Journal of Economics, Finance and Management Studies

ISSN (print): 2644-0490, ISSN (online): 2644-0504

Volume 06 Issue 10 October 2023

Article DOI: 10.47191/jefms/v6-i10-38, Impact Factor: 7.144

Page No: 5057-5066

Student's Cybersecurity Awareness in Post Covid-19 Pandemic

Amelia Setiawan[1], Samuel Wirawan[2], Hamfri Djajakerta[3], Haryanto Haryanto[4]

[1,2,3]Accounting Department, Faculty of Economics and Business, Parahyangan Catholic University, West Java, Indonesia.

[4]Accounting Department, Sekolah Tinggi Ilmu Ekonomi Mulia Singkawang, West Kalimantan, Indonesia.

Orcid: https://orcid.org/0000-0002-9386-7089[1] , Orcid: https://orcid.org/0000-0002-0627-8439[2],

Orcid: https://orcid.org/0009-0003-9474-1888[3], Orcid: https://orcid.org/0000-0002-9040-6578[4]

ABSTRACT: The study used the Theory of Planned Behavior to investigate the relationship between undergraduate accounting students' knowledge of internal control and cyber security and how it impacts their decision-making and behavior. The study was carried out on Indonesian students, and the data was analyzed by regression analysis. The results showed that students' attitudes and perceived behavioral control positively influenced their intention to practice cybersecurity. However, the effect of subjective norms and education on cyber security was insignificant. The four variables studied accounted for 41.2% of the total variance in behavioral intentions. At the same time, other factors contributed to the remaining variance. The findings suggest a need to assess the effectiveness of current cyber security education practices to achieve educational goals better. The negligible impact of the educational variable highlights the necessity of re-evaluating the current approach to cybersecurity education.

KEYWORDS: attitudes, subjective norms, theory of planned behavior

JEL codes: A100, A110

1. INTRODUCTION

The COVID-19 pandemic has brought very significant changes to human life today. This considerable change deserves the nickname Industrial Revolution 5.0 because, in many aspects, the way of working has changed to become significantly more digital compared to previous conditions, and adapting to this change must be carried out in a very short time. One of the professions that is affected substantially is the accounting profession. To answer the challenges faced by the accounting profession, the International Accounting Education Standards Board (IAESB) and the International Federation of Accountants (IFAC) require mastery of information technology for education related to the accounting profession[1].

Based on the IAESB and IFAC, one of the technical competencies accountants require is information technology (International Federation of Accountants, 2019). Required competencies include general control abilities related to information technology and relevant application controls, the ability to identify the contribution of information technology to data analysis and decision-making, and the use of information technology to support decision-making through business analysis. Apart from information technology competence, competence in governance, risk control, and internal control (Governance, Risk Management, and Internal Control or GRC) is also needed. Competencies in the field of GRC include the principles of good governance, analysis of governance components, risk management, and internal control in organizations. The Accounting Information Systems and Management Information Systems courses discuss organizational internal control. These two courses are mandatory at almost all universities that provide Undergraduate Accounting Study Programs in Indonesia. One of the internal control topics is securing company assets, including data.

The weakest link in a company's security system is humans. Sixty-four percent of data breaches are caused by human negligence and system disruption (Kennedy, 2016). Social engineering is the most frequent attack on company data (Salahdine & Kaabouch, 2019). Social engineering is an attack by tricking users into revealing confidential data or sensitive information (ISACA, 2015).

[1] https://www.iaesb.org/publications/2019-handbook-international-education-standards

Student's Cybersecurity Awareness in Post Covid-19 Pandemic

Adequate education is expected to change behavior, including information security awareness. Students who have received material about accounting information systems, including internal control, are expected to have a higher awareness, which will bring awareness to information security. Therefore, there is a demand that education, specifically accounting education, pay special attention to student behavior related to cyber. It is hoped that this education will change behavior.

Everyone risks being exposed to cyber threats, especially those who actively use social media. Research conducted in America (Kayes & Iamnitchi, 2017) found that social media users disclose personal data, including physical, psychological, cultural, and preference data. The most frequently uploaded data are photos, date of birth, place of residence and telephone number, political views, partner preferences, relationship status, and hobbies.

With the school-from-home regulations set by the Minister of Education and Culture of the Republic of Indonesia in May 2020[2], students are increasingly connected continuously to the internet. Everything is done digitally. The more digital activities are carried out, the more digital information is shared in cyberspace.

The amount of information that can be obtained about someone on social media creates cyber threats, such as the disclosure of personal data to the public or the disclosure of confidential company data (Lewis P. C, 2020; Nieto & Rios, 2019; Vargo et al., 2020). Social engineering is an attack method to exploit social weaknesses to access systems or information (ISACA, 2015). If related to students as Generation Z, based on research in Indonesia, it was found that 71 percent of respondents had an average level of awareness. This research concludes that the level of awareness is poor for smartphone users in Indonesia (Akraman et al., 2018).

This research aims to identify the influence of students' knowledge about internal control and cyber security on decisions and behavior to carry out cyber security using a behavioral theory approach. Even though there is much research on cyber security, there is not much research that connects cyber security with individual behavior regarding this matter (Addae et al., 2017). There is also no research with the unit of analysis being students during the COVID-19 pandemic, such as At the moment.

Previous research (Lebek et al., 2014; Pham et al., 2017) found that the behavioral theory most widely used in research on awareness and behavior related to information security is the Theory of Planned Behaviour (TPB). TPB is a social psychology model that is commonly used to predict a person's actions (Fu & Juan, 2017; Sasson & Mesch, 2016). However, several studies found that the factors stated in the TPB were deemed inadequate, so the researchers added other variables (Karlsson et al., 2018; Sommestad et al., 2019).

In TPB, attitudes are a person's beliefs that will influence that person's behavior. Previous research (Fu & Juan, 2017; Sasson & Mesch, 2016; Surifah et al., 2016) found a positive correlation between attitudes toward sharing information and these actions. In this research, the attitudes referred to are attitudes related to cyber security, including how a person sets privacy on social media, how a person responds to friendship invitations on social media, commenting habits, habits related to personal data, and cyber security habits carried out, including changing passwords. Regularly and habitually log off after accessing social media accounts.

Subjective norms in the TPB approach are beliefs people or groups believe that influence specific individuals, such as family or friends (Foltz et al., 2016; Nurwanah et al., 2018; Sasson & Mesch, 2016).

In TPB theory, perceived behavior control is considered one factor that influences a person's behavioral intentions (Alam et al., 2019; Sasson & Mesch, 2016). Behavioral control is an individual's perception of the ease or difficulty of engaging in a particular behavior, which is influenced by the individual's belief in the ability to control that particular behavior.

Knowledge will generally influence a person's perspective on something (Dwi S et al., 2013). A person's knowledge will generally influence a person's perspective on something (Doherty & Tajuddin, 2018; Hwang et al., 2017; Singh & Srivastava, 2018). In studies focusing on information systems, computer self-efficacy is often used to measure an individual's knowledge in the cyber world (Singh & Srivastava, 2018).

Interests are widely assumed to include factors that influence an individual's behavioral performance (Rajput, 2015). The behavior in this research is individual in the cyber world. An individual's behavior can be different between the real and cyber worlds. The assumption of anonymity in cyberspace allows an individual's behavior to change (Sasson & Mesch, 2016). The behavior in this research is individual in the cyber world. An individual's behavior can be different between the real and cyber worlds. The assumption of anonymity in cyberspace allows an individual's behavior to change.

Social media is a medium for socializing through online interactions (Sihombing, 2017). Attitude represents an individual's evaluation of a particular stimulus (Rajput, 2015). Based on previous research, it was found that attitudes towards certain social media have a positive effect on behavioral intentions to continue using that social media (Boateng & Okoe, 2015; Burns & Roberts, 2013; Jang et al., 2015; Liou et al., 2016; Rajput, 2015; Tanantaputra et al., 2017). Similar research in Indonesia found

[2] https://www.kemdikbud.go.id/main/blog/2020/05/kemendikbud-terbitkan-pedoman-penyelenggaraan-belajar-dari-rumah

that attitudes toward digital information positively affected behavioral intentions to choose based on that information (Sihombing, 2019). Based on previous research, the first hypothesis in this research is H1: Students' attitudes regarding information security influence behavioral intentions related to cyber security.

Subjective norms are social pressures individuals feel to perform or not perform certain behaviors (Burns & Roberts, 2013; Curras-Perez et al., 2014; Lin & Lu, 2015; Rajput, 2015; Sommestad et al., 2019). Based on previous research, the second hypothesis in this research is H2: Subjective norms held by students influence intentions related to cyber security.

Behavioral control refers to the perceived ease or difficulty of performing a particular behavior (Abdelhamid et al., 2019; Burns & Roberts, 2013; Camara et al., 2017; Curras-Perez et al., 2014; Rajput, 2015). Based on previous research, the third hypothesis in this research is H3: Students' perceived behavioral control influences behavioral intentions related to cyber security.

One of the variables added in the TPB research that is associated with cyber security awareness is education and training about cyber security (Sommestad et al., 2019). In company practice, company leaders often provide education about company policies and views on cyber security. In this research, this variable is considered to influence attitudes regarding cyber security (Hussein & Hassan, 2017; Singh & Srivastava, 2018). Based on previous research, the fourth hypothesis in this research is H4: Education about cyber security awareness influences behavioral intentions related to cyber security.

Intentions related to cyber security influence behavior related to cyber security (Sommestad et al., 2019). An individual's intention towards something will influence that individual's behavior. When related to cyber security, research in America found that intentions regarding cyber security will influence behavior related to cyber security (Burns & Roberts, 2013; Curras-Perez et al., 2014; Hussein & Hassan, 2017). Based on previous research, the fifth hypothesis in this research is H5: Students' attitudes regarding cybersecurity influence behavior related to cybersecurity.

2. METHODOLOGY

This research consists of six variables: attitudes, subjective norms, behavioral control, education, behavioral intentions, and behavior. Attitude variables, subjective norms, and behavioral control are measured through five social media indicators: privacy settings, online friend requests, comments, security, and personal data. Meanwhile, education is measured by the number of courses obtained by respondents during their undergraduate studies, including courses on information systems, internal control, information systems control, cyber security, and information technology security. Behavioral intentions are measured through four indicators related to social media: privacy settings, online friend requests, comments, and data security on social media. Behavioral variables are measured through frequency, tendencies, and habits on social media.

The respondents of this research are students from accounting study programs and study programs similar to accounting study programs who are still active students in Indonesia. Data was collected through online questionnaires by the approach taken in previous research (Foth, 2016).

3. RESULTS AND DISCUSSIONS

The six variables in this research are arranged in a research model as listed in Figure 1.

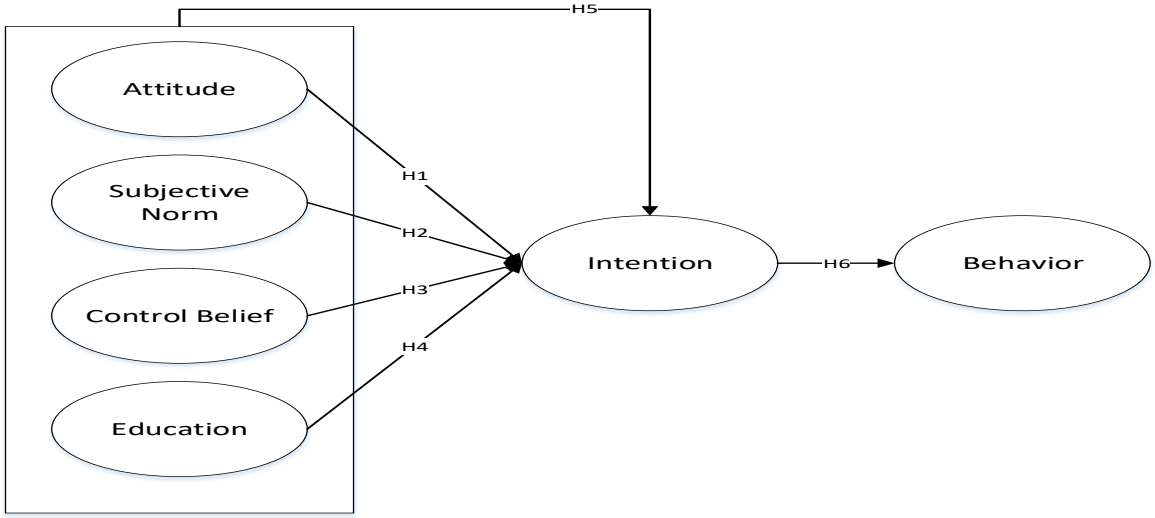

Figure 1: Research Model

Source: processed data (2021)

This research uses two regression models to test the six hypotheses proposed. The first model is used to test the first to fifth hypotheses with the following regression equation: Behavioral intention = β0 + β1 (Attitude) + β2 (Norms) + β3 (Behavior Control) + β4 (Education) + ε.

The second model tests the sixth hypothesis with the following regression equation: Behavior = β1 (Behavioral intention) + ε.

From the results of distributing the questionnaire, 283 respondents were obtained whose data could be processed for this research. Respondents for this research consisted of 111 men (39 percent) and 172 women (61 percent) from 33 universities in Indonesia. The average education level related to cyber security is 1.98, which means that the average respondent only received one course at the undergraduate level related to cyber security. As many as 88 percent of respondents are always or almost always careful about privacy settings, online friend requests, comments, and protecting personal data on social media. Most respondents (61 percent) are confident in their ability to be careful in privacy settings, online friend requests, comments, and safeguarding personal data on social media. Most respondents (80 percent) rarely or never share personal information on social media. However, only a small portion of respondents (11 percent) took active action regarding personal security on social media. Regarding gender, there is no significant difference in the tendency to respond to friendship invitations between male respondents and female respondents. Likewise, with the tendency to provide comments containing personal opinions on social media, there is no significant difference between male and female respondents. However, regarding comments with negative content and comments with political content, female respondents have a higher average score than male respondents. The same thing was found for sharing experiences and information about newly purchased items. The average value of female respondents is higher than that of male respondents.

Before the regression test is carried out, a classical assumption test is carried out on the data that has been collected. The classical assumption test was carried out to ensure that multicollinearity and autocorrelation were not found in the data collected. In addition, testing was also carried out on data distribution to ensure that the data collected was normally distributed. Table 1 contains the regression test results for model 1, and Table 2 contains the regression test results for model 2.

Table 1: Regression Model Result 1

Variable	Coefficient	p-value
Attitude	0,344	0,000
Norm	0,081	0,080
Behavior Control	0,392	0,000
Education	-0,034	0,464
Adj. R-squared		0,412

Source: processed statistics data (2021)

In Table 1, it can be seen that attitude has a p-value smaller than 5 percent and has a positive coefficient, so it can be concluded that it can be proven that attitude has a positive effect on behavioral intentions. The results indicate that students' attitudes regarding cybersecurity influence their behavioral intentions to implement cybersecurity. This study's results align with previous research (Boateng & Okoe, 2015; Burns & Roberts, 2013; Jang et al., 2015; Liou et al., 2016; Rajput, 2015; Tanantaputra et al., 2017). It can be concluded that how an individual assesses cyber security will influence his behavioral intentions regarding his own cyber security.

Based on the TPB, attitude is the main factor determining a person's behavioral intentions. Conceptually, attitude is a person's feelings or assessment of certain behavior. An individual can choose to be supportive, neutral, or opposed to certain behavior. This attitude will undoubtedly have a strong influence on behavioral intentions. In connection with cyber security, accounting students support the importance of cyber security for themselves, so this attitude is reflected in students' behavioral intentions in carrying out cyber security for themselves. Attitudes are measured using students' awareness of privacy settings, online friend requests, comments, and protecting personal data on social media.

In TPB, a person's attitude can be influenced by the individual's assessment of whether or not something is possible to do and whether it is beneficial for him or not (Fu & Juan, 2017; Sasson & Mesch, 2016). Because behavioral attitudes greatly influence behavioral intentions, awareness of the importance of cyber security must begin as early as possible and be carried out through various channels and possibilities. Various examples of cases that have had a detrimental impact must be conveyed to students, especially during online lectures where a lot of digital data will flow and be stored on the internet.

In relation to subjective norms, this variable cannot be statistically proven to influence behavioral intentions. The results of this study are in contrast to previous research (Sommestad et al., 2019), which found that subjective norms influence behavioral intentions. In this research, an individual's subjective norm is measured by how friends think about a particular individual's cyber security awareness.

Subjective norms in the TPB approach are beliefs people or groups believe that influence certain individuals, such as family or friends (Sasson & Mesch, 2016). This research stated that for individuals entering adulthood, subjective norms are influenced by friends in their environment. The research also found a relationship between norms and the risk of online behavior. How friends who are considered close assess an individual regarding their cyber security is the focus of subjective norm assessment in this research.

In the TPB, subjective norms are also the main determining factor influencing behavioral intentions (Sasson & Mesch, 2016). Conceptually, subjective norms influence the social environment at home and on campus, influencing students to do or not do something. Based on previous research, subjective norms positively influence behavioral intentions (Alam et al., 2019; Burns & Roberts, 2013; Foltz et al., 2016; Fu & Juan, 2017; Sasson & Mesch, 2016).

In this research, subjective norms did not affect cyber security intentions. One of the causes that might influence the results of this research is the distribution of data during a pandemic like now. During the pandemic, when social restrictions and physical meetings were implemented, relationships between friends were not carried out with the same intensity as before online lectures, where friendship interactions were carried out more intensively. This could be one reason subjective norms do not affect behavioral intentions. During online lectures where students interact more with their families at home, it can be understood that the subjective norms felt by students are those of their families. In general, after someone enters adulthood, the role models they look up to are friends of the same age, not their family.

Behavioral control can be statistically proven to affect behavioral intentions at a 95 percent confidence level. The results indicate that students' behavioral control regarding cyber security influences their behavioral intentions in implementing cyber security for themselves. This study's results align with previous research (Curras-Perez et al., 2014; Rajput, 2015), which found that behavioral control positively affects behavioral intentions. Behavioral control is an individual's belief in his ability to carry out cyber security. Suppose an individual feels capable of protecting himself, for example. In that case, personal data or comments in public, generally, the person concerned will have behavioral intentions that are as adequate as his beliefs.

Active students today are known as Generation Z. This generation has been accustomed to technology since childhood and has different knowledge and habits from previous generations (Fernández-Cruz & Fernández-Díaz, 2016; Hadad, 2019). Active students today are known as Generation Z, which is a generation that has been accustomed to technology since childhood and, therefore, has different knowledge and habits from previous generations.

Behavioral control is an individual's perception of the ease or difficulty of engaging in a particular behavior, which is influenced by the individual's belief in the ability to control that particular behavior (Sasson & Mesch, 2016). This research found that the tendency for risky behavior to be carried out online was based on the perception of anonymity in the cyber world. In the context of this research, behavioral control is how an individual can be confident in his ability to carry out cyber security for himself and his social media. Behavioral control includes how a person sets their privacy on social media, whether their information can only be seen by individuals on their friends list or whether the public can see it on a wide scale. The data that a person is willing to share on social media can also measure a person's behavioral control regarding cyber security.

Behavioral control variables are variables added to the TPB as a development of the previous theory. Behavioral control is added because behavioral intentions are often not the only determinant of actual behavior. Suppose a person feels he is able to control something. In that case, his confidence in his decisions will increase, ultimately encouraging behavior by his beliefs. Suppose someone believes they can carry out cyber security for themselves. In that case, this will influence their behavioral intention to carry out cyber security.

Fluency in using social media and the habit of using anonymity among Generation Z supports students' behavioral control over cyber security. Although not everyone does it with awareness of personal security, using aliases and camera effects on personal photos is one of the safeguards on social media.

The variable added in this research to the TPB is the education variable (Sommestad et al., 2019). This variable was added because education is considered to increase student's knowledge regarding the cyber risks faced by students. It is hoped that awareness of cyber risks will increase awareness of carrying out security measures or increase the intention of cyber security behavior, which will increase cyber security behavior. However, in this study, the educational variable could not be statistically proven to influence cybersecurity behavioral intentions.

The finding that education about internal controls and cybersecurity does not affect behavioral intentions raises the question, why doesn't education influence behavior? This question can be used for further research to identify why education does not affect students' behavioral intentions in implementing cyber security for themselves. The effectiveness of education at the undergraduate level, which should be able to raise students' awareness of the importance of cyber security, has not been achieved. This aligns with the findings regarding cyber security awareness and reality because students' knowledge tends to be technical, only computer knowledge, and less attention to information security (Stanciu & Tinca, 2016). Based on these findings,

learning designs can be recommended that can encourage students to implement what they have learned (Syifa & Mochamad, 2020). Sometimes limitations arise due to the limitations of the teacher, namely only teaching theory (Syifa & Mochamad, B, 2020). Developing learning designs can solve this problem because based on previous research, learning designs that can be considered effective are role-playing models (Saptono & Brataningrum, 2019).

However, it cannot be denied that this social media habit has been formed since these students started having social media accounts. Generation Z may have had social media accounts since high school. Therefore, if it is withdrawn, then basic education should also start discussing cyber risks so that as early as possible, every individual has adequate awareness of threats in the cyber world.

Education may not be successful in creating awareness effectively because there are internal factors within students that underlie students' emotional anger, which will ultimately influence their awareness of carrying out cyber security for themselves. Based on research conducted in Indonesia, the things that underlie emotions are intelligence, emotional maturity, desire for achievement, and integrity (Sitanggang & Luthan, 2018). Therefore, it can be concluded that educational variables may not be effective because other factors have a greater influence, such as student emotions.

Simultaneously, attitudes towards behavior, subjective norms, behavioral control, and education can statistically prove their influence on behavioral intentions. The magnitude of the influence of these four variables on behavioral intentions is 41.2 percent, while other factors influence the remainder (58.8 percent). Based on previous research, various factors that can influence personal cyber security intentions are commitment to the organization where the individual is located (Khansa et al., 2018), religion and gender (Gómez et al., 2019), abilities and competencies related to security information, lack of seminars related to information technology and lack of focus related to cyber security in the accounting profession (Stanciu & Tinca, 2016), awareness of personal privacy protection, and awareness of anonymity on the internet (Weinberger et al., 2017). Based on the results of the regression test, the equation for this research is as follows: Behavioral Intention = 0.823 + 0.344 (Attitude) + 0.081 (Norms) + 0.392 (Behavior Control) – 0.034 (Education) + ε.

The second regression equation in this research model was created to observe the influence of behavioral intentions on actual behavior. TPB intends to observe or predict a person's intention to do something and, ultimately, the actual behavior that is carried out. Based on statistical tests, which can be seen in Table 2, behavioral intentions can be proven to influence this research. The results indicate that students' behavioral intentions regarding cybersecurity influence their behavior in implementing cybersecurity for themselves. Based on the regression test results, the equation for this research is as follows: Behavior = 1.985 + 0.227 (Behavioral Intention) + ε.

Table 2: Regression Test Result Model 2

Variable	Coefficient	p-value
Intention	0,227	0,000
R-squared		0,051

Source: processed statistics data (2021)

The assumption of anonymity in cyberspace allows an individual's behavior to change (Sasson & Mesch, 2016). Behavior can be measured through various indicators. In this research, the indicator for measuring behavior related to cyber security is the response to online friendship invitations, which is also measured through the frequency of comments. The comments referred to in this research are personal opinions, comments with political content, and comments with negative emotional content. Another indicator used in this research is a person's tendency to share personal data in the form of address, status, family, location, hobbies, recent experiences, and items purchased.

In this research, the context of behavioral intention is a person's intention to carry out cyber security for their social media. One indicator that someone has the intention to secure their social media is through the privacy settings on their social media. When someone registers to have an account on social media, privacy is set to the public. This privacy means that the public can see everything the social media account owner shares without entering their network of friends.

However, even though its influence can be proven, there are still possible limitations in the TPB, namely the existence of internal and external needs that students may feel (Natawidjaja, 2018). Another limitation that may occur is the limited active behavior of students regarding their cyber security. If we observe the descriptive results, it can be seen that behavioral attitudes towards cyber security have a higher percentage than cyber security behavior. It can be concluded that respondents have confidence that they are capable and have carried out cyber security, but when assessing behavior, such as the habit of changing passwords on social media periodically, the habit of logging out after using social media, and various other security measures, it is not yet wholly done. Alternatively, another example is if a respondent believes they have secured their data. However, the

initial settings on social media have not been changed, so what is uploaded on social media can be accessed by anyone or the public.

The results indicate that students' intentions regarding cybersecurity influence their behavior in implementing cybersecurity for themselves. This research is in contrast to previous research, where a typical behavior among students is the tendency for male students to reveal more personal data compared to women (Rafique, 2017). The R-squared in this research is five percent, indicating that behavior related to cyber security is only slightly influenced by intentions related to cyber security. There are still many other influencing factors, such as gender, age, and external factors.

The R-squared in this research is five percent, indicating that behavior related to cyber security is only slightly influenced by intentions related to cyber security. There are still many other influencing factors, such as gender, age, and external factors (Akraman et al., 2018), which states that cyber security awareness in Indonesia is still poor. The most effective way to overcome social engineering is to educate users (Iovan & Iovan, 2016), one of which is by holding seminars related to information technology given to students (Stanciu & Tinca, 2016). Therefore, adequate education that will increase student awareness of the importance of cyber security must be designed adequately by including more knowledge related to information systems, information system security, cyber security, and internal control.

Based on this research, the following practical recommendations can be developed: 1. The teaching curriculum related to internal control and cyber security must be developed to provide an adequate portion for cyber security; 2. Teaching methods must be evaluated to produce effective methods that can ensure students' awareness of the importance of cyber security and support the implementation of cyber security; 3. The need to hold guest lectures or other types of enrichment from experts or practitioners expected to inspire students, increase student awareness, and encourage application in everyday life; and 4. There is a need to increase awareness that changing the lecture method to online lectures will make students share more digital data and be continuously connected to the internet. If the laptop used contains personal data, cyber threats increase.

Meanwhile, recommendations for further research can be carried out to answer the question of why education does not affect behavioral intentions. First, research can be carried out regarding the competence of teaching lecturers to observe whether the lecturers teaching this course also have adequate cyber security awareness and apply it in practice. Second, research can be carried out on the most appropriate learning designs to support the creation of cyber security awareness, for example, with learning designs that emphasize not only theory. Third, research can also be carried out by comparing the results before and after online lectures to see whether there are any anomalies in the results of this research due to online lecture factors.

4. CONCLUSION

After conducting a comprehensive analysis of the data, it was revealed that attitudes and behavioral control are the only independent variables that significantly positively impact intentions related to cyber security out of the four studied. These factors contribute to 41.2 percent of the influence on behavioral intentions, with the remaining 58.8 percent being attributed to other factors.

Interestingly, norms and education related to cyber security did not seem to significantly affect intentions related to cyber security. However, it is important to note that positive intentions towards cyber security favorably impact behavior, despite their relatively minor impact.

Further research is required to determine the effectiveness of education related to cyber security in achieving the desired goal of increasing awareness. Therefore, it is crucial to develop educational materials that concentrate on the factors that have a constructive impact on intentions related to cyber security, such as attitude and behavioral control.

5. LIMITATION

The limitation of this research is that the amount and distribution of data are inadequate, so the results cannot be generalized. Further research can be carried out with a more significant amount and distribution of data and can also be carried out for respondents other than students.

REFERENCES

1) ABDELHAMID, M., KISEKKA, V. and SAMONAS, S. (2019). Mitigating e-services avoidance: the role of government cybersecurity preparedness. Information Computer Security, 27(1): 26–46. https://doi.org/10.1108/ICS-02-2018-0024
2) ADDAE, J. H., BROWN, M., SUN, X., TOWEY, D. and RADENKOVIC, M. (2017). Measuring attitude towards personal data for adaptive cybersecurity. Information Computer Security, 25(5): 560–579. https://doi.org/10.1108/ICS-11-2016-0085
3) AKRAMAN, R., CIWAN, C. and PRIYADI, Y. (2018). Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada

Pengguna Smartphone roid Di Indonesia. Jurnal Sistem Informasi Bisnis, 8(2): 115. https://doi.org/10.21456/vol8iss2pp115-122

4) ALAM, M. M., SAID, J. and ABD AZIZ, M. A. (2019). Role of integrity system, internal control system leadership practices on the accountability practices in the public sectors of Malaysia. Social Responsibility Journal, 15(7): 955–976. https://doi.org/10.1108/SRJ-03-2017-0051
5) ALAM, M. Z., KOUSAR, S. and REHMAN, C. A. (2019). Role of entrepreneurial motivation on entrepreneurial intentions behaviour: theory of planned behaviour extension on engineering students in Pakistan. Journal of Global Entrepreneurship Research, 9(1): 1–21. https://doi.org/10.1186/s40497-019-0175-1
6) BOATENG, H. and OKOE, A. F. (2015). Consumers' attitude towards social media advertising their behavioural response: The moderating role of corporate reputation. Journal of Research in Interactive Marketing, 9(4): 299–312. https://doi.org/10.1108/JRIM-01-2015-0012
7) BURNS, S. and ROBERTS, L. (2013). Applying the Theory of Planned Behaviour to predicting online safety behaviour. Crime Prevention Community Safety, 15(1): 48–64. https://doi.org/10.1057/cpcs.2012.13
8) CAMARA, S. K., ENG-ZISKIN, S., WIMBERLEY, L., DABBOUR, K. S. and LEE, C. M. (2017). Predicting Students' Intention to Plagiarize: an Ethical Theoretical Framework. Journal of Academic Ethics, 15(1): 43–58. https://doi.org/10.1007/s10805-016-9269-3
9) CURRAS-PEREZ, R., RUIZ-MAFE, C. and SANZ-BLAS, S. (2014). Determinants of user behaviour recommendation in social networks: An integrative approach from the uses gratifications perspective. Industrial Management Data Systems, 114(9): 1477–1498. https://doi.org/10.1108/IMDS-07-2014-0219
10) DOHERTY, N. F. and TAJUDDIN, S. T. (2018). Towards a user-centric theory of value-driven information security compliance. Information Technology People, 31(2): 348–367. https://doi.org/10.1108/ITP-08-2016-0194
11) DWI S, H., SUMARDININGSIH, S., RESPATI, D. and WIDIATMONO, R. (2013). Efektivitas Pembimbingan Karya Tulis Online Melalui Website KTI. Jurnal Kependidikan: Penelitian Inovasi Pembelajaran, 43: 116–123.
12) FERNÁNDEZ-CRUZ, F. J. and FERNÁNDEZ-DÍAZ, M. J. (2016). Generation z's teachers their digital skills. Comunicar, 24(46): 97–105. https://doi.org/10.3916/C46-2016-10
13) FOLTZ, C. B., NEWKIRK, H. E. and SCHWAGER, P. H. (2016). An Empirical Investigation of Factors that Influence Individual Behavior toward Changing Social Networking Security Settings. Journal of Theoretical Applied Electronic Commerce Research, 11(2): 2–2. https://doi.org/10.4067/S0718-18762016000200002
14) FOTH, M. (2016). Factors influencing the intention to comply with data protection regulations in hospitals: Based on gender differences in behaviour deterrence. European Journal of Information Systems, 25(2): 91–109. https://doi.org/10.1057/ejis.2015.9
15) FU, X. and JUAN, Z. (2017). Understing public transit use behavior: integration of the theory of planned behavior the customer satisfaction theory. Transportation, 44(5): 1021–1042. https://doi.org/10.1007/s11116-016-9692-8
16) GÓMEZ, M. DEL C. O., CORDERO, R. L. and MOH, L. M. (2019). Religion Sex as Factors of Individual Differences of Reification in an Intercultural-Community-Based Society. Religions, 10(L621): 1–15. https://doi.org/10.3390/rel10110621
17) HADAD, S. (2019). Challenges for Banking Services in the Knowledge Economy. Management Dynamics in the Knowledge Economy, 7(3): 337–352. https://doi.org/10.25019/MDKE/7.3.04
18) HUSSEIN, R. and HASSAN, S. (2017). Customer engagement on social media: How to enhance continuation of use. Online Information Review, 41(7):1006–1028. https://doi.org/10.1108/OIR-02-2016-0047
19) HWANG, I., KIM, D., KIM, T. and KIM, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. Online Information Review, 41(1): 2–18. https://doi.org/10.1108/OIR-11-2015-0358
20) INTERNATIONAL FEDERATION OF ACCOUNTANTS. (2019). Hbook of International Education Pronouncements.
21) IOVAN, S. and IOVAN, A.-A. (2016). From Cyber Threats To Cyber-Crime. Journal of Information Systems andOperations Management, 425–434.
22) ISACA. (2015). Cybersecurity Fundamental. ISACA Elsevier: 1–196). https://doi.org/10.1016/B978-0-08-026495-0.50007-7
23) JANG, Y.-T., CHANG, S. E. and CHEN, P.-A. (2015). Exploring social networking sites for facilitating multi-channel retailing. Multimedia Tools Applications, 74(1): 159–178. https://doi.org/10.1007/s11042-013-1430-z
24) KARLSSON, M., DENK, T. and ÅSTRÖM, J. (2018). Perceptions of organizational culture value conflicts in information security management. Information Computer Security, 26(2): 213–229. https://doi.org/10.1108/ICS-08-2017-0058
25) KAYES, I. and IAMNITCHI, A. (2017). Privacy security in online social networks: A survey. Online Social Networks Media,

3–4(April 2015): 1–21. https://doi.org/10.1016/j.osnem.2017.09.001

26) KENNEDY, S. E. (2016). The pathway to security – mitigating user negligence. Information andComputer Security, 24(3): 255–264. https://doi.org/10.1108/ICS-10-2014-0065
27) LEBEK, B., UFFEN, J., NEUMANN, M., HOHLER, B. and H. BREITNER, M. (2014). Information security awareness behavior: a theory-based literature review. Management Research Review, 37(12): 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085
28) LEWIS, P. C. J. (2020). Class Action Trends Report, Summer 2020: Class Action Risks in a Pemic. Labor Law Journal, 71(3): 165–177.
29) LIN, K. Y. and LU, H. P. (2015). Predicting mobile social network acceptance based on mobile value social influence. Internet Research, 25(1):107–130. https://doi.org/10.1108/IntR-01-2014-0018
30) LIOU, D. K., CHIH, W. H., HSU, L. C. and HUANG, C. Y. (2016). Investigating information sharing behavior: the mediating roles of the desire to share information in virtual communities. Information Systems E-Business Management, 14(2):187–216. https://doi.org/10.1007/s10257-015-0279-2
31) NATAWIDJAJA, V. (2018). The Effect of Leadership Style, Organizational Culture, Motivation The Principles's Performance Level of Junior High School. Jurnal Kependidikan: Penelitian Inovasi Pembelajaran, 2(2):262–273. https://doi.org/10.21831/jk.v2i2.9430
32) NIETO, A. and RIOS, R. (2019). Cybersecurity profiles based on human-centric IoT devices. Human-Centric Computing Information Sciences, 9(1). https://doi.org/10.1186/s13673-019-0200-y
33) NURWANAH, A., T., S., ROSIDI, R. and ROEKHUDIN, R. (2018). Determinants of tax compliance: theory of planned behavior stakeholder theory perspective. Problems Perspectives in Management, 16(4):395–407. https://doi.org/10.21511/ppm.16(4).2018.33
34) PHAM, H. C., BRENNAN, L. and RICHARDSON, J. (2017). Review of Behavioural Theories in Security Compliance Research Challenges. Proceedings of the Informing Science Information Technology Education Conference, 3722: 65–76.
35) RAFIQUE, G. M. (2017). Personal Information Sharing Behavior of University Students via Online Social Networks. Library Philosophy Practice, February.
36) RAJPUT, H. (2015). Social Networking Sites Continuance: An Application of Extended Theory of Planned Behaviour. Telecom Business Review, 8(1). https://doi.org/10.21863/tbr/2015.8.1.006
37) SALAHDINE, F. and KAABOUCH, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4). https://doi.org/10.3390/FI11040089
38) SAPTONO, L. and BRATANINGRUM, N. P. (2019). The Development of Role-Playing learning Model Design on Accounting Subject. Jurnal Kependidikan: Penelitian Inovasi Pembelajaran, 3(2): 156–171. https://doi.org/10.21831/jk.v3i2.21312
39) SASSON, H. and MESCH, G. (2016). Gender Differences in the Factors Explaining Risky Behavior Online. Journal of Youth Adolescence, 45(5):973–985. https://doi.org/10.1007/s10964-016-0465-7
40) SIHOMBING, S. O. (2019). Analysis of the Relationship Between Image, Social Media, Attitude to Predict Intention to Choose: An Empirical Investigation of Presidential Election in Indonesia. International Review of Management Marketing, 9(5): 9–16. https://doi.org/10.32479/irmm.8386
41) SIHOMBING, S. O. (2017). Predicting intention to share news through social media: An empirical analysis in Indonesian youth context. Business Economic Horizons, 13(4): 468–477. https://doi.org/10.15208/beh.2017.32
42) SINGH, S. and SRIVASTAVA, R. K. (2018). Predicting the intention to use mobile banking in India. International Journal of Bank Marketing, 36(2), 357–378. https://doi.org/10.1108/IJBM-12-2016-0186
43) SITANGGANG, N. and LUTHAN, P. L. A. (2018). The Effects of Emotional Knowledge, Emotional Reconciliation, Emotional Authenticity on the Students' Emotional Spirituality. Jurnal Kependidikan: Penelitian Inovasi Pembelajaran, 2(1): 167–180. https://doi.org/10.21831/jk.v2i1.13722
44) SOMMESTAD, T., KARLZÉN, H. and HALLBERG, J. (2019). The Theory of Planned Behavior Information Security Policy Compliance. Journal of Computer Information Systems, 59(4):344–353. https://doi.org/10.1080/08874417.2017.1368421
45) STANCIU, V. and TINCA, A. (2016). Students' awareness on information security between own perception reality – an empirical study. Accounting Management Information Systems, 15(1): 112–130.
46) SURIFAH, MUSTIATI, E., SYAIFULLAH, M. Z. and BOWO, A. N. A. (2016). Pengaruh Motivasi terhadap Minat mahasiswa Mengikuti Pendidikan Profesi Akuntansi. Jurnal Kependidikan: Penelitian Inovasi Pembelajaran, 46(2): 246–258.

47) SYIFA, F. and MOCHAMAD, B, T. (2020). Pembelajaran Teknologi Informasi Dan Komunikasi Ditinjau Dari Minat Belajar. Jurnal Kependidikan, 4(2): 256–268. https://doi.org/https://doi.org/10.21831/jk.v4i2.24418
48) TANANTAPUTRA, J., CHONG, C. W. and RAHMAN, M. S. (2017). Influence of individual factors on concern for information privacy (CFIP), a perspective from Malaysian higher educational students. Library Review, 66(4–5): 182–200. https://doi.org/10.1108/LR-05-2016-0043
49) VARGO, D., ZHU, L., BENWELL, B. and YAN, Z. (2020). Digital technology use during COVID-19 pemic: A rapid review. Human Behavior Emerging Technologies, August, 1–13. https://doi.org/10.1002/hbe2.242
50) WEINBERGER, M., ZHITOMIRSKY-GEFFET, M. and BOUHNIK, D. (2017). Factors Affecting Users' Online Privacy Literacy Among Students in Israel. Online Information Review, 41(5): 655–671. https://doi.org/10.1108/OIR-05-2016-0127