students, and undergraduates or postgraduates). Data analysis was conducted via the latest version of IBM’s statistical analysis software package (SPSS, Version 25).

4. Results & Findings

4.1. Demographic Statistics

From the demographic statistics as summarized in Figure 2, with regards to the gender distribution, 44.6% were male students (N = 150) while the remaining 55.4% were female students (N = 186). For age group, the collected data was coded into two groups, students below 30 years were said to be younger students, while those above 30 were said to be older students; hence 65.5% (N= 220) of the students were in the younger students category, whereas 34.55 (N = 116) were older students (above 30 years of age). Concerning the educational level of the participants, 39% (N = 131) of them were undergraduate students while the remaining 61% (N = 205), were at the postgraduate level of study.

Figure 2. Demographic statistics
Other statistics such as the respondent’s internet usage level per day, level of internet expertise and social media usage was also gathered. Regarding the students daily usage of the internet, only 1.2% (N = 4) of the students claimed to make use of the internet less than an hour, while 35.1% (N = 118) reported to make use of the Internet 2-5 hours daily; Interestingly as was expected by the researchers, majority of the students with a percentage of 63.7%, attested to the fact that they made use of the internet more than 6 hours daily (N= 214). This tallies with the fact that the respondents were regular users of the internet and would have on several occasions being faced with cybersecurity issues. In trying to discover about the respondents Internet Expertise level, the following statistics is reported: Beginners were the lowest with 6.3% (N = 21), followed by the Experts who had the second place with 27.7% (N = 93) and majority of the respondents were at the intermediate level of Internet expertise, with 66.1% (N = 222). In a means of checking on the participants social media usage which is another means of them being faced with lot of cybersecurity challenges, we found out the following: only 1.8% (N = 6) of the students claimed to not make use of social media platforms, this was surprising although the researchers thought this could be due to the available options that was used for the study, which was WhatsApp and Facebook. However, 31.5% (N = 106) stated that they used only WhatsApp Messenger daily, while the bulk of the students, 66.7% (N = 224) made use of both WhatsApp and Facebook on a daily basis.

4.2. Age Impact & Differences
The relationship of age with the Cybersecurity scales was evaluated with a series of bi-serial point correlations with age being coded into two categories stated thus: 0 for younger students (below 30 years) and 1 for older students (above 30 years), as shown in Table 2. According to acceptable statistical significance level, results that were significant at an alpha level of <0.05 are discussed, in order to avoid over-interpreting of the relationships with effect sizes. From the results, the older students (those above the age of 30) as being represented in this study, reported to have slightly higher perceived vulnerability, perceived severity, response efficacy, Peer behavior, than the younger students (those below age 30). The only case where the younger students had higher means was in the case of their familiarity with cyber-threats (See Fig 3). This could imply that younger students were more familiar with cyber-threat than their counterparts, the older students. Furthermore, the largest impacts between younger and older student was observed on their Perceived Severity, where the older students perceived severity standard deviations score was 2.10 lower than that of the younger students, implicating that older students might be more careful about security issues. Also, older students scored higher in their peer behaviors in relation to cybersecurity behaviors than the younger students. Although this cannot be drawn to total conclusion as this differences are not too large, nevertheless, the findings suggest that age has an impact in the perceived severity of the students with regards to their cybersecurity behavior.

In a way of summarizing, there are five age impacts comprising: Perceived Vulnerability, Perceived Severity, Response Efficacy, Peer Behavior, and Familiarity with Cyber-threats. The biggest impact is on Perceived Severity (r = 0.166, p = 0.002) and the smallest impact is on Perceived Vulnerability (r = 0.126, p = 0.021).

Table 2: Results of the means, standard deviation, and point biserial correlation on the impact of age for the cybersecurity behaviors of tertiary institution students based on: Cybersecurity Behaviors (CSB), Perceived Vulnerability (PV), Perceived Barriers (PBr), Perceived Severity (PS), Security Self Efficacy (SSE), Response Efficacy (RE), Cues to Action (CA), Peer Behavior (PBhv), Computer Skills (CS), Internet Skills (IS), Prior Experience with Computer Security Practices (PE), Perceived Benefits (Pbf), and Familiarity with Cyber-Threats (FCT).

|                  | Younger Students(Below 30) (N = 220) | Older Students(Above 30) (N = 116) | r     | P      |
|------------------|-------------------------------------|-----------------------------------|-------|--------|
|                  | M        | SD | M        | SD |       |       |
| CSB              | 42.11    | 6.97 | 42.84    | 7.17 | 0.073 | 0.181 |
| PV               | 29.98    | 4.15 | 30.81    | 4.46 | 0.126* | 0.021 |
| PBr              | 12.41    | 2.61 | 11.97    | 2.87 | -0.058 | 0.293 |
| PS               | 16.69    | 2.71 | 17.59    | 2.10 | 0.166** | 0.002 |
Figure 3. Age differences for the different cybersecurity perception and behavior scales

4.3. Gender Impacts & Differences

The impacts of gender was achieved via series of point bi-serial correlations as well. Gender was coded as 0-for females and 1- for males. The findings that were obtained from the gender interactions are discussed and presented in this section. It was observed that the female and male students differed in their security self-efficacy, and in fact, the male students had a higher score in their security self-efficacy with a mean of 19.30. This could imply that with regards to this study, male students are surer of their cybersecurity skills as compared to their female counterparts. However, this is not enough reason to make conclusions on such issue, as it might be that the male students in this study may have answered the survey due to overconfidence, nevertheless, we can say that differences exist between the female and male students with regards to their security self-efficacy. Furthermore, another area of interest is with regards to the differences shown in the computer skills, where the male students again scored higher than the female students (see figure 4 for interactions and table 4 for detailed results). Here, it could be true that the male students might have more computer skills than the females, as most of the female students, around 77 of them, indicated in one of the survey questions that were not comfortable in dealing with technical issues such as: installing/upgrading computer software on their computers, as compared to the male students, where just 30 of them indicated such difficulties. Therefore, this could further indicate that institutions should organize scheduled computer training for the students.

Still from the results of the impacts of gender on cybersecurity beliefs and behaviors, female students obtained a higher mean score in their perceived severity than the male students, and coincidentally, this is the only aspect where the female students scored higher with regards to the cybersecurity scale. Hence,
this could be true because generally women are more afraid than men, and in the other way round, they are more careful as well. It could be that male students might be more careless about the consequences of violating cybersecurity rules. In view of this, ICT centers/cybersecurity units of tertiary institutions should therefore create more awareness about the severity of cyber-threats to all students.

In summary, the impacts and differences of gender on the cybersecurity behavior scale, with regards to tertiary institution students are: Cybersecurity Behavior, Perceived Severity, Security Self-Efficacy, Computer Skills, and Prior Experience with Computer Security Practices. The highest impact was found on: Security Self-Efficacy, while the lowest was found on: Prior Experience with Computer Security Practices.

**Table 3.** Results of the means, standard deviation, and point biserial correlation on the impact of gender for the cybersecurity behaviors of tertiary institution students based on: Cybersecurity Behaviors (CSB), Perceived Vulnerability (PV), Perceived Barriers (PB), Perceived Severity (PS), Security Self Efficacy (SSE), Response Efficacy (RE), Cues to Action (CA), Peer Behavior (PBhv), Computer Skills (CS), Internet Skills (IS), Prior Experience with Computer Security Practices (PE), Perceived Benefits (PBnf), and Familiarity with Cyber-Threats (FCT).

|          | Female (N = 186) | Male (N = 150) | r     | P     |
|----------|-----------------|----------------|-------|-------|
| M        | SD              | M              | SD    |       |
| CSB      | 41.50           | 7.17           | 43.42 | 6.75  | 0.151** | 0.006 |
| PV       | 30.48           | 3.94           | 30.00 | 4.66  | -0.031  | 0.575 |
| PBr      | 12.24           | 2.80           | 12.27 | 2.63  | -0.002  | 0.978 |
| PS       | 17.30           | 2.45           | 16.64 | 2.62  | -0.150** | 0.006 |
| SSE      | 15.52           | 4.62           | 19.30 | 5.04  | 0.354** | <0.001 |
| RE       | 15.82           | 2.57           | 15.83 | 2.35  | 0.016   | 0.763 |
| CA       | 10.70           | 3.29           | 10.59 | 3.68  | -0.005  | 0.928 |
| PBhv     | 12.00           | 2.55           | 11.86 | 2.72  | -0.037  | 0.504 |
| CS       | 14.57           | 2.89           | 15.92 | 2.72  | 0.215** | <0.001 |
| IS       | 25.79           | 5.19           | 27.03 | 4.75  | 0.096   | 0.078 |
| PE       | 17.69           | 4.03           | 18.67 | 4.26  | 0.111*  | 0.042 |
| PBnf     | 23.85           | 3.20           | 23.61 | 3.58  | -0.031  | 0.571 |
| FCT      | 46.29           | 12.90          | 48.45 | 11.96 | 0.070   | 0.201 |

**Figure 4.** Gender differences for the different cybersecurity perception and behavior scales
4.4. Educational Level Impact & Differences

Finally with regards to our result, we discovered that Educational level was not totally left out even though just two out of the 13 components had some effects and they are Cues to Action (r = -0.161, p = 0.003) and Familiarity with Cyber-Threats (r = -0.110, p = 0.045). When the means were compared for the Educational level component, it was discovered that for Cues to Action, undergraduates seemed to act more promptly to security cautions when faced with security challenges than the postgraduate students. This could be due to the fact that most of the undergraduate students are still young and can still be controllable or teachable, because they are being sponsored by either their parents or guardians, unlike the postgraduate students who might have made more advances and progress in life, and may not necessarily care about such issues. Interestingly, we also found out that the Undergraduate students scored higher in the familiar with cyber-threats than the Postgraduate students, although the results doesn’t give a clear backing for this due to the weak p-value and the negative correlation coefficient. However, it is still an issue of interest because the correlation coefficient is actually negative which means in overall, a lot of the undergraduate and postgraduate students are not very familiar with most of the cyber-threats. Furthermore, and based on the results, it can be inferred that the undergraduate students might actually have not have the tendency of better knowledge and exposure to more cyber-threats than the postgraduate students, due to their upcoming stage of life and perhaps lack of experience. Although, it is also possible that undergraduate students can have better chances of communicating with peers as they still attend class lectures, and in such instances might learn from their colleague’s threat experiences. This is unlikely with the postgraduate students as most of them are always on their personal study for their research, except for a few who still offer courses. Table 4 and Figure 5 offers the detailed results and interactions of the educational level impact.

**Table 4.** Results of the means, standard deviation, and point biserial correlation on the impact of gender for the cybersecurity behaviors of tertiary institution students based on: Cybersecurity Behaviors (CSB), Perceived Vulnerability (PV), Perceived Barriers (PB), Perceived Severity (PS), Security Self Efficacy (SSE), Response Efficacy (RE), Cues to Action (CA), Peer Behavior (PBhv), Computer Skills (CS), Internet Skills (IS), Prior Experience with Computer Security Practices (PE), Perceived Benefits (PBnf), and Familiarity with Cyber-Threats (FCT).

|                | Undergraduates (N = 131) | Postgraduates (N = 205) | P     | r     |
|----------------|--------------------------|--------------------------|-------|-------|
|                | M            | SD          | M           | SD          |       |
| CSB            | 42.50        | 7.84        | 42.27        | 6.49        | 0.006  | 0.917 |
| PV             | 30.35        | 3.61        | 30.21        | 4.66        | 0.010  | 0.859 |
| PBr            | 12.44        | 2.34        | 12.14        | 2.92        | -0.032 | 0.556 |
| PS             | 16.92        | 2.35        | 17.06        | 2.67        | 0.052  | 0.340 |
| SSE            | 17.27        | 5.07        | 17.16        | 5.23        | -0.017 | 0.762 |
| RE             | 15.61        | 2.09        | 15.96        | 2.68        | 0.104  | 0.057 |
| CA             | 11.33        | 3.28        | 10.22        | 3.52        | -0.161*| 0.003 |
| PBhv           | 11.94        | 2.74        | 11.94        | 2.55        | -0.024 | 0.659 |
| CS             | 14.86        | 2.75        | 15.38        | 2.97        | 0.083  | 0.128 |
| IS             | 25.73        | 4.71        | 26.75        | 5.19        | 0.105  | 0.055 |
| PE             | 18.09        | 4.22        | 18.16        | 4.13        | -0.008 | 0.882 |
| PBnf           | 24.04        | 3.25        | 23.56        | 3.44        | -0.061 | 0.261 |
| FCT            | 48.60        | 12.95       | 46.39        | 12.19       | -0.110*| 0.045 |
5. Conclusions

This study was aimed at discovering if age, gender, and educational level has an impact on the cybersecurity behavior and beliefs of tertiary institution students, and to find out to what extent this differences exists. Hence the paper presents in the previous sections detailed results with regards to the investigation conducted. From the results conducted so far, it was found out that all the three factors: age, gender and educational level, in one way or the other have some impacts in mediating the relationship between the cybersecurity behaviors of tertiary institution students. However, among the three, the factors of age and gender are more important as they attracted more impacts with good statistical significances than the educational level factor. This could imply that the level of education may not necessarily influence our cybersecurity behaviors, hence everyone needs to be aware and secure while surfing the internet or using any technological tool.

Our study have some significant correlations with previous studies. One of the very interesting of such is with regards to the results we obtained from the impact of gender. In our study, we discovered that Security Self Efficacy, Computer Skills and Prior Experience were among the cybersecurity scales that were impacted by gender. Similarly in a study by [5], they found out that gender had effects on these three constructs as well, even though their target population was employees in a business organization. Nevertheless, in their study, Perceived Severity didn’t have any effect on the gender differences between the employees, whereas this was discovered in our own study to have effect on the tertiary student’s cybersecurity behavior. With regards to age differences, a study found out that younger adults had a marginal significance with regards to a hacking incidence perceptions of severity [9], however in our own study, we discovered that higher effect was found on the older students with regards to perceived severity. In a study that conducted an investigation on the familiarity with threat among undergraduate students in a US university, they found out that most of the undergraduate students were not familiar with many of the cyber-threats [7]. In the current study, it was also discovered that both undergraduate and postgraduate students are not familiar with some of the common cyber-threats, hence this calls for awareness in the higher institution to train and update students with latest and common threat outbreaks in order to get them familiar with it.

In summary and as a way of concluding, all the three factors of age, gender and educational level have some vital impacts on the components of cybersecurity perceptions and behaviors of students in the tertiary institution. The practical importance of our study is that our findings can instigate the need for more specific/focused cybersecurity training and interventions for different groups of students in the tertiary institutions. Also, it can help cybersecurity training units of tertiary institutions to target on the most important components of the cybersecurity behavior model for the purpose of enhancing the attitudes and behaviors of tertiary institution students on the internet. This research can be furthered by investigating on the effects and impacts of other factors that might affect and impact the cybersecurity behaviors of tertiary institution students in particular, some of which could be: cultural background,
academic performance, health habits, among others. Also, future work should ensure a larger dataset, as in this study, the limitation was in getting a larger dataset, as the population size could also affect the outcome of the results. More practical approaches of investigating the cybersecurity behaviors of tertiary institution students could also be adopted in the future, since most of these tertiary institutions have adequate computer labs for such experiments.

Finally, it is important to suggest that institutions should maintain an active cybersecurity unit as many of the respondents reported that their institutions does not have such in place, and those that have do not update the students with cybersecurity news-letters, and scam alerts. If the students are well secured, then the webservers of the universities/colleges can also be free from some kind of cyber-assaults.

References
[1] Gratian M, Bandi S, Cukier M, Dykstra J, Ginther A. Correlating human traits and cyber security behavior intentions. Computers and Security. 2018;73:345-58.
[2] Mohebzada J, El Zarka A, BHojani AH, Darwish A, editors. Phishing in a university community: Two large scale phishing experiments. Innovations in Information Technology (IIT), 2012 International Conference on; 2012: IEEE.
[3] Yan Z, Robertson T, Yan R, Park SY, Bordoff S, Chen Q, et al. Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? Computers in Human Behavior. 2018;84:375-82.
[4] Ogutcu G, Tastik OM, Chouseinoglou O. Analysis of personal information security behavior and awareness. Computers & Security. 2016;56:83-93.
[5] Anwar M, He W, Ash I, Yuan X, Li L, Xu L. Gender difference and employees’ cybersecurity behaviors. Computers in Human Behavior. 2017;69:437-43.
[6] Zhang J, Reithel BJ, Li H. Impact of perceived technical protection on security behaviors. Information Management & Computer Security. 2009;17(4):330-40.
[7] Jeske D, van Schaik P. Familiarity with Internet threats: Beyond awareness. Computers & Security. 2017;66:129-41.
[8] Kearney WD, Kruger HA. Can perceptual differences account for enigmatic information security behaviour in an organisation? computers & security. 2016;61:46-58.
[9] Chakraborty R, Lee J, Bagchi-Sen S, Upadhyaya S, Raghav Rao H. Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. Decision Support Systems. 2016;83:47-56.
[10] Whitty M, Doodson J, Creese S, Hodges D. Individual differences in cyber security behaviors: an examination of who is sharing passwords. Cyberpsychology, Behavior, and Social Networking. 2015;18(1):3-7.
[11] Darwish A, El Zarka A, Aloul F, editors. Towards understanding phishing victims' profile. 2012 International Conference on Computer Systems and Industrial Informatics; 2012: IEEE.
[12] Sheng S, Holbrook M, Kumaraguru P, Cranor LF, Downs J, editors. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems; 2010: ACM.
[13] Arachchilage NAG, Love S. Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior. 2014;38:304-12.
[14] Becker MH, Radius SM, Rosenstock IM, Drachman RH, Schubert KC, Teets KC. Compliance with a medical regimen for asthma: a test of the health belief model. Public Health Reports. 1978;93(3):268-77.
[15] Maddux JE, Rogers RW. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology. 1983;19(5):469-79.
[16] Mohamed N, Ahmad IH. Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. Computers in Human Behavior. 2012;28(6):2366-75.
[17] Ng B-Y, Kankanhalli A, Xu Y. Studying users' computer security behavior: A health belief perspective. Decision Support Systems. 2009;46(4):815-25.
[18] Furnell S, Bryant P, Phippen AD. Assessing the security perceptions of personal Internet users. Computers & Security. 2007;26(5):410-7.
[19] Rhee H-S, Kim C, Ryu YU. Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security. 2009;28(8):816-26.
[20] Vance A, Siponen M, Pahnila S. Motivating IS security compliance: insights from habit and protection motivation theory. Information & Management. 2012;49(3-4):190-8.
[21] Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems. 2009;18(2):106-25.
[22] Rajivan P, Moriano P, Kelley T, Camp LJ. Factors in an end user security expertise instrument. Information and Computer Security. 2017;25(2):190-205.
[23] Ifinedo P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security. 2012;31(1):83-95.
[24] Ng B-Y, Xu YC. Studying Users’ Computer Security Behavior Using the Health Belief Model. 2007.
[25] Ifinedo P. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information & Management. 2014;51(1):69-79.
[26] Anderson CL, Agarwal R, editors. Practicing safe computing: Message framing, self-view, and home computer user security behavior intentions. ICIS 2006 Proceedings - Twenty Seventh International Conference on Information Systems; 2006.
[27] Chan M, Woon I, Kankanhalli A. Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. Journal of Information Privacy and Security. 2005;1(3):18-41.
[28] Schulenberg SE, Yutzenka BA, Gohm CL. The computer aversion, attitudes, and familiarity index (CAAFI): A measure for the study of computer-related constructs. Journal of Educational Computing Research. 2006;34(2):129-46.
[29] Smith AD. Exploring security and comfort issues associated with online banking. International Journal of Electronic Finance. 2006;1(1):18-48.
[30] Aytes K, Connolly T. Computer security and risky computing practices: A rational choice perspective. Advanced Topics in End User Computing. 42005. p. 257-79.
[31] Shih DH, Lin B, Chiang HS, Shih MH. Security aspects of mobile phone virus: a critical survey. Industrial Management & Data Systems. 2008;108(4):478-94.
[32] Davinson N, Silence E. It won’t happen to me: Promoting secure behaviour among internet users. Computers in Human Behavior. 2010;26(6):1739-47.
[33] Suleman T, Burhan-Ul-Haq H, Zafar S. User Trust on Online Social Network on the basis of Security and privacy. International Journal for Electronic Crime Investigation. 2017:35.
[34] Garg V, Camp J, editors. End user perception of online risk under uncertainty. System Science (HICSS), 2012 45th Hawaii International Conference on; 2012: IEEE.
[35] Jeske D, van Schaik P. Familiarity with threats, Internet experience and user behaviors. 2016.