Analysis of Security Awareness in using Technology and Social Media at Muhammadiyah University of Riau

Soni
Department of Informatics Engineering
Universitas Muhammadiyah Riau

Afdhil Hafid
Department of Informatics Engineering
Universitas Muhammadiyah Riau

Didik Sudyana
Department of Informatics Engineering
STMIK Amik Riau

ABSTRACT
Students are one of the many users of technology and the internet. So that the potential for students to become victims of cybercrime continues to increase. It happens because many internet users are not careful in using it. Cybercrime will not occur if there are awareness and caution from its users who, unfortunately, there are still many users not care about this. For this reason, it is necessary to conduct an analysis related to the awareness of social media and technology users of the danger of cybercrime for students. In this research, an analysis of students' awareness is carried out in the informatics engineering study program at Muhammadiyah University of Riau to find out how much the level of awareness about the dangers of cybercrime. The analysis is based on three categories, namely social media, cyber fraud, and user awareness. From the results of the study, it was concluded that the students of the Department of Informatics Engineering had a pretty good level of awareness. In the social media category, an average level of awareness was found at 84.2%, in the Cyber Fraud category at 81.75%, and in the user awareness category at 72.7%. So based on this value, the relevant authorities can compile policies related to appropriate education for students to avoid cybercrime.

Keywords
Student awareness, cybercrime, level of awareness.

1. INTRODUCTION
The development of information technology and the internet is overgrowing. This affects the increasing use of the internet and gadgets among students and the public. Based on statistics released by [1], there are 171 million or 64.8% of Indonesia's population using the internet and 93.9% using smartphones as media in accessing the internet. Nevertheless, the increased use of this gadget has increased cybercrime. Based on data obtained from the Directorate of Cyber Crimes in the Indonesian Police [2] during January-October 2017, the National Police in Indonesia handled 1,763 cybercrime cases throughout 2017, and the most common cybercrime cases are frauds with technology, pornography, insults and also defamation.

Students very often use technology and the internet. Based on data from [1], it is stated that as many as 100% of student respondents stated that they use the internet every day so that the potential for students to become victims of cybercrime continues to increase [3].

The high case of cybercrime in Indonesia has become a threat to security stability with escalating high enough. The government and its legal instruments have not been able to balance the techniques of crimes committed by computer technology, especially on the internet and computer networks [4].

Cybercrime can be avoided if the user is careful and aware when using the internet. Then also the high rate of cybercrime can be reduced by providing information related to awareness in activities such as providing training, providing rules, or making regulations regarding awareness in using technology [5].

Unfortunately, many internet users ignore things related to vigilance. Users often do things that they think are not a problem but can cause users to become victims of cybercrime, such as writing their identity on social media, and posting about the locations visited so that anyone can find out the user's position.

For this reason, it is necessary to analyze the student's awareness regarding the use of technology and social media. In conducting this research, an analysis of the awareness of the students of the Muhammadiyah University of Riau will be carried out by distributing questionnaires to the informatics engineering department.

The results of this analysis will be useful to find out how much the level of awareness of students in the department of informatics engineering, the Muhammadiyah University of Riau towards cybercrime. The final result of this research is to find out the percentage of the level of awareness of Muhammadiyah University of Riau students towards cybercrime so that it can be input for the university to determine policies related to student safety in using technology and social media.

2. LITERATUR REVIEW
Several previous studies have been conducted related to the analysis of the use of technology. Beginning with research conducted by [6] regarding the legal awareness of students in technology and its development. The research resulted that there were 95% of students always using cellphones and laptops as a medium for technology. Then from the results of his research also resulted that some of them said that they were very compliant with the regulations in the Indonesian Law related Information and Electronic Transactions, and did not spread information that was not necessarily true.

Further research conducted by [7] regarding credit card crime. Credit card data theft that has occurred so far has been carried out by persons who understand the transaction mechanism and network techniques in the intended bank as the object of burglary. This allows parties to contribute to the theft of credit card data. The parties who stole credit card data always using a variety of techniques, such as buying customer data, falsifying documents, and setting up fake online sites.

Another study conducted [8] said that cybercrime cases were mostly experienced by women related to love scams, the communication patterns launched by cybercrimes who were

just known to victims, were more trusted, compared to direct communication from people who were known to be close. The author conducts research aimed at describing communication patterns in cybercrime cases. Criminals usually take victim data through social media owned by the victim.

Then [9] also conducted a study entitled "Cybercrime over Internet Love Scams in Malaysia: A Discussion on the Theoretical Perspectives, Connecting Factors and Keys to the Problem". His research concluded that the action of love scammers not only violates the law but also violates morals. It is vital to have a collaborative partnership framework that connects the embassy office with the police and the immigration department to combat the misuse of student visas. Even more important is that individuals themselves are equipped with the knowledge to never share their personal information with anyone by practicing several preventative measures before being deceived.

Then, [10] also researched by analyzing that many people have conversations with strangers, some even claim to be lovers. Love scan victims are also educated people. In his research also said that education and employment could not provide a guarantee that they will not be exposed to cases of love scam. Social media should be used for things that educate, in cyberspace, the community must also have moral and ethical values in using and utilizing social media to facilitate their affairs. From this research also can make other people who read to be more cautious in using social media.

3. RESEARCH METHODOLOGY

This research will use five steps to gather information and analyze the data. The research steps are carried out as follows:

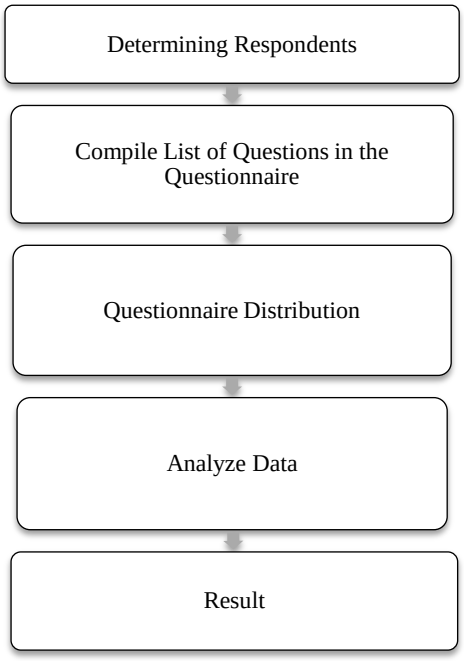

Figure 1 – Research Methodology

Figure 1 shows the five steps of research methodology, namely (1) Determining respondents (2) Compiling questionnaire and questions (3) Distributing Questionnaires (4) Data Analysis (5) Results.

4. RESULT AND DISCUSSION

4.1 Determining Respondents

Respondents were selected from the Department of Informatics Engineering, Muhammadiyah University of Riau (UMRI). At present, the total population of informatics engineering students is 574 people. Determination of the number of respondents using the Isaac and Michael Table method with an error rate of 5%. So with a total population of 574 people, based on Isaac and Michael's table, the closest number of 574 people is 600 people with a minimum sample of 221 people. So in this study using 221 people as a minimum number for the sample.

In determining sample selection, the Simple Random Sampling method is used. So the sample is chosen randomly without regard to academic levels, knowledge, and others.

4.2 Compile List of Questions in the Questionnaire

In compiling a list of questions related to student awareness analysis, the questionnaire was divided into five instruments, namely personal information, social media, online fraud, and user awareness. The detailed list of questions that have been compiled is contained in table 1.

Table 1. Question Lists

Personal Information	
1	Choose your gender. a. Male b. Female
2	How old are you? c. 17-19 d. 20-22 e. 23-25 f. 26-28 g. Above 29
SOCIAL MEDIA	
1	How many hours do you access the internet in one day? h. Below 2 hours i. 3 – 5 hours j. Above 6 hours
2	What activities do you often use using the internet [answers may be more than 1]? k. Social Media l. Online shopping m. Browsing n. Online Game o. Others

3	Choose the social media that you have and most often use it according to the selection below [answer may be more than 1]? a. Facebook b. Google Plus c. Twitter d. Instagram e. Line f. Ask.fm g. Others:
4	Do you provide an identity such as your home address, date of birth, cellphone number on your profile page? a. Yes b. No
5	Do you tell about what you are going through (like making a new post when sad) on your social media? a. Yes b. No
6	Do you often tell the location that you are visiting via social media? a. Often b. Rarely c. Never
7	Are there confidential and personal data (such as private photos, confidential chats) on social media that if it is known to the public will make things worse for you? a. Yes b. No
8	Do you accept friend requests on your social media from strangers? a. Yes b. No
9	Do you provide personal information (such as your parents' name, home address, cellphone number, or personal details) to someone you know while chatting? a. Yes b. No
10	Have others hacked your social media? a. Yes b. No
11	When your social media is hacked, does the hacker use your social media to contact or defraud your friends? a. Yes b. No If not, mention what the hacker did with your account .....
Online Fraud	
1	Do you know about cyber fraud? a. Yes b. No
2	Have you ever been a victim of online fraud? a. Ever b. Never If ever, what online fraud have you experienced?_____
User Awareness	
1	Do you know that your credit card data can be stolen online and used by wild parties? a. Know b. No, just heard this time
2	Did you know that giving your data to the internet can make you one of the targets of online crime and fraud victims? a. Know b. No, just heard this time
3	Did you know that your data (such as account password) can be stolen when you access public WiFi? a. Know b. No, just heard this time
4	Choose the actions below that you use for your internet accounts (email, social media, online shopping, etc.)! a. Use security advice recommended by the provider b. Only use a combination of suggested passwords (combined letters, numbers, symbols) c. Ignore the recommended safety recommendations because it is complicated d. A simple password, because it is easier to remember (passwords like birthdays, boyfriend's names, anniversary dates) e. Not concerned with the above, the important thing is to have an account and can be used.

4.3 Questionnaire Distribution

The questionnaire was distributed using the help of Google forms to facilitate the data collection process. Then involving several lecturers in the Informatics Engineering Department to share the Google form link to students and fill it in before the teaching and learning process begins. The process of distributing questionnaires lasted for 3 (three) months from 10 July 2019 to 15 September 2019.

Based on the results of the questionnaire data that entered the Google Form system, it was known that 316 people filled out the questionnaire form. This number has exceeded the minimum sample size of 221 people based on the predetermined Isaac and Michael tables.

4.4 Analyze Data

Obtained 316 respondent data based on the results of the distribution of questionnaires conducted for three months, obtained 316 respondent data. This number has exceeded the pre-determined minimum sample of 221 people. So then 316 respondents' data will be further analyzed.

Based on the 316 respondents, 204 (64.44%) were male, while the remaining 112 (35.4%) were female. Next, 173 (55%) of respondents were in the age range of 20-22 and 71 (22%) were in the age range of 17-19. Then as many as 57 (18%) respondents were in the age range of 23-25. According to WHO, the age range for teenagers is from 17-25 years. So that the total respondents included in the teenager's category in this study were 95%.

4.4.1. Media Social Categorization

In the social media category, the number of internet usage per day among students is quite high. This can be seen from the questionnaire, there are 162 students (51.3%) accessing the internet on average 3-5 hours a day, in the second position, 121 students (38.3%) access the internet over 6 hours while the remaining 33 students (10.4%) only uses the internet for 2 hours.

Furthermore, when using the internet, 90.5% of respondents chose social media as their primary activity. The most popular social media used by students are Instagram (83.8%) and Facebook (44.8%). So it can be seen that the use of the internet for social media is very massive used by students.

Based on the questionnaire data, it is obtained that the average student has a relatively good level of vigilance in using social media. This can be seen from the seven indicators contained in the social media category, which have excellent values. Table 2 summarizes the questionnaire data related to the seven indicators.

Table 2. Summary on Social Media Categories

Social Media	Answer	
	Yes (%)	No (%)
Share personal identities on social media profile pages	36.2	63.8
Share current situation feelings that are being experienced	18.4	81.6
Having confidential and personal data that is known to the public is bad for users	15.6	84.8
Receive friendships from strangers on social media	6.3	93.7
Share personal information with new people through chat	2.9	97.1

Furthermore, there were 18.4% of students who stated that they had never notified the most recent location they visited, and 76.2% said they rarely shared their current location. Only 5.4% stated that they often shared the current location.

Overall, Muhammadiyah University of Riau students already had a good understanding related to awareness in using social media. However, based on questionnaire data, there were 28.3% of students stating that irresponsible people had hacked their social media and 27.9% stated that their hacked accounts had been used for fraud by contacting the friendship list on their social media. Also, there are two other categories carried out by hackers on their social media accounts which can be seen in table 3.

Table 3. Summary of Hacker Activities on Hacked Account

No	Categories	Percentage
1	Just change the password without taking any action.	26.9%
2	Take action on social media accounts such as writing new statuses, deleting data, and changing social media profiles	36.5%

4.4.2. Online Fraud

In the online fraud category, based on questionnaire data, it was found that there were 15.9% of UMRI students who did not know the term cyberfraud, while the remaining 84.1% knew about cyberfraud. Then, there were 20.6% of UMRI students who had been victims of online fraud. This is quite high and quite dangerous because the number of online fraud victims can increase because there are still 15.9% of students who do not know anything about cyberfraud.

From 20.6% of students who claimed to have been victims of online fraud, there are three types of crimes committed to students and are summarized in Table 4.

Table 4. Summary type of crimes committed students

No	Categories	Percentage
1	Online shopping scams. As has already made a payment but the item purchased did not arrive or is not appropriate	84 %
2	Fraud with social engineering techniques to get a certain amount of credit	7 %
3	Fraud with social engineering techniques to get a certain amount of credit	9 %

4.4.3. User Awareness

In the category of user awareness, based on questionnaire data, it was found that 61.9% of students knew and were aware that credit card data could be stolen online and used by irresponsible parties, while 38.1% did not know it that can be seen on figure 2. This is quite a concern because there are 76.8% of students who already have a credit card. So the potential for misuse of credit cards is quite high.

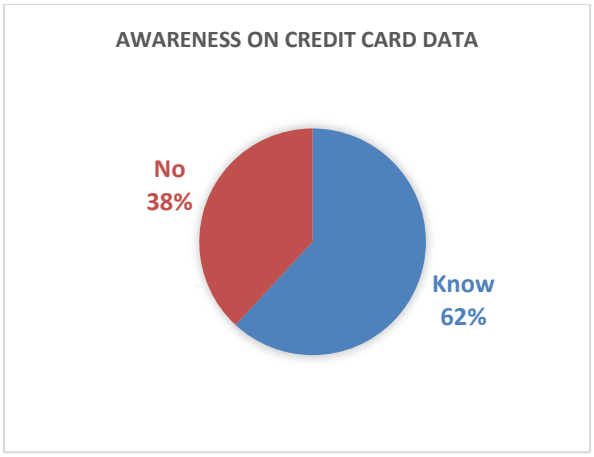

Figure 2 - Awareness of Credit Card Data

Then 85.1% of students already know and aware that providing personal data to the internet can cause cybercrime and cyber fraud. This is good because only 14.6% of students still do not know that.

The next thing to note is that there are 47.9% of students who do not know that using public wifi can pose a risk of data theft. So students still do not have the right level of awareness in this category.

Finally, in the category of user awareness related to the use of security recommendations on internet accounts such as social media, online shopping, it is known that overall students are quite concerned about the security of their accounts. This can be seen from the data obtained that there are 35.6% of students who have used all available security recommendations. Then also, 56.8% of students only use passwords following existing recommendations. Although there are only a few students who use security recommendations, the use of suggested passwords is also one aspect of security recommendations. The graphic about this category can be seen in figure 3.

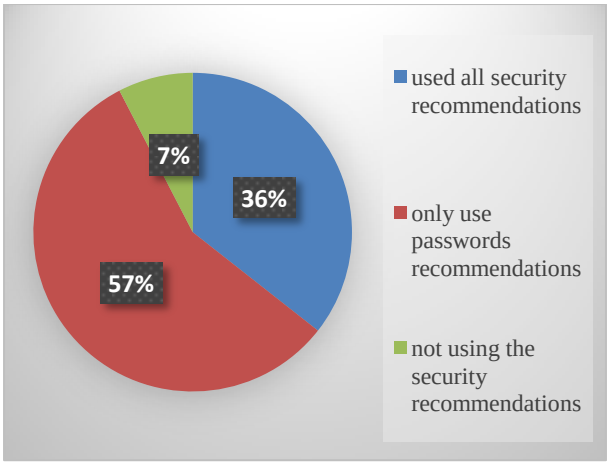

Figure 3 – Security Recommendations

However, there are still 3.7% of students still using predictable passwords such as birth dates, boyfriend names, and so on. Then there are also 2.5% of students who feel unconcerned about the security of their accounts, and there are 1.2% of students who ignore all security recommendations. Although this number is only a minority, still they could potentially become victims in the future.

4.4.4. User Awareness Level Analysis

Based on the three categories outlined previously, the overall data is summarized in Table 5 to see the average level of student awareness per category.

The average level of awareness in the social media category was obtained based on the average number of answers chosen by students from 5 questions. The consideration is because the answer "No" in this category is a choice that states whether students are aware of it or not.

The average level of online fraud is based on the average value of the answer "Yes" to the question about "knowing cyber fraud or not" and based on the average answer "Never" to the question about "becoming a victim of cyber fraud". The two average values are then averaged back to get an awareness level figure in the online fraud category.

The average level of user awareness is based on the average value of three questions with the answer "Know". Then also based on the average value for answers "following all recommendations" and "only using password recommendations". So the five indicators are used to get the average value of the level of student awareness regarding the category of user awareness.

Table 5. The Level of Student Awareness

No	Categories	Average
1	Social Media	84.2 %
2	Cyber Fraud	81.75 %
3	User Awareness	72.7%

Based on Table 5 above, it can be concluded that Muhammadiyah University of Riau students have a reasonably good level of awareness. However, the university still has to provide assistance, education or socialization for students who do not have a right level of awareness.

5. CONCLUSION

Based on the results and analysis process carried out in this study, it can be concluded that students of the department of informatics engineering at Muhammadiyah University of Riau (UMRI) have a right level of awareness with a total average value of 84.2% in the social media category, 81.75% in the Cyber category Fraud, and the category of user awareness of 72.7%. So the risk of UMRI students becoming victims of cybercrime in the future is also small because they already have a right level of awareness.

6. ACKNOWLEDGEMENT

Thanks to Minister of Research, Technology, and Higher Education of the Republic of Indonesia that funded this research on the project “Penelitian Dosen Pemula (PDP) 2019”.

7. REFERENCES

[1] Asosiasi Penyedia Jasa Internet Indonesia, “Penetrasi & Profil Perilaku Pengguna Internet Indonesia 2018,” Jakarta, 2018.

[2] P. Batubara, “Tahun 2017, Polisi Tangani 1.763 Kasus Kejahatan Siber,” okezone, Jakarta, Dec-2017.

[3] S. Wahyu, “Remaja Rentan Jadi Korban Kejahatan di Dunia Maya,” Republika, Jakarta, 09-Apr-2013.

[4] B. Suhariyanto, Tindak Pidana Teknologi Informasi

[Cybercrime] - Urgensi Pengaturan dan Celah Hukumnya. 2012.

[5] G. Bougaardt and M. Kyobe, "Investigating the factors inhibiting SMEs from recognizing and measuring losses from cybercrime in South Africa," The Electronic Journal Information Systems Evaluation, vol. 14, no. 2, pp. 167–178, 2011.

[6] L. Mahfiana, "Kesadaran hukum mahasiswa terhadap teknologi dan perkembangannya," Prosiding Seminar Nasional & Temu Ilmiah Jaringan Peneliti IAI Darussalam Blokagung Banyuwangi, pp. 1–13, 2003.

[7] N. Sulisrudatin, "Analisa Kasus Cybercrime Bidang Perbankan," Ilmiah Dirgantara, vol. 9, no. 1, pp. 26–39, 2018.

[8] C. Juditha, "(Kasus Love Scams) Communication Patterns in Cybercrime (Love Scams Case)," pp. 29–41, 2015.

[9] A. S. Hamsi, F. D. S. Bahry, S. N. M. Tobi, and M. Masrom, "Cybercrime over Internet Love Scams in Malaysia: A Discussion on the Theoretical Perspectives, Connecting Factors and Keys to the Problem," Journal of Management Research, vol. 7, no. 2, p. 169, 2015.

[10] J. Cinta, S. Di, Z. Ismail, and A. Aziz, "Love Scam in Malaysia : The Exploration of Victim Experiences," Journal of Social Sciences and Humanities, vol. 16, no. 4, pp. 1–10, 2018.