Journal of Electrical Engineering and Computer (JEECOM)
Vol. 7, No. 2 (2025), DOI: 10.33650/jeecom.v4i2
p-ISSN: 2715-0410; e-ISSN: 2715-6427

Analysis of Cybersecurity Awareness Among Social Media Users Among Teenagers Using *Exploratory Factor Analysis* (EFA) & *Confirmatory Factor Analysis* (CFA) Methods

Sofia Angela[1], Muhamat Maariful Huda[2], Rizqi Darma Rusdiyan Yusron[3]
[1,2,3] Computer Science, Faculty of Exact Sciences, Nahdlatul Ulama University of Blitar
[1]angelasofia170602@gmail.com, [2] hudha.maariful@gmail.com, [3]rizqidarma.rusdiyanyusron@gmail.com

Article Info

Article history:

Received Mey 26, 2025
Revised Juni 04, 2025
Accepted Sept 17, 2025

Keywords:

cybercrime, social media, Exploratory Factor Analysis, Confirmatory Factor Analysis, awareness.

ABSTRACT

Nowadays, security awareness is very important for social media users, especially teenagers. Many users become victims of cybercrime due to the lack of education about cybersecurity awareness. This case began with many complaints submitted by teenagers from SMP Negeri 2 Ngoro, one of whom was a victim of cybercrime on Instagram social media whose account was hijacked by unknown individuals. This also happens on WhatsApp social media where there are criminals who steal someone's identity to be used as a victim and commit fraudulent money transfers, credit and other fraud. The purpose of this study was to assess and ensure the level of cybersecurity awareness among the three most significant social media platforms in Indonesia, namely WhatsApp, Instagram, and TikTok. The Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA) methods were used to analyze the online survey data set. The EFA results obtained were 6.67% insignificant in one of the factors contained in the knowledge variable and 93.33% EFA results stated significant. Meanwhile, the CFA calculation results obtained 80% results which were stated as Fit, indicating that the model accurately represented the data, 20% of the CFA calculation results stated Moderate Fit because they reflected values that were almost close to the fit value.

Corresponding Author:
Sofia Angela,
Computer Science, Faculty of Exact Sciences, Nahdlatul Ulama University of Blitar, Jl. Masjid No.22, Kauman, Kepanjenkidul, Blitar City (66117), East Java, Indonesia
Email: angelasofia170602@gmail.com

1. INTRODUCTION

In this modern era, human life has been filled with various fields of advanced technology that make it easier for daily needs. Social media is one example of technological progress. Social media is an information tool that is needed in today's environment because it allows people to interact with each other from anywhere in the world [1]. With the development of this technology, almost all users forget about cybersecurity awareness which of course greatly affects activities in social media. But there are still many users who do not understand cybercrime on social media which results in cyber attacks being increasingly rampant on social media today.

From the many complaints submitted by teenagers from SMP Negeri 2 Ngoro, one of them was a victim of cybercrime on Instagram social media. The victim's Instagram was hijacked by an unknown person then entered the victim's account and the perpetrators of the crime updated the status of things that were not good and not pleasing and the perpetrators of the crime made trouble by sending fraudulent messages to the victim's friends asking for a certain amount of funds to be sent to the perpetrators of the crime who claimed to be the owner of the victim's account. This also happens on WhatsApp social media where there are perpetrators of crime who steal someone's identity to be used as a victim and commit fraudulent money transfers, credit and other fraud.

Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA) are two statistical methods used in factor analysis to understand the structure of relationships between variables [2]. Exploratory Factor Analysis (EFA) is a method used to explore data and identify factor structures without initial hypotheses. EFA is used to explore factor structures from previously unknown data. In cybersecurity awareness, EFA can be used to identify variables that contribute

ISSN: 2715-6427

to user awareness of cyber threats. For example, researchers can conduct EFA on survey data that measures aspects such as knowledge of cyber threats, attitudes toward cybersecurity, and personal experiences with cyber attacks. Confirmatory Factor Analysis (CFA) is used to test previously proposed models. CFA aims to confirm whether the data fits a predetermined model and test the construct validity of the measuring instrument. Based on the results of EFA, researchers formulate a conceptual model that shows the relationship between latent variables (for example: knowledge of cyber threats and attitudes toward cybersecurity). Protecting information, data, accounts, has become very important, especially for ourselves. Maintaining security for the sake of privacy that not everyone should know. Therefore, the use of cybersecurity technology is very important to protect valuable data, especially our own data [3].

This is due to the lack of awareness of the risks associated with cybercrime. In this study, researchers will observe and measure the level of awareness in terms of cybersecurity among adolescents at SMP Negeri 2 Ngoro by examining the factors of awareness, knowledge, and habits that are often carried out when interacting with cyberspace. This study was motivated by the lack of knowledge about cybersecurity. Based on these problems, researchers will observe and measure the awareness of adolescents at SMP Negeri 2 Ngoro towards cybersecurity by analyzing factors of awareness, knowledge, and habits that are often carried out when interacting with cyberspace. This study aims to determine the level of cybersecurity knowledge awareness among adolescent social media users and their behavioral patterns and to identify and measure the level of cybersecurity awareness among adolescent social media users, to find the main factors that shape cybersecurity awareness among adolescents in using social media, through exploratory factor analysis (EFA), to test the validity and reliability of the factor structure using confirmatory factor analysis (CFA), the level of cybersecurity awareness among adolescents, to provide recommendations for strategies to increase cybersecurity awareness among adolescents based on the results of factor analysis and confirmation models. Meanwhile, the benefits of this study are to broaden understanding of cybersecurity, increase awareness of cybersecurity and be able to use social media wisely so that problems such as hacking, spreading hoax news, hate speech, cyberbullying, and so on can at least be reduced in the future.

2. LITERATURE REVIEW

Previous research by Raja Rizky Riyandhika (2020) explained how cybersecurity awareness is among social media users, from the results of the study it was found that students in Indonesia already have knowledge and awareness of cybersecurity which is quite high, but the level of knowledge and awareness that is quite good is still influenced by demographic factors owned by each student in Indonesia. Factors that influence cybersecurity awareness among students in Indonesia are Age, Gender, Pocket Money and Domicile of each student. Also the factor of Education Level and Type of College, there is no influence whatsoever on the knowledge and awareness of cybersecurity of students in Indonesia [4].

This study will analyze adolescent awareness and lack of awareness of cybersecurity in using social media that is currently trending, the EFA method is used first to identify latent factors underlying the variables being measured, while CFA is used to confirm the factor structure that has been found through EFA. This approach is common in research and measurement of cybersecurity awareness so that the instruments used are valid and reliable. This study focuses on supporting variables such as Knowledge Variables, Action Variables and Attitude Variables.

From the problems above, this study was conducted in order to help many people, one of whom is among teenagers who often use social media WhatsApp, Instagram, and TikTok for their needs. This study aims to analyze awareness among teenagers towards cybersecurity in order to avoid the threat of cybercrime. And another goal is to find out various factors that can influence the level of cybersecurity awareness in social media users among teenagers at SMPN 2 Ngoro.

Many studies use EFA & CFA methods separately, for example EFA & SEM methods, CFA & SEM methods, do not combine EFA & CFA methods in detail. EFA without being continued with CFA according to researchers is still lacking because the construct validity has not been confirmed. This causes limitations in ensuring that the factors found are truly stable and can be generalized. There has been no study that specifically measures adolescent cybersecurity awareness in Indonesia using a valid and empirically tested EFA-CFA approach so that researchers use both methods.

EFA (*Exploratory Factor Analysis*)

The *Exploratory Factor Analysis* (EFA) method is a statistical methodology used to determine the latent structure of data consisting of many variables [5]. *Exploratory Factor Analysis* (EFA) is a form of factor analysis used to determine the relationship between independent variables in the development of a construct. *Exploratory Factor Analysis* (EFA) is used when researchers are unsure about the appropriate grouping of variables for a hypothesis. The absence of information about the grouping of variables usually results in a lack of knowledge about the latent variables or factors needed. Researchers are allowed to decide the number of components to be used in the study[6]. The loading factor value indicates the extent to which a variable can contribute to a particular factor in the EFA technique. The loading factor value indicates the level of relationship between the established factor and the variable. Higher loading factor values more significantly affect the grouping of each variable.

In this study using EFA in the analysis of cybersecurity awareness because of its ability to identify and group the main factors that shape awareness, reduce data complexity, validate constructs, and support further statistical analysis for a deeper and more accurate understanding of the phenomenon of cybersecurity awareness.

In other studies, problems arise when EFA results are not explored in depth. Sometimes, EFA is only used as a "black box" to generate factors, without a rich interpretation of the theoretical implications of item grouping. In addition, EFA assumptions are often not considered critically. This makes researchers interested in exploring using the CFA method.

CFA (*Confirmatory Factor Analysis*)

According to the researcher, other studies require confirmatory factor analysis (CFA) in instrument development as a better validity test tool than relying on EFA alone. Thus, research that integrates EFA and CFA can make a significant contribution to the development of valid and reliable instruments and strengthen the theoretical basis in various research fields. This emphasizes the urgency and relevance of research that uses both factor analysis approaches.

Confirmatory Factor Analysis (CFA) is a statistical technique used to evaluate the construct validity of a model, especially in the analysis of cybersecurity awareness [7]. *Confirmatory Factor Analysis* (CFA) is one of the statistical techniques used to evaluate the factor structure of a set of specific variables. The purpose of CFA is to assess the extent to which the factor structure explains the relationship between variables. In this case, CFA facilitates the formulation and assessment of hypotheses, along with the evaluation of the measurements taken [8]. CFA includes two categories of variables: latent variables (unobserved variables) and manifest variables (observed variables).
The difference between manifest and latent variables is that manifest variables can be measured directly, while latent variables are structures that cannot be measured [9].

In this study, the CFA method was used because the CFA method is a strong and appropriate method for analyzing cybersecurity awareness because it rigorously tests and validates the measurement model, ensures that the construct is reliable and valid, and supports the analysis of factors that influence complex and theory-driven awareness.

Population

Population is the entire group to be studied at a certain place and time, based on characteristics that have been selected by the researcher. The population will provide research data. Therefore, researchers will choose the target population according to their objectives [10]. An area or region is said to be populated if there are a number of people living there. Population also means a group of people, objects, or entities that can be used as a basis for sampling. Population can be used to collect statistics. Based on this, this group has characteristics that are equivalent to the conditions for solving research problems [11].

Cybersecurity

Cybersecurity is still a matter of debate and may have many meanings. Before engaging effectively, it is important to have a solid understanding of cybersecurity [12]. Cybersecurity comes from the terms cyber and security. Cyber refers to cyberspace or the internet, while security means protection. Therefore, the basic concept of cybersecurity is cyber protection. Cybersecurity encompasses the identification, mitigation, and reduction of risks associated with cyber threats and attacks, as well as any and all activities that have the potential to compromise the security of cyber system components, such as hardware, software, data, and infrastructure[13]. Cybersecurity awareness refers to an individual's ability to apply security measures when using internet network platforms, as well as having an understanding of the importance of ensuring the security of personal and organizational information in that context [14].

Understanding cybersecurity awareness is essential for businesses, companies, and individuals who utilize the internet to reduce disruptions, cyber threats, and attacks that may occur at any time. Increasing an individual's understanding of cybersecurity, including maintaining the security of personal information and ensuring the security of devices through password protection, can significantly reduce the dangers of disruptions, threats, and attacks on something. Previous studies have shown that while one has taken important initial steps in cybersecurity awareness, major challenges remain, especially in terms of social media. Cases of major data breaches and increasing cyberattacks underscore the urgency of further research to strengthen cyber resilience.

Social Media

Social media is essentially the most advanced development of new web technology based on the internet. This particular technology makes it easy for individuals to connect, participate, share, and build networks online, and also allows individuals to broadcast their own material [14].

It can be concluded that users of social media platforms use these platforms as a way to engage in social activities in the realm of cyberspace. In a broad sense, the operation of social media platforms is no different from computers. Just as computers are able to build systems, social media is able to create systems between individuals and society.

The three components of socialization related to social media are introduction, communication, and cooperation. The way users interact with social media platforms can have both positive and negative effects, depending on the nature of the social media platform itself.

In this study, researchers used the first social media, namely WhatsApp. WhatsApp is an application that is already very well known in Indonesia and throughout the world, it is currently one of the most widely used applications. This application offers many functions that can help us communicate long distance or for business matters. WhatsApp provides many advantages in communicating, but WhatsApp is also often used by online criminals, such as WhatsApp Fraud [15]. The second social media used in this study is Instagram. Instagram is one of the social media platforms that is widely used and talked about by many people. The Instagram application provides a platform for its users to upload their pictures and videos. Users can show what they are doing and provide instructions about the places they are visiting, just like when they communicate or share information. However, in the case of cybersecurity awareness, we need to be aware so that we as users of Instagram accounts are not easily hijacked by others [16]. Finally, researchers use social media Tik Tok as a research. Tik Tok is one of the most widely used social media today. You can find some public reactions that fall into the neutral, negative, or positive categories. The application admits that there is a negative impact on TikTok, considering the large number of underage users. Because users can rate videos uploaded in the comments section of the application, bullying and narcissism are the negative impacts. Users are allowed to use any language in the comments section, but this does not change the fact that the comments are offensive and even target the video uploader, leading to bullying [17].

ISSN: 2715-6427

The impact of social media is still high and the lack of cybersecurity education requires further research to develop strategies to increase awareness and user protection. The lack of education about cybersecurity causes many social media users to become victims of cybercrime such as the spread of hoaxes, hate speech, and cyberbullying. The rapid development of social media has both positive impacts and significant risks to user security and safety.

3. RESEARCH METHODS

This research was conducted in stages by utilizing the specified method. The stages of the research are as follows:

Literature Review

The literature review in this study is a critical analysis of relevant materials used to develop a theoretical framework and support the research approach. This process involves collecting, evaluating, and synthesizing information from many sources, such as books, journals, and scientific articles. Literature reviews help researchers understand the context of the problem and find new ideas. This methodology also includes inclusion and exclusion criteria for selecting appropriate literature and analysis techniques for drawing conclusions from the data that has been collected.

Observation & Interview

Research steps in collecting information or data on adolescents of SMP Negeri 2 Ngoro by means of observation conducted on adolescents in grades 7 and 8. This observation was carried out by filling out a questionnaire with questions about cybersecurity awareness. The questionnaire was designed based on three main dimensions of information security awareness, namely knowledge, attitude, and behavior. Questions were made using a Likert scale (Strongly Agree to Strongly Disagree) to measure the level of awareness quantitatively. The focus of the questions covered important aspects such as password security, wise internet use, device security, incident reporting, and awareness of the consequences of actions in cyberspace. The questionnaire was distributed online through digital survey platforms such as Google Form and WhatsApp social media to facilitate access and data collection. Respondents filled out the questionnaire independently, answering questions that had been prepared according to the specified scale. The next stage was an interview with direct questions and answers about the research.

Determination of Research Design

a. Type of Research

Descriptive Quantitative: Using a questionnaire to collect data from respondents of students of SMPN 2 Ngoro and analyze their level of awareness. Through surveys or questionnaires, the quantitative approach allows data collection from a population or sample sufficient to allow generalization of the study findings to a larger population. With quantitative data, analysis can be conducted using objective and measurable statistical techniques such as EFA and CFA, which facilitate the identification of factors that influence cybersecurity awareness systematically.

b. Research Design

Questionnaire Survey: To measure awareness and knowledge through structured questions. Here are some questions regarding cybersecurity awareness analysis :

1. I understand the characteristics of a strong password.
2. I recognize the need for periodic password updates.
3. I know about two-factor authentication (2FA).
4. I am aware of the sexual content of the video.
5. I understand the act of taking over someone else's content.
6. The action I took was that I implemented a strong password.
7. The action I will take is that I will implement periodic password changes.
8. The action I will take is that I will implement two-factor authentication (2FA) for all social media logins.
9. Actions I take to access pornographic video content.
10. The action I took was that I took over someone else's content.
11. How important do I feel it is to use a strong, different password for each account.
12. How important is it for me to be aware of the dangers & risks of cybercrime.
13. How important is it for me to be aware of not being easily fooled by hoax news.
14. How important is it for me to be aware not to spread fake news.
15. How important is it for me to be aware of not doing cyberbullying.

Research Location and Time

This research will be conducted at SMP Negeri 2 Ngoro located at Dsn. Sugo, Ds. Tambakrejo, Kec. Ngoro (61385), Kab. Mojokerto. The time used by researchers for this research is planned to be carried out in December 2024.

Research Population and Sample

Adolescents at SMPN 2 Ngoro who are active on social media and aged between 13 and 15 years are the research population for the analysis of cybersecurity awareness using the EFA and CFA methods. Researchers used a sampling strategy involving an online survey distributed to SMPN 2 Ngoro students via WhatsApp groups. This was done after researchers determined the size of the population. The sampling of 100 questionnaires for cybersecurity awareness analysis is based on several reasons:

1. Representative: A sample of 100 respondents is considered representative enough for a large population, exceeding the minimum limit of 30 respondents suggested by various experts.
2. Data Validity: Collecting data from various respondents allows researchers to identify differences in awareness analysis.
3. Time Efficiency: Using 100 respondents allows for faster data collection compared to larger samples.

This study aims to understand the factors that influence cybersecurity awareness through primary data collection from questionnaires distributed online.

Analysis test using the *Exploratory Factor Analysis* (EFA) Method

In the analysis of cybersecurity awareness, EFA can help group factors that influence user awareness of cybersecurity, especially among social media users.

Analysis test using the *Confirmatory Factor Analysis* (CFA) Method

This method allows researchers to determine the extent to which the measured variables are in accordance with existing theories. The following are the steps and relevant results of the application of CFA in the analysis of cybersecurity awareness.

4. RESULTS AND DISCUSSION

The data collected came from a questionnaire distributed to students of SMPN 2 NGORO. The results of this questionnaire were then collected and processed into raw data that would be used in the next procedure. The data was collected from 100 respondents with the following information:

1. Age

From the data obtained, there is a range of respondents' ages:

- 11 years old: 4 respondents
- 12 years old: 20 respondents
- 13 years old: 31 respondents
- 14 years old: 36 respondents
- 15 years old: 9 respondents

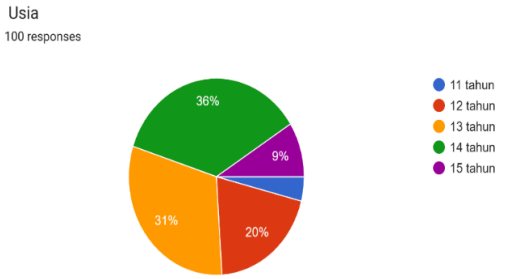

Figure 1. Pie Chart of Respondents' Age

2. Gender

From the data obtained, there were 34% male respondents and 66% female respondents.

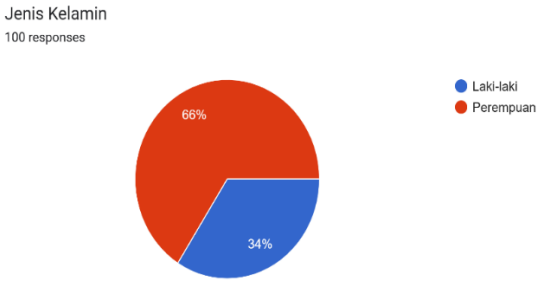

Figure 2. Pie Chart of Respondents' Gender

3. Domicile

From the respondent data obtained, there are 19% of respondents who live in the northern part of Ngoro, there are 19% of respondents who live in the southern part of Ngoro, there are 18% of respondents who live in the western part of Ngoro,

ISSN: 2715-6427

there are 41% of respondents who live in the eastern part of Ngoro, there are 3% of respondents who live outside the Ngoro area.

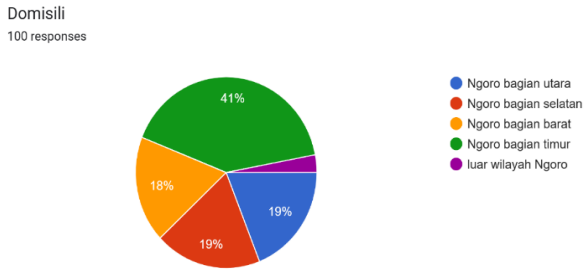

Figure 3. Pie Chart of Respondents' Domiciles

4. Class

From the respondent data obtained, there were 54% of respondents from class 7, and 46% of respondents from class 8.

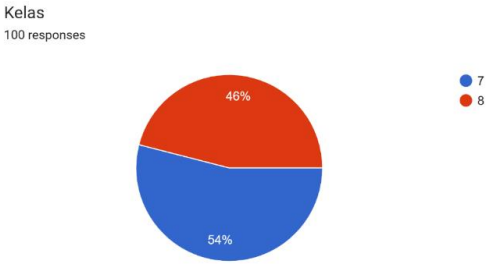

Figure 4. Pie Chart of Respondents' Class Origin

5. Social media

The social media used were taken from the 3 most widely used social media platforms, namely WhatsApp, Instagram, and Tik Tok. Based on the data obtained, 100% of respondents use WhatsApp. 85% of respondents are Instagram users, 15% are not Instagram users. And 83% of respondents are Tik Tok users, 17% are not Tik Tok users.

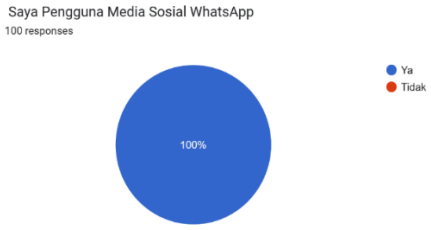

Figure 5. WhatsApp User Pie Chart

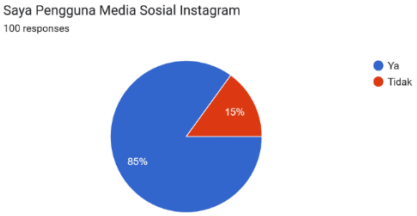

Figure 6. Instagram User Pie Chart

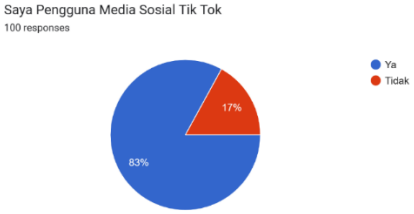

Figure 7. Tik Tok User Circle Diagram

In data collection there are several variables that support the process of filling out the questionnaire. The supporting variables are as follows:

Table 1. Supporting Variables Table

Variable	Symbol	Indicator
Knowledge Variable	P1	I understand the characteristics of a strong password.
	P2	I recognize the need for periodic password updates.
	P3	I know about two-factor authentication (2FA)
	P4	I am aware of the sexual content of the video.
	P5	I understand the act of taking over someone else's content.
Action Variable	T1	The action I took was that I implemented a strong password.
	T2	The action I will take is that I will implement periodic password changes.
	T3	The action I will take is that I will implement two-factor authentication (2FA) for all social media logins.
	T4	Actions I take to access pornographic video content
	T5	The action I took was that I took over someone else's content.
Attitude Variable	S1	How important do I feel it is to use a strong, different password for each account
	S2	How important is it for me to be aware of the dangers & risks of cybercrime
	S3	How important is it for me to be aware of not being easily fooled by hoax news
	S4	How important is it for me to be aware not to spread fake news
	S5	How important is it for me to be aware of not doing cyberbullying

EFA (*Exploratory Factor Analysis)*

Questionnaire data testing

- *Kaiser-Meyer-Olkin* (KMO): Calculate the KMO value to ensure that the data is suitable for factor analysis. The KMO value should be more than 0.5, and ideally more than 0.7. The results of all variables except variable P5 show that the KMO results in EFA are significant, because the results in variable P5 are less than the standard KMO value [18].

Table 2. KMO Calculation Table

Kaiser-Meyer-Olkin Test

VARIABLE	MSA	RESULTS
P1	0.753	Significant
P2	0.778	Significant
P3	0.759	Significant
P4	0.515	Significant
P5	0.495	Not Significant
T1	0.848	Significant
T2	0.721	Significant
T3	0.794	Significant
T4	0.526	Significant
T5	0.533	Significant
S1	0.908	Significant
S2	0.840	Significant
S3	0.868	Significant
S4	0.833	Significant
S5	0.776	Significant

- *Bartlett's Test of Sphericity*: Perform this test to ensure that there is a relationship between variables. Significant results ($p < 0.005$) indicate that the data can be analyzed further. The results of the *Bartlett's Test of Sphericity* calculation obtained significant results [18].

Table 3. Bartlett's Test Table

Bartlett's Test

X^2	df	p	Hasil
731.145	105.000	< 0.001	Signifikan

- *Parallel Analysis* or *Scree Plot.* This helps in determining how many factors significantly explain the variance in the data.

ISSN: 2715-6427

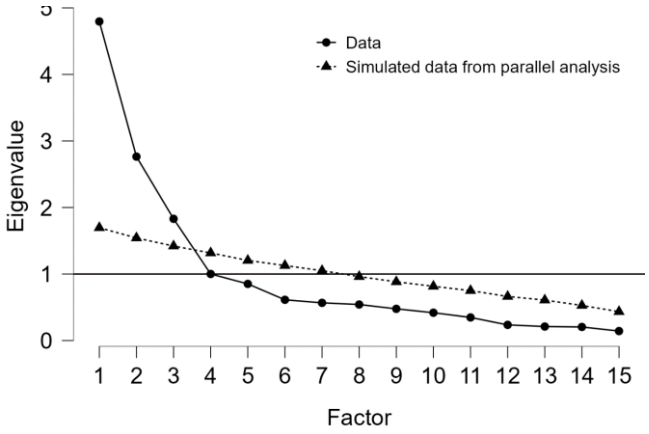

Figure 8. EFA Scree Plot

- *Factor Loading*: Review the factor loading of each item. Items with loadings above 0.4 are usually considered significant and can be considered for inclusion in the final model [18].

Table 4. Factor Loading Table

Factor Loadings (Structure Matrix)

Variable	Factor 1	Factor 2	Factor 3	Results
P1		0.752		Significant
P2		0.737		Significant
P3		0.436		Significant
P4			0.902	Significant
P5			0.363	Not Significant
T1	0.630			Significant
T2		0.629		Significant
T3		0.543		Significant
T4			0.627	Significant
T5		0.414		Significant
S1	0.576			Significant
S2	0.717			Significant
S3	0.872			Significant
S4	0.838			Significant
S5	0.731			Significant

The EFA result of 6.67% was not significant because there was 1 out of 15 variables that produced less than the standard value, namely the knowledge variable. 14 out of 15 other variables obtained a significant EFA result of 93.33% because their wealth had met the standard value of the EFA method.

CFA (*Confirmatory Factor Analysis*)

1.*Chi square*

Tabel 5. Tabel *Chi-square test*

Chi-square test

Model	X^2	df	p
Baseline model	784.771	105	
Factor model	417.150	90	< .001

Note. -

2. *Goodness of* fit test

GFI

Goodness-of-Fit Index (GFI) is one of the model fit measures used in *Confirmatory Factor Analysis* (CFA) to evaluate how well the hypothesized model fits the observed sample data[19]. GFI measures the proportion of variance and covariance in the sample covariance matrix that can be explained by the analyzed model. In the CFA goodness of fit test, the result was 0.613 which is said to be Fit where the result meets the GFI standard value.

TLI

Tucker-Lewis Index (TLI), also known as Non-Normed Fit Index (NNFI), is one of the fit indices used in Confirmatory Factor Analysis (CFA) to evaluate how well the hypothesized model fits the observed data[19]. TLI is very useful because it provides a penalty for complex models (with many parameters). In the CFA goodness of fit test, the result was 0.439 which is said to be Fit where the result meets the TLI standard value.

RSMEA

RMSEA (*Root Mean Square Error of Approximation*)

RMSEA is one of the most commonly used goodness-of-fit measures in CFA. RMSEA indicates how well a model can approximate the true model in the population. In other words, RMSEA measures the error of approximation of the model to the data[19]. A lower value indicates a superior model fit. In the CFA goodness of fit test, the result was 0.191 which is said to be Moderate Fit because the result exceeds the standard RMSEA value.

SRMR

Standardized Root Mean Square Residual (SRMR) is a fit index used in *Confirmatory Factor Analysis* (CFA), to measure the average difference between the observed correlations in the sample data and the correlations predicted by the analyzed model. SRMR measures how well the model replicates the observed covariance or correlation matrix [19]. A low SRMR value indicates that the model is able to replicate the data well, while a high value indicates a significant difference between the data and the model. In the CFA goodness of fit test, the result was 0.065 which is said to be Fit where the results meet the standard SRMR value.

CFI

Comparative Fit Index (CFI) is a fit index used in Confirmatory Factor Analysis (CFA), to evaluate how well the studied model fits the observation data [19].

CFI compares the fit of the tested model (proposed model) with the fit of the baseline model or null model (independence model). This baseline model is usually a model in which all variables are assumed to be uncorrelated with each other (independent). In the CFA goodness of fit test, the result was 0.519 which is said to be Fit where the result meets the CFI standard value.

Table 6. *Goodness of fit* test table

Indeks	Standard	Mark	Information
Goodness of fit index (GFI)	≥ 0.9	0,4256944	Fit
Tucker-Lewis Index (TLI)	≥ 0.9	0,3048611	Fit
Root mean square error of approximation (RMSEA)	≤ 0.08	0,1326389	Moderate Fit
Standardized root mean square residual (SRMR)	≤ 0.08	0.065	Fit
Comparative Fit Index (CFI)	≥ 0.9	0,3604167	Fit

It can be concluded from the table above that the research model used is stated as Fit for the GFI, TLI, SRMR, and CFI indices. The term "Fit" indicates that the model accurately represents the data. However, the RMSEA index reflects a value that is almost close to the fit value, which can be categorized as Moderate Fit. This indicates that the model is still acceptable even though it slightly exceeds the recommended standard threshold.

ISSN: 2715-6427

5. CONCLUSION

After conducting an analysis using the Exploratory Factor Analysis (EFA) method to identify the basic factor structure of the cyber awareness measurement instrument, a number of factors were obtained that met the factor loading criteria. The results of this EFA provide an initial overview of the dimensions underlying the cyber awareness construct. Furthermore, to test the validity of the factor structure that has been found and ensure the suitability of the model to the data, a Confirmatory Factor Analysis (CFA) was conducted. CFA is used to confirm the factor model formed from EFA and to assess the extent to which the model fits the empirical data. In this CFA process, a goodness-of-fit evaluation is carried out and model modifications are made if necessary to achieve a valid and reliable model in measuring cyber awareness. The results of factor exploration with confirmation steps are sequential and clear, in accordance with the practice of factor analysis commonly used in cybersecurity awareness analysis. This study aims to analyze the level of cybersecurity awareness among social media users among adolescents at SMPN 2 Ngoro. Through the use of the *Exploratory Factor Analysis* (EFA) and *Confirmatory Factor Analysis* (CFA) methods the EFA result of 6.67% is not significant in one of the factors contained in the knowledge variable, which means that the insignificant variable can consider eliminating or improving the model to improve the accuracy and strength of the model. The insignificant variable does not provide a significant contribution to the understanding of cybersecurity awareness as a whole and the EFA result of 93.33% is significant, which means that the proportion of significant variables of indicates that the model built using the EFA method has good validity and can be relied on to measure overall cybersecurity awareness. This shows that the factors analyzed truly reflect important aspects of cybersecurity awareness.. While the results of the CFA calculation obtained 80% results which were stated as Fit which indicated that the model accurately represented the data, 20% of the CFA calculation results stated Moderate Fit because they reflected values that were close to the fit value. The EFA results showed that cybersecurity awareness can be measured through several main factors, such as knowledge, Actions towards cybersecurity, and attitudes towards cybersecurity. Furthermore, the CFA results confirmed the validity and reliability of the cybersecurity awareness model formed from the EFA. This model shows that these variables significantly contribute to the overall cybersecurity awareness construct. The results of the study indicate that the level of cybersecurity awareness among adolescents at SMPN 2 Ngoro regarding knowledge of cybersecurity awareness still needs to be improved. Although most teenagers have a basic understanding of the risks of social media, there is still a lack of daily security practices and the ability to identify more complex threats. This can provide an understanding of the need for more effective education to improve cybersecurity awareness and behavior among teenagers. By increasing cybersecurity awareness, it is hoped that teenagers can use social media more safely and responsibly, and avoid various detrimental cyber threats.

ACKNOWLEDGEMENTS

The author would like to express his deepest gratitude to all parties who have provided support and assistance during the research process. Special thanks are given to the research supervisor, who has provided invaluable guidance, direction, and input in the preparation and completion of this research. The author would also like to thank Nahdlatul Ulama University of Blitar, which has provided support and the opportunity to conduct this research. Not to forget, appreciation is given to family, friends, and all parties who cannot be mentioned one by one for the moral support and motivation given. Hopefully the results of this research can provide benefits and positive contributions to the development of science.

REFERENCES

[1] D. B. M. Satata and R. Nopriyanto, "5020-23181-2-Pb," *J. Din. Sos. Budaya*, vol. 25, no. 2, pp. 86–93, 2023.
[2] E. W. Prihono, "Validitas Instrumen Kompetensi Profesional pada Penilaian Prestasi Kerja Guru," *Ekspose J. Penelit. Huk. dan Pendidik.*, vol. 18, no. 2, pp. 897–910, 2020, doi: 10.30863/ekspose.v18i2.529.
[3] N. Fauziah, N. Hartini, W. Hendriani, and F. Fajriyanthi, "Confirmatory Factor Analysis pada Pengukuran Keharmonisan Keluarga (FHS-24)," *J. Ilmu Kel. dan Konsum.*, vol. 14, no. 3, pp. 227–240, 2021, doi: 10.24156/jikk.2021.14.3.227.
[4] R. Riyandhika and R. Pratama, "Analisis Kesadaran Cybersecurity pada Kalangan Mahasiswa di Indonesia," *Uii*, vol. 1, no. 2, p. 1, 2020.
[5] R. Rosnawati, U. N. Yogyakarta, I. Artikel, E. Test, and J. Education, "ANALISIS EXPLORATORY FACTOR ANALYSIS (EFA) PADA," vol. 12, no. 3, pp. 70–76, 2024.
[6] S. E. M. S. Dr. Sigit Hermawan and S. E. M. M. Amirullah, *METODE PENELITIAN BISNIS: Pendekatan Kuantitatif & Kualitatif*. Media Nusa Creative (MNC Publishing), 2021. [Online]. Available: https://books.google.co.id/books?id=tHNMEAAAQBAJ
[7] M. F. Arkanuddin, M. A. Firmansyah, M. B. Fakhruddin, C. H. Dewani, and T. E. Kridaningsih, "The Analysis Of Satisfaction On Digital Business Sector: Expectation Confrimation Model Validation," *EKOMBIS Rev. J. Ilm. Ekon. dan Bisnis*, vol. 11, no. 2, pp. 1781–1800, 2023, doi: 10.37676/ekombis.v11i2.4843.
[8] L. Ambarwati and A. Saikhu, "ANALISIS EFEKTIVITAS APLIKASI MYITS THESIS MENGGUNAKAN

CONFIRMATORY FACTOR ANALYSIS UNTUK PENINGKATAN LAYANAN PENYELENGGARAAN UJIAN PADA PROGRAM DOKTOR ILMU KOMPUTER ANALYSIS OF THE EFFECTIVENESS OF THE MYITS THESIS APPLICATION USING CONFIRMATORY FACTOR A," vol. 9, no. 2, pp. 175–188, 2024.

[9] J. E. FoEh, K. I. Meutia, and R. Basuki, "Faktor-Faktor Yang Mempengaruhi Kinerja Karyawan RSUD S.K. Lerik Kota Kupang," *J. Kaji. Ilm.*, vol. 21, no. 3, pp. 275–292, 2021, doi: 10.31599/jki.v21i3.701.

[10] R. Priyanda *et al.*, *Metodologi Penelitian Kuantitatif*. Pradina Pustaka, 2022. [Online]. Available: https://books.google.co.id/books?id=B5t1EAAAQBAJ

[11] N. Suriani, Risnita, and M. S. Jailani, "Konsep Populasi dan Sampling Serta Pemilihan Partisipan Ditinjau Dari Penelitian Ilmiah Pendidikan," *J. IHSAN J. Pendidik. Islam*, vol. 1, no. 2, pp. 24–36, 2023, doi: 10.61104/ihsan.v1i2.55.

[12] T. Setiadi *et al.*, *Sistem Informasi Cyber Security*. CV. Gita Lentera, 2024. [Online]. Available: https://books.google.co.id/books?id=ExALEQAAQBAJ

[13] G. Rahmadi and A. R. Pratama, "Analisis Kesadaran Cyber Security pada Kalangan Pelaku e-Commerce di Indonesia," *Automata*, vol. 1, no. 2, p. 7, 2020, [Online]. Available: https://journal.uii.ac.id/AUTOMATA/article/view/15399

[14] V. A. Kairupan and A. A. Rahman, "Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Kalangan Mahasiswa Kota Bandung," *J. Darma Agung*, vol. 30, no. 1, p. 1164, 2022, doi: 10.46930/ojsuda.v30i1.3167.

[15] M. W. A. Prastya, M. Tahir, A. A. Ningrum, and A. P. Zaibintoro, "Analisis Ancaman Pishing melalui Aplikasi WhatsApp : Review Metode Studi Analisis Ancaman Pishing melalui Aplikasi WhatsApp : Review Metode Studi Literatur," no. May, 2024, doi: 10.32672/jnkti.v7i3.7551.

[16] N. F. Utami and N. Yuliati, "Pemanfaatan Media Sosial Instagram sebagai Media Informasi," *Bandung Conf. Ser. Public Relations*, vol. 2, no. 2, 2022, doi: 10.29313/bcspr.v2i2.3334.

[17] Y. H. Pratama, "The Role of Multimedia Platforms in Education : A Study on TikTok Usage by Generation Z," vol. 2, no. 2, pp. 58–63, 2024.

[18] Princen, D. Sugianto, and E. J. Simanjuntak, "Pengembangan Skala Cyberchondria Versi Pendek," *J. Penelit. dan Pengukuran Psikol. JPPP*, vol. 13, no. 1, pp. 34–42, 2024, doi: 10.21009/jppp.131.05.

[19] L. Bognár and L. Bottyán, "Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students," *Educ. Sci.*, vol. 14, no. 6, 2024, doi: 10.3390/educsci14060588.