**Journal of Informatics and Vocational Education (JOIVE)**
Vol.7, No.2, July 2024, pp. 67~77
ISSN: 2746-7813


# Analysis of Information Security Awareness Against Social Engineering Attacks

**Fariz Fakhrul Arifin*, Puspanda Hatta, Endar Suprih Wihidayat**
Department of Informatics Education, Universitas Sebelas Maret, Indonesia

**Article Info**

***Article history:***

Received Sep 28, 2022
Revised Jul 08, 2024
Accepted Jul 11, 2024

***Corresponding Author:***

Fariz Fakhrul Arifin,
Departement of Informatics Education, Universitas Sebelas Maret, Jl Ahmad Yani, Pabelan, Kartasura, Surakarta, Central Java, 57169, Indonesia.
Email:
rdnfariz@student.uns.ac.id

**ABSTRACT**

Social engineering is a significant threat to information security, where attackers manipulate users to obtain highly confidential information. These attacks can target anyone, but people who are less vigilant are especially vulnerable. In a campus environment, it is crucial that students, who will soon enter the workforce, fully understand the dangers of social engineering and the potential impact on their future employers. This study aims to determine the level of information security awareness at the V campus of UNS Pabelan, with a focus on FKIP-PTIK students from the 2019-2020 classes. The research employed quota sampling, a technique for selecting a sample from a population based on specific characteristics until a desired size is reached. Using a Google Form questionnaire to collect primary and secondary data, the study analyzed the information with a quantitative descriptive approach. The results found that key indicators—including awareness, attitude, knowledge, and behaviors related to information security against social engineering attacks—were all in a "good" category.

**Keywords:** Information security, information security awareness, social engineering attacks

## 1. INTRODUCTION

The rapid development of the internet has enabled the instantaneous exchange of information through social media, e-commerce, and messaging platforms. This exchange includes both public and confidential data. Unfortunately, when confidential information is shared, it often loses its privacy and becomes a prime target for social engineering attacks (Amin, 2014).

Information security is the practice of protecting information assets from potential threats (Sarno & Iffano, 2009). To be secure, information must meet several criteria: it must be accurate and complete (integrity), accessible only to authorized individuals (confidentiality), and available when needed (availability). However, security systems often fail and information is leaked, primarily due to a lack of security awareness among users.

Social engineering is a type of attack that exploits human psychology. These attacks typically unfold in four phases: information gathering, relationship development, exploitation, and execution (Zulkurnain et al., 2015). Victims are often unaware their information is being stolen. Therefore, the most effective defense against these attacks is user awareness and caution when sharing information. Social engineering can happen anywhere—on campus, in the office, or in the community—by taking advantage of human weaknesses.

For example, incidents of social engineering have occurred at V Campus UNS Pabelan, where students have fallen victim to phishing attacks they did not recognize. Besides phishing, other common methods include Dumpster Diving, Shoulder Surfing, and Reverse Social Engineering. Phishing is one of the most frequently used tactics, where attackers create deceptive web pages that mimic legitimate banks, social media sites, or e-commerce platforms to trick victims into revealing sensitive information (Anti-Phishing Working Group, 2014). Furthermore, attacks on social media are common due to user negligence, such as entering a username and password into a third-party website promising to increase Instagram followers.

Research by Safitri et al. (2022) confirms that security attacks on information systems are increasingly common. Cybercrime is often perpetrated by individuals or groups aiming to breach a security system to find, access, alter, or delete information. Their findings highlight that social engineering uses psychological manipulation to trick victims into making security mistakes and providing sensitive data. Hackers frequently use this technique because they understand that humans are the weakest link in any network security system.

Humans play a critical role in the success or failure of information security. As security experts Mitnick and Simon (2002) famously stated, humans, not technology, are the weakest link in the security chain. Therefore, this "human dimension" must be addressed by raising awareness of information security's importance to prevent threats.

Based on this background, this study will assess the level of information security awareness within a campus environment, which is an ideal setting to instill this knowledge before students enter the professional world. This research aims to contribute to the prevention of social engineering by promoting greater awareness. The central research question is: "What is the level of information security awareness regarding social engineering attacks within the V campus environment of UNS?".

## 2. LITERATURE REVIEW

### 2.1. INFORMATION SECURITY

According to Simons (2015), information security is the method by which users can prevent or at least detect fraud within an information-based system, where the information itself has no physical meaning. Information security is often defined by the "4Rs": Right Information, Right People, Right Time, and Right Form. This framework is considered the most efficient way to maintain and control the value of information (APCICT, 2009). Right Information refers to the accuracy and completeness of data, which ensures its integrity. Right People means that information is available only to authorized individuals, which guarantees its confidentiality. Right Time refers to the accessibility and use of information upon request by an authorized entity, ensuring its availability. Right Form refers to providing information in an appropriate and usable format. To maintain information security, the principles of confidentiality, integrity, and availability must be consistently applied when handling information.

### 2.2. INFORMATION SECURITY AWARENESS

Information security awareness is a field of security science focused on the human factors involved in protecting information assets. Knowledge, particularly from education, is the main element in creating security awareness within individuals. Additionally, understanding information technology is necessary to implement security measures effectively.

According to Schlienger & Teufel (2003), information security awareness and training programs can be divided into three parts (see Figure 1) and are explained below.

a. Education: Employees must understand why information security is critical to the organization.
b. Training: Employees need to know how to implement security practices. This includes training on security equipment and features built into applications.
c. Awareness: Education and training form the basis of a security program. A successful program moves individuals from simply "being aware" to being actively "aware" and finally "conscious" of security, which fundamentally changes the security culture.

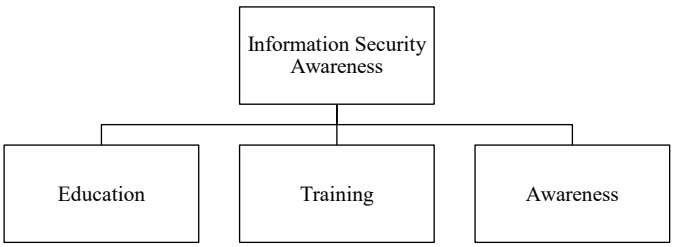


Figure 1. Security Awareness Training

### 2.3. CYBERCRIME

Cybercrime is a social problem that has emerged from societal development. Hunton (2009) defines cybercrime as a type of digital or 'hi-tech' crime that uses network technology as a primary or secondary tool.

According to Sun et al. (2015), a key difference between traditional crime and cybercrime is that evidence from a cybercrime scene exists in an electronic format. Cybercrime includes two main categories:

a. Blue-Collar Crime: This refers to conventional criminal acts, such as theft, murder, and other traditional offenses.
b. White-Collar Crime: This category is divided into four types: cooperative crimes, bureaucratic crimes, malpractice crimes, and individual crimes (Abidin, 2015).

The classifications of cybercrime are as follows:

a. Crimes Against Individuals: These crimes are committed against individuals and include the dissemination of pornography, threats, email-based harassment, defamation, hacking, email spoofing, human trafficking, phishing, credit card theft, and software piracy.
b. Crimes Against Organizations: These are crimes committed against organizations, with cyber-terrorism being the most common. This often involves the destruction of an organization's or country's public service systems to disable them.
c. Crimes Against Property: These crimes include destroying another person's data, intellectual property theft, and making threats.
d. Crimes Against Society: This includes acts like cyber-terrorism, embezzlement, selling illegal goods, data fraud, and spreading fake news by hacking public service websites.

### 2.4. SOCIAL ENGINEERING

According to Richardus Eko Indrajit (2013), social engineering is a technique for stealing confidential information by using social interaction mechanisms. In other words, it is a technique of obtaining sensitive data by exploiting human weaknesses. Hackers commonly use several types of social engineering attacks, including:

a. Phishing: This is a common attack where perpetrators attempt to obtain personal and confidential information from a target via telephone or email by posing as a trustworthy entity.
b. Spear Phishing: This is a more targeted form of phishing that focuses on specific individuals rather than a large group. This method is more difficult than a standard phishing attack because the hacker must first gather detailed information about the target, such as their characteristics, interests, and routines. A spear-phishing attack can take weeks or even months to execute, depending on the target.
c. Pop-up Windows Attack: This attack involves displaying a new pop-up window on the victim's screen. Interacting with the pop-up can trigger the installation of malicious software, which may then cause the user's internet connection to drop or be compromised.

## 3. RELATED RESEARCH

In their research, Banu and Banu (2013) explain various types of phishing attacks, from computer-based to mobile-based, and their results show that phishing remains a highly successful attack method, especially against inexperienced internet users. Amin (2014) explains that information security awareness must be continuously improved because security is not only a technical issue; human negligence is another major factor that creates security vulnerabilities. His research utilized the Information Security Index (KAMI), an evaluation tool for analyzing the security readiness of government agencies. Edwards (2015) explores the relationship between security awareness and the security behavior of home users, including how other factors intervene. His study shows that most home users are aware of security, at least in the context of computer-based social engineering.

Ghafir et al. (2016) explain that social engineering victims are often exploited to obtain information or gain system access from unsuspecting employees. Their research also presents the background of social engineering, its techniques, and defense strategies. Finally, Destya (2018) measures information security awareness using three scales: the Risky Behavior Scale (RBS), the Conservative Behavior Scale (CBS), and the Exposure to Offense Scale (EOS).

## 4. RESEARCH METHOD

### 4.1. RESEARCH APPROACH

This study uses a quantitative research approach, which involves objective measurements to collect numerical data for answering questions or testing predetermined hypotheses (Donald, 2010). According to Sugiyono (2010), quantitative research employs clear data analysis techniques directed at answering the research questions or testing formulated hypotheses.

A descriptive method was chosen to allow for a deeper exploration of the research problem, enabling the researcher to focus on specific attitudes and behaviors within a social group. Arikunto (2010) defines the quantitative descriptive method as one that aims to objectively describe a situation using numbers, encompassing data collection, interpretation, and presentation of the results. Similarly, Komalasari (2009) states that the purpose of descriptive research is to create a systematic, factual, and accurate description of the facts and characteristics of a specific research object.

### 4.2. RESEARCH VARIABLES AND OPERATIONAL DEFINITIONS

A research variable is an attribute, value, or characteristic of people, objects, or activities that has variations set by the researcher to be studied so that conclusions can be drawn (Sugiyono, 2010). The variables in this study are detailed in Table 1.

Table 1. Research Variables

| No | Variable | Indicator | Factor | Grid |
|---|---|---|---|---|
| 1 | Awareness is someone who has good abilities and can also carry out security practices well (Afandi et al., 2017) | Awareness | Aw | 1. Different platforms<br>2. Update<br>3. Account Privacy<br>4. Uploading content<br>5. Maintain digital records. |
| | Behavior, knowledge, and also attitude are components in measuring cognition, affection, and also behavior (Kearney & Kruger, 2013) | Behavior | B | 1. Scan and change passwords regularly<br>2. Attitude to receiving SMS, Email, and Spam calls.<br>3. Forwarding spam messages |
| | | Knowledge | K | 1. Using some features to support security in digital devices<br>2. Distinguishing good and bad digital track records |
| | | Attitude | At | 1. Report suspicious actions.<br>2. Save important numbers in case of suspicious actions<br>3. Re-checking the digital footprint |
| 2 | Where a successful social engineering attack uses reliable sources. | Trust | T | 1. Website cloning<br>2. Claiming to be someone convincing<br>3. Limit data sharing |
| | Behavior, knowledge, and also attitude are components in measuring cognition, affection, and also behavior (Kearney & Kruger, 2013) | Knowledge | K | 1. Understand the concept of information security<br>2. The danger of leaking an information<br>3. Can distinguish cloned websites<br>4. Understanding threats in maintaining information security |
| | | Behaviour | B | 1. Scan and change passwords regularly<br>2. Attitude to receiving SMS, Email, and Spam calls.<br>3. Forwarding spam messages<br>4. Upload relevant personal data |

### 4.3. POPULATION AND SAMPLE

A population is a complete collection of objects that share the same characteristics as the individuals in the sample group (Harland, 2011). The population for this study comprised all students from the PTIK UNS Classes of 2019 and 2020.

According to Arikunto (2009), a sample is a part or representative of the population that is considered to reflect the characteristics of the entire group. The sample for this study consisted of 20 students from the PTIK Class of 2019 and 20 students from the PTIK Class of 2020, for a total of 40 students.

### 4.4. SAMPLING TECHNIQUE

This study utilized the Quota Sampling technique. Sugiyono (2010) describes quota sampling as a technique for selecting a sample from a population that has specific characteristics until a desired number is reached. This method involves selecting typical cases from various strata of a population based on its known characteristics (Donald, 2010).

### 4.5. DATA COLLECTION TECHNIQUES

The data used in this study include primary and secondary data. Primary data is obtained directly from the research subjects, while secondary data is obtained indirectly through other parties such as institutions, libraries, or archives (Tika, 2006).

The primary data collection technique was a questionnaire. This method involves collecting data by asking respondents written questions. The purpose of the questionnaire was to obtain data on the level of information security awareness regarding cybercrime, specifically social engineering. The questionnaire, a modification of the KAMI Index Version 4.2 (May 2021), used a modified 4-point Likert scale for response options (see Table 2). The Likert scale is used to measure the attitudes, opinions, and perceptions of an individual or group regarding a social phenomenon (Riduwan, 2015).

Table 2. Likert scale

| Positive Statement | | Negative Statemnt | |
|---|---|---|---|
| **Answer** | **Score** | **Answer** | **Score** |
| Very Rare | 1 | Very Rare | 4 |
| Rare | 2 | Rare | 3 |
| Often | 3 | Often | 2 |
| Very Often | 4 | Very Often | 1 |

### 4.6. DATA ANALYSIS TECHNIQUES

#### 4.6.1. Data Description

This study uses descriptive analysis with a quantitative approach. This statistical method aims to describe or provide an overview of the research object as it exists within the population, without making broader generalizations. Descriptive analysis was performed with the assistance of the SPSS program. The data was described by calculating the Mean (Average) for each indicator and presenting the results in tables and charts.

#### 4.6.2. Mean (m)

The mean, or average, is a value that represents a group of data. It is calculated by summing all individual data points in a group and then dividing by the total number of individuals in that group (see Formula (1)).

$$m = \frac{\sum x_i}{n} \quad (1)$$

Where: M : Mean (Average)
$\Sigma X_i$ : The sum of all data scores
N : The number of data points or samples

After calculating the mean, the value for each indicator was interpreted. An indicator with a value below the overall average was considered 'weak,' while an indicator with a value above the average was considered 'strong.'

## 5. RESULT AND DISCUSSION

### 5.1. RESULT

#### 5.1.1. SESSION 1 (AWARENESS, ATTITUDES, BEHAVIOR, AND KNOWLEDGE)

##### 5.1.1.1. AWARENESS

Based on data from 7 statements related to Awareness of information security against social engineering attacks, 57.2% are in the good category (more than 50%). These statements include uploading only personal

data that is relevant to the public (77.7%), being aware of the digital footprints I left (75.6%), periodically setting up digital platform account privacy settings (65.0%), and having passwords for various digital platforms (59.8%). Meanwhile, some statements regarding awareness are in the poor category (less than 50%), including changing a password if there are indications an account is used by others (48.1%), uploading positive content (42.3%), and limiting data sharing (31.7%).

#### 5.1.1.2. ATTITUDE

Based on data from 8 statements related to Attitude on information security, 57.5% are in the good category (more than 50%). These statements include deleting data before selling or giving a device to others (82.1%), having experienced account hacks (64.2%), reporting actions related to personal data to the platform manager (64.4%), reporting digital problems encountered (61.5%), and always checking digital backtraces left behind (54.6%). Meanwhile, some statements regarding attitude are in the poor category (less than 50%). These include changing passwords regularly (41.0%), reporting to the digital device manager if there is an issue related to personal document storage (43.3%), and contacting important numbers if there is misuse of personal data (43.3%).

#### 5.1.1.3. BEHAVIOR

Based on data from 11 statements related to Behavior on information security, 58.0% are in the good category (more than 50%). These statements include changing passwords or screen patterns periodically (77.3%), performing data backups (74.2%), performing antivirus scans regularly (73.8%), performing password strength tests using free applications (71.7% and 62.9%), receiving spam emails (66.9%), and forwarding chain messages about bounties/help announcements (60.6%). Meanwhile, some statements regarding behavior are in the poor category (less than 50%). These include receiving spam SMS (40.4%), receiving spam calls (40.4% and 36.3%), clicking on links in spam emails/SMS (37.9%), and receiving chain messages about prize announcements (35.8%).

#### 5.1.1.4. KNOWLEDGE

Based on data from 7 statements related to Knowledge on information security, 76.2% are in a good category (more than 50%). These statements include reporting to the manager if there are actions related to personal data (81.7%), using a VNC application to move document files on damaged devices before service (80.0%), creating a good digital footprint (80.0%), using the Remote Wipe Feature to find digital devices (77.7%), distinguishing good and bad digital traces (77.5%), using a shredder feature to permanently delete files (77.3%), and using multiple digital device protection features (59.2%). No statements in this category were in the poor category. In every aspect of social engineering attacks—confidentiality, integrity, and availability—there are various threats. Similarly, there are various security technologies used to protect against these threats. Firewalls, IDSs, antivirus systems, and cryptographic systems are the security technologies of choice for protecting information systems in different security aspects (Bustami and Bahri, 2016).

### 5.1.2. SESSION 2 (KNOWLEDGE, TRUST, BEHAVIOR)

#### 5.1.2.1. KNOWLEDGE

Based on data from 19 statements related to Knowledge on information security, 78.8% are in the good category (more than 50%). These statements include questions like "Are there any differences in the picture below?" (98.3%), "Look at the picture below, is it necessary to use the digital protection feature?" (97.5%), "In information security, is it necessary to stay safe with anxiety about the threat of cyber-attacks?" (95.8%), and "Is the picture below a threat to information security?" (93.3%). One statement was in the poor category: "In your opinion, does using a password like this make the password stronger?" (50.0%).

#### 5.1.2.2. TRUST

Based on data from 5 statements related to Trust in information security, 67.8% are in the good category (more than 50%). These statements include questions like "If you get a call from someone on behalf of an e-commerce company saying you won a prize but they ask for your personal data, is providing it the correct step?" (91.7% answered correctly), "When getting an unknown email that contains a link, is opening the link the correct step?" (73.3% answered correctly), "Have you ever opened a link from a message like the image below?" (70.4%), and "Is it necessary to avoid sharing other people's personal data, including family?" (53.8%). One statement was in the poor category: "If you get a call from someone claiming to be from e-commerce and

they send you an OTP (One Time Password) and ask you to tell them the contents of the OTP, will you provide it?" (50.0%).

#### 5.1.2.3. BEHAVIOR

Based on data from 15 statements related to Behavior on information security, 64.7% are in the good category (more than 50%). These statements include questions like "Do you think it is necessary to test password strength using freely available applications?" (97.5%), "In your opinion, if there is an indication that your account is being used by someone else, do you need to change the password?" (96.3%), "In your opinion, is it necessary to delete data before selling or giving digital devices to others?" (71.7%), and "Do you use protection features on more than one digital device?" (71.3%). One statement was in the poor category: "In your opinion, is it necessary to periodically adjust account privacy settings on digital platforms?" (29.6%).

The Ministry of Communication and Information Technology, as the state institution responsible for communication and information technology, has the duty to raise public awareness of the importance of information security. For this reason, it is necessary to conduct research to measure the level of public awareness of information security to identify which domains need improvement as a first step in developing strategies for information security methods for IT users (Mukhlis Amin, 2014).

### 3.2. DISCUSSION

Social engineering is a crime that takes advantage of a victim's weaknesses to obtain sensitive information or data belonging to the victim. There are several common types of social engineering attacks, such as phishing, baiting, and scareware. However, these attacks can be avoided by using cybersecurity programs, spam filters, password generators, and multi-factor authentication. In addition, many other things can be done to avoid social engineering attacks. In E.B. Tylor's theory, he explains that several factors affect the occurrence of social engineering, including habits, culture, knowledge, and beliefs. A false sense of security (the belief that social engineering crimes cannot succeed due to good technology) is also a factor. This can be countered by implementing a clean desk policy, requiring data requests to be made using letters, and sending email blasts regarding information security warnings (Suharman, et al., 2017).

#### 3.2.1. ATTITUDE ON INFORMATION SECURITY AGAINST SOCIAL ENGINEERING ATTACKS

Students change their passwords regularly. This shows they are aware, particularly while learning from home, that using passwords with combinations of letters, a Personal Identity Number (PIN), and a One-Time Password (OTP) is very important in protecting data and information. Students are also aware that the smartphone devices they use need to be protected. Therefore, the solution is to reinforce cybersecurity awareness, emphasizing that the use of passwords, PINs, and OTPs is very important for protecting information and account data.

Regarding students reporting actions related to personal documents, the study shows that to create legal certainty, it is necessary to form a law that specifically, clearly, and comprehensively regulates the protection of personal data. This law must also harmonize existing regulations and establish clear mechanisms for coordination between law enforcement agencies. In this regard, the solution must be to establish norms that regulate criminal sanctions to act as a deterrent, as well as to reconstruct and reformulate current regulations on personal data protection (Situmeang, 2021).

#### 3.2.2. BEHAVIOR ON INFORMATION SECURITY AGAINST SOCIAL ENGINEERING ATTACKS

When students receive messages about prize announcements, the unwitting misuse of personal data can occur due to the negligence of potential victims in their daily activities. For example, when we receive a message about a prize that requires us to register by downloading an application or filling out a form, personal data is collected. This data can then be misused by a third party without our knowledge, potentially causing harm to the data owner. Additionally, with the development of technology, big data is now popularly used by both government and private sectors because it can process large, varied data and create accurate graphs.

When students receive spam calls, this is a similar risk. Business actors or electronic system operators may collect personal data from customers in deceptive ways. This digital data can then be traded or misused without the data owner's knowledge and permission, or it can be hijacked or hacked by third parties (Situmeang, 2021). Therefore, caution is needed when receiving spam calls in daily digital activities.

Regarding students receiving spam SMS, it is difficult to prevent irresponsible parties from sending fraudulent messages. A solution is that the Indonesian Telecommunications Regulatory Agency (BRTI)

provides a complaint service that the public can use if they receive spam SMS, whether it involves fraud, offers for venture capital, or other disturbances.

### 3.2.3. KNOWLEDGE OF INFORMATION SECURITY AGAINST SOCIAL ENGINEERING ATTACKS

The ease of obtaining information is a vulnerability factor caused by human negligence. As a result of this negligence, many companies or agencies are harmed through the theft of confidential information that should have been protected. As Purba Kuncara states, humans are the weakest link in a computer network system (Suharman, et al., 2017).

Students still don't use the shredder feature to permanently delete document files on digital devices. A file shredder is software that destroys files permanently so they cannot be recovered. When you want to permanently delete a file, simply deleting it and emptying the recycle bin is not enough, as the file can still be restored with software. The file shredder method is a good data protection solution because it permanently deletes files from the hard disk using special methods like DoD 5220.22-M or AFSSI-5020, which are typically found in file shredder software (Situmeang, 2021).

The research also obtained the following data from questionnaires about information security knowledge, beliefs, and habits.

#### 3.2.3.1. KNOWLEDGE

The knowledge of information security against social engineering attacks has good criteria with an average score of 98.3%, where students often distinguish between the images in the questionnaire. This may be because users already understand common security policies.

However, the total score for knowledge on information security is in the sufficient category (78.8%). The level of knowledge of a person is certainly different from one another. Sometimes, an employee does not know the confidentiality level of information or the methods of social engineering actors, so they are easily trapped. A low level of knowledge provides a great opportunity for attackers to get what they want (Suharman, et al., 2017).

For instance, only 50.0% of students believed a certain password example was strong, and only 51.3% recognized a suspicious link in an unknown email as a threat to information security.

#### 3.2.3.2. TRUST

Trust in information security against social engineering attacks has good criteria with an average of 67.8%. However, in this study, the level of trust is classified as low because many students showed appropriate distrust when asked if they would provide personal data to a caller claiming to be from an e-commerce company offering a prize.

Students need to avoid sharing other people's personal data, including that of family. In cybersecurity, we recognize two types of valuable data: “digital identity” (account names, passwords, OTP codes) and “personal data” (name, address, financial information). This information can be used to break into digital wallets like Go-Pay and OVO, for example, when a hacker has a user's number and sends a fraudulent message asking for an OTP code (Novi Kurnia, 2021). To prevent this, we can use strong security passwords on social media and other digital services, combining letters, numbers, and symbols so they are not easily guessed. Passwords should also be updated regularly and be different for each platform. In addition, temporary codes like OTPs must always be kept secret.

#### 3.2.3.3. BEHAVIOR

Behavior regarding information security against social engineering attacks has good criteria with an average of 64.7%. However, this level is classified as low because of a specific weakness: only 29.5% of students see the need to periodically adjust account privacy settings on digital platforms. This is illustrated by the questionnaire results where students still needed to be prompted about deleting data before selling a device or adjusting their account privacy.

Students need to periodically make account privacy settings on digital platforms. The fact that digital platforms exploit large amounts of personal data should be accompanied by a legal umbrella to prevent data leakage or Cyber Surveillance. In the context of Cyber Surveillance, there are at least three stages to determine if an act can be categorized as a violation: data collection, data analysis (including algorithmic filtering), and inspection. This means that when a digital platform has collected data from users, it can be considered Cyber Surveillance.

For files that you want to protect, you need a perfect password to ensure no one can access them without permission. A strong password is usually at least 8 characters long and includes numbers, special characters, and capital letters. Using these characters helps to avoid something easy to guess, such as the file name, your name, or a common password (like "password").

## 6. CONCLUSION

The assessment of information security awareness regarding social engineering attacks among FKIP-PTIK students at Sebelas Maret University Surakarta can be summarized as follows:

a. The results showed that the levels of awareness (57.2%), attitude (57.5%), behavior (58.0%), and knowledge (76.2%) are all in the 'good' category.
b. Furthermore, the results for knowledge (78.8%), trust (67.8%), and behavior (64.7%) were also in the 'good' category

Based on the research conducted, the following suggestions are offered:

a. For students, it is important to raise students' awareness of social engineering and its threats. This will also prepare them for the professional world, where companies should have clear information security documents, such as standards, procedures, and policies.
b. For ssocial media users, beyond simply having policies, it is crucial to increase the knowledge of social media users so they are aware of social engineering methods and the risks of a successful attack. Because humans are a weak point in the security chain, education is an essential factor.
c. For further research, tthis research can be used as a reference for future studies related to information security against social engineering attacks.

## REFERENCES


Abidin, D. Z. (2015). Kejahatan dalam teknologi informasi dan komunikasi. *Jurnal Ilmiah Media Processor, 10*(2), 1–8. http://ejournal.stikom-db.ac.id/index.php/processor/article/view/107/105

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.

Amin, M. (2014). Pengukuran tingkat kesadaran keamanan informasi menggunakan multiple criteria decision analysis (mcda). *Jurnal Penelitian Dan Pengembangan Komunikasi Dan Informatika, 5*(1), 15–24.

Anti-Phishing Working Group. (2014). *Phishing activity trends report 4th quarter 2015*.

APCICT. (2009). *Keamanan jaringan dan keamanan informasi dan privasi*.

Ardhana, Y. M. K. (2012). Keamanan sistem informasi. *Jurnal Media Aplikom, 2*(2).

Arikunto, S. (2010). *Prosedur penelitian pendekatan praktik edisi revisi VI*. Rineka Cipta.

Banu, M. N., & Banu, S. M. (2013). A comprehensive study of phishing attacks. *International Journal of Computer Science and Information Technologies, 4*(6), 783–786. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.643.766&rep=rep1&type=pdf

Birrul Amri, B. (2019). Penggunaan media sosial melunturkan identitas bangsa. *Jurnal Informatika, 4*(1).

Breda F., & T., B. H. M. (2017). *Social engineering and cyber security* [Paper presentation].

Bustami, A., & Bahri, S. (2020). Ancaman, serangan dan tindakan perlindungan pada keamanan jaringan atau sistem informasi: Systematic review. *Jurnal Pendidikan dan Aplikasi Industri (UNISTEK), 7*(2).

Chan, H., & Mubarak, S. (2011). *Information security awareness level of TAFE South Australia employees*.

Darci, H., & Harland, J. (2011). *Student research handbook*.

Destya, S. (2018). *Model pengukuran tingkat kesadaran keamanan*.

Dewi, N. C. (2011). Pengaruh penggunaan media sosial pada remaja. *Jurnal Teknik Informatika, 1*(1).

Direktorat Jenderal Aptika. (2012). *Indeks KAMI versi 2.2*. Kementerian Komunikasi dan Informatika.

Djaali, H., & M., D. P. (2000). *Pengukuran dalam bidang pendidikan*. Grasindo Publisher.

Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers and Security, 26*(1), 73–80. https://doi.org/10.1016/j.cose.2006.10.009

Edwards, K. (2015). *Examining the security awareness, information privacy, and the security behaviors of home computer user* [Disertation, College of Engineering and Computing Nova Southeastern University].

Farooq, U. (2018). Network security challenges. https://doi.org/10.13140/RG.2.2.27478.34885

Fitri, M. E. Y., & Chairoel, L. (2019). Penggunaan media sosial berdasarkan gender terhadap prestasi belajar

mahasiswa. *Jurnal Benefita, 4*(1), 162-181.
Ghafir, I., Prenosil, V., Alhejailan, A., & Hammoudeh, M. (2016). Social engineering attack strategies and defence approaches. *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*, 145–149. https://doi.org/10.1109/FiCloud.2016.28
Harriansa. (2015). *Pengertian dan teori gender*.
Hunton, P. (2009). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law and Security Review, 25*(6), 528–535. https://doi.org/10.1016/j.clsr.2009.09.005
Indrajit, R. E. (2013). Social engineering. *Encyclopedia of Information Assurance, 6*(November), 1–6. https://doi.org/10.1081/e-eia-120046852
Ivaturi, K., & Janczewski, L. (2011). *A taxonomy for social engineering attacks* [Paper presentation]. Proceedings of CONF-IRM.
Jacobs, L. C., & Sorensen, C. (2010). *Introduction to research in education* (8th ed.). Wadsworth.
Jumiati, Indarjani, S., & Destrya, D. (2011). Pembinaan kesadaran keamanan informasi di lingkungan sekolah tinggi sandi negara berdasarkan standar national institute of standard and telecommunication (NIST SP 800-100). *e-Indonesia Initiative*, 394-402.
Kearney, W. D., & Kruger, H. A. (2013). Phishing and organisational learning. *IFIP Advances in Information and Communication Technology, 405*, 379–390. https://doi.org/10.1007/978-3-642-39218-4_28
Khan, R. (2017). Network threats, attacks and security measures: a review. *International Journal of Advanced Research in Computer Science, 8*(8), 116–120. https://doi.org/10.26483/ijarcs.v8i8.4641
Komalasari, K. (2009). The effect of contextual learning in civic education on students' civic competence. *Journal of Social Science, 5*(4).
Komunikasi dan Informatika. (2018). *Big data, kecerdasan buatan, blockchain, dan teknologi finansial di Indonesia usulan desain, prinsip, dan rekomendasi kebijakan*. Centre for Innovation Policy and Governance (CIPG).
Kruger, H., & Kerney, W. (2005). *[Title of work]*. icsa.cs.up.ac.za.
Kruger, H. A., Flowerday, S., Drevin, L., & Steyn, T. (2011). *An assessment of the role of cultural factors in information security awareness*. ISSA.
Krugger, H. A., & Kearney, W. D. (2006). A prototype for assesing information security awareness. *Computer & Securitiy*, 289-296.
Kurnia, N. (2021, September 12). *Dari pembobolan akun sampai 'sextortion': Risiko besar kebocoran data pribadi*. Magdalene. https://magdalene.co/story/apa-saja-risiko-kebocoran-data-pribadi
Muchtar, Y. (2002). *Pendidikan berperspektif keadilan gender*. Depdiknas.
Papagiannakis, K., Visser, A. de., & Pijl, G. van der. (2011). *An overview of the current level of security awareness in Greek companies*. Security. http://thesis.eur.nl/pub/10958/MA13-Papagiannakis_345386.pdf
Poonia, A. S. (2014). Cyber crime: Challenges and its classification. *Bikaner, 3*(6), 119–121.
Prakasa, J. E. W. (2020). Peningkatan keamanan sistem informasi melalui klasifikasi serangan terhadap sistem informasi. *Jurnal Ilmiah Teknologi Informasi Asia, 14*(2).
Priyandoyo, A. (2006). Vulnerability assesment untuk meningkatkan kesadaran pentingnya keamanan informasi. *Jurnal Sistem Informasi*.
Putri, K. A. W. K. (2016). Pemanfaatan gadget pada mahasiswa universitas muhammadiyah surakarta. *Jurnal Psikologi, 4*(5).
Rahmawan, D., Mahameruaji, J. N., & Anisa, R. (2019). Pengembangan konten positif sebagai bagian dari gerakan literasi digital. *Jurnal Kajian Komunikasi, 7*(1), 31-43.
Riduwan. (2015). *Metode dan teknik menyusun skripsi dan tesis*. Alfabeta.
S, J. A., & Putra, Y. M. (2019). Keamanan informasi. *Jurnal Informatika, 2*(1).
Safitri, E. M., Ameilindra, Z., & Yulianti, R. (2020). Analisis teknik social engineering sebagai ancaman dalam keamanan sistem informasi: Studi literatur. *JIFTI, Jurnal Ilmiah Teknologi Informasi dan Robotika, 2*(2).
Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet, 11*(4). https://doi.org/10.3390/FI11040089
Saputra, A. (2019). Survei penggunaan media sosial di kalangan mahasiswa kota padang menggunakan teori

uses and gratifications. *Baca, Jurnal Dokumentasi dan Informasi, 40*(2), 207-216.
Sarno, R., & Iffano, I. (2009). *Sistem manajemen keamanan informasi*.
Schlienger, T., & Teufel, S. (2003). Information security culture – from analysis to change. *South African Computer Journal*.
Senie, D. (2020). Pengukuran tingkat kesadaran keamanan informasi berdasarkan behavior dan offence scale. *CESS (Journal of Computer Engineering System and Science), 5*(2).
Septiani, D. R., Widiyasono, N., & Mubarok, H. (2016). Investigasi serangan malware njrat pada PC. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN), 2*(2), 123–128. https://doi.org/10.26418/jp.v2i2.16736
Setyadani, N. A., Amatullah, N., Ramadhanty, S., & Ramli, T. S. (2021). Perlindungan data pada platform digital melalui pembentukan komisi privasi dan data protection officer (DPO). *Jurnal Hukum, 4*(5). https://kliklegal.com/perlindungan-data-pada-platform-digital-melalui-pembentukan-komisi-privasi-dan-data-protection-officer-dpo/
Situmeang, S. M. T. (2021). Penyalahgunaan data pribadi sebagai bentuk kejahatan sempurna dalam perspektif hukum siber. *Jurnal Sasi, 27*(1), 38-52.
Sugiyono. (2010). *Metode penelitian bisnis. Pendekatan kuantitatif, kualitatif dan R & D*. Alfabeta.
Suharman, Rosadi, S. D., & Pratama, G. G. (2017). Perlindungan privasi dan data pribadi dalam era ekonomi digital di Indonesia. *VeJ, 4*(1).
Suherman, & Widodo, P. (2016). Efektivitas keamanan informasi dalam menghadapi ancaman social engineering. *Jurnal Pertahanan & Bela Negara, 6*(1), 73-90.
Sulthon, M., & R, A. (2021). Analisis kesadaran keamanan di kalangan pengguna e-wallet di Indonesia. *Automata, 2*(1).
Sun, J. R., Shih, M. L., & Hwang, M. S. (2015). A survey of digital evidences forensic and cybercrime investigation procedure. *International Journal of Network Security, 17*(5), 497–509.
Tika, M. P. (2006). *Metodologi riset bisnis*. PT Bumi Aksara.
Wolf, M., Haworth, D., & Pietron, L. (2011). Measuring an information security awareness program. *Review of Business Information Systems, 15*(1), 9-22.
Zulkurnain, A. U., Kamal, A., Kamarun, B., Husain, A. Bin, & Chizari, H. (2015). Social engineering attack mitigation. *International Journal of Mathematics and Computational Science, 1*(4), 188–198. http://www.aiscience.org/journal/ijmcs