Cyber Fraud Prevention and Financial Management Readiness: A Framework for Accessible Education Settings

Ryxon Ladjahasan Hamsan[1], Joy N. Savellano[2], Angelo R. Santos[2]

[1]Institute of Criminal Justice Studies, Criminology Department, Tawi-Tawi Regional Agricultural College, Nalil, Bongao, Tawi-Tawi, Philippines

[2]College of Management and Business Technology, Nueva Ecija University of Science and Technology, Cabanatuan City, Philippines

HOW TO CITE:
Ryxon Ladjahasan Hamsan, Joy N. Savellano, Angelo R. Santos (2026). Cyber Fraud Prevention and Financial Management Readiness: A Framework for Accessible Education Settings. International Journal of Special Education, 41(13s), 1043-1053

COPYRIGHT STATEMENT:
Copyright: © 2026 Authors. Open access publication underthe terms and conditions of the Creative CommonsAttribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

ABSTRACT:
This study examined cyber fraud prevention and financial management readiness among students in accessible education settings in Bongao, Tawi-Tawi, Philippines. It aimed to describe students' awareness and practices in preventing cyber fraud and assess their readiness in managing personal financial resources amid increasing use of digital transactions and online financial services. A descriptive quantitative research design was used, involving 57 student-respondents who voluntarily participated and completed a structured Likert-type survey questionnaire. The data were analyzed using frequency, percentage, mean, and standard deviation. The findings revealed that the respondents had a high level of cyber fraud prevention, particularly in identifying suspicious messages, protecting passwords, safeguarding personal information, and avoiding phishing links. However, reporting possible cyber fraud incidents received the lowest rating among the cyber fraud prevention indicators. The respondents also demonstrated a high level of financial management readiness, especially in budgeting, responsible use of digital payment platforms, saving readiness, and spending control. Meanwhile, decision-making in managing personal financial resources received the lowest rating. The study concludes that students possess foundational digital safety awareness and financial readiness but still need stronger support in fraud reporting, financial risk awareness, and applied financial decision-making. The study recommends accessible learner support programs integrating cyber fraud prevention and financial literacy.

Keywords: cyber fraud prevention, financial management readiness, accessible education settings, digital safety, financial literacy

1. Introduction

The rapid expansion of digital transactions has changed how learners manage money, access services, communicate with institutions, and participate in academic and community life. While digital platforms create opportunities for

faster access to financial information and services, they also expose learners to risks such as phishing, identity theft, online scams, social engineering, fraudulent links, and unauthorized financial transactions. Cybersecurity awareness has therefore become an important educational concern because students must be equipped not only with digital access but also with the knowledge, attitudes, and behaviors needed to protect themselves in online environments (Erendor & Yildirim, 2022). In accessible education settings, this concern becomes more significant because digital participation must be safe, understandable, and responsive to learners with diverse needs.

Cyber fraud prevention refers to the knowledge and practices that help individuals identify, avoid, and respond to fraudulent digital activities. These practices may include recognizing suspicious messages, protecting passwords and personal information, verifying online payment channels, avoiding unsafe links, understanding privacy risks, and reporting possible fraud. Studies on cybersecurity awareness emphasize that students and academic communities need structured training because online education and digital communication can increase exposure to cyber risks when learners are not adequately prepared (Alqahtani & Kavakli, 2020; Erendor & Yildirim, 2022). In this context, cyber fraud prevention is not only a technical concern but also an educational responsibility that supports learner protection, digital inclusion, and responsible participation in technology-mediated environments.

Financial management readiness is also an essential competency for learners because it supports informed decision-making, budgeting, saving, spending control, risk awareness, and responsible use of financial products and services. Financial literacy has been consistently linked to financial behavior, particularly in the way individuals plan, manage resources, evaluate risks, and make financial decisions (Stolper & Walter, 2017). In the digital era, financial readiness must also include the ability to understand online financial tools, digital payment systems, and financial risks associated with technology. Digital financial literacy studies show that individuals who understand digital financial services are more likely to demonstrate improved financial behavior and decision-making (Rahayu et al., 2022). Similarly, the OECD financial literacy framework emphasizes that young people need knowledge, skills, attitudes, and behaviors that allow them to make sound financial decisions in increasingly complex financial environments (OECD, 2023). The relationship between cyber fraud prevention and financial management readiness is important because many financial risks now occur through digital channels. Learners who lack awareness of cyber fraud may become vulnerable to scams, unsafe transactions, account compromise, and poor financial decisions. Conversely, learners who understand digital safety may be more prepared to manage money responsibly, evaluate financial information, and protect their personal and financial data. Digital financial literacy research supports the view that financial behavior in modern contexts is shaped not only by knowledge of money management but also by the ability to use digital financial systems safely and critically (Aryan et al., 2024; Febrianty et al., 2024; Rahayu et al., 2022). Therefore, cyber fraud prevention and financial management readiness should be examined together, especially in education settings where learners are being prepared for independent financial and digital participation.

Accessible education settings provide an important context for this study because accessibility is not limited to physical access or instructional accommodation. It also includes access to safe, usable, and inclusive digital systems that allow learners to participate meaningfully in academic and financial activities. Research on accessible education emphasizes that learners with diverse needs may experience barriers related to institutional systems, digital tools, communication practices, and support services (Marquis et al., 2016). Digital inclusion literature further explains that technology may either promote participation or deepen exclusion depending on how accessible, understandable, and supportive digital environments are for users

(Nguyen, 2020). Thus, cyber fraud prevention and financial management readiness are relevant to accessible education because learners must be protected not only from academic barriers but also from digital and financial risks that may affect their participation and well-being.

This issue is particularly relevant in local education contexts such as Bongao, Tawi-Tawi, Philippines, where students may encounter varying levels of digital access, financial exposure, and institutional support. As learners increasingly use online communication, digital payment channels, mobile banking, e-wallets, and internet-based transactions, they need practical readiness to manage financial decisions and avoid cyber fraud. However, limited research has examined how cyber fraud prevention relates to financial management readiness among students in accessible education settings. Existing studies commonly examine cybersecurity awareness, digital financial literacy, or financial behavior separately, but fewer studies connect these constructs within an inclusive and accessibility-oriented education framework (Erendor & Yildirim, 2022; OECD, 2023; Rahayu et al., 2022).

This study is to examine cyber fraud prevention and financial management readiness among 57 students in Bongao, Tawi-Tawi. Specifically, the study seeks to determine the level of students' cyber fraud prevention awareness, assess their financial management readiness, and examine the relationship between the two variables. The findings may provide a basis for designing learner-centered programs, digital safety instruction, financial literacy activities, and accessible student support mechanisms. The study may also contribute to the field of special and inclusive education by emphasizing that learner protection in accessible education settings should include not only academic participation but also digital safety, financial readiness, and responsible engagement with online systems.

2. Methodology

This study utilized a descriptive quantitative research design to assess the level of cyber fraud prevention and financial management readiness among students in accessible education settings. The design was appropriate because the study focused on describing the respondents' awareness, practices, and readiness based on measurable survey responses. Through this approach, the study generated numerical data that served as basis for identifying areas of strength and areas needing improvement in digital safety, financial literacy, and learner support. The descriptive design also supported the development of a proposed framework for strengthening cyber fraud prevention and financial management readiness in accessible education settings.

The respondents of the study were 57 students from Bongao, Tawi-Tawi, Philippines. They were included because they represented the learner group relevant to the study's focus on digital safety, financial readiness, and accessibility-oriented educational support. The respondents were officially enrolled students who voluntarily participated in the study and completed the survey questionnaire. Students who were not willing to participate or who submitted incomplete responses were not included in the final analysis. The total number of valid responses used in the study was 57.

The study used a structured survey questionnaire as the primary data-gathering instrument. The questionnaire consisted of items that measured two major areas: cyber fraud prevention and financial management readiness. The cyber fraud prevention items focused on students' awareness and practices in identifying suspicious messages, avoiding phishing links, protecting passwords, safeguarding personal information, verifying online transactions, recognizing fraudulent digital activities, and reporting possible cyber fraud incidents. The financial management readiness items focused on students' preparedness in budgeting, saving, spending control, financial planning, risk awareness, responsible use of digital payment platforms, and decision-making in managing personal financial resources.

The survey items were presented using a Likert-type scale to allow the respondents to indicate the extent of their agreement or perceived readiness.

The instrument was reviewed for clarity, relevance, and suitability to the respondents and the local context of the study. The questionnaire was designed to be understandable and accessible so that respondents could answer the items based on their actual experiences with online transactions, digital safety practices, and financial management activities.

The data-gathering process was conducted in Bongao, Tawi-Tawi. Before administering the questionnaire, the purpose of the study was explained to the respondents. They were informed that their participation was voluntary and that their responses would be treated with confidentiality. After consent was secured, the questionnaire was distributed to the respondents. They were given sufficient time to answer the items independently. After retrieval, the questionnaires were checked for completeness, and only valid responses were encoded for analysis.

The data were analyzed using descriptive statistics. Frequency and percentage were used to describe the distribution of responses when applicable. Mean and standard deviation were used to determine the level of cyber fraud prevention and financial management readiness. The mean scores were interpreted using a descriptive scale to classify the level of respondents' awareness, practices, and readiness. The results were organized according to the study objectives and were used as basis for developing a framework for accessible education settings.

3. Results

3.1. Level of Cyber Fraud Prevention

The results showed that the respondents had a high level of cyber fraud prevention, with an overall mean score of 3.31 and a standard deviation of 0.44. Among the measured indicators, identifying suspicious messages obtained the highest mean score of 3.46 with a standard deviation of 0.41. This was followed by protecting passwords, which obtained a mean score of 3.39 and a standard deviation of 0.43. Safeguarding personal information recorded a mean score of 3.37 with a standard deviation of 0.45, while avoiding phishing links obtained a mean score of 3.34 with a standard deviation of 0.46. Verifying online transactions obtained a mean score of 3.28 with a standard deviation of 0.48. Recognizing fraudulent digital activities recorded a mean score of 3.24 with a standard deviation of 0.49. Reporting possible cyber fraud incidents obtained the lowest mean score among the indicators, with a mean of 3.11 and a standard deviation of 0.53.

In terms of distribution, 10 respondents, or 17.54%, rated their cyber fraud prevention as very high. Thirty-nine respondents, or 68.42%, rated it as high, while 8 respondents, or 14.04%, rated it as moderate. No respondent obtained a low or very low rating. The overall result indicated that the respondents generally had favorable awareness and practices in identifying suspicious online activities, protecting personal information, and avoiding unsafe digital transactions. However, the lowest mean score for reporting possible cyber fraud incidents suggested that students may still need additional guidance on proper reporting channels and response procedures.

3.2. Level of Financial Management Readiness

The results showed that the respondents had a high level of financial management readiness, with an overall mean score of 3.22 and a standard deviation of 0.48. Among the measured indicators, budgeting obtained the highest mean score of 3.35 with a standard deviation of 0.44. This was followed by responsible use of digital payment platforms, which obtained a mean score of 3.31 and a standard deviation of 0.46. Saving readiness recorded a mean score of 3.24 with a standard deviation of 0.49, while spending control obtained a mean score of 3.20 and a standard deviation of 0.50. Financial planning obtained a mean score of 3.18 with a standard deviation of 0.51. Financial risk awareness recorded a mean score of 3.15 with a standard deviation of 0.52. Decision-making in managing personal financial resources obtained the lowest mean score among the indicators, with a mean of 3.10 and a standard deviation of 0.55.

In terms of distribution, 8 respondents, or 14.04%, rated their financial management readiness as very high. Thirty-seven respondents, or 64.91%, rated it as high, while 12 respondents, or 21.05%, rated it as moderate. No respondent obtained a low or very low rating. The findings indicated that the respondents generally demonstrated favorable readiness in budgeting, using digital payment platforms responsibly, saving, and controlling spending. However, the comparatively lower mean scores for financial risk awareness and decision-making suggested the need to strengthen practical learning activities related to evaluating financial risks, comparing financial choices, and making responsible personal finance decisions.

3.3. Comparative Summary of the Two Major Variables

The overall mean score for cyber fraud prevention was 3.31 with a standard deviation of 0.44, while the overall mean score for financial management readiness was 3.22 with a standard deviation of 0.48. Both variables were interpreted as high. Cyber fraud prevention obtained a slightly higher mean score than financial management readiness, indicating that the respondents reported stronger awareness and practices in digital safety than in personal financial management.

The highest-rated indicator under cyber fraud prevention was identifying suspicious messages, while the lowest-rated indicator was reporting possible cyber fraud incidents. For financial management readiness, the highest-rated indicator was budgeting, while the lowest-rated indicator was decision-making in managing personal financial resources. These findings showed that the respondents were generally aware of cyber fraud risks and were moderately prepared to manage their finances, but they still needed improvement in response-based cyber fraud actions and applied financial decision-making.

3.4. Key Findings for Framework Development

The quantitative findings provided a basis for developing a framework for accessible education settings. The high level of cyber fraud prevention suggested that students already had foundational awareness of digital safety practices, particularly in recognizing suspicious messages, protecting passwords, and safeguarding personal information. However, the lower score for reporting possible cyber fraud incidents indicated the need for a clearer learner support mechanism, including orientation on where, when, and how to report cyber fraud concerns.

The high level of financial management readiness also showed that students had basic readiness in budgeting, saving, spending control, and responsible use of digital payment platforms. However, the lower scores for financial risk awareness and decision-making indicated that the proposed framework should include practical activities on financial planning, risk identification, fraud-related financial decision-making, and responsible use of online financial services. Overall, the results supported the development of a framework that combines cyber fraud prevention, financial literacy, digital safety practices, and accessible student support.

4. Discussion

The findings revealed that the respondents had a high level of cyber fraud prevention, with an overall mean score of 3.31 and a standard deviation of 0.44. This result indicates that the students in Bongao, Tawi-Tawi generally possessed favorable awareness and practices in protecting themselves from common online risks. The highest-rated indicator was identifying suspicious messages, suggesting that the respondents were more confident in recognizing warning signs in digital communication. This finding is consistent with studies emphasizing that cybersecurity awareness among students is shaped by their exposure to online learning, digital communication, social media, and internet-based activities (Alharbi & Tassaddiq, 2021; Erendor & Yildirim, 2022; Tirumala et al., 2016). Since students increasingly interact with

online platforms for academic and personal purposes, their ability to identify suspicious messages is an important first layer of protection against phishing, fraud, and social engineering attacks (Baadel et al., 2021; Chatchalermpun & Daengsi, 2021).

The relatively high scores in protecting passwords, safeguarding personal information, and avoiding phishing links further suggest that the respondents had foundational digital safety habits. These findings support the view that cybersecurity awareness should not be limited to technical knowledge but should include practical behaviors such as using secure passwords, avoiding unsafe links, verifying information, and protecting personal data (Alqahtani & Kavakli, 2020; Alharbi & Tassaddiq, 2021). Cybersecurity education studies have also shown that students may demonstrate awareness of basic online risks but still need continuous instruction, simulation, and reinforcement to convert awareness into consistent protective behavior (Erendor & Yildirim, 2022; Chatchalermpun & Daengsi, 2021). In this study, the high mean scores show that the respondents were generally aware of cyber fraud prevention practices, but the need for structured and accessible instruction remains important.

The lowest-rated indicator under cyber fraud prevention was reporting possible cyber fraud incidents, with a mean score of 3.11 and a standard deviation of 0.53. Although this score was still interpreted as high, it was lower than the other cyber fraud prevention indicators. This suggests that students may know how to recognize suspicious online activities but may be less prepared to take the next step of reporting fraud incidents to proper authorities, school personnel, platform administrators, or financial service providers. This finding is supported by cybersecurity literature showing that awareness does not always translate into reporting behavior or active response, especially when users are unsure about reporting channels, consequences, or institutional procedures (Baadel et al., 2021; Chatchalermpun & Daengsi, 2021). Therefore, accessible education settings should not only teach students how to detect cyber fraud but also provide clear, visible, and student-friendly mechanisms for reporting suspicious digital activities.

The distribution of responses showed that 17.54% of the respondents rated their cyber fraud prevention as very high, 68.42% rated it as high, and 14.04% rated it as moderate. No respondent obtained a low or very low rating. This distribution indicates that most respondents already had a favorable level of cyber fraud prevention awareness and practices. However, the presence of moderate ratings also shows that not all students had the same level of preparedness. This variation may be influenced by differences in internet exposure, access to digital devices, prior training, online transaction experience, and availability of guidance from family, school, or community. Studies on cybersecurity awareness among students likewise show that learners may differ in their security behavior depending on their familiarity with technology, frequency of internet use, and exposure to awareness programs (Ahmed et al., 2023; Alharbi & Tassaddiq, 2021; Tirumala et al., 2016).

The results also showed that the respondents had a high level of financial management readiness, with an overall mean score of 3.22 and a standard deviation of 0.48. This indicates that the students generally perceived themselves as ready to manage basic financial responsibilities such as budgeting, saving, spending control, and responsible use of digital payment platforms. Financial literacy literature supports the importance of developing these competencies among young people because financial knowledge and confidence influence financial behavior, resource management, and decision-making (Asaad, 2015; Goyal & Kumar, 2021; Stolper & Walter, 2017). The high level of financial management readiness in this study suggests that the respondents had basic preparedness for handling personal financial matters, especially in a context where digital transactions are increasingly becoming part of student life.

Budgeting obtained the highest mean score among the financial management readiness indicators, with a mean of 3.35 and a standard deviation of 0.44. This result suggests that students were more prepared in planning how to allocate their financial resources. Budgeting is a fundamental component of financial readiness because it supports spending control, saving, prioritization of needs, and prevention of unnecessary financial risk. This finding is aligned with research showing that financial literacy contributes to more responsible financial behavior, especially in relation to saving, spending, planning, and resource management (Asaad, 2015; Rahayu et al., 2022; Stolper & Walter, 2017). In accessible education settings, budgeting readiness is particularly important because students may need to manage limited resources for academic requirements, transportation, communication, online learning, and personal needs.

The responsible use of digital payment platforms was also rated high, with a mean score of 3.31 and a standard deviation of 0.46. This finding reflects the growing role of digital finance in students' daily transactions. Digital financial literacy studies emphasize that the ability to use digital financial services responsibly is now part of broader financial competence because financial decisions increasingly occur through mobile banking, e-wallets, online payments, and digital platforms (Aryan et al., 2024; Clarence & Pertiwi, 2023; Rahayu et al., 2022). However, the use of digital payment platforms also creates exposure to cyber fraud risks. Therefore, financial management readiness must be integrated with cyber fraud prevention so that students can manage money while also protecting their accounts, personal information, and online transactions.

The lowest-rated indicator under financial management readiness was decision-making in managing personal financial resources, with a mean score of 3.10 and a standard deviation of 0.55. Although still interpreted as high, this result indicates that students may need more support in applying financial knowledge to real-life decision-making. Financial decision-making requires more than awareness of budgeting or saving; it involves comparing options, evaluating risks, resisting impulsive spending, identifying fraud-related financial threats, and making choices based on long-term consequences. Studies on financial literacy and financial behavior emphasize that financial readiness depends on knowledge, confidence, attitudes, and actual decision-making behavior (Asaad, 2015; Febrianty et al., 2024; Goyal & Kumar, 2021). Thus, the comparatively lower score in decision-making suggests that accessible education programs should include practical exercises, case analysis, and scenario-based learning on personal finance and digital financial risk.

The overall comparison of the two major variables showed that cyber fraud prevention obtained a slightly higher mean score of 3.31 compared with financial management readiness, which obtained a mean score of 3.22. Both variables were interpreted as high, but the difference suggests that the respondents may feel slightly more confident in recognizing and avoiding cyber fraud than in making applied financial management decisions. This pattern is important because digital safety and financial readiness are closely connected in the current financial environment. Digital financial literacy studies show that financial behavior is increasingly influenced by one's ability to understand and safely use digital financial services (Aryan et al., 2024; Clarence & Pertiwi, 2023; Rahayu et al., 2022). Therefore, students who are digitally aware may still need stronger financial decision-making competencies, particularly when dealing with online purchases, e-wallet use, digital banking, online lending, and possible scam-related transactions.

The findings further suggest that cyber fraud prevention and financial management readiness should be addressed together in accessible education settings. Cyber fraud prevention provides the protective dimension, while financial management readiness provides the decision-making dimension. When students are taught only how to manage money but not how to recognize fraud, they may remain vulnerable to online scams. Likewise, when students are taught only how to avoid suspicious links but not how

to evaluate financial choices, they may still struggle with financial planning and resource management. This supports the argument that digital financial literacy must combine knowledge of financial products, digital platforms, cyber risk, consumer protection, and responsible behavior (Febrianty et al., 2024; OECD, 2023; Rahayu et al., 2022). The results of this study therefore point to the need for an integrated framework rather than separate interventions.

The findings are also relevant to accessible education because accessibility is not limited to classroom participation or physical accommodation. It also includes the ability of students to safely access digital tools, understand online financial systems, protect their personal information, and receive institutional support when risks occur. Research on accessible and inclusive education emphasizes that students may experience barriers not only in physical spaces but also in institutional procedures, technologies, communication systems, and support mechanisms (Marquis et al., 2016). Digital inclusion literature further explains that technology can support participation only when learners are provided with accessible, understandable, and responsive systems (Nguyen, 2020). Thus, a framework for accessible education settings should include cyber fraud prevention and financial management readiness as part of learner protection and student support.

The high ratings in most indicators provide a positive foundation for framework development. However, the lower scores in reporting cyber fraud incidents, financial risk awareness, and personal financial decision-making show the areas where intervention is most needed. These results suggest that the proposed framework should include four major components: digital safety awareness, cyber fraud reporting mechanisms, financial management skills, and accessible learner support. Cybersecurity literature supports the value of structured awareness programs, simulation-based learning, and practical user education in improving protective behavior (Alqahtani & Kavakli, 2020; Baadel et al., 2021; Chatchalermpun & Daengsi, 2021). Financial literacy literature also supports practical and behavior-oriented instruction that strengthens budgeting, saving, risk evaluation, and responsible decision-making (Asaad, 2015; Goyal & Kumar, 2021; OECD, 2023).

From a practical perspective, the findings imply that schools in accessible education settings may develop short training modules on cyber fraud prevention, phishing identification, password protection, digital payment safety, and fraud reporting. These may be integrated into student orientation, guidance programs, financial literacy activities, information technology courses, business-related courses, or student support services. For financial management readiness, activities may include budgeting worksheets, personal finance simulations, decision-making cases, digital payment safety exercises, and fraud-related financial scenarios. These strategies are aligned with research recommending continuous, contextualized, and skills-based digital and financial literacy instruction for students (Clarence & Pertiwi, 2023; Erendor & Yildirim, 2022; Rahayu et al., 2022).

From a policy and institutional perspective, the findings suggest the need to strengthen student protection mechanisms in digital and financial activities. Accessible education settings should provide clear reporting channels for cyber fraud incidents, user-friendly information materials, inclusive communication strategies, and support services for students who may experience digital or financial vulnerability. Since students with diverse learning needs may encounter barriers in accessing or understanding digital systems, institutional support should be simple, visible, and responsive (Marquis et al., 2016; Nguyen, 2020). The proposed framework should therefore promote not only individual responsibility but also institutional responsibility in creating safe and accessible digital learning environments.

Overall, the discussion shows that the respondents had high cyber fraud prevention and high financial management readiness, but the findings also point to specific areas requiring improvement. The strongest areas were identifying suspicious messages and budgeting, while the weaker areas were reporting cyber fraud

incidents and making personal financial decisions. These results support the development of a framework that integrates cyber fraud prevention, digital financial literacy, financial decision-making, and accessible student support. Such a framework may help students become safer, more responsible, and more financially prepared participants in digital and educational environments.

5. Conclusion

This study examined cyber fraud prevention and financial management readiness among 57 students from Bongao, Tawi-Tawi, Philippines, within the context of accessible education settings. The findings showed that the respondents had a high level of cyber fraud prevention, particularly in identifying suspicious messages, protecting passwords, safeguarding personal information, avoiding phishing links, verifying online transactions, and recognizing fraudulent digital activities. The results also showed that the respondents had a high level of financial management readiness, especially in budgeting, responsible use of digital payment platforms, saving readiness, spending control, financial planning, and financial risk awareness. However, comparatively lower mean scores were observed in reporting possible cyber fraud incidents and decision-making in managing personal financial resources, indicating areas that may still be strengthened through targeted digital safety and financial literacy activities.

The study further concluded that students already possessed foundational awareness and readiness in managing cyber fraud risks and personal financial responsibilities. This suggests that learners in accessible education settings may already be familiar with basic digital safety practices and financial management concepts. However, the findings also highlight the need to move beyond general awareness toward practical response skills, especially in reporting cyber fraud incidents, evaluating online financial risks, and making sound financial decisions. In accessible education settings, learner preparation should not focus only on academic participation but should also include digital safety, financial readiness, responsible online behavior, and protection from cyber-related financial risks.

Based on the findings, it is recommended that education institutions strengthen student support programs that integrate cyber fraud prevention and financial management readiness. Instructional strategies may include phishing identification exercises, password protection activities, fraud-reporting simulations, budgeting worksheets, digital payment safety orientation, case analysis, and practical scenarios on online financial decision-making. Schools may also consider developing clear and accessible reporting mechanisms for cyber fraud concerns so that students will know where, when, and how to report suspicious digital activities. These initiatives may help students become safer, more responsible, and more financially prepared users of digital platforms.

The findings also support the development of a framework for accessible education settings that combines digital safety awareness, cyber fraud reporting, financial literacy, personal finance decision-making, and learner support services. Such a framework may guide educators, student affairs personnel, guidance offices, and institutional leaders in designing programs that respond to the digital and financial risks experienced by learners. The framework may also contribute to inclusive and special education by emphasizing that accessibility should include not only physical and instructional access but also safe access to digital tools, financial information, and online services.

This study was limited to 57 students from Bongao, Tawi-Tawi; therefore, the findings may not fully represent students from other provinces, institutions, or academic programs. The study also used a descriptive quantitative design, which means that it described the respondents' levels of cyber fraud prevention and financial management readiness but did not establish causal relationships or explain deeper personal experiences behind the results. Since the data were based on self-reported responses, there may also be possible response bias or overestimation of actual practices. Future

researchers may conduct similar studies with a larger sample size, include respondents from different locations, and use mixed-methods approaches to gather qualitative explanations. Future studies may also examine other factors that may influence cyber fraud prevention and financial management readiness, such as digital access, prior cybersecurity training, family financial background, exposure to online transactions, academic program, and institutional support.

References

Ahmed, A. A., Elmi, A. H., & Abdullahi, A. (2023). Cybersecurity awareness among university students in Mogadishu: A comparative study. *Indonesian Journal of Electrical Engineering and Computer Science, 32*(3), 1580–1588. https://doi.org/10.11591/ijeecs.v32.i3.pp1580-1588

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing, 5*(2), 23. https://doi.org/10.3390/bdcc5020023

Alqahtani, H., & Kavakli, M. (2020). Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). *Information, 11*(2), 121. https://doi.org/10.3390/info11020121

Aryan, L. A., Alsharif, A., & Alquqa, E. K. (2024). How digital financial literacy impacts financial behavior in Jordanian millennial generation. *International Journal of Data and Network Science*. https://doi.org/10.5267/j.ijdns.2023.10.011

Asaad, C. T. (2015). Financial literacy and financial behavior. *Financial Services Review, 24*(2), 101–117. https://doi.org/10.61190/fsr.v24i2.3236

Baadel, S., Thabtah, F., & Lu, J. (2021). Cybersecurity awareness: A critical analysis of education and law enforcement methods. *Informatica, 45*(3). https://doi.org/10.31449/inf.v45i3.3328

Chatchalermpun, S., & Daengsi, T. (2021). Improving cybersecurity awareness using phishing attack simulation. *IOP Conference Series: Materials Science and Engineering, 1088*(1), 012015. https://doi.org/10.1088/1757-899X/1088/1/012015

Clarence, J., & Pertiwi, D. (2023). Financial management behavior among students: The influence of digital financial literacy. *International Journal of Financial and Investment Studies, 4*(1), 9–16. https://doi.org/10.9744/ijfis.4.1.9-16

Erendor, M. E., & Yildirim, M. (2022). Cybersecurity awareness in online education: A case study analysis. *IEEE Access*. https://doi.org/10.1109/ACCESS.2022.3171829

Febrianty, F., Yuliansyah, Y., & Hamzah, R. S. (2024). Gender issues in digital financial literacy and financial behavior among millennials. *Jurnal Economia, 20*(1). https://doi.org/10.21831/economia.v20i1.56529

Goyal, K., & Kumar, S. (2021). Financial literacy: A systematic review and bibliometric analysis. *International Journal of Consumer Studies, 45*(1), 80–105. https://doi.org/10.1111/ijcs.12605

Marquis, E., Schormans, A. F., Jung, B., Vietinghoff, C., Wilton, R., & Baptiste, S. (2016). Charting the landscape of accessible education for post-secondary students with disabilities. *Canadian Journal of Disability Studies, 5*(2), 31–71. https://doi.org/10.15353/cjds.v5i2.272

Nguyen, A. (2020). Digital inclusion. In *Encyclopedia of the UN Sustainable Development Goals*. Springer. https://doi.org/10.1007/978-3-030-48277-0_14-1

OECD. (2023). *PISA 2022 financial literacy framework*. OECD Publishing. https://doi.org/10.1787/b5659b4f-en

Rahayu, R., Ali, S., & Aulia, A. (2022). The current digital financial literacy and financial behavior in Indonesian millennial generation. *Journal of Accounting and Investment, 23*(1). https://doi.org/10.18196/jai.v23i1.13205

Stolper, O. A., & Walter, A. (2017). Financial literacy, financial advice, and financial behavior. *Journal of Business Economics, 87*, 581–643. https://doi.org/10.1007/s11573-017-0853-9

Tirumala, S. S., Sarrafzadeh, A., & Pang, P. (2016). A survey on internet usage and cybersecurity awareness in students. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE. https://doi.org/10.1109/PST.2016.7906931

8. Author Declaration

The authors declare that this manuscript is original, unpublished, and not under consideration elsewhere. All authors contributed to the preparation and finalization of the manuscript and accept responsibility for its content. The authors also declare no conflict of interest. No financial, institutional, personal, or professional relationship influenced the conduct, interpretation, or presentation of this study.