Analysis of Public Awareness of Cybercrime in The Form of Adware

Suprih Murdyantara[1*], Kholiq Budiman[2]
[1,2]Affiliation, Institution, City, Country
[2]Department of Computer Science, Universitas Negeri Semarang, Semarang, Indonesia
* Corresponding Author

ABSTRACT

The development of information technology has had a big impact on human life. The impact of the development of information technology is the internet, which reaches all circles of society. The development of the internet has positive and negative impacts. The positive impact of the internet is that it helps humans get information quickly and can be reached anywhere. Meanwhile, the negative impact of the internet itself is the existence of cybercrime. There are various modes of cybercrime, one of which is the most often encountered by the public: adware-type malware, often known as malicious online advertising. The purpose of this study is to determine the factors that influence public awareness of cybercrime in adware. This research uses a quantitative method approach with sample criteria for respondents who live on Java Island with an age range of 18–45 years and actively use the internet. The data from the distributed questionnaires was processed with the partial least squares structural equation model (PLS-SSEM) using SmartPLS 4. The results obtained showed that of the 10 hypotheses that had been proposed, 8 were accepted. Based on these results, there are factors that influence public awareness of cybercrime, including the use of social media, cybercrime information and news, cybercrime law enforcement, and adware knowledge. Furthermore, adware knowledge is influenced by cybercrime information, news, and social media usage

ARTICLE HISTORY

Received 20 April 2024
Revision 30 April 2024
Accepted 3 Mei 2024

KEYWORD

Cybercrime Awareness
Adware
Social Media
Cybercrime Information and News
Online Advertising
Cybercrime Law Enforcement

1 Introduction

The development of technology has positive and negative impacts (Mashlahah & Arifin, 2023). The positive impact of the internet is that it helps humans get information quickly and can be reached anywhere. Meanwhile, the negative impact of the internet itself is cybercrime. Based on Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions, cybercrime can be defined as any illegal act that uses computer technology or internet networks as a means or target of crime. Under this law, various forms of cybercrime are regulated, including illegal access, interference with data or systems, and the dissemination of unlawful information.

Cybercrime has diverse impacts, affecting both devices (computer systems) and users (Wati et al., 2024). The effects can range from minor to major material losses and induce an undetectable fear of cyberspace. Victims often experience significant psychological and emotional consequences (Krisna et al., 2023). Due to boundary violations and uncertainty about online dangers, victims frequently suffer high anxiety and stress, resulting in ongoing insecurity and detrimental effects on their psychological health. Cybercrime erodes trust, a crucial component of both online and offline interactions. Victims may become more suspicious and distrustful of online platforms and people, weakening their ability to build and maintain trustworthy relationships (Hawdon, 2021). Understanding the impacts on victims highlights the importance of examining the actions of hackers in creating these situations. Hackers often seek confidential information from their victims, commonly using deceptive pop-up ads to lure internet users to dangerous links (Sriramachandramurthy et al., 2009). Victims are easily trapped by adware due to a lack of knowledge about cyber threats and the social engineering techniques hackers use, such as fake emails and websites that resemble official sites. Adware is often inserted in popular free software or through misleading pop-up ads, such as fear-inducing fake security alerts. Users who are in a hurry, don't read terms of service, or don't have updated security software are more vulnerable to these attacks. Hackers also pretend to be trusted entities to deceive users. Therefore, it is important for users to raise awareness and knowledge about cyber threats, be careful when clicking on links or downloading software, and use updated security software. Clickbait is another common method used to attract victims to harmful links (Solihin et al., 2022) These messages often contain enticing language to encourage clicks, which can lead to data theft or device damage. Many free Android/iOS applications also include pop-up ads, known as adware, which automatically display or download advertisements to the user's device (Suresh et al., 2019). Understanding adware is crucial, as it can negatively impact user experience and device security by slowing down performance, causing annoying ad disruptions, and potentially violating privacy by collecting data without consent.

Studies, such as those by Harsono et al. (2020), demonstrate how pop-up ad malware can operate, sending SMS without the user's knowledge and stealing information like IMEI and IMSI. This underscores the importance of public awareness about cybercrime to prevent such threats. Cybercrime awareness involves understanding safe practices when using the internet and the significance of protecting personal data (Afandi et al., 2017). Awareness can help individuals recognize and mitigate risks associated with cybercrime, thereby protecting sensitive information and reducing financial losses.

Research has explored factors influencing cybercrime awareness. Yadav et al. (2019) examined internet habits and cyber awareness in India, revealing that many respondents engaged in unsafe online behaviors. Other studies, such as Ramadhani and Pratama (2020) and (Pudjiarti et al., 2023), investigated how demographics affect cybercrime awareness, finding that age, residence, and education level play significant roles. Effective law enforcement is also crucial, but challenges remain due to limited resources and expertise (Habibi & Liviani, 2020).

Given the increasing prevalence of cybercrime, analyzing public awareness regarding adware and pop-up ads is vital. The constant evolution of online fraud methods necessitates staying informed about the latest threats. By understanding these threats, society can better protect itself against cybercrime. This research aims to provide a comprehensive analysis of cybercrime awareness, focusing on adware as a form of malware, and to identify factors that influence this awareness, such as cybercrime information and news, use of social media, cybercrime law enforcement, and adware knowledge.

2 Research Framework

The research framework is a conceptual model used as a theoretical basis for the research subject (Sugiyono, 2013). In addition, the framework provides a clear and logical research flow. In this study, there are three types of variables: independent variables, mediator/intervening variables, and dependent variables. The independent variables are the use of social media, cybercrime law enforcement, and cybercrime information and news. The mediator/intervening variable is adware knowledge. The dependent variable is cybercrime awareness. The description of these three variables can be seen in Figure 1.

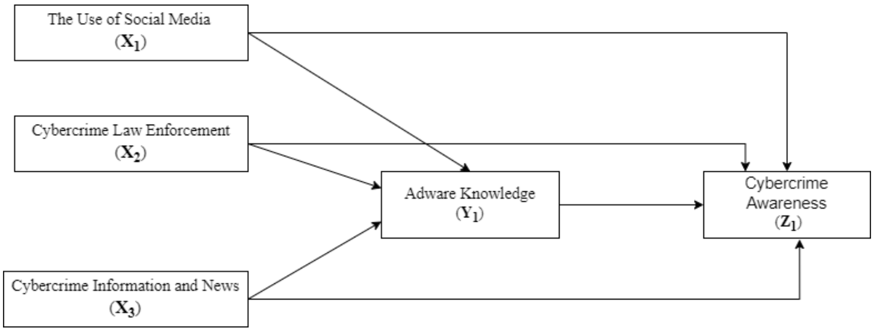

Figure 1. Research Framework

From the research framework, hypotheses for this study were developed. The proposed hypotheses are as follows:

H1: The use of social media significantly affects cybercrime awareness.
H2: The use of social media significantly affects adware knowledge.
H3: The use of social media significantly affects cybercrime awareness through adware knowledge as a mediator.
H4: Cybercrime law enforcement significantly affects cybercrime awareness.
H5: Cybercrime law enforcement significantly affects adware knowledge.
H6: Cybercrime law enforcement significantly affects cybercrime awareness through adware knowledge as a mediator.
H7: Information and news on cybercrime significantly affect cybercrime awareness.
H8: Information and news on cybercrime significantly affect adware knowledge.
H9: Information and news on cybercrime significantly affect cybercrime awareness through adware knowledge as a mediator.
H10: Adware knowledge significantly affects cybercrime awareness.

3 Method

3.1 Sample

The sampling method used is purposive sampling with predetermined sample criteria (Lenaini, 2021). The criteria for respondents are individuals aged 18 to 45 years, residing in Java, and frequent internet users. These criteria were established based on the reasoning that individuals aged 18 to 45 years have logical thinking and are considered mature (Hurlock, 1991). Additionally, they are presumed to have experienced cybercrime while using the internet, enabling them to provide honest assessments based on their experiences. In the context of sample size determination, the researcher used the Slovin's formula to determine the minimum sample size for this study. According to this formula, a minimum of 100 samples is required. The population used in this study consists of internet users on the island of Java.

3.2 Research Instrument

The research instrument utilizes a questionnaire consisting of two parts created in Google Forms, and it is distributed through social media platforms such as Facebook, Telegram, X, Instagram, and WhatsApp. The first part includes demographic profile questions of respondents, consisting of several questions: gender, education, province of residence, and experience with cybercrime. The second part contains statements indicating variables in detail, as seen in Appendix 1. This study employs measurements using a 5-point Likert scale with two types of questions: positive and negative. For positive questions, the five response options are as follows: strongly disagree with a value of 1 (one), disagree with a value of 2 (two), neutral with a value of 3 (three), agree with a value of 4 (four), and strongly agree with a value of 5 (five). The opposite applies for negative questions.

3.3 Data Analysis

In this study using data analysis Partial Least Squares – Structural Equation Model (PLS-SEM). PLS-SEM is used to test and validate causal relationships between latent (unobserved) variables by examining the relationships between observed variables (indicators) that measure these latent constructs (Hair et al, 2020). here are two sub-models in this analysis, the inner model and the outer model.

3.3.1 Outer Model

The outer model is used to test the validity of data through validity and reliability. In this test, it takes at least 30 respondents to test the instrument. (Notoatmodjo, 2012). The validity of the data requires a minimum of 30 respondents to test the instrument (Notoatmodjo, 2012). In the validity test with the PLS-SEM model, there are two types of validity tests: convergent validity and discriminatory validity.

3.3.2 Inner Model

The inner model is used to examines the relationships between latent constructs to test the hypothesized causal paths or relationships (Hair et al, 2020) . The objective of the inner model is to observe the values of impact size, predictive relevance, path coefficients, and coefficients of determination (Duryadi, 2021).

4 Results and Discussion

4.1 Demographic Analysis

The total data collected was 157 with 10 data not passing the screening. Then there are 147 data that pass and are used. From the data obtained, respondents in this study were dominated by female with a percentage of 60% (88 people). Meanwhile, male have a percentage of 40% (59 people). Based on the average age, respondents aged 18-25 years dominate with a percentage of 73% (107 people). Furthermore, respondents aged 26-35 years were 25% (37 people) and the remaining 2% (3 people) of respondents aged 36-45 years. Furthermore, based on education, most respondents have the last education is SMA / SMK with a total of 86 people. The second highest number of respondents were respondents who had the last education S1 as many as 57 people. While the rest for junior high school and master's education amounted to 2 people each. For respondents with elementary and doctoral education there are none. From these results, this study has respondents who are quite well educated where the average respondent is well educated with the lowest respondent's last education being junior high school. Based on the experience of cybercrime with Respondents are considered to have known various modes and have experienced them at least once, the most common mode experienced by respondents is fraudulent message crime as many as 44 people. Furthermore, phishing as many as 36 people, then malware and hacking modes have been experienced by 33 people each. The remaining one person answered others by adding that the respondent had been a victim of fraud through e-wallets. Demographic characteristics respondents can be seen in Table 1.

Table 1. Demographic Characteristics Respondents

Respondent profile	Total	Percentage
Gender		
Male	59	40%
Female	88	60%
Age		
18-25 years	107	73%
26-35 years	37	25%
36-45 years	3	2%
Educational stage		
junior high school (SMP)	2	1.36%
High school (SMA/SMK)	86	58.50%
Undergraduate (S1)	57	38.78%
Graduate (S2)	2	1.36%
Experience of cybercrime		
Fraudulent message crime	44	29.93%
Phishing	36	24.49%
Malware	33	22.45%
Hacking	33	22.45%
Others	1	0.68%

4.2 Outer Model

4.2.1 Convergent Validity

According to Hair et al. (2017) Convergent validity is a measure of the extent to which a measure is positively related to alternative measures of the same construct. To be considered valid, each indicator must have an outer loading value greater than 0.7. The results of the calculation of the outer loading value of each indicator can be seen in Table 3 in bold.

The next stage is to calculate the Average Variance Extracted (AVE) value which aims to determine the validity of each variable based on how well each variable explains most of the variance of each indicator, with a minimum value of 50% or 0.50. This means that the variable must have an AVE value of at least 0.5 so that it can be stated that the variable is good for research (Hair et al., 2017). The result of AVE values can be seen in table 2.

Table 2. Results of AVE

Variable	***Average Variance Extracted* (AVE)**	**Information**
Information and news on cybercrime (INC)	0,538	valid
Cybercrime awareness (CA)	0,604	valid
Use of social media (USM)	0,764	valid
Adware knowledge (AK)	0,774	valid
Cybercrime law enforcement (CLE)	0,693	valid

The AVE value of each variable in this study has met the requirements with an AVE value > 0.5. This shows that all variables have been declared valid and eligible.

4.2.2 *Discriminant Validity*

In this Discriminant Validity test, data testing is carried out using the calculation of the cross loading value with the aim of knowing the Discriminant Validity of each indicator. There are conditions that must be met, namely the outer loading value of each indicator must be greater than the outer loading value on other variables. Table 3 shows the results of the calculation of the cross loading value of each indicator on all variables.

Table 3. Results of Cross Loading

	INC	**CA**	**USM**	**AK**	**CLE**
INC2	**0,889**	0,457	0,052	0,120	0,715
INC3	**0,704**	0,057	-0,298	-0,254	0,479
INC4	**0,777**	0,270	-0,036	-0,180	0,329
CA1	0,474	**0,757**	-0,032	0,068	0,683

	INC	CA	USM	AK	CLE
CA2	0,363	**0,805**	0,067	0,088	0,529
CA3	0,397	**0,774**	0,342	0,240	0,486
CA4	0,168	**0,773**	0,352	0,445	0,435
USM4	-0,198	0,113	**0,885**	0,575	-0,316
USM5	0,193	0,310	**0,863**	0,448	0,020
AK1	0,014	0,349	0,448	**0,809**	0,167
AK2	-0,081	0,253	0,596	**0,871**	-0,053
AK3	0,032	0,271	0,448	**0,935**	0,062
AK4	0,014	0,267	0,579	**0,935**	0,073
AK5	-0,092	-0,018	0,486	**0,841**	-0,143
CLE1	0,721	0,477	-0,327	-0,102	**0,872**
CLE2	0,511	0,729	0,019	0,155	**0,836**
CLE3	0,587	0,405	-0,242	-0,042	**0,787**

Table 3 shows that the outer loading value of each indicator on its variable is greater than the outer loading value of indicators on other variables. So all indicators are declared valid and qualified. The next testing stage in the Discriminant Validity test is the Fornell - Larcker criterion. This test uses the square root of the AVE of each variable to be greater than the other variables so that it can be called a valid variable. Table 4 shows the results of the Fornell - Larcker criterion calculation.

Table 4. Results of Fornell-Lacker Criterion

	INC	CA	USM	AK	CLE
INC	**0,733**				
CA	0,452	**0,777**			
USM	-0,012	0,237	**0,874**		
AK	-0,022	0,275	0,588	**0,879**	
CLE	0,709	0,689	-0,177	0,037	**0,832**

Based on Table 4, it can be seen that the AVE square root value of each variable on the same variable is higher than the value of variables on different variables. Therefore, the table has shown that the level of discriminant validity of each variable is valid.

4.2.3 Reliability

This test is a testing process to measure the extent to which a measuring instrument or research instrument is consistent and reliable in producing similar results in repeated measurements. There are conditions that must be met, namely the composite reliability value must be more than 0.7. Table 5 shows the results of the reliability test calculation.

Table 5. The Results of Reliability

Variable	*Composite reliability*
Information and news on cybercrime (INC)	0,772

Cybercrime awareness (CA)	0,859
Use of social media (USM)	0,866
Adware knowledge (AK)	0,945
Cybercrime law enforcement (CLE)	0,871

Based on Table 5, it is known that the results of the reliability test calculations show that the composite reliability value for each variable has exceeded the threshold of 0.7. Therefore, these variables meet the criteria to be considered valid and are deemed reliable for testing.

4.3 Inner Model

4.3.1 Coefficient Determination (R-square)

R-square test is used to measure the extent to which the independent variables in the regression model can explain the variation in the dependent variable. R-square is also known as the coefficient of determination, ranging from 0 to 1. There are criteria if the R-square value < 0.25 means weak, 0.25 - 0.75 means moderate, and > 0.75 means strong. Table 6 shows the results of the R-square calculation.

Table 6. Results of R-square

Variable	*R-square*	Information
Cybercrime awareness (CA)	0,440	Moderate
Adware knowledge (AK)	0,354	Moderate

Based on Table 6, it is known that the results of R-square show this research discovered that all the dependent variables are classified as moderate.

4.3.2 Effect Size (F-square)

F-square is a measure to evaluate the relative influence of influencing (exogenous) variables on influenced (endogenous) variables. The F-square criterion for a large effect is 0.35 or higher, the F-square criterion for a moderate effect is between 0.15 - 0.35 while the small effect is between 0.02 - 0.14 and less than 0.02 has no effect (Hair et al., 2020). The results of the F-square test are shown in Table 7.

Table 7. Results of F-Square

	INC	CA	USM	AK	CLE
INC		0,030		0,037	
CA					
USM		0,243		0,380	
AK		0,022			
CLE		0,834		0,005	

Based on Table 7, it is known that there are variables that show large influence criteria, namely the USM - AK and CLE - CA variables. There are also variables that show moderate influence, namely USM - CA. Meanwhile, there are three variables that have a small influence INC - CA, INC - AK, and AK - CA and there is one variable that has no influence is CLE - AK.

4.3.3 Predictive Relevance (Q-square)

Q-square is a measure used in regression analysis to gauge how well the regression model accurately predicts the dependent variable. The productive relevance of the path model can be measured using a Q-square value greater than zero (Q-square > 0) for the dependent construct of the reflection. If the Q-square value exceeds zero, then the model is considered to have predictive relevance. However, if the Q-square value is less than zero, then the model is considered to have no predictive relevance. Table 8 shows the results of the Q-square calculation.

Table 8. Results of Q-square

	Q-square	**Information**
CA	0,051	*Predictive Relevance*
AK	0,310	*Predictive Relevance*

Based on Table 8, it is known that the CA and AK variables have a Q-square value greater than 0. This proves that the dependent variable in this study shows good Predictive Relevance.

4.3.4 Path Coefficient (Hypothesis Testing)

To determine whether the hypothesis that has been formulated is accepted or rejected, bootstrapping testing is carried out on SmartPLS 4. The aim is to determine the value of the path coefficient t-statistics and p-value. Table 9 shows the results of the hypothesis test.

Table 9. results of hypothesis test

Hypothesis		***Path coefficient***	***T-statistics***	***P-value***	**Information**
H1	USM → CA	0,390	4,090	0,000	Accepted
H2	USM → AK	0,647	11,565	0,000	Accepted
H3	USM → AK → CA	0,238	4,518	0,000	Accepted
H4	CLE → CA	0,846	4,414	0,000	Accepted
H5	**CLE → AK**	**-0,068**	**1,152**	**0,249**	**Rejected**
H6	**CLE → AK → CA**	**-0,025**	**1,115**	**0,265**	**Rejected**
H7	INC → CA	0,479	2,914	0,000	Accepted
H8	INC → AK	0,363	3,763	0,005	Accepted
H9	INC → AK → CA	0,123	2,748	0,000	Accepted
H10	AK → CA	0,368	4,861	0,000	Accepted

A more detailed analysis and interpretation of the hypothesis test results is explained in the following discussion.

4.3.4.1 Hypothesis 1

Based on the results of hypothesis testing, it is known that the effect of the USM variable on CA shows a value of 0.390, indicating a positive relationship. When viewed from the t - statistics, it shows that the relationship between the two variables is significant with a value of 4.409 and the p-value is 0.000, so **H1 is accepted**. This is supported by Ramadhani & Pratama (2020) that the quality of social media usage plays a role in cybercrime awareness in society. In addition, the acceptance of H1 has proven the diffusion-innovation theory of (Lazarsfeld et al., 1944) which states that mass media has an important role in shaping public perceptions. The acceptance of H1 shows that the better the community uses social media, the better the community's awareness of cybercrime. This means that the use of social media is one of the factors that influence public awareness of cybercrime.

4.3.4.2 Hypothesis 2

Based on the results of hypothesis testing, it is known that the effect of USM variables on AK shows a value of 0.647, indicating a positive relationship. When viewed from the t - statistics, it shows that the relationship between the two variables is significant with a value of 11.565 and the p-value is 0.000, so **H2 is accepted**. The acceptance of H2 indicates that there is a positive correlation between people's level of social media usage and their knowledge of adware. The higher people's level of social media usage, the greater their understanding of the adware threat. This is reinforced by the data which shows that all indicators used to measure both variables of quality of social media usage and knowledge of adware proved to be valid and reliable.

4.3.4.3 Hypothesis 3

Based on the results of hypothesis testing, it is known that the effect of the USM variable on CA with the AK variable as a mediator shows a value of 0.238, indicating a positive relationship. When viewed from the t - statistics, it shows that the relationship between the two variables is significant with a value of 4.518 and the p-value is 0.000, so **H3 is accepted**. From these results it can be concluded that the adware knowledge variable can mediate the relationship between the social media usage variable and the cybercrime awareness variable. This means that a good knowledge of adware not only affects the way individuals use social media, but also increases their awareness of the various cybercrime threats they may face on the platform.

4.3.4.4 Hypothesis 4

Based on the results of hypothesis testing, it is known that the effect of the CLE variable on CA shows a value of 0.846, indicating a positive relationship. When viewed from the t - statistics, it shows that the relationship between the two variables is significant with a value of 4.414 and the p-value is 0.000, so **H4 is accepted**. Based on these results, it is known that cybercrime law enforcement has an influence on cybercrime awareness in society. This is also reinforced in Nurahman (2019) by stating that the existence of a cybercrime law enforcement policy has a major influence on cybercrime prevention efforts. So the importance of the role of law enforcement officials in not only handling cybercrime cases but also in efforts to educate and increase public awareness.

4.3.4.5 Hypothesis 5

Based on the results of hypothesis testing, it is known that the effect of the CLE variable on CA with the AK variable as a mediator shows a value of -0.068, indicating a negative relationship. When viewed from the t - statistics, it shows that the relationship between the two variables is significant with a value of 1.152 and the p-value is 0.249, so **H5 is rejected**. The rejection of this hypothesis proves that law enforcement has no influence on adware knowledge. The effect of cybercrime law enforcement is more focused on preventing, prosecuting, and deterring cybercrime in general, rather than increasing knowledge about adware specifically. This finding has important implications for adware countermeasure strategies.

4.3.4.6 Hypothesis 6

Based on the results of hypothesis testing, it is known that the effect of the CLE variable on CA with the AK variable as a mediator shows a value of -0.025, indicating a negative relationship. When viewed from the t - statistics, it shows that the relationship between the two variables is significant with a value of 1.115 and the p-value is 0.265, so **H6 is rejected**. Based on these results, it is concluded that the adware knowledge variable cannot mediate the relationship between the cybercrime law enforcement variable and the cybercrime awareness variable. This means that in the relationship between cybercrime law enforcement and cybercrime awareness, knowledge about adware may not be relevant and does not rule out the possibility for other factors to become mediator variables.

4.3.4.7 Hypothesis 7

Based on the results of hypothesis testing, it is known that the influence of INC variables on CA shows a value of 0.479, indicating a positive relationship. When viewed from the t - statistics, it shows that the relationship between the two variables is significant with a value of 2.914 and the p-value is 0.000, so **H7 is accepted**. These results are in line with the research of Yadav et al.(2019)where information obtained by the public affects awareness of cybercrime crimes. The acceptance of this hypothesis can be concluded that the more people receive information or news about cybercrime, the more their awareness of cybercrime will increase. Information and news about cybercrime can increase public awareness about the threats and risks associated with cybercrime security. Exposure to stories about cybercrime attacks, online fraud schemes, and information security practices can help individuals understand how important it is to protect themselves.

4.3.4.8 Hypothesis 8

Based on the results of hypothesis testing, it is known that the effect of INC variables on AK shows a value of 0.363, indicating a positive relationship. When viewed from the t - statistics, it shows that the relationship between the two variables is significant with a value of 3.763 and the p-value is 0.005, so **H8 is accepted**. Based on these results, it can be concluded that the more people get information and news about cybercrime, the more people's adware knowledge will increase. Information and news are not only through mass media but can also be through seminars or socialization regarding the mode of cybercrime more specifically discussing adware. In addition, cybercrime information and news often provide education on how to detect and prevent cyber attacks, including attacks involving adware. This information can help increase public knowledge about the signs of adware, how it works, and steps that can be taken to reduce the risk of being attacked.

4.3.4.9 Hypothesis 9

Based on the results of hypothesis testing, it is known that the effect of the USM variable on AK shows a value of 0.123, indicating a positive relationship. When viewed from the t - statistics, it shows that the relationship between the two variables is significant with a value of 2.748 and the p-value is 0.000, so **H9 is accepted**. From these results it can be concluded that the adware knowledge variable can mediate the relationship between the cybercrime information and news variable and the cybercrime awareness variable. This means that information and news about cyber developments accompanied by good adware knowledge in the community make them tend to be more sensitive to various types of cyber threats including adware.

4.3.4.10 Hypothesis 10

Based on the results of hypothesis testing, it is known that the effect of USM variables on AK shows a value of 0.368, indicating a positive relationship. When viewed from the t-statistics, it shows that the relationship between the two variables is significant with a value of 4.861 and the p-value is 0.000, so **H10 is accepted**. These results are in line with (Simpson & Simpson, 2004) where adware knowledge has an influence on cybercrime awareness. From these results it can be concluded that the better adware knowledge the community has, the more sensitive the community will be to cybercrime. Suresh et al. (2019) added that better knowledge of adware can affect individual internet usage behavior. That way, individuals who have a deep understanding of adware will be more alert to suspicious online activities, such as deceptive advertisements or potentially dangerous links.

5 Conclusion

Based on the results of the research that has been conducted, there are 8 accepted hypotheses and 2 rejected hypotheses. From the results of these hypotheses it can be concluded that the factors that influence public awareness of cybercrime include cybercrime information and news, use of social media, cybercrime law enforcement, and adware knowledge. Based on the effect size test, the most influential factor is cybercrime law enforcement followed by the use of social media, cybercrime information and news, and the factor with the least influence is adware knowledge.

Factors that influence knowledge about adware in the community are influenced by cybercrime information and news and the use of social media. Meanwhile, cybercrime law enforcement is not a factor that affects adware knowledge in the community. The most influential factor is the use of social media while cybercrime information and news have little influence.

In the influence relationship between social media use and cybercrime awareness, as well as the influence relationship between cybercrime information and news with cybercrime awareness, the adware knowledge variable has an important role as a mediator or reinforcing factor. The use of social media can increase cybercrime awareness by providing a platform for information distribution and education regarding cybercrime threats. Similarly, cybercrime information and news disseminated through various information channels can significantly increase public awareness of cybercrime risks and prevention.

6 Appendices

No	Variable	Question	Code
1	Cybercrime awareness (CA)	Do you have any knowledge about cybercrime?	CA1
		Do you know the types cybercrime what commonly happens?	CA2
		Do you know the impact of cybercrime?	CA3
		Do you consider it important to increase public knowledge about cybercrime?	CA4
		Do you know how to protect yourself from attacks cybercrime?	CA5
		Do you know the importance of using a strong and unique password in security cybercrime?	CA6
		I am aware of ignoring prize messages via SMS/WhatsApp/Telegram.	CA7
		I easily trust strangers on the internet.	CA8
		I often download officially licensed applications.	CA9
		I am conscious not to give personal information to strangers.	CA10
2	Adware knowledge (AK)	Do you know what it is adware (advertisement online which is dangerous)?	AK1
		I easily believe advertising content online.	AK2
		I am easily attracted by the appearance of advertisements online.	AK3
		I'm easily attracted to clickbait on pop-up ads.	AK4
		I am easily entertained by attractive gift offers in advertisements.	AK5
		I feel annoyed when advertising pop-up appears in the app.	AK6
		I feel annoyed when advertising pop-up appears on the website page.	AK7

		I am aware to use ad blocker on browser me.	AK8
3	Use of Social Media (USM)	I know that my private data on social media can be stolen.	USM1
		I didn't know if my social media could be hacked.	USM2
		I am aware that if I upload my personal data (such as ID card, account number and cellphone number) on social media, it could lead to crime cybercrime.	USM3
		I easily believe the advertisements that appear on my social media.	USM4
		One password for all my social media accounts.	USM5
		Use account security recommendations suggested by the application system.	USM6
4	Cybercrime law enforcement (CLE)	In my opinion, law enforcement is about crime cybercrime it's maxed out.	CLE1
		How much confidence do you have in the performance of law enforcement officials in handling cases? cybercrime in Indonesia?	CLE2
		I understand the law about crime cybercrime in Indonesia.	CLE3
5	Information and News cybercrime (INC)	Information or news about crime cybercrime, made me understand the existence of crime cybercrime.	INC1
		I am interested in news about crime cyber.	INC2
		How often do you read or watch news/information about cybercrime on social media, online, or print?	INC3
		How high is your level of concern about the issue cybercrime after reading or watching news/information about cybercrime?	INC4

7 References

Afandi, I. A., Kusyanti, A., & Wardani, N. H. (2017). Analisis hubungan kesadaran keamanan , privasi informasi , perilaku keamanan pada para pengguna media sosial Line. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *1*(9), 783–792.

Duryadi. (2021). METODE PENELITIAN ILMIAH. Metode penelitian empiris model path analysis dan analisis menggunakan SmartPLS. *Penerbit Yayasan Prima Agus Teknik*, *7*(1 SE-Judul Buku). https://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/283

Habibi, M. R., & Liviani, I. (2020). Kejahatan teknologi informasi (cyber crime) dan penanggulangannya dalam sistem hukum Indonesia. *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, *23*(2), 400–426. https://doi.org/10.15642/alqanun.2020.23.2.400-426

Hair, J. J. F., Howard, M. C., & Nitzl, C. (2020). Assessing measurement model quality in PLS-SEM using confirmatory composite analysis. *Journal of Business Research*, *109*, 101–110. https://doi.org/10.1016/j.jbusres.2019.11.069

Hair Jr, J. F., Sarstedt, M., Ringle, C. M., & Gudergan, S. S. (2017). *Advanced issues in partial least squares structural equation modeling.* New York: SAGE Publication.

Harsono, H., Sahfitri, V. S. V., & Ferdiansyah, F. (2020). Analisis forensik malware pop-up ads iklan pada platform android. *Eprints.Binadarma.Ac.Id*, http://eprints.binadarma.ac.id/3861/%0Ahttp://eprints.binadarma.ac.id/3861/1/Analisis Forensik Malware Pop-Up Ads Iklan pada Platform Android.pdf

Hawdon, J. (2021). Cybercrime: Victimization, Perpetration, and Techniques. *American Journal of Criminal Justice*, *46*(6), 837–842. https://doi.org/10.1007/s12103-021-09652-7

Hurlock, E. B. (1991). *Psikologi perkembangan : suatu pendekatan sepanjang rentang kehidupan (Edisi 5)*. Jakarta: Erlangga.

Krisna, D., Septika Sari, K., Anggraini, N., & Royani, W. (2023). Kejahatan cyber: Tinjauan psikobehavioristik. *ISTISYFA : Journal of Islamic Guidance and Conseling*, *2*(02), 256–265. https://ejournal.iainbengkulu.ac.id/index.php/istisyfa

Lazarsfeld, P. F., Berelson, B., & Gaudet, H. (1944). *The people's choice*. Columbia: Duell, Sloan & Pearce.

Lenaini, I. (2021). Teknik pengambilan sampel purposive dan snowball sampling. *Historis : Jurnal Kajian, Penelitian Dan Pengembangan Pendidikan Sejarah*, *Vol 6, No 1 (2021): JUNE*, 33–39. http://journal.ummat.ac.id/index.php/historis/article/view/4075/pdf

Notoatmodjo, S. (2012). *Metodologi penelitian kesehatan*. Jakarta: Rineka Cipta.

Nurahman, D. (2019). Nasional cybercrime law enforcement policy and the juridical evidence in national criminal law system. *Jurnal Fakultas Hukum Universitas Tulang Bawang*, *17*(2), 145–157.

Pudjiarti, E., Faizah, S., & Hardani, S. (2023). Analisa kesadaran masyarakat terhadap bahaya cybercrime pada penggunaan teknologi dan media sosial. *Bina Insani Ict Journal*, *10*(1), 210–223.

Ramadhani, M. R., & Pratama, A. R. (2020). Analisis kesadaran cybersecurity pada pengguna media sosial di Indonesia. *Automata*, *1*(2), 1–8.

Seputar undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik (uu ite). (2008). Jakarta: *Depkominfo RI*.

Simpson, P. M., & Simpson, C. L. (2004). Beware of adware : Internet user awareness *,* *Issues in Information Systems*, *V*(1), 301–307.

Solihin, Rahmawati W, Haryati, Mogot, Nurhadi, W. (2022). Tinjauan tentang clickbait media. *Jurnal Komunikasi Dan Media*, *7*(1), 74–84.

Sriramachandramurthy, R., Balasubramanian, S.K. and Alexandra Hodis, M. (2009). Spyware and adware: How do internet users defend themselves? *American Journal of Business*, *24*(2), 41–52. https://doi.org/10.1108/19355181200900010

Sugiyono. (2013). *Metode penelitian pendidikan pendekatan kuantitatif, kualitatif dan R&D*. Bandung: Alfabeta.

Suresh, S., Di Troia, F., Potika, K., & Stamp, M. (2019). An analysis of android adware. *Journal of Computer Virology and Hacking Techniques*, *15*(3), 147–160. https://doi.org/10.1007/s11416-018-0328-8

Wati, D. S., Nurhaliza, S., Sari, M. W., & Amallia, R. (2024). Dampak cyber crime terhadap keamanan nasional dan strategi penanggulangannya: Ditinjau dari penegakan hukum. *Jurnal Bevinding*, *2*(1), 44–55. https://makassar.tribunnews.com/2019/06/26/ditudingakan-salah-gunakan-data-peserta-tryout-tes-cpns-

Yadav, D., Singh, G., Dave, K., & Rai, R. S. (2019). Internet users’ habits and cyber awareness: A cross sectional study. *Pacific Business Review International*, *11*(10), 56–66.