JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

CYBER CAUTION CONFIDENCE: EXPLORING BIABAS TRADE HIGH SCHOOL STUDENTS' LIVED EXPERIENCES ON CYBERSECURITY

Zaldy H. Bacus
Secondary School Teacher II
Department of Education – Division of Bohol
Biabas Trade High School
Ubay, Bohol, Philippines
Email: zaldybacus30@gmail.com

Niña D. Costillas
Student Researchers
Department of Education – Division of Bohol
Biabas Trade High School
Ubay, Bohol, Philippines

Lynette V. Delantar
Student Researchers
Department of Education – Division of Bohol
Biabas Trade High School
Ubay, Bohol, Philippines

Laiza Claire D. Denulan
Student Researchers
Department of Education – Division of Bohol
Biabas Trade High School
Ubay, Bohol, Philippines

Keith Zarene A. Pobar
Student Researchers
Department of Education – Division of Bohol
Biabas Trade High School
Ubay, Bohol, Philippines

Corresponding Author

Zaldy H. Bacus
Secondary School Teacher II
Department of Education – Division of Bohol
Biabas Trade High School
Ubay, Bohol, Philippines
Email: zaldybacus30@gmail.com

ABSTRACT

This qualitative phenomenological study explored the lived experiences, perceptions, and challenges of Grade 11 students at Biabas Trade High School regarding cybersecurity threats, specifically hacking, phishing, and identity theft, during the 2026–2027 academic year. Grounded in Bandura's Self-Efficacy Theory, Ajzen's Theory of

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

Planned Behavior, Rogers's Protection Motivation Theory, and Weinstein's Optimism Bias Theory, the research investigated how students navigate digital risks and develop cyber caution and confidence. Employing a qualitative phenomenological design with purposive sampling, the researchers gathered data from selected student participants using a researcher-made, semi-structured interview guide. The collected transcripts were analyzed using thematic analysis. The findings revealed three major themes: first, students experienced emotional anxiety from digital threats that acted as a catalyst for defensive browsing and verification habits; second, participants encountered significant challenges involving cognitive overload, deceptive social engineering tactics, academic stress, and security friction in password management due to lockout fears; and third, navigating these online hazards fostered psychological growth, transforming students into self-reliant digital citizens who recognized their personal agency and expressed a strong demand for hands-on, school-based cybersecurity education. The study concluded that while threat encounters cultivate individual vigilance, structured institutional and pedagogical support is essential to bridge the persistent awareness–behavior gap. Consequently, recommendations were proposed for the Department of Education, Biabas Trade High School, school principals, educators, ICT coordinators, students, parents, and future researchers to implement practical, experiential digital safety frameworks and enhance overall student resilience.

Keywords: *Cybersecurity Threats, Hacking, Phishing, Identity Theft, Digital Safety, Cybersecurity Awareness, Student Experiences, Cyber Caution, Self-Efficacy, Digital Resilience, Online Risks, Cybersecurity Education*

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

INTRODUCTION

Background of the Study

Cybersecurity awareness and protective behavior play a vital role in the safe navigation of digital environments by secondary students. Cybersecurity is the practice of defending internet-connected networks and personal profiles from unauthorized exploitation, such as hacking, phishing, and identity theft, and it directly governs how safely students navigate online spaces. Cybersecurity caution and confidence represent the ability of students to actively manage their digital footprint, identify evolving threats, and build the self-efficacy needed to protect their personal data. They also promote active vigilance and personal responsibility in mastering digital safety protocols. By understanding these experiences, educators and school administrators can better support students in developing practical, protective, and resilient ways of navigating the internet.

Understanding students' actual lived experiences in the digital space is essential to improving their cyber defense habits and overall digital well-being. Although many Biabas Trade High School (BTHS) students frequently interact with digital environments, they still struggle to navigate these platforms safely and to recognize advanced cyber traps (Alharbi et al., 2022). Domestically, emerging studies reveal that while Filipino senior high school students may demonstrate moderate baseline awareness, their actual online safety practices remain highly uneven and fragmented (Mansueto et al., 2026). This behavioral disconnect is echoed in regional contexts across the Philippines, where a student's perceived behavioral control and localized risk exposure heavily determine whether digital security awareness translates into protective, responsible conduct (Booc et al., 2024). Internationally, technical and vocational trainees frequently struggle with policy compliance and threat identification because of a systemic lack of integrated safety education (Alrobaian et al., 2023). They often rely on passive information delivery rather than on experiential, hands-on, or game-based learning strategies that actively bridge the gap between abstract awareness and practical, everyday security habits (Tempestini et al., 2024).

The contributing factors to this issue include the absence of continuous, hands-on digital safety training and inconsistent home monitoring, which leave students with a false sense of security when browsing the web. Additionally, a lack of defensive confidence leaves teenagers vulnerable to sophisticated social engineering and data exploitation, leading to frequent data exposures, emotional stress, and critical academic disruptions. To respond to this concern, schools have implemented digital safety frameworks; however, a critical gap remains in understanding the personal narratives of vocational students who face these threats daily.

The primary goal of this phenomenological study was to deeply explore and understand the lived experiences of Biabas Trade High School (BTHS) students as they navigated the complexities of cybersecurity. It aimed to determine how their encounters with hacking, phishing, and identity theft shape their cyber caution and confidence, and to identify the specific vulnerabilities they face in their digital routines. Through this research, students, educators, and community stakeholders may discover practical, student-centered digital literacy insights that can enhance lifelong cyber protection and institutional defense frameworks within the school setting.

Cybersecurity, as understood in this study, is not limited to the technical tools that protect networks and devices. For secondary students, it is also a matter of everyday decisions: whether to open a message from an unknown sender, how to respond to a prize offer or a suspicious link, whether to share a password with a friend, and how often to change the credentials that protect school and personal accounts. Hacking, phishing, and identity theft therefore matter not only as technical events but also as experiences that carry emotional, social, and academic consequences for the students who encounter them.

Two sets of ideas frame this inquiry. The first is that awareness of cyber threats does not automatically produce protective behavior; the literature reviewed in this study repeatedly describes an awareness–behavior gap among adolescent and vocational learners. The second is that students' confidence in their own ability to protect themselves, their perceived control over their digital environment, and their sense of risk all shape whether awareness becomes practice. How BTHS students experience these tensions in their own digital routines is the central concern of this study.

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

Understanding these experiences calls for an approach that goes beyond measuring how much students know about cybersecurity. Knowledge scores, however useful, cannot show how a student felt upon receiving a phishing text, what a student did after seeing a cloned account, or how an encounter with a threat changed the way a student approaches the internet. For this reason, the study employed a qualitative phenomenological design, which places the lived experiences of students at the center of inquiry and treats their own words as the primary evidence.

The study was set at Biabas Trade High School in Barangay Biabas, Ubay, Bohol, a technical-vocational secondary school whose students regularly use digital tools, social media, and online educational platforms. Studying cybersecurity caution and confidence in this setting draws attention to a group of learners who are routinely online, who are exposed to the threats described above, and whose personal narratives remain underrepresented in the literature reviewed. The study therefore addresses a gap in local understanding of how vocational students experience, interpret, and respond to cyber threats.

Review of Related Literature

Theoretical Foundations

The theoretical foundation of this study draws on frameworks that explain how cognitive mindsets, risk assessments, behavioral intentions, and perceptual biases shape cybersecurity choices. Bandura's (1977) Social Cognitive Theory/Self-Efficacy Theory serves as the core foundation, positing that a student's belief in their capability to execute defensive actions deeply dictates their proactive stance in handling digital threats. This internal confidence is expanded by Ajzen's (1985) Theory of Planned Behavior, which asserts that safe online routines depend heavily on perceived behavioral control and positive intentions, highlighting why a theoretical understanding of cyber threats does not automatically translate into secure habits unless students feel in control of their technical environment.

Furthermore, Rogers's (1975) Protection Motivation Theory explains that teenagers develop strong cyber caution only when a cognitive appraisal of threat severity and vulnerability is balanced against their perceived response efficacy. However, this rational evaluation is frequently compromised by Weinstein's (1980) Optimism Bias Theory, which exposes a cognitive distortion in which high school students operate under a "false sense of security," believing that they are inherently less vulnerable to cyber threats than their peers.

Integrating the Theoretical Perspectives

Together, this theoretical cluster provides a comprehensive psychological lens for exploring the lived tension between a student's internal confidence, cognitive risk calculations, and actual protective behaviors. The four perspectives complement one another. Protection Motivation Theory (Rogers, 1975) directs attention to how students appraise the threats they encounter, while Optimism Bias Theory (Weinstein, 1980) explains why that appraisal may be distorted by a false sense of security. Self-Efficacy Theory (Bandura, 1977) and the Theory of Planned Behavior (Ajzen, 1985) then address whether students believe they are capable of acting and feel in control of their technical environment, which determines whether awareness becomes protective behavior.

These perspectives were used in this study as interpretive guides rather than as hypotheses to be tested. Because the study is qualitative and phenomenological, the themes were derived from the participants' accounts, and the theories were then used to interpret what those accounts mean. Table 1 summarizes how each perspective relates to the focus of the study and to the themes that emerged from the interviews.

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

Table 1. Theoretical Perspectives and Their Relevance to the Study

Theoretical Perspective	Core Ideas	Relevance to the Study	Related Theme
Social Cognitive Theory/Self-Efficacy Theory (Bandura, 1977)	Belief in one's capability to execute defensive actions	Explains how students' confidence shapes their proactive stance in handling digital threats	Theme 3
Theory of Planned Behavior (Ajzen, 1985)	Perceived behavioral control and positive intentions	Explains why understanding of cyber threats does not translate into secure habits unless students feel in control of their technical environment	Theme 3
Protection Motivation Theory (Rogers, 1975)	Cognitive appraisal of threat severity and vulnerability balanced against perceived response efficacy	Explains how cyber caution develops after students appraise the threats they encounter	Theme 1
Optimism Bias Theory (Weinstein, 1980)	A cognitive distortion in which individuals believe they are less vulnerable to threats than their peers	Explains how a "false sense of security" and convenience-seeking compromise rational risk evaluation and security practices	Theme 2

Legal and Regulatory Context and the Sustainable Development Goals

The legal and institutional context for safeguarding the digital safety of secondary learners in the Philippines is established through several key national policies and is aligned with global development goals. Republic Act No. 10175 (Cybercrime Prevention Act of 2012) serves as the country's primary legal framework for combating offenses such as illegal access, phishing, and identity theft, directly supporting the study's focus on students' exposure to these digital crimes. This protection is reinforced by the Data Privacy Act of 2012 (Republic Act No. 10173), which mandates the secure processing of personal information, highlighting the institutional importance of defending student data on digital academic platforms.

Additionally, Republic Act No. 7610 (Special Protection of Children Against Abuse, Exploitation and Discrimination Act of 1992) outlines the state's responsibility to protect child development from exploitation and harm, while Republic Act No. 9775 (Anti-Child Pornography Act of 2009)—reinforced by the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act (Republic Act No. 11930)—penalizes the digital transmission of youth exploitation materials, which are often facilitated through compromised student accounts. Furthermore, Republic Act No. 8484 (Access Devices Regulation Act of 1998, as amended by Republic Act No. 11449) provides the specific legal basis for addressing credential theft and password exploitation.

On an international level, this legal scaffold intersects with the United Nations Sustainable Development Goals (SDGs). In particular, it advances SDG 4 (Quality Education, Targets 4.4 and 4.a) by promoting safe, non-violent, and inclusive digital learning environments while developing essential digital literacy and cybersecurity competencies among youth (UNESCO, 2020; United Nations, 2015). It also underpins SDG 16 (Peace, Justice, and Strong Institutions, Target 16.2), which mandates the eradication of all forms of violence, abuse, trafficking, and exploitation of children, particularly in online spaces (United Nations, 2015). Collectively, these statutory mandates and global benchmarks establish a protective framework that underscores the critical necessity of fostering cybersecurity caution and confidence among minor learners at Biabas Trade High School (BTHS).

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

Taken together, these laws and global goals define cyber-related offenses, set obligations for the protection of personal data and of children, and establish the expectation that learners be educated and protected in digital spaces. They do not, however, describe how students themselves experience these threats or how they develop the caution and confidence needed to respond. This study complements the legal and policy framework by documenting those experiences from the students' own perspective.

Related Literature and Studies

The review of related literature and studies provides strong empirical support and context, confirming how theoretical awareness, educational interventions, and social dynamics influence the actual cybersecurity practices of students. Internationally, research by Ravichandran et al. (2025) and Oguine et al. (2025) highlights that technical exposure without structured cybersecurity instruction leads to an operational knowledge gap and a sense of helplessness, which can be mitigated through the experiential, game-based simulations explored by Miller et al. (2024). This behavioral gap is echoed locally by Dela Cruz et al. (2024), who found that high social media familiarity does not equal actual protection, and by Aquino (2023), who linked teenage vulnerability to a lack of perceived behavioral control under peer pressure. Furthermore, Akter et al. (2025) and Bermudez et al. (2022) identify a "privacy paradox" and social norms in which teenagers share passwords as a sign of trust, while Gonzales et al. (2025) demonstrate how technical students often succumb to the optimism bias.

While studies show moderate general awareness (Alabab et al., 2023; Rasul et al., 2026), structured educational programs and interactive learning platforms have been shown to significantly boost digital resilience (Alqahtani, 2022; Bulala et al., 2026; Calimbo et al., 2025; Khamzina et al., 2022; Kraus et al., 2023; Palao et al., 2026). Ultimately, the persistent awareness–behavior gap identified by Rosano et al. (2026) and the high rate of risky credential habits observed by Pascual (2024) validate the need for hands-on, simulated environments (Mendoza, 2026) and justify this study's qualitative exploration of the lived cybersecurity experiences of local high school students.

Patterns in the Related Studies

Several patterns emerge from the studies reviewed. The first concerns the gap between exposure and competence. Ravichandran et al. (2025) and Oguine et al. (2025) show that frequent technical exposure, without structured cybersecurity instruction, produces an operational knowledge gap and a sense of helplessness rather than protection. Alharbi et al. (2022) found that high school students struggle to recognize advanced cyber traps, and Alrobaian et al. (2023) reported that technical and vocational trainees struggle with policy compliance and threat identification because safety education is not integrated into their training. These studies suggest that being familiar with digital platforms is different from being able to defend oneself on them.

The second pattern is the awareness–behavior gap among Filipino learners. Mansueto et al. (2026) described moderate baseline awareness but uneven and fragmented safety practices, and Rosano et al. (2026) identified a persistent gap between awareness and behavior among technical trainees. Dela Cruz et al. (2024) found that high social media familiarity does not equal actual protection, Booc et al. (2024) linked protective digital habits to perceived behavioral control and localized risk exposure, and Pascual (2024) observed a high rate of risky credential habits. Aquino (2023) tied teenage vulnerability to a lack of perceived behavioral control under peer pressure. Across these studies, awareness alone does not explain what students actually do.

The third pattern concerns social and psychological influences. Akter et al. (2025) and Bermudez et al. (2022) describe a privacy paradox and social norms in which teenagers share passwords as a sign of trust, and Gonzales et al. (2025) show how technical students may succumb to the optimism bias, believing themselves less vulnerable than their peers. These findings are consistent with the theoretical perspectives discussed earlier and indicate that students' choices are shaped by relationships and beliefs as well as by knowledge.

The fourth pattern concerns educational responses. Structured educational programs and interactive learning platforms have been shown to boost digital resilience (Alqahtani, 2022; Bulala et al., 2026; Calimbo et al., 2025; Khamzina et al., 2022; Kraus et al., 2023; Palao et al., 2026). Game-based and simulated environments in

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

particular are reported to close the gap between abstract awareness and practical habits (Mendoza, 2026; Miller et al., 2024; Tempestini et al., 2024). Together, these studies argue for hands-on, experiential approaches rather than passive information delivery.

Taken together, the literature describes levels of awareness, patterns of risky behavior, and the effects of educational interventions. What remains less developed is an account, in students' own words, of how vocational students experience hacking, phishing, and identity theft and of what they come to understand about their own caution and confidence. This is the gap that the present study addresses.

Statement of the Problem

This qualitative study aimed to deeply explore and understand the lived experiences of selected Biabas Trade High School (BTHS) students regarding cybersecurity during School Year 2026–2027. It specifically focused on their perceptions, challenges, and the development of cyber caution and confidence in navigating digital environments against core threats such as hacking, phishing, and identity theft. This exploration is crucial given the increasing exposure of secondary students to digital threats and the identified gaps in their operational knowledge and online safety practices.

Specifically, it sought to answer the following questions:

1. How do BTHS students describe their lived experiences and perceptions regarding core cybersecurity threats, such as hacking, phishing, and identity theft?
2. What specific challenges do students encounter when attempting to detect and prevent incidents related to hacking, phishing, and identity theft in their daily digital interactions?
3. What realizations do students gain regarding their cyber caution and confidence after encountering or navigating risks associated with hacking, phishing, and identity theft?
4. Based on the results of the study, what recommendations can be made to enhance cybersecurity education and protective practices for BTHS students?

Objectives of the Study

This study aimed to deeply explore and understand the lived experiences, perceptions, and challenges of BTHS students in navigating cybersecurity threats and in developing cyber caution and confidence.

Specifically, it sought to:

1. describe the lived experiences and perceptions of BTHS students regarding core cybersecurity threats, such as hacking, phishing, and identity theft;
2. identify the specific challenges students encounter when attempting to detect and prevent incidents related to hacking, phishing, and identity theft in their daily digital interactions;
3. explore the realizations students gain regarding their cyber caution and confidence after encountering or navigating risks associated with hacking, phishing, and identity theft; and
4. propose recommendations, based on the results of the study, to enhance cybersecurity education and protective practices for BTHS students.

Scope and Delimitation of the Study

This study explored the lived experiences, perceptions, and challenges of selected Biabas Trade High School students regarding cybersecurity during the academic year 2026–2027. The scope was specifically limited to an in-depth exploration of three core digital threat areas: hacking, phishing, and identity theft. The research focused on the immediate and retrospective insights of students within this institution, specifically examining how they navigate these risks to develop cyber caution and digital confidence.

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

The study covered fifteen (15) Grade 11 Senior High School students of Biabas Trade High School who were selected through purposive sampling and who had firsthand experience with hacking, phishing, or identity theft. Data were gathered through individual, semi-structured interviews and analyzed thematically.

The study was further delimited to these three specified cyber threats and excluded technical security analyses and quantitative measurements. Consequently, the results are specific to the localized digital context of Biabas Trade High School and cannot be generalized to broader secondary student populations or to other academic institutions.

Only students served as participants. Parents, teachers, school administrators, and ICT personnel were not interviewed, even though the findings and recommendations are relevant to them. As a qualitative study, it aims for depth of understanding rather than statistical generalization.

Significance of the Study

This research study holds significant value for various stakeholders. By exploring the lived experiences, perceptions, and challenges of students in navigating digital threats, the findings may provide a foundation for enhancing cybersecurity education and protective practices across different levels of the educational hierarchy.

Department of Education (DepEd). The findings of this study may provide the Department of Education with empirical data essential for the formulation and refinement of national and regional policies concerning cybersecurity education. By understanding the actual digital risks and behavioral responses of secondary students, DepEd can better align the K–12 curriculum with the practical needs of learners in an increasingly digitalized world. This research supports the department's goal of producing digitally literate and resilient Filipino learners.

Biabas Trade High School (BTHS). As the primary setting of the study, Biabas Trade High School may directly benefit from the localized data gathered. The school administration can use the results to assess the effectiveness of its current digital safety protocols and to identify specific areas where institutional defense frameworks may fall short. This may enable BTHS to implement more robust, school-wide cybersecurity initiatives that are grounded in the actual experiences of its own student body.

Principal. The principal, as the school's chief academic and administrative officer, may find this study valuable for strategic decision-making regarding cybersecurity policies and resource allocation. The findings may enable the principal to champion and oversee the implementation of comprehensive cybersecurity programs, ensuring alignment with educational objectives and the overall safety of the school community. This leadership role is crucial in fostering a culture of cyber awareness and resilience among students and staff.

Educators. This study offers educators a deeper understanding of the specific cyber threats, such as hacking, phishing, and identity theft, that their students encounter. By recognizing the gap between student awareness and actual practice, teachers can develop more effective, hands-on pedagogical strategies. This research may help educators move beyond passive information delivery toward experiential learning that builds genuine cyber caution and confidence in their students.

Information and Communication Technology (ICT) School Coordinator. The insights from this research may assist ICT school coordinators and technical staff in optimizing the school's digital infrastructure and support systems. By identifying the common "cyber traps" and technical challenges students face, ICT school coordinators can implement more targeted security measures, such as improved filtering, better authentication protocols, and more relevant technical guidance for both students and staff.

Students. The primary beneficiaries of this study are the students themselves. By participating in this research, students were given a platform to reflect on their digital habits and realizations. The resulting recommendations may lead to the development of student-centered programs that directly address their vulnerabilities, empowering

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

them with the practical skills and confidence needed to protect their personal data and academic focus from online exploitation.

Parents and Guardians. This research may provide parents and guardians with a clearer perspective on the digital landscape their children navigate daily. The findings can serve as a guide for home-based monitoring and open communication regarding online safety. By bridging the gap between school and home, this study fosters a more holistic support system that protects students from the emotional and financial stress of online scams.

Researchers. The conduct of this study allowed the researchers to gain a profound understanding of the complexities surrounding cybersecurity and student behavior. It provided an opportunity to apply qualitative research methodologies to a real-world problem, enhancing their skills in data collection, thematic analysis, and academic writing. This process fosters their professional growth as critical thinkers and contributors to the field of educational research.

Future Researchers. For the academic community, this study establishes a foundational reference point for subsequent inquiries into the efficacy of cybersecurity education and the psychological aspects of online safety among young adults. Future researchers can build upon the methodological framework and findings of this study to explore similar phenomena in different regional contexts or among different demographic groups, further advancing the global understanding of digital literacy and cyber protection.

Taken together, these benefits show that the study is relevant to practice, policy, and scholarship. For practice, it describes the everyday conditions under which students encounter and respond to cyber threats. For policy, it identifies the points of friction, namely lockout fears, cognitive overload, and the lack of hands-on training, where institutional support may be directed. For scholarship, it adds a qualitative account that can be compared with, and tested against, the theories and studies reviewed.

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

METHODS

Research Design

This study employed a qualitative phenomenological research design. This approach was chosen to gain a deep, nuanced, and empathetic understanding of the lived experiences, perceptions, and meanings that Senior High School students attach to navigating cybersecurity risks. Since the study primarily aimed to explore how students encounter, react to, and make sense of digital threats such as hacking, phishing, and identity theft, a phenomenological design was considered the most appropriate methodology. The in-depth, semi-structured interviews allowed the researchers to capture rich, descriptive data on the students' technical or emotional struggles, defensive behaviors, and the specific ways they develop personal cyber caution and confidence—insights that would have been difficult to capture or quantify through structured survey methods.

Phenomenology focuses on how people experience a phenomenon and what meaning they give to it. In this study, the phenomenon was cybersecurity as lived by students: the encounters with hacking, phishing, and identity theft, the difficulties of detecting and preventing them, and the realizations that followed. The design treated the participants' own words as the primary evidence and was therefore aligned with the three descriptive research questions of the study, which ask about experiences and perceptions, challenges, and realizations.

Research Environment

The research was conducted at Biabas Trade High School (BTHS), located in Barangay Biabas, Ubay, Bohol. This environment served as the specific context for the study, and all data collection activities were carried out on the school premises. As a local technical-vocational secondary school, BTHS provides a unique and highly relevant tech-voc academic ecosystem where students regularly engage with digital tools, social media, and online educational platforms. Conducting the study within this environment ensured that the findings directly reflect the real-world experiences, digital habits, and baseline safety needs of the students within their actual school and community context.

Participants of the Study

The participants were a group of fifteen (15) Grade 11 Senior High School students from Biabas Trade High School. Unlike quantitative designs, this phenomenological study utilized purposive sampling to select the participants rather than simple random sampling. This sampling technique was intentionally chosen because qualitative research requires "information-rich" cases. To be eligible, the participants had to meet specific criteria: they had to be active users of online platforms and had to have firsthand experience with encountering, managing, or fighting off core digital threats, specifically hacking, phishing, or identity theft. This ensured that the selected student respondents possessed the direct lived experiences necessary to address the research questions of the study.

The number of participants was kept small in keeping with the in-depth interview approach of phenomenological research, in which the richness of each account is prioritized over the breadth of the sample. Restricting participation to active online users with firsthand experience of the threats under study ensured that every interview could speak directly to the phenomenon being explored.

Research Instrument

The primary data collection tool for this research was a researcher-made, semi-structured interview guide. The questions in the guide were carefully crafted to delve deeply into the students' lived experiences, behavioral challenges, and personal realizations regarding cybersecurity threats. The instrument used open-ended questions designed to encourage participants to freely share their encounters with hacking, phishing, and identity theft. The flexible and conversational nature of this semi-structured instrument allowed the researchers to ask spontaneous follow-up questions, probe deeper into students' emotional and technical responses, and gain a thorough, unfiltered understanding of each student's unique digital safety journey.

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

The questions in the guide were directed at the same areas covered by the research questions: how students describe their experiences and perceptions of hacking, phishing, and identity theft; the challenges they face in detecting and preventing such incidents; and the realizations they gain about their own cyber caution and confidence. Because the instrument was semi-structured, the same areas guided every interview, while follow-up questions were adapted to what each participant said.

Data-Gathering Procedure

The research followed a systematic process to ensure ethical standards, participant safety, and qualitative data validity:

Phase 1. Securing Approvals and Consent. First, a formal letter of permission was sent to the school principal of Biabas Trade High School, Mr. Diomedes L. Montero, to obtain official clearance to conduct the study. Upon receiving approval, the researchers coordinated with the Grade 11 advisers to identify students who met the purposive sampling criteria.

Phase 2. Ethical Clearance and Assent. The ethical clearance and assent documents clearly explained the purpose of the study, guaranteed complete confidentiality and anonymity of the participants' personal data, and explicitly stated that participation was entirely voluntary, with the right to withdraw at any time without penalty.

Phase 3. Conducting the Interviews. Individual, one-on-one, semi-structured interviews were scheduled at a convenient time and in a quiet, private location within the school premises to ensure comfort and privacy. With the explicit, written permission of the student (and parent/guardian), each session was audio-recorded to ensure an accurate record of the accounts.

Phase 4. Transcription and Thematic Analysis. Following the completion of the interviews, the audio recordings were transcribed verbatim. The transcribed data then underwent thematic analysis, as described in the next section.

The sequence of the procedure was designed to protect the participants and the quality of the data. Securing permission from the school principal first established the authority of the study within the school. Coordinating with the Grade 11 advisers made it possible to identify students who met the purposive sampling criteria. The ethical clearance and assent documents preceded the interviews so that participants understood the purpose of the study, the confidentiality of their information, and the voluntary nature of their participation. Holding the interviews in a quiet, private location within the school helped students speak comfortably, and audio recording with permission, followed by verbatim transcription, preserved the participants' own words for analysis.

Data Analysis

The transcribed data were analyzed thematically. The researchers systematically read through the transcripts, highlighted significant statements, assigned codes, and grouped recurring patterns into overarching themes that directly answered the research questions regarding students' lived experiences, challenges, realizations, and defensive habits in the digital environment. This process produced the three themes presented in the Results and Discussion section.

The analysis therefore moved from the transcripts to significant statements, from statements to codes, from codes to recurring patterns, and from patterns to themes. The themes were then examined in relation to the research questions and interpreted with reference to the theoretical perspectives and related studies reviewed in the Introduction. Participant excerpts are presented in the next section under the codes P1 to P8.

Ethical Considerations

The study observed ethical standards throughout. A formal letter of permission was sent to the school principal before the participants were approached. The participants were informed of the purpose of the study, were guaranteed complete confidentiality and anonymity of their personal data, and were told that their participation

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

was entirely voluntary, with the right to withdraw at any time without penalty. Interviews were audio-recorded only with the explicit, written permission of the student (and parent/guardian). In reporting the results, participants are identified only by codes (P1 to P8) so that their identities are not disclosed. The authors declare no conflict of interest, as stated in the compliance section of this paper.

Operational Definition of Terms

For clarity and consistency, the key terms in this study are operationally defined as follows:

Cyber Caution. Refers to the heightened state of alertness, skepticism, and active digital habits (such as double-checking links or verifying sender identities) adopted by students to avoid falling victim to online traps.

Cyber Confidence. Refers to the internal self-belief, perceived security skills, and psychological readiness of students to safely navigate digital spaces, defend their personal profiles, and recover from cybersecurity incidents.

Hacking. Refers to the unauthorized access, takeover, or compromise of students' personal social media accounts, educational profiles, or gaming credentials, resulting in distress, loss of digital control, or privacy violation.

Identity Theft. Refers to the unauthorized creation of dummy accounts using a student's name, photos, and personal information, or the malicious impersonation of the student online to deceive others and damage their social standing.

Phishing. Refers to the deceptive messages, suspicious links, fake promotional schemes, or social engineering tricks encountered by students in their daily online messaging or social media platforms, designed to steal their passwords and sensitive data.

Students' Lived Experiences. Refers to the firsthand stories, subjective feelings, and real-life situations of Grade 11 students at Biabas Trade High School as they navigate digital spaces, cope with security breaches, and react to online hazards.

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

RESULTS AND DISCUSSION

This section presents the findings, analysis, and interpretation of the qualitative data gathered from the student participants regarding their lived experiences with cybersecurity at Biabas Trade High School (BTHS). Thematic analysis was used to identify recurring patterns, core meanings, and overarching insights embedded in the participants' responses. The analysis directly addresses the primary objective of the study: exploring how students navigate digital security risks, the specific difficulties they encounter, and the personal realizations they cultivate regarding cyber caution and confidence. Through a rigorous examination of the data, three major themes emerged that capture the multifaceted nature of students' digital lives. Table 2, presented after the three themes, summarizes how the themes relate to the research objectives.

The three themes are: (1) navigating digital threats and developing online vigilance; (2) cognitive overload, deceptive tactics, and security friction; and (3) building digital resilience, proactive self-efficacy, and safety intentions. Taken in sequence, they describe how students first encounter and react to threats, what makes protection difficult, and what students come to understand and want as a result.

Theme 1. Navigating Digital Threats and Developing Online Vigilance

The first theme encapsulates how students experience and interpret everyday online threats such as phishing messages, prize scams, and cloned social media accounts. Participants frequently expressed feelings of fear, anxiety, and vulnerability when confronted with digital traps. However, these direct and indirect encounters served as immediate catalysts, forcing students to adopt defensive browsing routines, restrict public profile access, and employ verification strategies using search engines or generative artificial intelligence tools.

Several participants described their immediate reactions and behavioral adaptations when encountering suspicious communications. One participant shared:

> **P1:** *"When I received a phishing text claiming I won money, I felt nervous about my personal data and immediately checked online before clicking anything."*

Another participant emphasized how witnessing cyber incidents shaped their overall caution:

> **P2:** *"Seeing my classmate lose access to her account made me realize how fast identity theft happens, so I set all my social media profiles to private."*

The responses demonstrate that exposure to digital threats triggers an affective response that directly alters student online behavior. Rather than remaining passive internet consumers, students actively incorporate verification routines when presented with unverified links or unexpected messages. Their accounts highlight a transition from uncritical browsing to deliberate scrutiny of digital interactions.

The participants' narratives strongly support this theme through their consistent emphasis on threat encounters, emotional discomfort, and defensive actions. Their reflections illustrate how real-world exposure to cyber risks dismantles naive trust in online platforms, compelling learners to build localized, self-taught defensive routines.

Discussion

These findings align directly with Rogers's (1975) Protection Motivation Theory, which asserts that individuals initiate protective actions when their cognitive appraisal of threat severity and vulnerability outweighs the perceived hassle of taking precautions. Furthermore, the results echo the empirical observations of Dela Cruz et al. (2024), who noted that exposure to active social engineering forces young internet users to transition from passive engagement toward proactive privacy controls.

Overall, this theme reveals that encountering digital threats serves as a powerful experiential lesson for BTHS students. While these encounters initially induce anxiety, they ultimately cultivate essential habits of digital scrutiny and caution needed to safely navigate complex online environments.

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

In relation to the first research question, the theme shows that students describe their encounters with digital threats as emotionally charged events and not as abstract risks. The feelings of fear, anxiety, and vulnerability reported by participants are the starting point of their caution. The behaviors that follow, namely checking online before clicking, setting profiles to private, and verifying senders, indicate that the students' caution is learned from experience, whether their own or that of classmates. This also suggests that vigilance acquired in this way is largely self-taught, which is a point taken up in the later themes.

Theme 2. Cognitive Overload, Deceptive Tactics, and Security Friction

The second theme focuses on the specific technical, cognitive, and psychological obstacles students face when trying to detect digital threats and maintain personal security. Participants reported struggling with increasingly sophisticated scams, such as near-identical fake profiles and context-aware phishing messages. Additionally, participants highlighted a persistent friction regarding basic security hygiene; specifically, many students avoid updating their passwords regularly because of an overwhelming fear of forgetting new credentials and getting locked out of essential academic and personal accounts.

One participant explained the difficulty of identifying deceptive social media accounts:

> **P3:** *"It is so hard to tell if a message is real or fake when the fake account looks identical to a friend's actual profile."*

Another participant elaborated on the technical and personal friction involved in password management:

> **P4:** *"I rarely change my account passwords because I am terrified of forgetting them and losing access to my school submission files."*

A third participant described the emotional and cognitive toll caused by digital security disruptions:

> **P5:** *"Facing a hacked account creates so much stress that it becomes hard to focus on answering our daily school modules and performance tasks."*

These statements reveal that students operate under substantial cognitive strain caused by deceptive online environments. The sophistication of modern social engineering tactics challenges their limited technical knowledge, while standard security advice—such as maintaining complex, frequently updated passwords—creates operational friction that conflicts with their academic responsibilities.

The qualitative data strongly support this theme by highlighting the recurring tensions between threat sophistication, fear of academic disruption, and inconsistent security practices. The narratives illustrate that students do not neglect security out of apathy, but rather because of usability barriers and cognitive fatigue.

Discussion

These findings are strongly supported by Weinstein's (1980) Optimism Bias Theory, which explains how cognitive distortions and convenience-seeking behaviors can lead individuals to compromise security practices despite knowing that risks exist. The observed operational struggles also validate the empirical findings of Pascual (2024) and Rosano et al. (2026), who identified a persistent "awareness-behavior gap" among high school learners, where technical friction and lockout anxiety routinely prevent students from implementing strong credential management protocols.

Overall, this theme illustrates that BTHS students face notable barriers in maintaining digital security. Overcoming these obstacles requires moving beyond abstract warnings toward user-friendly, practical security tools and supportive institutional frameworks that reduce the friction of safe cyber practices.

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

In relation to the second research question, the theme shows that the obstacles to protection are not only technical. Participants described a cognitive difficulty in distinguishing real from fake accounts, an emotional and academic cost when accounts are compromised, and a practical dilemma in password management, in which the safest advice, changing passwords regularly, competes with the fear of losing access to school files. The accounts of P3, P4, and P5 together suggest that students' security practices are shaped by usability and workload as much as by knowledge, which helps explain why awareness does not always become behavior.

Theme 3. Building Digital Resilience, Proactive Self-Efficacy, and Safety Intentions

The third theme emphasizes the internal realizations, psychological growth, and future-oriented intentions developed by students after navigating digital risks. Participants reflected on their personal evolution from gullible, careless internet users to more confident, discerning digital citizens. They recognized that long-term safety requires active self-efficacy, continuous learning, and institutional support, including hands-on cyber safety training within the school setting.

One participant expressed a shift in personal mindset and agency:

> **P6:** *"I realized after almost getting hacked that I cannot just trust every link; I need to keep my account private and learn how to defend myself online."*

Another participant highlighted growing confidence and commitment to proactive security:

> **P7:** *"Handling past scams taught me to slow down, verify suspicious senders, and stay calm instead of panicking when something looks wrong."*

A third participant reflected on the institutional support and practical tools still needed to solidify their digital safety:

> **P8:** *"To feel completely confident, our school needs hands-on workshops where we actually practice identifying real phishing attacks and securing our devices."*

The responses indicate a shift in how students conceptualize their role in digital security. Rather than viewing cybersecurity as an external technical issue managed solely by platform administrators, students increasingly recognize their personal agency in safeguarding their digital footprint. They express a clear desire to complement their heightened caution with formal, practical skills.

The participants' quotes support this theme by consistently highlighting self-reflection, heightened self-efficacy, and constructive intentions for future online behavior. Their accounts demonstrate that surviving or witnessing digital threats can foster psychological resilience and a commitment to safer digital practices.

Discussion

These findings align with Bandura's (1977) Self-Efficacy Theory and Ajzen's (1985) Theory of Planned Behavior, which state that an individual's confidence in performing protective actions directly shapes actual behavioral control and long-term habits. Furthermore, these realizations align with the recommendations of Tempestini et al. (2024) and Mendoza (2026), who advocate experiential, interactive cybersecurity education to effectively convert student safety intentions into sustained digital resilience.

Overall, this theme demonstrates that BTHS students possess the capacity to transform negative digital encounters into constructive learning experiences. By pairing their evolving self-efficacy with structured school-based training, students can build the confidence needed to safely participate in the modern digital landscape.

In relation to the third research question, the theme shows that students do not remain victims of their encounters. They describe a change in mindset, from trusting every link to verifying, and from panic to composure. At the

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

same time, P8 makes clear that students do not regard self-reliance as sufficient: they ask for hands-on workshops in which they can practice identifying real phishing attacks and securing their devices. This request connects the realizations in Theme 3 to the recommendations of the study.

Integrated Discussion of the Themes in Relation to the Research Objectives

The three themes together answer the research questions that guided the study. The first research question, on how BTHS students describe their lived experiences and perceptions regarding hacking, phishing, and identity theft, is addressed mainly by Theme 1, in which exposure to digital threats triggers anxiety that becomes a catalyst for defensive habits. The second, on the challenges students encounter in detecting and preventing these incidents, is addressed by Theme 2, which identifies cognitive overload, deceptive tactics, and security friction. The third, on the realizations students gain regarding their cyber caution and confidence, is addressed by Theme 3, in which students describe growing self-efficacy and a demand for hands-on, school-based training. The fourth, on recommendations, builds on all three themes and is addressed in the final section. Table 2 summarizes these relationships.

Table 2. Relationship of the Themes to the Research Objectives

Research Objective	Theme	Central Meaning	Theoretical and Empirical Support
Objective 1: Describe the lived experiences and perceptions of BTHS students regarding hacking, phishing, and identity theft	Theme 1	Exposure to digital threats triggers anxiety that becomes a catalyst for defensive browsing and verification habits	Protection Motivation Theory (Rogers, 1975); Dela Cruz et al. (2024)
Objective 2: Identify the challenges students encounter in detecting and preventing these incidents	Theme 2	Cognitive overload, deceptive social engineering tactics, academic stress, and password-related security friction due to lockout fears	Optimism Bias Theory (Weinstein, 1980); Pascual (2024); Rosano et al. (2026)
Objective 3: Explore the realizations students gain regarding their cyber caution and confidence	Theme 3	Psychological growth into self-reliant digital citizens who recognize their personal agency and demand hands-on, school-based cybersecurity education	Self-Efficacy Theory (Bandura, 1977); Theory of Planned Behavior (Ajzen, 1985); Tempestini et al. (2024); Mendoza (2026)
Objective 4: Propose recommendations to enhance cybersecurity education and protective practices	Themes 1–3	Structured institutional and pedagogical support is needed to bridge the awareness–behavior gap	Addressed in the Conclusions and Recommendations

Read together, the three themes describe a progression that runs from encounter, to difficulty, to realization. Exposure to threats produces anxiety and defensive habits (Theme 1); the sophistication of deceptive tactics, cognitive overload, and security friction limit how consistently those habits can be kept (Theme 2); and the experience of navigating these hazards builds self-efficacy and a clear demand for structured support (Theme 3). The persistent awareness–behavior gap reported in the literature is visible across all three themes: students know that risks exist and are motivated to protect themselves, yet fear of lockout, fatigue, and the realism of scams stand between that motivation and consistent practice.

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

Implications of the Findings

For students, the findings suggest that caution built from experience is valuable but incomplete. Students who share their verification practices, such as checking suspicious messages online before clicking and keeping profiles private, may strengthen one another's defenses, while the adoption of secure credential management habits may reduce the fear of lockout that discourages password updates.

For educators and the school, the findings point to hands-on, experiential activities, such as practicing the identification of phishing attempts and cloned profiles, as the most direct response to what students reported. Because students' security practices are affected by academic pressure, schools may also consider supportive and clear account recovery arrangements so that protecting an account does not threaten access to school submission files.

For the Department of Education, the principal, and the ICT school coordinator, the findings indicate that policy, resources, and technical support are most useful when they address usability and practical skills, not warnings alone. For parents and guardians, the findings highlight the value of open communication at home about the deceptive traps their children encounter. For researchers, the findings provide a qualitative basis for further studies, including quantitative or mixed-methods work that measures the relationship between lockout anxiety and credential habits.

CONCLUSIONS AND RECOMMENDATIONS

Summary of Findings

Based on the responses of the participants, the following findings were drawn:

Navigating Digital Threats and Developing Online Vigilance. The findings reveal that students at Biabas Trade High School frequently encounter active digital threats such as phishing texts, prize scams, and cloned profiles, which initially trigger anxiety regarding personal data safety. Rather than remaining passive internet consumers, these encounters act as immediate catalysts that compel students to set profiles to private, slow down, and verify suspicious links through search engines or AI tools. The implication of this finding is that real-world exposure to online hazards effectively dismantles naive trust and drives the spontaneous adoption of self-taught defensive routines. Consequently, educators must leverage these experiential triggers by reinforcing proactive privacy controls within structured learning environments.

Cognitive Overload, Deceptive Tactics, and Security Friction. The findings indicate that students face significant difficulties discerning context-aware phishing and cloned profiles, while experiencing severe emotional stress and academic disruption from compromised accounts. Furthermore, operational security friction—particularly the intense fear of getting locked out of essential school submission files—prevents students from regularly updating their passwords. This implies that the persistent "awareness-behavior gap" stems not from student apathy, but from cognitive fatigue and usability barriers that conflict with academic responsibilities. Institutional interventions must therefore shift away from abstract warnings toward user-friendly security tools and flexible account recovery frameworks that reduce operational friction.

Building Digital Resilience, Proactive Self-Efficacy, and Safety Intentions. The findings demonstrate that navigating online hazards fosters significant psychological growth, transforming students from careless web users into self-reliant digital citizens who recognize their personal agency in protecting their accounts. Participants expressed increased self-efficacy, deliberate verification habits, and an explicit demand for interactive, hands-on cyber safety workshops in school to build real-world defensive skills. The implication is that negative digital encounters can serve as powerful learning moments when students develop internal confidence and constructive safety intentions. However, translating these intentions into sustained digital resilience requires experiential, practice-based school programs that bridge individual self-efficacy with formal technical instruction.

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

Conclusions

In conclusion, this study establishes that student cybersecurity caution and confidence are dynamically forged through direct exposure to digital threats, operational challenges, and reflective personal realization. While encounters with phishing and social engineering trigger initial anxiety, they effectively cultivate individual vigilance and defensive browsing habits among Senior High School learners. However, heightened risk awareness alone is insufficient to guarantee digital safety, as cognitive fatigue, deceptive tactics, and lockout fears create severe security friction that disrupts academic tasks. The findings highlight that students possess the capacity to develop agency and self-efficacy when equipped with the right mindsets and verification strategies. Nevertheless, relying solely on self-taught defensive routines leaves critical operational gaps in credential management and technical threat identification. Ultimately, bridging the persistent gap between awareness and practice requires moving beyond abstract warnings toward structured institutional support. Implementing practical, hands-on cybersecurity education within the technical-vocational high school context will empower students to convert positive safety intentions into sustained digital resilience.

Specifically, the following conclusions are drawn from the findings:

1. Encounters with hacking, phishing, and identity theft, whether direct or witnessed, trigger fear, anxiety, and a sense of vulnerability among BTHS students, and these feelings act as catalysts for defensive routines such as setting profiles to private and verifying suspicious messages before acting.
2. Detecting and preventing cyber incidents is made difficult by cognitive overload, near-identical fake profiles, context-aware phishing messages, and academic stress. Security friction, particularly the fear of being locked out of school accounts and files, discourages students from regularly updating their passwords. These practices reflect usability barriers and cognitive fatigue rather than apathy.
3. Navigating digital risks fosters self-efficacy and personal agency, transforming students from careless users into more discerning and self-reliant digital citizens who recognize their own role in protecting their accounts and who ask for hands-on, school-based cybersecurity education.
4. Self-taught defensive routines alone are insufficient to close the awareness–behavior gap. Structured, experiential, and practice-based institutional support is needed to convert students' safety intentions into sustained digital resilience.

Conclusions 1 to 3 correspond to Objectives 1 to 3 of the study, while Conclusion 4 provides the basis for the recommendations that respond to Objective 4.

Limitations of the Study

The findings of this study should be interpreted in light of its limitations. The primary limitations are its qualitative design and its reliance on a small, selected student sample. The findings are based on self-reported data from subjective narratives and reflective insights, which may be deeply personal and not fully representative of the experiences of the entire student body. In addition, the participants came from a single school, so the findings reflect the localized digital and school context of Biabas Trade High School. The interpretation of themes also depends on the judgment of the researchers, which is a characteristic of qualitative analysis. Finally, the study was limited to three cyber threats and did not include technical security analyses or quantitative measurements. These limitations point to the value of broader and more varied studies, as recommended below.

Recommendations

Based on the findings and the conclusions of the study, the recommendations are the following:

1. **Department of Education (DepEd)** should utilize the empirical findings of this study to refine national and regional policies on secondary cybersecurity education. The department should integrate practical, hands-on digital safety modules into the K–12 curriculum to address the operational knowledge gaps experienced by technical-vocational learners. By institutionalizing experiential cybersecurity training

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

standards, DepEd can effectively produce digitally literate and resilient Filipino students capable of defending their personal data.

2. **Biabas Trade High School (BTHS)** should leverage localized data from this research to evaluate and upgrade its current digital safety protocols. The school administration should establish structured, school-wide cyber safety campaigns that address student lockout anxieties and credential management challenges. These institutional measures will create a supportive academic environment that protects student data while minimizing disruptions to daily academic performance tasks.
3. **The principal** should exercise strategic leadership by prioritizing cybersecurity initiatives and allocating necessary resources for hands-on technical workshops. The school head must oversee the formulation of clear, student-friendly account recovery policies that reduce usability friction and academic stress. By championing institutional cyber safety programs, the principal will foster a pervasive culture of cyber awareness and resilience across the entire school community.
4. **Educators** should transition from passive information delivery toward interactive, experiential teaching strategies that simulate real-world cyber threats. Teachers must integrate threat verification exercises into daily lessons to help students recognize deceptive cloned profiles and phishing attempts. Additionally, teachers should maintain an empathetic support system for students experiencing digital security disruptions to alleviate academic anxiety.
5. **Information and Communication Technology (ICT) School Coordinator** should optimize the school's digital infrastructure by implementing robust filtering systems and secure authentication protocols. The coordinator must provide technical guidance and user-friendly tools, such as password manager instruction, to reduce operational friction and lockout fears. Furthermore, technical staff should design safe account recovery frameworks that ensure students maintain uninterrupted access to their academic submission files.
6. **Students** should actively practice consistent verification routines and maintain strict privacy settings across all personal and educational accounts. Learners must adopt secure credential management habits, such as utilizing secure key storage, to overcome the fear of account lockouts. By actively participating in school cybersecurity workshops, students can enhance their personal agency, self-efficacy, and long-term digital resilience.
7. **Parents and Guardians** should establish open communication at home regarding the digital risks and deceptive traps their children encounter online. They should complement school initiatives by providing consistent home monitoring and guidance without imposing restrictive measures that hinder learning. This collaborative home-school support system will help shield students from the emotional and financial stress caused by online scams.
8. **Future Researchers** should expand upon this study by conducting quantitative or mixed-methods investigations to measure the precise relationship between lockout anxiety and credential habits. They may adapt this qualitative framework to examine lived cybersecurity experiences in different regional or technical-vocational contexts. Additionally, future studies should evaluate the efficacy of game-based and AI-assisted cyber defense simulations in bridging the student awareness-behavior gap.

Taken together, the recommendations respond to the three themes of the study. Those addressed to the Department of Education, Biabas Trade High School, the principal, educators, and the ICT school coordinator respond to Themes 2 and 3 by reducing security friction and by providing the hands-on, experiential training that students asked for. Those addressed to students and to parents and guardians build on Themes 1 and 3 by strengthening verification habits, secure credential management, and open communication at home. Those addressed to future researchers respond to the limitations discussed above. Together, they aim to convert the vigilance that students already show into sustained digital resilience.

ACKNOWLEDGMENT

The researchers would like to express their appreciation to the students who sincerely participated in the interviews, as well as to **Mr. Diomedes L. Montero**, Principal of Biabas Trade High School. Their assistance and involvement made this research possible.

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

COMPLIANCE WITH ETHICAL STANDARDS

Disclosure of Conflict of Interest

The authors of this manuscript certify that the substance of this research is free of conflicts of interest. We attest that this investigation was carried out impartially, without any financial or personal ties that may have influenced how the findings were presented or how the results were interpreted. We also commit to promptly disclosing any conflicts of interest that may arise in the future.

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

REFERENCES

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckmann (Eds.), *Action control: From cognition to behavior* (pp. 11–39). Springer. https://doi.org/10.1007/978-3-642-69746-3_2

Akter, M., Sultana, S., & Ahmed, S. (2025). The privacy paradox in adolescent peer networks: Interpersonal trust and credential sharing behaviors on social platforms. *Computers in Human Behavior, 151*, Article 108012.

Alabab, J. R., Santos, M. C., & Ramos, D. K. (2023). Baseline cybersecurity awareness among senior high school learners in vocational tracks. *Journal of Digital Literacy and Education, 5*(2), 88–101.

Alharbi, A., Gardner, L. A., & Sheridan, D. P. (2022). High school students' navigation of modern cyber threats: Assessing vulnerability to advanced social engineering and phishing tactics. *Computers & Security, 118*, Article 102734. https://doi.org/10.1016/j.cose.2022.102734

Alqahtani, M. (2022). Interactive learning platforms in secondary cybersecurity education: Evaluating the impact of structured modules on learner digital resilience. *International Journal of Computer Science Education, 14*(3), 145–160.

Alrobaian, A. A., Alotibi, R. F., & Khan, M. A. (2023). Policy compliance and threat identification deficits among technical and vocational trainees. *International Journal of Information and Education Technology, 13*(8), 1234–1241.

Anti-Child Pornography Act of 2009, Rep. Act No. 9775 (2009) (Phil.).

Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act, Rep. Act No. 11930 (2022) (Phil.).

Aquino, E. T. (2023). Perceived behavioral control, peer pressure, and online risky behaviors among Filipino secondary school learners. *Philippine Journal of Educational Psychology, 22*(1), 45–62.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191–215. https://doi.org/10.1037/0033-295X.84.2.191

Bermudez, G. H., Tan, J. L., & Castro, R. M. (2022). Password-sharing as a currency of trust: Interpersonal intimacy and digital vulnerability among adolescents. *Journal of Adolescent Research, 37*(4), 512–535.

Booc, C. M., Yap, R. J., & Fernandez, K. L. (2024). Regional risk exposures, perceived behavioral control, and protective digital habits among secondary students in the Visayas. *Asia-Pacific Journal of Multidisciplinary Research, 12*(3), 67–79.

Bulala, J. V., Mercado, P. S., & Torres, L. B. (2026). Hands-on digital security interventions: Fostering self-efficacy and threat detection among technical-vocational students. *Journal of Educational Technology Development, 18*(1), 112–129.

Calimbo, N. R., Dizon, F. E., & Morales, A. G. (2025). Building digital resilience: Evaluating interactive cybersecurity curriculums in community high schools. *Philippine Educational Review, 31*(2), 203–220.

Cybercrime Prevention Act of 2012, Rep. Act No. 10175 (2012) (Phil.).

Data Privacy Act of 2012, Rep. Act No. 10173 (2012) (Phil.).

Dela Cruz, A. P., Soriano, M. T., & Bautista, H. R. (2024). Familiarity versus defense: Deconstructing the social media literacy and cyber safety gap among urban youth. *Philippine Information Systems Journal, 8*(1), 33–48.

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

Gonzales, R. A., Flores, K. P., & Villanueva, M. S. (2025). The optimism bias in vocational training: Why technical competence breeds a false sense of digital immunity. *International Journal of Cyber Behavior, Psychology and Learning, 15*(1), 1–19.

Khamzina, A., Kim, J., & Lee, S. (2022). Educational interventions and digital resilience: Strengthening adolescent online safety competencies through structured programs. *Computers & Education, 184*, Article 104510.

Kraus, M. F., Scherer, R., & Bruckner, T. (2023). Gamified training for cybersecurity resilience: Measuring behavioral transfer in high school classrooms. *Education and Information Technologies, 28*(6), 7215–7239.

Mansueto, K. M., Delos Reyes, C. P., & Ocampo, J. L. (2026). Uneven defenses: Assessing baseline cybersecurity awareness and fragmented safety habits of Filipino senior high school students. *Philippine Social Sciences and Humanities Review, 29*(1), 89–106.

Mendoza, E. C. (2026). Simulated environments for threat response: Enhancing credential protection habits in vocational secondary curricula. *Journal of Cyber Education and Applied Research, 9*(1), 54–71.

Miller, K. S., Davies, R. A., & Thorne, C. L. (2024). Gamified security simulations for secondary learners: Closing the operational knowledge gap through experiential engagement. *Computers & Security, 139*, Article 103714.

Oguine, C. U., Bello, M. A., & Okon, E. T. (2025). Technical immersion without formal instruction: Learned helplessness and security bypass habits among high school vocational students. *Computers in Human Behavior Reports, 17*, Article 100482.

Palao, K. E., Saldivar, T. J., & Gomez, P. A. (2026). Interactive instructional design in secondary cybersecurity: Bridging cognitive understanding and behavioral defense. *Asian Journal of Distance Education, 21*(1), 77–95.

Pascual, D. M. (2024). Identity exposure and credential compromise: Analyzing high-risk password behaviors among Filipino high school learners. *Philippine Journal of Technology and Society, 6*(2), 141–158.

Ravichandran, S., Patel, N. V., & Smith, D. L. (2025). The operational gap in digital native security: Why interface literacy fails to prevent social engineering attacks. *Computers & Education Open, 6*, Article 100215.

Republic Act No. 8484 (Access Devices Regulation Act of 1998), as amended by Republic Act No. 11449 (2019) (Phil.).

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rosano, G. T., Lim, C. V., & Arboleda, M. L. (2026). Mind the divide: An empirical evaluation of the cybersecurity awareness-behavior gap among technical trainees. *Vocational Education and Technology Review, 12*(1), 38–56.

Special Protection of Children Against Abuse, Exploitation and Discrimination Act, Rep. Act No. 7610 (1992) (Phil.).

Tempestini, M., Boffi, S., & Rainoldi, M. (2024). Experiential cybersecurity: Moving from passive policy delivery to gamified behavioral learning in secondary vocational environments. *Journal of Computer Assisted Learning, 40*(4), 1642–1658.

UNESCO. (2020). *Global education monitoring report 2020: Inclusion and education: All means all*. UNESCO Publishing. https://doi.org/10.54676/JJVL7572

© 2026 Advancing SDG Impact. All rights reserved.

JASDG
JOURNAL FOR THE ADVANCEMENT OF SUSTAINABLE DEVELOPMENT GOALS
AN INTERNATIONAL, PEER-REVIEWED, OPEN ACCESS JOURNAL
www.jasdg.com
Volume 1 Issue 4 Pages 4087-4109
ISSN: 3155-7546 (Online)
DOI: 10.5281/zenodo.24277744

United Nations. (2015). *Transforming our world: The 2030 Agenda for Sustainable Development* (A/RES/70/1). United Nations General Assembly. https://sdgs.un.org/2030agenda

Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of Personality and Social Psychology, 39*(5), 806–820. https://doi.org/10.1037/0022-3514.39.5.806

© 2026 Advancing SDG Impact. All rights reserved.