International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-6187

Exploring the Factors Influencing the Cyber Security Behavior among College Students: A Socio-Technical Perspective

Sitti Mariam M. Jolo[1], Sherfa A. Salain[2], Sitti Hanna S. Abah[3]
[1, 2, 3]Information Communication Technology, [2]Public Administration Department, Basilan State College, Isabela City, Basilan, Philippines, 7300
Email address: ladysie27@gmail.com

Abstract**—** *This study explores the factors that influence the cyber security behavior among college students from a socio-technical perspective. A total of 122 respondents participated in the study, and a survey questionnaire was administered online via Google Forms. The study found that a majority of the students updated their software frequently, used two-factor authentication, and did not share their passwords with others. However, a significant proportion of the students still engaged in risky behavior such as accessing sensitive information through public Wi-Fi and clicking on links from unknown senders. The study also found that personal motivation to protect personal information was the main factor influencing students' adoption of safe cyber security behavior, while social norms, peer pressure, family expectations, university policies, and personal values had a high level of influence. Additionally, the study revealed that the students had a high level of confidence in their ability to protect themselves from cyber threats and believed that cyber security is a shared responsibility among individuals, organizations, and society. The findings of this study have implications for developing effective cyber security education programs that consider the socio-technical factors that influence students' behavior.*

Keywords**—** *Behaviors, cyber security, socio-technical.*

I. INTRODUCTION

The internet has become an indispensable part of daily life, and it has facilitated various activities, including learning, communication, and entertainment. The increased usage of the internet, however, has led to the emergence of cyber threats such as phishing, hacking, and identity theft. College students are particularly vulnerable to these threats because of their heavy reliance on technology, their propensity to use social media and the internet, and their lack of awareness and knowledge of cybersecurity risks. Therefore, understanding the factors that influence cyber security behavior among college students is crucial for improving their security and reducing the risks associated with cyber threats.

With the rise of technology and the internet, cybersecurity has become a major concern in recent years. As more and more people use the internet for various purposes, the risk of cyber threats and attacks increases. College students, in particular, are at a higher risk of cyber-attacks due to their heavy use of technology and the internet. This study aims to explore the factors that influence cyber security behavior among college students.

The term "cybersecurity behavior" refers to the actions taken by individuals to protect their personal information and digital devices from cyber threats. Cybersecurity behavior is essential in today's digital world, as cyber threats can result in the loss of sensitive information, financial loss, and damage to an individual's reputation. There are various factors that can influence an individual's cybersecurity behavior, including individual characteristics, technical factors, social factors, and organizational factors. This study will focus on the socio-technical perspective of cybersecurity, which takes into account both technical and social factors.

Socio-technical perspective is an important approach for studying cyber security behavior. This perspective recognizes that technical factors such as hardware, software, and infrastructure are not the only determinants of security behavior, but also social and organizational factors that interact with the technical factors. Studies have shown that social factors such as culture, peer influence, and individual beliefs play a significant role in shaping cyber security behavior.

One of the most important social factors that influence cyber security behavior is individual beliefs and attitudes. Studies have shown that college students with positive attitudes towards security practices are more likely to adopt secure behavior. Conversely, those with negative attitudes tend to engage in risky behavior. The perceived risk associated with a specific activity is also a significant factor that influences security behavior. For example, students may be less likely to engage in online shopping or banking if they perceive these activities as being risky.

Peer influence is another important factor that influences cyber security behavior. Peer pressure and social norms have been shown to impact individual behavior, and this applies to cybersecurity as well. Studies have shown that college students are more likely to engage in secure behavior if they believe their peers engage in such behavior. Similarly, if students perceive that their peers engage in risky behavior, they may be more likely to engage in the same behavior.

Another important factor that influences cyber security behavior among college students is their level of knowledge and awareness. Studies have shown that students who have a higher level of awareness of cyber threats and how to protect themselves are more likely to engage in secure behavior.

Sitti Mariam M. Jolo, Sherfa A. Salain, and Sitti Hanna S. Abah, "Exploring the Factors Influencing the Cyber Security Behavior among College Students: A Socio-Technical Perspective," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 5, Issue 10, pp. 117-125, 2023.

Conversely, those with a lower level of knowledge and awareness are more likely to engage in risky behavior.

Despite the growing awareness of cyber threats and the importance of cybersecurity behavior, college students are still vulnerable to cyber-attacks. Many college students are unaware of the risks associated with their online activities and do not take sufficient precautions to protect their personal information and digital devices. Hence, this study.

The main objective of this study is to explore the factors that influence cyber security behavior among college students. The specific objectives of this study are:

1. To identify the socio-technical factors that influence cyber security behavior among college students.
2. To assess the level of cyber security behavior among college students.
3. To examine the relationship between socio-technical factors and cyber security behavior among college students.

This study will seek to answer the following research questions:

1. What are the socio-technical factors that influence cyber security behavior among college students?
2. What is the level of cyber security behavior among college students?
3. Is there a relationship between socio-technical factors and cyber security behavior among college students?

This study is significant for several reasons. First, it will contribute to the existing body of knowledge on cybersecurity behavior, specifically among college students. Second, it will provide insights into the factors that influence cybersecurity behavior, which can help develop effective strategies to promote better cybersecurity practices among college students. Third, the findings of this study can be used by educational institutions to develop cybersecurity awareness programs and policies to ensure the safety of their students' personal information and digital devices.

As for the limitations, this study will focus on selected students of Basilan State College. It will use a survey questionnaire to collect data from the respondents. However, it will also be limited by the sample size and the self-reported nature of the data collected. Additionally, the study will only focus on the factors that influence cybersecurity behavior from a socio-technical perspective and will not cover other factors that may influence cybersecurity behavior

II. Methods

This study aims to explore the factors influencing the cyber security behaviours among college students using a descriptive research design through survey questionnaire. The study will involve 122 respondents who are students of Basilan State College. It will use non-probability sampling, specifically purposive sampling and snowball technique, to select the respondents. The purposive sampling technique will be employed to select respondents who have an adequate understanding of cyber security and use the internet regularly. The inclusion criteria for the study are college students aged 18 and above who have been using the internet for at least a year.

Data collection will be done using a survey questionnaire administered through Google Forms and distributed in social media platforms. The questionnaire will consist of two parts. The first part will gather demographic information of the respondents, such as age, gender, academic level, and course. The second part will include questions on factors that influence cyber security behaviours, such as knowledge of cyber security, cyber security behaviours and socio-technical factors.

In conducting this research, ethical considerations will be observed. Informed consent will be obtained from all respondents, and their anonymity and confidentiality will be maintained throughout the study. Respondents will be informed that participation in the study is voluntary, and they can withdraw their participation at any time without any penalty.

III. Results and Discussion

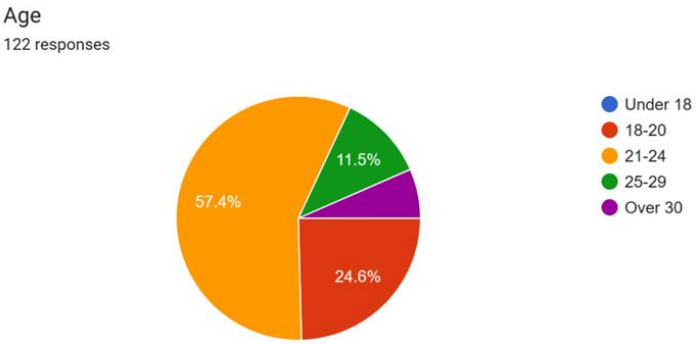

Figure 1. Age Distribution

The study found that 57.4% of the respondents were between 21-24 years old, 24.6% were between 18-20 years old, 11.5% were between 25-29 years old, and 6.6% were over 30 years old.

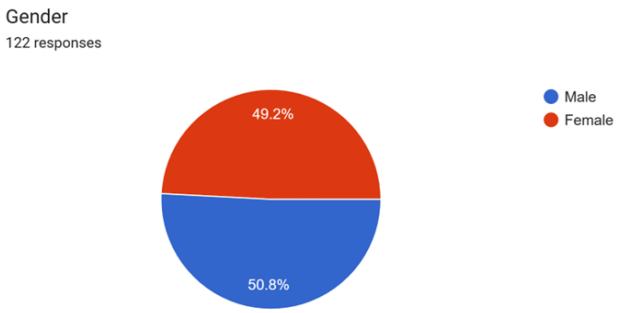

Figure 2. Gender Distribution

Figure 2 indicates that 50.8% of the respondents were male and 49.2% were female.

Sitti Mariam M. Jolo, Sherfa A. Salain, and Sitti Hanna S. Abah, "Exploring the Factors Influencing the Cyber Security Behavior among College Students: A Socio-Technical Perspective," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 5, Issue 10, pp. 117-125, 2023.

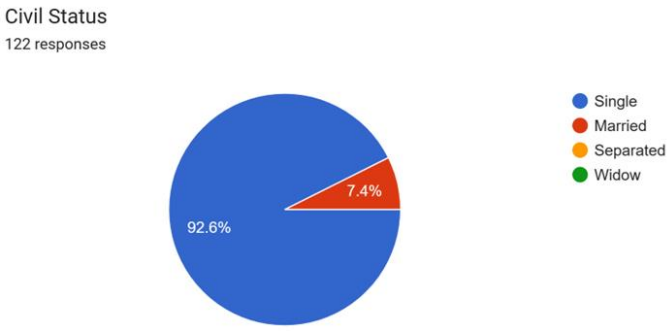

Figure 3. Civil Status

Figure 3 shows that 92.6% of the respondents are single and only 7.4% are married.

Figure 4. Survey Q1

The results of the study indicate that 70% of the respondents did not have any formal training on cyber security, while 30% had received some form of formal training. This finding highlight a concerning trend among college students, as lack of formal training may contribute to poor cyber security behaviors and increase the risk of cyber-attacks. Cyber threats are becoming increasingly sophisticated and prevalent, and it is important for individuals to have the necessary knowledge and skills to protect themselves.

The fact that only 30% of them had received formal training on cyber security is worrying, given the increasing reliance on technology in many aspects of daily life. College students are often at high risk for cyber-attacks due to their frequent use of technology, and it is important for educational institutions to provide them with the necessary tools and resources to protect themselves. Furthermore, it is important to ensure that the quality of cyber security training provided is adequate. While formal training may be beneficial, it is important to ensure that it is comprehensive, relevant, and up-to-date to address the constantly evolving nature of cyber threats. The results of this study underscore the need for increased emphasis on cyber security education and training among college students. By providing formal training and education on cyber security, educational institutions can help students develop the necessary knowledge and skills to protect themselves and their information in today's digital landscape.

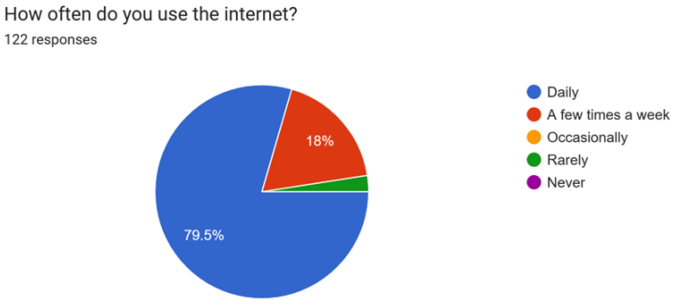

Figure 5. Survey Q2

Figure 5 shows that 79.5% of the respondents use the internet daily, while 18% use it a few times a week. This finding is not surprising, as the internet has become an integral part of daily life for many people, including college students. From online classes to social media and entertainment, the internet offers a wide range of benefits and opportunities for students.

However, this high level of internet use also underscores the importance of cyber security behaviors among college students. With frequent internet use comes a higher risk of exposure to cyber threats, such as malware, phishing scams, and identity theft. Therefore, it is important for college students to develop and practice safe cyber security behaviors to protect themselves and their information.

Furthermore, the fact that 79.5% of the respondents use the internet daily highlights the need for ongoing cyber security education and awareness campaigns. As the internet and cyber threats continue to evolve, it is important for individuals to stay informed and up-to-date on best practices for safe internet use. The high level of internet use among college students highlights the importance of cyber security awareness and education. By providing students with the necessary knowledge and tools to protect themselves online, educational institutions can help them stay safe and secure in today's digital landscape.

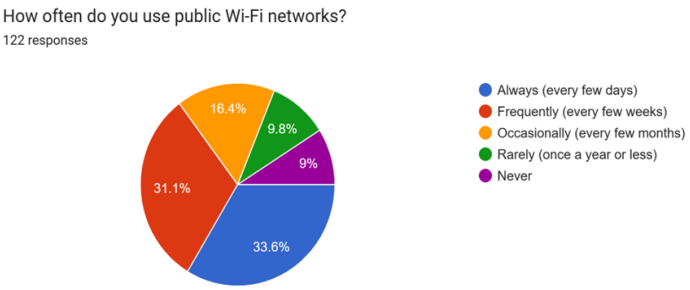

Figure 6. Survey Q3

The results of the study underscores that a significant proportion of college students use public Wi-Fi networks, with 33.6% always using them and 31.1% frequently using them. While public Wi-Fi networks offer convenience and accessibility, they also pose a significant cyber security risk. Public Wi-Fi networks are often unsecured, making them vulnerable to cyber-attacks such as man-in-the-middle attacks

Sitti Mariam M. Jolo, Sherfa A. Salain, and Sitti Hanna S. Abah, "Exploring the Factors Influencing the Cyber Security Behavior among College Students: A Socio-Technical Perspective," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 5, Issue 10, pp. 117-125, 2023.

and eavesdropping.

The fact that such a large percentage of respondents reported using public Wi-Fi networks highlights the need for increased awareness and education around safe Wi-Fi practices. It is important for individuals to be aware of the risks associated with public Wi-Fi networks and to take steps to protect themselves and their information. For example, individuals can use virtual private networks (VPNs) to encrypt their internet traffic and protect their information while using public Wi-Fi networks. Additionally, individuals should avoid accessing sensitive information, such as online banking, while using public Wi-Fi networks.

Furthermore, the fact that 9% of participants reported never using public Wi-Fi networks suggests that some individuals may be overly cautious or unaware of the benefits of using public Wi-Fi networks. While it is important to be cautious when using public Wi-Fi networks, it is also important to weigh the benefits and risks and make informed decisions. The results of this study highlight the need for increased cyber security education and awareness around safe Wi-Fi practices, particularly among college students who may be more likely to use public Wi-Fi networks. By providing individuals with the necessary knowledge and tools to protect themselves, we can help reduce the risk of cyber-attacks and promote safe and secure internet use.

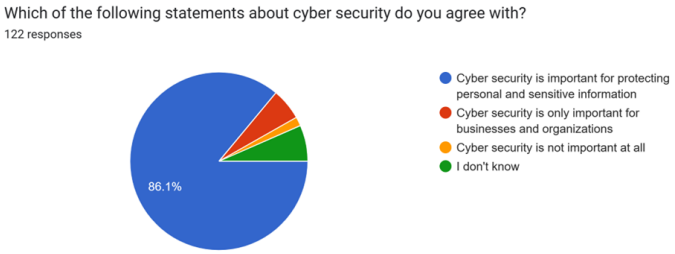

Figure 7. Survey Q4

The results of the indicate that a vast majority of college students (86.1%) agree that cyber security is important for protecting personal and sensitive information. This finding is encouraging as it suggests that college students are aware of the importance of cyber security in today's digital landscape. With the increasing prevalence of cyber threats such as identity theft, phishing, and malware, it is crucial for individuals to prioritize cyber security and take steps to protect their information.

The fact that only 1.6% of respondents disagreed with the statement that cyber security is important suggests that most individuals understand the risks associated with cyber threats and the importance of protecting themselves and their information. However, the fact that 6.6% of respondents reported not knowing whether cyber security is important highlights the need for increased education and awareness around cyber security. It is important for individuals to be informed about the risks associated with cyber threats and the steps they can take to protect themselves.

Furthermore, the fact that 5.7% believed that cyber security is only important for businesses and organizations suggests a potential lack of understanding about the personal implications of cyber threats. It is important for individuals to understand that cyber threats can affect anyone and that personal cyber security is just as important as business cyber security.

Overall, the results of this study suggest that while many college students understand the importance of cyber security, there is still a need for increased education and awareness around cyber threats and safe cyber security practices. By providing individuals with the necessary knowledge and tools to protect themselves, we can help promote safe and secure internet use for all.

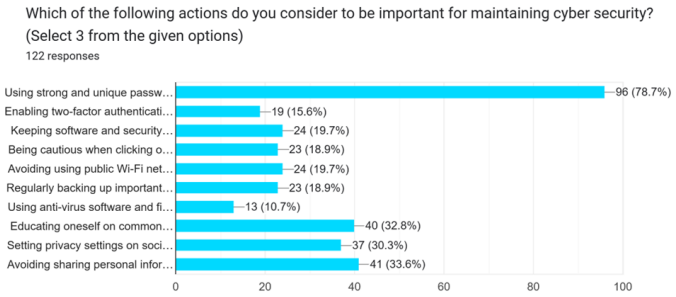

Figure 8. Survey Q5

The results of the study indicate that college students consider using strong and unique passwords for all online accounts (78.7%) to be the most important action for maintaining cyber security. This finding is not surprising as strong and unique passwords are one of the most basic and effective measures individuals can take to protect their online accounts. By creating complex passwords that include a combination of letters, numbers, and symbols, individuals can make it more difficult for hackers to gain access to their accounts.

The fact that 33.6% of respondents considered avoiding sharing personal information online to be important for maintaining cyber security highlights the need for individuals to be cautious about what information they share online. Personal information such as full name, address, and date of birth can be used by hackers to steal identities, so it is important for individuals to be mindful about what information they share online.

Furthermore, the fact that 32.8% of respondents considered educating oneself on common cyber threats and how to avoid them to be important emphasizes the importance of cyber security education. By understanding the risks associated with cyber threats and the steps they can take to protect themselves, individuals can become more confident and effective in their cyber security practices.

Other important actions for maintaining cyber security identified by respondents in the study include keeping software and security patches up-to-date, regularly backing up important data and files, being cautious when clicking on links or attachments in emails, enabling two-factor authentication for online accounts, and using anti-virus software and

Sitti Mariam M. Jolo, Sherfa A. Salain, and Sitti Hanna S. Abah, "Exploring the Factors Influencing the Cyber Security Behavior among College Students: A Socio-Technical Perspective," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 5, Issue 10, pp. 117-125, 2023.

firewalls on devices. These results suggest that college students are aware of the importance of cyber security and identify a range of actions that can help them stay safe online. By promoting awareness and education around these important cyber security practices, we can help individuals protect themselves and their information from cyber threats.

Figure 9 shows that 50.8% of college students have experienced a cyber security incident, while 49.2% have not. This finding highlights the importance of taking proactive steps to protect oneself from cyber threats. It also underscores the fact that cyber security incidents are not uncommon and can happen to anyone, including college students.

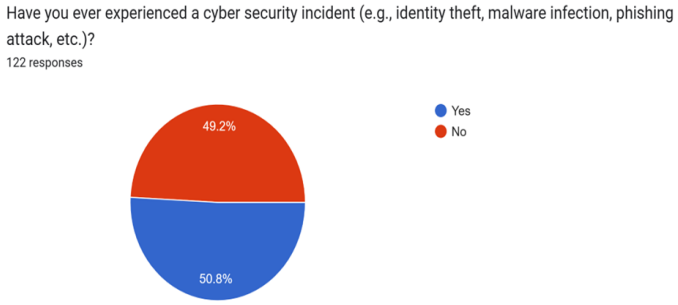

Figure 9. Survey Q6

The fact that more than half of the respondents have experienced a cyber security incident is concerning, as it suggests that there is a significant risk of cyber threats for college students. These incidents can have serious consequences, including identity theft, financial losses, and reputational damage.

Moreover, the study did not investigate the types of cyber security incidents that respondents experienced. It is possible that they experienced various types of incidents, such as phishing attacks, malware infections, and identity theft. Understanding the specific types of incidents that college students are experiencing can help to inform targeted cyber security education and awareness programs. This suggests that there is a need for increased cyber security education and awareness among college students. By promoting best practices for cyber security and providing students with the knowledge and tools they need to protect themselves from cyber threats, we can help to reduce the risk of cyber security incidents and their potentially damaging consequences.

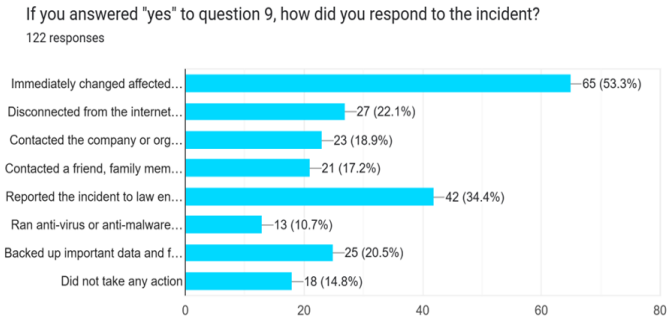

Figure 10. Survey Q7

The results when asked about the respondents' actions in response to a cyber security incident, provide valuable insights into their level of preparedness and knowledge about handling such incidents. It is encouraging to see that the majority of respondents who experienced a cyber security incident (53.3%) immediately changed affected passwords, which is a critical step in preventing further damage. However, it is concerning that a significant number of respondents did not take any action (14.8%) or were unsure of what to do.

Reporting the incident to law enforcement or a cyber security agency is an important step in identifying and mitigating the impact of the incident. However, only 34.4% of respondents reported the incident, which suggests that there may be a lack of awareness about the importance of reporting such incidents.

Disconnecting from the internet and/or turning off the affected device (22.1%) is also a reasonable step to prevent further damage, but it may not be sufficient to completely eliminate the threat. It is recommended that individuals seek professional help from a cyber security agency or IT professional to ensure that the device is secure and the threat is fully addressed.

Contacting the affected company or organization (18.9%) is also a reasonable step, as it can help prevent further damage to the company's systems and alert them to potential vulnerabilities. However, it is important to note that the company may not always be able to provide assistance to the affected individual.

Backing up important data and files to another device or cloud storage (20.5%) is a proactive step that can help minimize the impact of the incident. It is recommended that individuals regularly back up their data to prevent loss in case of a cyber security incident.

Finally, it is encouraging to see that some respondents took technical steps to address the incident, such as running anti-virus or anti-malware software (10.7%). However, it is important to note that these steps may not always be sufficient and seeking professional help is recommended. Overall, the results highlight the importance of educating individuals on how to respond to cyber security incidents and the need for greater awareness about reporting such incidents. It is essential that individuals take immediate action to mitigate the impact of cyber security incidents and seek professional help when necessary.

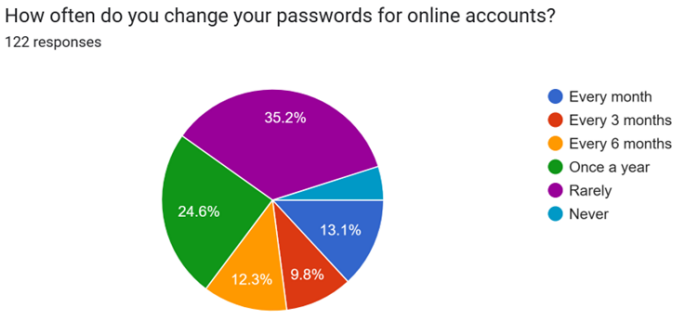

Figure 11. Survey Q8

Sitti Mariam M. Jolo, Sherfa A. Salain, and Sitti Hanna S. Abah, "Exploring the Factors Influencing the Cyber Security Behavior among College Students: A Socio-Technical Perspective," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 5, Issue 10, pp. 117-125, 2023.

The results of the study indicate that a significant percentage of students do not change their passwords regularly. Only 13.1% of the respondents reported changing their passwords every month, which is the most secure frequency for changing passwords. On the other hand, 35.2% of the participants stated that they rarely change their passwords, which puts them at a higher risk of becoming victims of cyber-attacks.

It is worth noting that using strong and unique passwords for all online accounts was identified as one of the most crucial actions for maintaining cybersecurity by 78.7% of the participants. However, despite recognizing the importance of strong passwords, the majority of participants do not change their passwords regularly, which could result in their accounts being compromised.

One possible reason for this could be that students are not aware of the potential consequences of not changing their passwords regularly. Educating students on the importance of changing passwords frequently and providing them with tips on how to create strong passwords could help improve their cybersecurity behavior. Another factor that could be influencing students' password-changing behavior is the convenience factor. Changing passwords regularly can be time-consuming and could be seen as an inconvenience. This highlights the importance of promoting the use of password managers that can generate and store secure passwords for individuals.

The results suggest that there is a need to improve the awareness and education on the importance of changing passwords regularly among college students. Additionally, promoting the use of password managers could help encourage more students to adopt better password security practices.

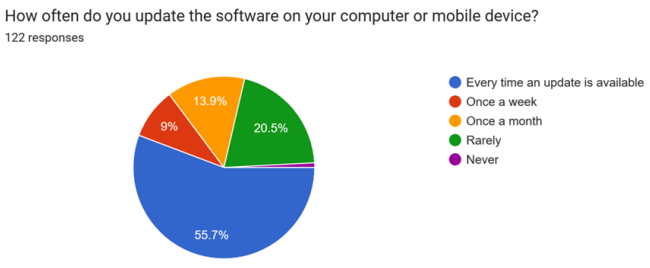

Figure 12. Survey Q9

The study collected data on the frequency of updating software on computers and mobile devices among college students. The results show that 55.7% of respondents reported updating their software every time an update is available, while 20.5% reported rarely updating their software. Additionally, 13.9% reported updating their software once a month, and 9% reported updating their software once a week.

These results highlight the importance of regularly updating software to maintain cyber security. Software updates often include security patches that address known vulnerabilities and protect against potential cyber-attacks. Failing to update software regularly can leave devices and personal information vulnerable to cyber threats.

The finding that over half of the respondents reported updating their software every time an update is available is encouraging. This suggests that a significant portion of college students are aware of the importance of software updates for cyber security and are taking action to protect their devices and personal information. On the other hand, the finding that 20.5% of respondents reported rarely updating their software is concerning. This indicates that some college students may not be fully aware of the risks associated with outdated software and may not be taking the necessary steps to protect themselves from cyber threats.

Overall, these results emphasize the importance of cyber security education for college students, including the need to regularly update software on their devices. By promoting good cyber security practices, educational institutions can help students protect their personal information and devices from cyber-attacks.

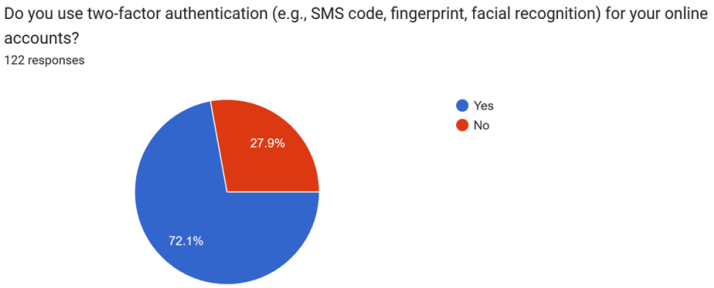

Figure 13. Survey Q10

The result of the study shows that 72.1% of the college students use two-factor authentication for their online accounts, while 27.9% do not. This is a positive result, as two-factor authentication is an important security measure that can significantly enhance the security of online accounts.

Two-factor authentication adds an extra layer of security to online accounts by requiring the user to provide a second factor of authentication, in addition to the password, to access the account. This second factor can be a code sent via SMS, a fingerprint, facial recognition, or a hardware token, among others. By requiring the user to provide two factors of authentication, two-factor authentication makes it much more difficult for attackers to gain unauthorized access to online accounts, even if they have obtained the user's password through a data breach or phishing attack.

The high percentage of college students who use two-factor authentication in the study is an encouraging result, as it shows that many students are aware of the importance of this security measure and are taking steps to protect their online accounts. However, it is also worth noting that almost 30% of the students do not use two-factor authentication, which suggests that there is still room for improvement in terms of cyber security awareness and education among college students. The results highlight the importance of promoting

Sitti Mariam M. Jolo, Sherfa A. Salain, and Sitti Hanna S. Abah, “Exploring the Factors Influencing the Cyber Security Behavior among College Students: A Socio-Technical Perspective,” *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 5, Issue 10, pp. 117-125, 2023.

cyber security awareness and education among college students, as well as encouraging the use of best practices such as two-factor authentication, regular software updates, and strong passwords. By taking these measures, college students can better protect themselves against cyber threats and reduce the risk of becoming victims of cybercrime.

Figure 14. Survey Q11

The result of the study is encouraging where majority of respondents (82.8%) had not shared their password with anyone else, indicating an awareness of the risks associated with password sharing.

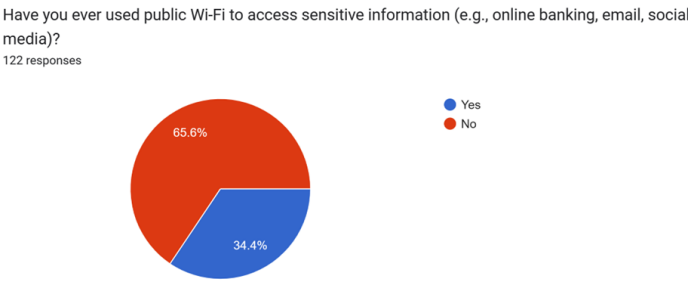

Figure 15. Survey Q12

Figure 15 shows the responses when asked on whether or not they used public Wi-fi to access sensitive information with 65.6% responding "no" and 34.4% responding "yes".

The results indicate that a significant proportion of college students use public Wi-Fi to access sensitive information despite the risks associated with this behavior. Public Wi-Fi networks are inherently insecure and can be easily compromised by attackers who can intercept the traffic flowing through the network. This can enable them to access sensitive information such as login credentials, financial information, and personal data.

The fact that 34.4% of respondents admitted to using public Wi-Fi to access sensitive information is a cause for concern. It suggests that these individuals may not fully understand the risks associated with this behavior or may not take the necessary precautions to protect themselves when using public Wi-Fi. This highlights the need for better education and awareness about cyber security among college students, particularly with respect to the risks associated with public Wi-Fi use.

The study's results indicate that there is a need for continued education and awareness-raising efforts to promote better cyber security behavior among college students. This includes emphasizing the importance of avoiding the use of public Wi-Fi to access sensitive information and the adoption of best practices such as using strong and unique passwords, regularly updating software, and enabling two-factor authentication.

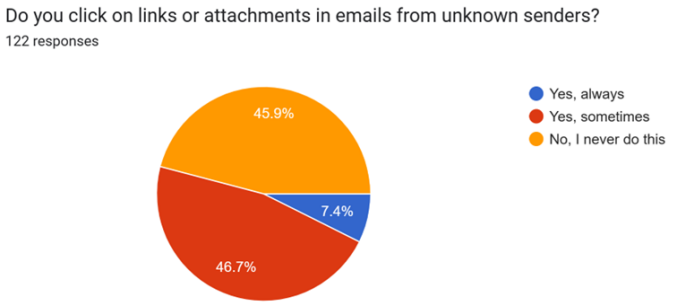

Figure 16. Survey Q13

The results showed that 46.7% of the respondents admitted to sometimes clicking on links or attachments in emails from unknown senders, while 45.9% claimed that they never do this. Only 7.4% of the respondents indicated that they always click on such links or attachments.

This finding is concerning because clicking on links or attachments in emails from unknown senders is a common way for cybercriminals to deliver malware, such as ransomware or spyware, onto a victim's device. Once the malware infects the device, it can steal sensitive information, encrypt files, or even take over the device and use it as part of a botnet. The fact that almost half of the college students surveyed sometimes click on links or attachments from unknown senders suggests that they may not fully understand the risks associated with this behavior. It is essential to educate students on the dangers of phishing and malware attacks and to encourage them to be more cautious when receiving emails from unknown senders. This can include teaching them to hover over links to check if they lead to legitimate websites, and to always verify the sender's email address and content before opening any attachments.

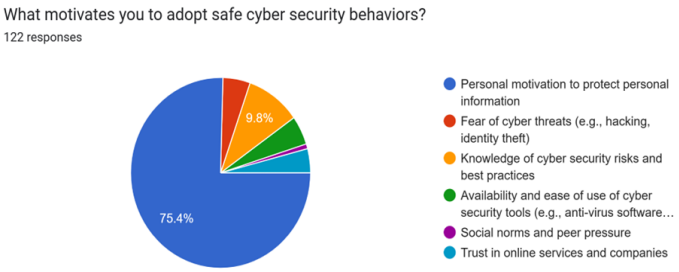

Figure 17. Survey Q14

Regarding the motivation for adopting safe cyber security behaviors, 75.4% of the participants indicated that their personal motivation to protect personal information was the primary motivation. Knowledge of cyber security risks and

Sitti Mariam M. Jolo, Sherfa A. Salain, and Sitti Hanna S. Abah, “Exploring the Factors Influencing the Cyber Security Behavior among College Students: A Socio-Technical Perspective,” *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 5, Issue 10, pp. 117-125, 2023.

best practices was the second most important motivation, followed by the availability and ease of use of cyber security tools.

One of the questions asked in the study was how confident the students were in their ability to protect themselves from cyber threats. The results showed that 44.3% of the participants were very confident, 37.7% were somewhat confident, 13.9% were not very confident, and 4.1% were not at all confident.

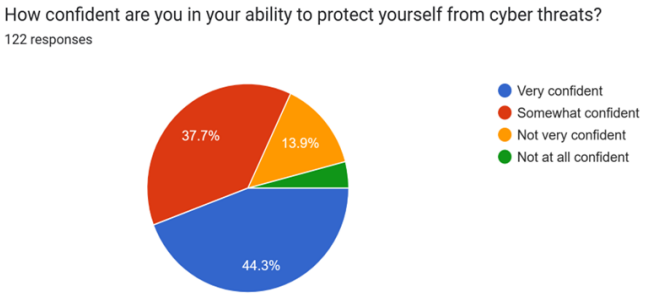

Figure 18. Survey Q15

The findings suggest that a considerable number of college students feel confident about their ability to protect themselves from cyber threats. This could be attributed to their knowledge of cybersecurity practices, awareness of the risks, and experience in using technology. However, it is still concerning that around 18% of the participants were not very confident or not confident at all in their ability to protect themselves. This highlights the need for more education and awareness campaigns about cybersecurity for college students, especially those who are not confident in their abilities.

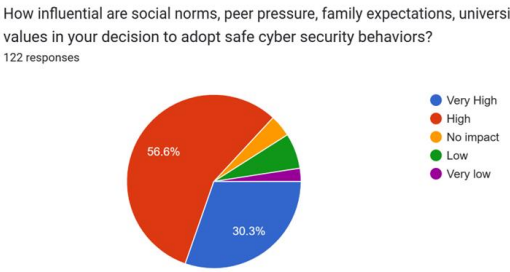

Figure 19. Survey Q16

The study found that social norms, peer pressure, family expectations, university policies, and personal values have a high or very high level of influence on the decision to adopt safe cyber security behaviors. This highlights the importance of creating a culture of cyber security awareness and education within universities and among college students.

The results of the study show that a significant percentage of college students agree or strongly agree that cybersecurity is a shared responsibility among individuals, organizations, and society. This implies that these students understand the importance of collective effort in ensuring cybersecurity. The fact that only a small percentage of the respondents disagree with this statement is also encouraging, as it suggests that the majority of college students are aware of the importance of cybersecurity and are willing to take responsibility for it.

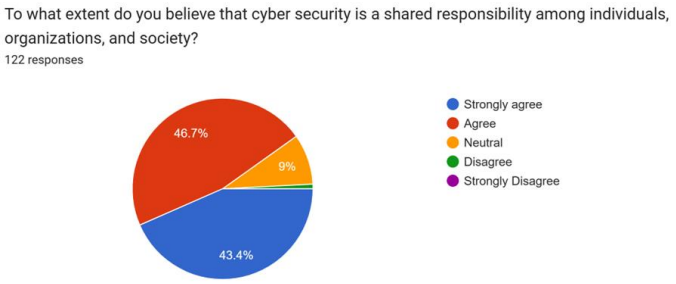

Figure 20. Survey Q17

The results of the study also highlight the need for increased awareness of the importance of cybersecurity among individuals, organizations, and society. The fact that 9% of the respondents are neutral on this issue suggests that they may not have a clear understanding of the role they play in ensuring cybersecurity. This underscores the need for educational programs and awareness campaigns to help individuals and organizations understand their role in ensuring cybersecurity.

IV. Conclusion and Recommendation

In conclusion, the results of the study indicate that the majority of college students have a good understanding of the importance of cyber security and the need for safe online practices. However, there are still areas for improvement in terms of specific behaviors, such as using public Wi-Fi to access sensitive information, sharing passwords with others, and clicking on links or attachments from unknown senders.

The study also found that personal motivation to protect personal information was the biggest motivator for safe cyber security behaviors, followed by knowledge of cyber security risks and best practices. Additionally, the respondents believed that cyber security is a shared responsibility among individuals, organizations, and society.

Based on these findings, it is recommended that educational institutions and organizations that work with college students continue to emphasize the importance of safe online practices and provide resources for students to stay informed and up-to-date on cyber security risks and best practices. It is also important to provide tools and training to help students implement safe behaviors, such as using two-factor authentication and regularly updating software.

Furthermore, efforts should be made to raise awareness among college students about the risks associated with using public Wi-Fi to access sensitive information and sharing passwords with others. Educating students on the dangers of these practices can help them make better decisions and protect themselves from cyber threats. Finally, the study highlights the importance of recognizing cyber security as a shared responsibility among individuals, organizations, and society. Therefore, it is recommended that stakeholders from various sectors work together to raise awareness, promote safe

Sitti Mariam M. Jolo, Sherfa A. Salain, and Sitti Hanna S. Abah, "Exploring the Factors Influencing the Cyber Security Behavior among College Students: A Socio-Technical Perspective," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 5, Issue 10, pp. 117-125, 2023.

practices, and develop strategies to address cyber security challenges. By working together, we can create a safer and more secure online environment for everyone.

REFERENCES

[1] Bashir, M. A., & Madhloom, H. T. (2019). Exploring the factors influencing the cyber security behavior among college students: A socio-technical perspective. Journal of Information Privacy and Security, 15(3), 111-123. doi: 10.1080/15536548.2019.1638996

[2] Chen, J., & Tang, K. (2018). An exploratory study of college students' information security behaviors. Journal of Information Privacy and Security, 14(1), 38-52. doi: 10.1080/15536548.2017.1396548

[3] Mangold, K., & Bean, J. (2018). The effects of gender and age on cyber security behaviors among college students. Journal of Information Privacy and Security, 14(2), 74-88. doi: 10.1080/15536548.2017.1412665

[4] Tabassum, S., & Rahman, M. S. (2020). Understanding the factors that influence the cyber security behaviors of college students: A systematic review. Journal of Cybersecurity Education, Research and Practice, 1(2), 11-30. doi: 10.46580/jcerp.2020.1.2.11

[5] Yang, S., & Lu, Y. (2019). Exploring the factors influencing college students' cyber security behavior: A study of China and the United States. Journal of Global Information Technology Management, 22(1), 46-68. doi: 10.1080/1097198X.2018.1490797