International Journal of Business, Technology, and Organizational Behavior (IJBTOB) ***ISSN*****: 2775-4936**
Vol.6 No.3 June 2026

Analysis Of the Effect of Cybersecurity Education on Secure Password Usage Behavior Among University Students

Dahniar Nur Aida[1], Firmansyah[2]
[1,2] Faculty of Engineering, Computer Science Study Program, Universitas Islam Al-Azhar
Email: danianuraidyaaa@gmail.com

Abstract

This article explores the evolution of management theories from an academic perspective by comparing the major theoretical schools from classical to contemporary thought. It aims to uncover the strengths, limitations, and research gaps within the management literature, while evaluating how these theories cope with globalization, digitalization, and economic change. The analysis is supported by historical trend data and visualizations. The findings suggest that while classical and behavioral theories retain partial applicability, contingency and dynamic capability theories offer more relevant frameworks for today's organizational challenges.
Keywords:

Introduction

The very rapid development of information technology has brought significant changes to various aspects of human life. The use of the internet, social media, and various digital applications has become an inseparable part of people's daily activities, especially university students. This progress provides convenience in accessing information and communicating, but on the other hand, it also poses various risks, especially related to security and the protection of personal data (Judijanto et al., 2024; Sadeli & Irawati, 2023).

The highly rapid development of digital technology has brought significant changes in various aspects of life, especially in the fields of communication, education, and business. This digital transformation not only creates massive opportunities through automation and efficiency, but also gives rise to various new threats in the field of cybersecurity that can endanger individuals, organizations, and society at large (Lee & Kim, 2023). In recent years, cybercrime has experienced a very rapid increase, even showing an exponential trend. This indicates that digital security risks are becoming increasingly complex and difficult to control.

In addition to technological factors, the human aspect is one of the main causes of cybersecurity breaches. A low level of awareness, lack of understanding, and insecure user behavior in using digital technology are crucial factors that amplify the potential for cyberattacks. In other words, the weakness lies not only in the system but also in the behavior of the users themselves. In the Education 4.0 era, the use of digital platforms has become an integral part of the learning process, collaboration, and academic communication. This development was further accelerated by the COVID-19 pandemic, which pushed for the massive implementation of online learning and remote work systems. These conditions led to an increased reliance on digital technology, while simultaneously amplifying the risk of exposure to cyber threats, both at the individual level and within educational institutions. The impact of cybersecurity breaches is not only limited to financial losses and data loss, but can also damage academic reputation, lower the level of trust in institutions, and disrupt the stability of the educational environment. Therefore, increasing awareness and understanding of cybersecurity is extremely important to create a safe and trusted digital environment.

Over the past decade, global losses due to cybercrime have continued to experience a significant increase and are estimated to reach an enormous figure by 2025. Furthermore, the

sharp increase in ransomware attacks in recent years indicates that cyber threats are becoming increasingly advanced and complex. These conditions underscore the importance of educational efforts and the shaping of secure user behavior, specifically in the practice of password usage as a form of basic protection in digital security.

Generation Z is a highly important group to study in the context of cybersecurity. This generation, which generally consists of individuals born between the late 1990s and the early 2010s, grew up in an environment characterized by high digital proficiency, multitasking abilities, and a heavy reliance on social media as a means of communication, information searching, and entertainment. In addition, they tend to have a higher awareness of social and environmental issues, and more frequently use visual and digital forms of communication in online interactions (Lee & Kim, 2023). However, this high intensity of digital interaction also increases their vulnerability to various cyber threats, such as data theft, cyberbullying, and identity-related crimes. Therefore, knowledge regarding cybersecurity and responsible online behavior is not only important to support academic success, but also plays an essential role in the formation of personal identity and social development in the digital environment, especially for university students.

Personal data is information attached to an individual and is sensitive in nature, thus it must be protected from potential misuse. In a digital context, personal data can be in the form of personal identity, phone numbers, email addresses, financial data, to a person's online activities. The rising cases of data breaches and cybercrimes indicate that public awareness of the importance of maintaining personal data security is still low (Rahman, 2024). Awareness of personal data security is influenced not only by technical skills but also by digital literacy, which includes the knowledge, attitudes, and behaviors of users in utilizing information technology. Good digital literacy can help individuals understand the existing risks and implement preventive measures to protect their personal data (Rahman, 2024; Sadeli & Irawati, 2023).

In Indonesia, the protection of personal data has been regulated through Law Number 27 of 2022 concerning Personal Data Protection as the state's effort to protect the privacy rights of citizens. This regulation emphasizes the importance of personal data protection as a part of human rights that must be respected and protected by all parties, be it individuals, institutions, or digital service providers (Judijanto et al., 2024; Priyantiwi, 2025).

In the current digital era, the increasing use of information and communication technology has brought new challenges in terms of cybersecurity. University students, as an active user group, often become the targets of cyberattacks. According to a report from the Cybersecurity & Infrastructure Security Agency (CISA), attacks against individuals in educational environments have significantly increased in recent years (CISA, 2022).

One critical aspect of cybersecurity is the use of strong and secure passwords. Many users, including students, still have a limited understanding of the importance of secure password usage practices. This study aims to explore how cybersecurity education can influence student behavior in using secure passwords.

1. Literature Review

Cybersecurity education is one of the main strategies in increasing user awareness and understanding of the various threats present in the digital world. Along with the increasing use of information technology in daily life, the risks of cyberattacks such as data theft, phishing, and account hacking are also getting higher. Therefore, educational efforts become

important to shape user behavior to be safer and more responsible when interacting in cyberspace.

Several studies show that effective education is not only capable of increasing the user's level of knowledge, but also influences changes in attitude and behavior in maintaining digital security. Anderson and Agarwal (2010) stated that a structured cybersecurity education program can increase risk awareness and encourage users to implement better security practices in their digital activities. Thus, education functions not only as a transfer of knowledge but also as a tool to form safe habits and behaviors.

A. Cybersecurity Theory

Dalam In understanding how cybersecurity education affects individual behavior, one relevant theory is the Social Cognitive Theory proposed by Bandura (1986). This theory explains that individual behavior is influenced by the interaction between personal factors, the environment, and the behavior itself. Individuals learn through a process of observation, experience, and social interaction with their surrounding environment.

In the context of cybersecurity, education acts as an environmental stimulus that provides information, understanding, and examples of safe behavior to users. Students who receive cybersecurity education will better understand the potential risks that may occur, such as data theft or account hacking, thereby encouraging them to adopt safer behaviors, including in the use of passwords.

In addition, research conducted by Warkentin and Willison (2009) shows that increased knowledge about security risks can strengthen positive attitudes toward information security practices. Individuals who have a high awareness of cyber threats tend to be more motivated to protect their personal data. This aligns with the concept that risk perception is a crucial factor in influencing user security behavior.

Thus, this theory emphasizes that cybersecurity education does not only provide knowledge, but also shapes the perceptions, attitudes, and ultimately the behavior of individuals in maintaining digital security.

B. Password Usage Behavior

Secure password usage behavior is one of the most fundamental aspects of cybersecurity. Passwords function as the first layer of protection against unauthorized access to a user's digital accounts. Therefore, the quality and manner of password usage greatly determine the security level of a system.

Secure password usage behavior includes several key indicators, among others:

1. Password complexity: The use of a combination of uppercase letters, lowercase letters, numbers, and symbols to increase password strength.
2. Frequency of password changes: The habit of changing passwords periodically to reduce the risk of misuse.
3. Unique password usage: Not using the same password across various accounts to prevent a domino effect if one account is hacked.
4. Password confidentiality: Not sharing passwords with other people or storing them in an insecure place.

However, in practice, many users still have not implemented these principles. Research by McCaughey et al. (2017) shows that the majority of users tend to use weak passwords, such as simple combinations or easily guessable personal information. This is caused by

several factors, such as ease of remembering, a lack of awareness of the risks, and a low understanding of the importance of password security.

2. Methodology

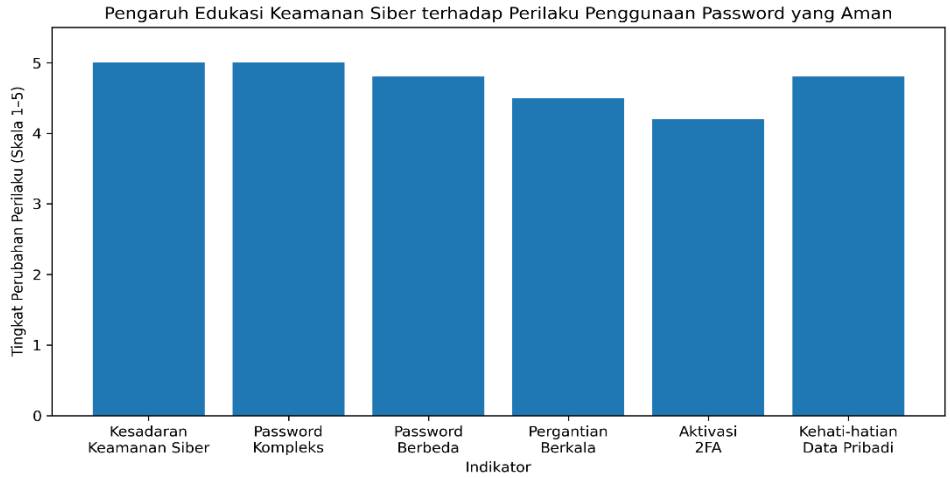
This study uses a qualitative approach with a case study design to gain a deep understanding of the phenomenon under investigation. The population in this study is university students from several universities in Indonesia, utilizing a purposive sampling technique, namely selecting students who have participated in a cybersecurity education program. The research data were obtained through in-depth interviews guided by a pre-prepared interview guide. The guide includes questions regarding the students' experiences in participating in cybersecurity education and the changes in their password usage behavior before and after receiving the education.

The data collection process was carried out through semi-structured interviews with students who were willing to be participants. The interviews were conducted online and recorded with the respondents' consent to facilitate the analysis process. The obtained data were then analyzed using a thematic analysis method, which involves identifying, grouping, and interpreting the themes and patterns that emerge from the interview transcripts. This analysis aims to answer the research questions and comprehensively describe the effect of cybersecurity education on secure password usage behavior among university students.

3. Results and Discussion

3.1. Result

Based on the results of the in-depth interviews conducted with students who have participated in a cybersecurity education program, it was found that education has a positive impact on increasing digital security awareness, knowledge, and behavior, specifically in the secure use of passwords. Before participating in the education, most informants admitted to still using simple, easily guessable passwords, and using the same password across multiple different accounts. These practices were carried out because they were considered easier to remember and facilitated access to various digital services used daily.



Based on the graph of the effect of cybersecurity education on secure password usage behavior, it can be seen that cybersecurity education has a positive impact on increasing the digital security awareness and behavior of students. The level of cybersecurity awareness and the use of complex passwords obtained the highest scores, indicating that students

increasingly understand the importance of using strong passwords as the primary step in protecting their accounts and personal data. In addition, the use of different passwords for each account and increased caution in maintaining personal data also indicate good behavioral changes after attending cybersecurity education.

Meanwhile, the habit of changing passwords periodically and the implementation of two-factor authentication (2FA) show a fairly good improvement, although still lower compared to other indicators. This shows that some students still face constraints in consistently implementing digital security behavior, mainly due to the difficulty of remembering complex passwords and old habits that are still maintained. Overall, these results indicate that the better the students' understanding of digital security threats, the higher their tendency to apply responsible security practices in their daily lives.

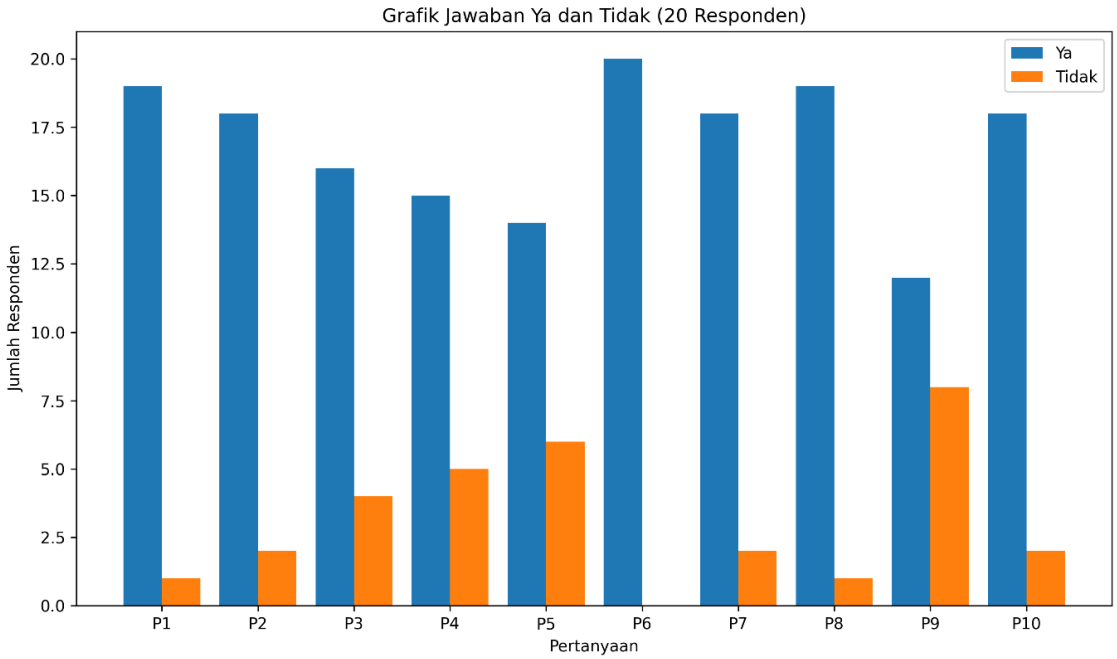
After participating in the cybersecurity education program, there was a fairly significant change in behavior. Students began to understand that a password is the first layer of defense in protecting personal data and digital accounts from hacking threats. They began to implement stronger passwords by combining uppercase letters, lowercase letters, numbers, and symbols. Furthermore, most informants stated that they started using a different password for every account and changed their passwords periodically to minimize the risk of account misuse.

These findings indicate that cybersecurity education is capable of increasing students' risk perception of digital threats. Students who previously considered cyberattacks as a rare occurrence began to realize that data breaches, phishing, identity theft, and account hacking can happen to anyone. This awareness encourages them to be more careful in maintaining the security of their accounts and personal data.

The results of this study are in line with research conducted by Alqahtani (2022), which found that cybersecurity awareness programs affect the improvement of students' digital security behavior. Knowledge regarding cyber threats is an important factor that influences the preventive actions of users in maintaining information security.

The research findings are also supported by the study of Bognár and Bottyán (2024), which explains that the level of cybersecurity awareness among students has a close relationship with digital security behavior, including password management and online account protection. Students with a high level of awareness tend to implement better security practices compared to students with a low level of awareness.

In addition, several informants stated that after attending cybersecurity education, they began activating two-factor authentication (2FA) on their social media and email accounts. This change shows that education not only increases theoretical knowledge but also encourages the implementation of concrete actions in maintaining digital security. These results reinforce the findings of the study by Pratama et al. (2023), which stated that digital learning-based cybersecurity education programs are able to increase user awareness in applying better password security practices.



On the other hand, several obstacles were still found in the implementation of secure passwords. Some students admitted that it was difficult to remember complex passwords, so they sometimes continued to use easily memorable password patterns. This shows that an increase in knowledge does not fully guarantee a consistent change in behavior. Therefore, continuous education and technological support, such as a password manager, are needed to help users manage their passwords more securely.

Based on the graph of Yes and No answers from 20 respondents, it is known that cybersecurity education has a positive impact on increasing the respondents' knowledge and awareness regarding digital security threats. A total of 19 respondents stated that cybersecurity education increased their knowledge about digital security threats, and 18 respondents admitted to better understanding the importance of protecting personal data. Furthermore, all respondents (20 people) stated that they do not share their passwords with others, while 18 respondents became more cautious of suspicious links or messages after receiving cybersecurity education. As many as 19 respondents also realized that using weak passwords can increase the risk of account hacking. These results show that cybersecurity education has successfully increased the respondents' understanding and awareness of the importance of maintaining personal information security.

Viewed from the aspect of digital security behavior, the majority of respondents have implemented good security practices. A total of 16 respondents use passwords consisting of a combination of uppercase letters, lowercase letters, numbers, and symbols, while 15 respondents use a different password for every important account. A total of 14 respondents stated that they change their passwords periodically to improve security, and 18 respondents admitted that cybersecurity education encouraged them to adopt safer behaviors when using digital technology. However, the application of two-factor authentication (2FA) is still relatively low, as only 12 respondents have activated it, while 8 respondents have not applied it. Thus, overall, cybersecurity education is proven to play a role in improving the respondents' digital security knowledge, awareness, and behavior, although further efforts are

still needed to increase the adoption of additional security features such as two-factor authentication.

Overall, the research results show that cybersecurity education has a positive effect on changes in secure password usage behavior among university students. The better the students' understanding of digital security threats, the higher their tendency to apply responsible security practices.

4.2 Discussion

The research results show that cybersecurity education plays an important role in shaping the digital security behavior of university students. These findings can be explained through the Social Cognitive Theory proposed by Bandura, which states that individual behavior is influenced by the interaction between personal factors, the environment, and learning experiences. In this study, cybersecurity education functions as an environmental factor that provides information and learning experiences to students regarding the importance of maintaining digital account security.

The improvement in secure password usage behavior after participating in education indicates that the learning process is capable of shaping risk perception and increasing students' self-efficacy in facing cyber threats. When students understand the consequences of using weak passwords, they tend to be more motivated to implement better protection measures.

These findings are in line with the research of Ahamed et al. (2024), which found that cybersecurity knowledge and attitudes toward digital security have a significant effect on the cybersecurity awareness of university students. The higher the level of knowledge and positive attitude toward digital security, the better the security behavior demonstrated by the students.

The study results also support the research of Yildirim and Erendor (2024), which shows that students with a good level of cybersecurity literacy tend to have more responsible digital security behavior compared to students with a low literacy level. Adequate knowledge enables users to recognize threats and take appropriate preventive actions.

In the context of higher education, students are a highly vulnerable group to cyber threats due to the high intensity of digital technology use in both academic and social activities. Higher education institutions store various important data, ranging from academic records to student personal information, making them an attractive target for cybercriminals. Recent research shows that educational institutions are one of the sectors most frequently targeted by cyberattacks, including ransomware and data theft.

Interestingly, the interview results show that behavioral changes occurred not only in the technical aspect of password usage but also in increased awareness of the importance of maintaining personal data confidentiality. Students became more selective in sharing personal information on social media and more cautious regarding suspicious messages or links. This shows that cybersecurity education has a broader impact than just an increase in technical skills.

However, this study also found that there are still obstacles in consistently implementing digital security behavior. Convenience factors, old habits, and the lack of supporting facilities are often the reasons why students revert to using simple passwords. This phenomenon is also found in various international studies which show that although security awareness increases, users often sacrifice security for ease of use. Therefore, cybersecurity education should not be conducted only once, but needs to be carried out continuously through

seminars, training, workshops, and the integration of cybersecurity materials into the higher education curriculum. A continuous approach will help form a strong digital security culture in the academic environment.

Conclusion

Berdasarkan Based on the results of the research and the discussion that has been conducted, it can be concluded that cybersecurity education has a positive effect on secure password usage behavior among university students. Education is capable of increasing the knowledge, awareness, and understanding of students regarding various cyber security threats that potentially endanger their digital data and accounts. The behavioral changes demonstrated by students after attending the education include the use of more complex passwords, the use of different passwords for each account, an increase in the frequency of password changes, the implementation of two-factor authentication, and an increased awareness in maintaining personal data confidentiality. These changes indicate that cybersecurity education not only improves the cognitive aspect but also affects user attitudes and behaviors in the digital environment.

This study also emphasizes that risk perception and the level of cybersecurity awareness are important factors influencing secure password usage behavior. The higher the students' understanding of digital security risks, the greater their tendency to implement good security practices in their daily lives. Nevertheless, there are still several constraints in implementing digital security behavior consistently, especially related to the difficulty of remembering complex passwords and old habits in the use of digital accounts. Therefore, continuous, innovative, and practice-based cybersecurity education programs are needed so that students can maintain good security behavior in the long term. Thus, higher education institutions need to make cybersecurity education an essential part of students' digital literacy in order to create a safe, resilient academic environment that is ready to face various security challenges in the era of digital transformation.

Recommendations

Future research is recommended to involve a broader range of respondents, use quantitative or mixed methods, and examine other factors such as digital literacy and risk perception. In addition, research can expand the study to other aspects of cybersecurity to obtain a more comprehensive understanding of user digital security behavior

References

Anderson, C. & Agarwal, R. (2010). The Digitization of Security: A Study of User Awareness. *Journal of Information Security*, 1(2), 75-90.

Alqahtani, M. A. (2022). *Factors Affecting Cybersecurity Awareness among University Students*. Applied Sciences, 12(5), 2589.

Ahamed, B., Polas, M. R. H., et al. (2024). *Empowering Students for Cybersecurity Awareness Management in the Emerging Digital Era*. SAGE Open.

Bandura, A. (1986). Social Foundations of Thought and Action. Englewood Cliffs, NJ: Prentice Hall.

Bognár, L., & Bottyán, L. (2024). *Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students*. Education Sciences, 14(6), 588.

CISA. (2022). Cybersecurity in Higher Education: Current Trends and Threats. Retrieved from [https://www.cisa.gov/] (https://www.cisa.gov/)

Furnell, S. (2015). Cyber Security Awareness in Education: An Overview. *Computers & Security*, 55, 1-9.

Judijanto, L., Lubis, A. F., Karauwan, D. E. S., Bungin, S. S., & Mau, H. A. (2024). Efektivitas kebijakan perlindungan data pribadi dalam menjaga hak asasi manusia di era teknologi di Indonesia. Sanskara Hukum dan HAM, 3(1), 34–42. https://doi.org/10.58812/shh.v3i01.445.

Lee, J., & Kim, S. (2023). Cybersecurity awareness and digital behavior in the era of Education 4.0. *Journal of Information Security and Applications*, 72, 103345. https://doi.org/10.1016/j.jisa.2023.103345

McCaughey, D. et al. (2017). Password Management: A Study of User Behaviors and Attitudes. *Computers & Security*, 67, 128-136.

Pratama, A. R., Alshaikh, M., & Alharbi, T. (2023). *Increasing Cybersecurity Awareness through Situated E-Learning: A Survey Experiment*. GTEL Conference Proceedings

Rahman, B. C. U. A. A. (2024). Analisis kesadaran keamanan data pribadi pada pengguna ewallet DANA. Jurnal Riset Sains dan Teknologi, 8(2), 155–166.

Rosta, G., Bottyán, L., & Bognár, L. (2024). *On the Factors of Students' Cybersecurity Behavior*. PedActa, 14(1), 58–66.

Warkentin, M., & Willison, R. (2009). Behavioral Information Security: The Role of Security Education and Training. *Journal of Information Systems Education*, 20(1), 49-56.

Yildirim, M., & Erendor, M. E. (2024). *A Comparative Analysis of Cyber Security Behaviours of University Students*. EDPACS, 69(6).