

InfoShield: Assessing the Cybersecurity Awareness of College Students in Protecting Personal Information Online.

Mohamad, Shikaina Fiona T.

*Bachelor of Science Information Technology – Mobile Development, College of Computing and Information Science,
Systems Plus College Foundation, Angeles City, Pampanga
shikainafionam@gmail.com*

Limio, Jessa Mae M.

*Bachelor of Science Information Technology – Mobile Development, College of Computing and Information Science,
Systems Plus College Foundation, Angeles City, Pampanga
Jessalimio05@gmail.com*

Pasca, Pamela V.

*Bachelor of Science Information Technology – Mobile Development, College of Computing and Information Science,
Systems Plus College Foundation, Angeles City, Pampanga
Pamelapasca786@gmail.com*

Gaudia, Mary Jane V.

*Bachelor of Science Information Technology – Mobile Development, College of Computing and Information Science,
Systems Plus College Foundation, Angeles City, Pampanga
maryjanevgaudia@gmail.com*

Varona, Aaron Gabriel M.

*Bachelor of Science Information Technology – Mobile Development, College of Computing and Information Science,
Systems Plus College Foundation, Angeles City, Pampanga
12humssdesales.varonaaaron@gmail.com*

ABSTRACT

The increasing use of digital platforms has made college students more dependent on the internet for education, communication, social media, online transactions, and other daily activities. However, increased online activity also exposes students to cybersecurity risks such as phishing, scams, weak passwords, privacy violations, and unauthorized access to personal information. This study aims to assess the cybersecurity awareness of college students in protecting their personal information online. It will focus on password security, phishing and scam awareness, privacy protection, social engineering awareness, and safe browsing and online practices. The study will use a quantitative descriptive-correlational research design and a structured questionnaire to gather data from selected college students. The study will also examine the relationship between cybersecurity awareness and students' protective online behaviors. Based on the findings, the researchers will identify areas that need improvement and propose an awareness-based prototype called InfoShield.: The proposed prototype will provide cybersecurity information, quizzes, privacy-checking activities, and recommendations to help students practice safer online behavior.

Keywords: Cyber Security Awareness, College students, Personal Information, Online Privacy, Information Security

SECTION I — INTRODUCTION (THE PROBLEM AND ITS SETTING)

1.1 Introduction

The internet has become an important part of college students' everyday lives. Students use social media, online learning platforms, messaging applications, cloud services, online shopping, and other digital platforms for academic and personal activities. Because of this, students regularly provide and exchange personal information online.

Although technology provides convenience, it also creates cybersecurity risks. Students may encounter phishing messages, online scams, account hacking, identity theft, data breaches, and unauthorized use of personal information. Cybersecurity awareness is therefore important because knowing how to recognize and avoid online threats can help reduce the risk of personal information being compromised.

One important concern is that being aware of cybersecurity risks does not always mean that students practice safe online behavior. A recent study involving college students in the Philippines found high cybersecurity awareness but moderate data privacy skills and behavioral compliance, suggesting a gap between what students know and what they actually practice.

Other recent studies involving Filipino students have also examined cybersecurity awareness, password practices, phishing, public Wi-Fi, and sharing of personal information. These studies show the importance of strengthening cybersecurity education among college students.

This study therefore aims to assess the cybersecurity awareness of college students in protecting their personal information online. It will determine their level of awareness, examine their cybersecurity practices, identify common risks, and propose an awareness-based prototype called InfoShield.

1.2 Background of the Study

College students are among the frequent users of digital platforms. They use online services for submitting school requirements, communicating with classmates and instructors, accessing information, and managing personal accounts. As their online activities increase, the amount of personal information they provide online also increases.

Cybersecurity awareness includes understanding common cyber threats and knowing how to protect accounts and personal information. Some basic cybersecurity practices include using secure passwords, recognizing suspicious links and messages, reviewing privacy settings, avoiding unnecessary sharing of personal information, and using additional account security such as multifactor authentication.

The National Institute of Standards and Technology (NIST) emphasizes the importance of stronger authentication methods such as multifactor authentication because passwords can be compromised through phishing and other methods.

Recent research in the Philippines has also identified cybersecurity concerns among students. One study reported that some students reused passwords, rarely changed passwords, had limited knowledge of multifactor authentication, and experienced difficulty identifying phishing attempts. Another recent study involving Filipino youth found that cybersecurity awareness could be relatively high while the relationship between awareness and some protective behaviors remained weak.

These findings show the importance of studying not only cybersecurity knowledge but also how students apply cybersecurity practices in their daily online activities. This study will therefore assess both cybersecurity awareness and protective online behavior among college students.

1.3 Objectives of the Study

- **General Objective:**

The general objective of this study is to assess the level of cybersecurity awareness of college students in protecting their personal information online.

- **Specific Objectives:**

The study specifically aims to:

Determine the level of cybersecurity awareness of college students in terms of password security, phishing and scam awareness, privacy protection, social engineering awareness, safe browsing and online practices.

1. Assess the cybersecurity practices of college students in protecting their personal information online.
2. Identify the common cybersecurity risks and vulnerabilities encountered by college students.
3. Determine the relationship between cybersecurity awareness and protective online behaviors among college students.
4. Identify areas of cybersecurity awareness that require improvement.

Propose an awareness-based prototype or program that may help college students improve their cybersecurity practices and protection of personal information

1.4 Scope and Limitation of the Study

- **Scope:**

This study focuses on the cybersecurity awareness of college students in protecting their personal information online. It covers five major areas: password security, phishing and scam awareness, privacy protection, social engineering awareness, and safe browsing and online practices.

The study will gather information from selected college students through a structured questionnaire. It will measure their cybersecurity awareness, reported protective behaviors, and common cybersecurity risks encountered while using online platforms.

The proposed InfoShield prototype will be designed as an awareness and educational tool. It may include cybersecurity learning materials, quizzes, privacy-checking activities, security tips, and recommendations based on the identified areas of weakness.

- **Limitation:**

The study will be limited to the selected college students who will participate as respondents. The

results may not represent all college students in other schools or locations.

The study will also depend on the respondents' answers to the questionnaire. The researchers will not collect actual passwords, account credentials, or other highly sensitive personal information.

The InfoShield prototype will focus on cybersecurity awareness and education. It will not function as an actual antivirus program, penetration-testing tool, password manager, or complete cybersecurity protection system.

1.5 Significance of the Study

The study will be limited to the selected college students who will participate as respondents. The results may not represent all college students in other schools or locations.

The study will also depend on the respondents' answers to the questionnaire. The researchers will not collect actual passwords, account credentials, or other highly sensitive personal information.

The InfoShield prototype will focus on cybersecurity awareness and education. It will not function as an actual antivirus program, penetration-testing tool, password manager, or complete cybersecurity protection system.

1.6 Definition of Terms

Cybersecurity Awareness – The knowledge and understanding of a person regarding cybersecurity threats and ways of protecting digital information.

Personal Information – Information that identifies or relates to a person, such as name, contact information, birthday, location, and account information.

Password Security – Practices used to create, maintain, and protect passwords from unauthorized

access.

Phishing – A form of online deception that attempts to convince a person to provide sensitive information through fake messages, websites, or links.

Scam – A dishonest activity intended to deceive a person into giving information, money, or access.

Privacy Protection – Practices used to control and protect personal information when using digital platforms.

Social Engineering – The use of deception or manipulation to convince a person to reveal information or perform an unsafe action.

Safe Browsing – The practice of using the internet carefully by avoiding suspicious websites, links, downloads, and online activities.

Protective Online Behavior – Actions taken by users to reduce cybersecurity and privacy risks while using digital platforms.

InfoShield – The proposed cybersecurity awareness prototype designed to provide information, assessments, quizzes, and recommendations related to online safety.

SECTION II — LITERATURE REVIEW

2.1 Introduction to the Review

This chapter presents literature and studies related to cybersecurity awareness among college students. The review focuses on cybersecurity awareness, password security, phishing and scams, privacy protection, social engineering, safe browsing, and protective online behavior.

The reviewed literature provides a basis for understanding the common cybersecurity risks experienced by students and the importance of improving cybersecurity education. It also helps

establish the research gap addressed by the present study.

2.2 Review of Related Literature and Studies

Cybersecurity Awareness Among College Students

Cybersecurity awareness is important for college students because of their frequent use of digital platforms.

Students may have knowledge about common threats but may still engage in risky online behaviors.

A study conducted among college students in the Philippines used a descriptive-correlational approach to examine cybersecurity awareness and reported cybersecurity practices.

A more recent Philippine study involving 573 college students also examined cybersecurity knowledge, attitudes, practices, and risky behaviors. The study found that students generally demonstrated high to very high awareness, but some risky behaviors continued to occur, particularly those related to passwords, personal information sharing, and unsecured networks.

These findings show that cybersecurity awareness should be studied together with actual online practices.

Password Security

Passwords are commonly used to protect online accounts. However, using weak or repeated passwords may increase the possibility of unauthorized access.

NIST explains that passwords can be compromised through methods such as phishing and recommends using additional security measures such as multifactor authentication when available.

A Philippine municipal-college study found that password reuse and infrequent password changes were among the cybersecurity concerns identified among students. Because students often maintain several online accounts, password security is an important area to include in measuring cybersecurity awareness.

Phishing and Scam Awareness

Phishing is one of the common methods used to trick users into revealing sensitive information. It may appear through emails, text messages, social media messages, or fake websites.

NIST describes phishing as a method in which attackers may trick users into providing usernames and passwords through fake websites or messages.

NIST's research on phishing also emphasizes the importance of understanding why users click suspicious content and how users can improve their ability to recognize phishing attempts. A recent study of Filipino youth reported relatively high awareness of phishing, scams, and identity theft, but found weak relationships between awareness and some protective behaviors.

This supports the need to assess both students' knowledge and their reported online practices.

Privacy Protection

Privacy protection involves controlling the personal information shared online and understanding how digital platforms collect and use information.

Students may share birthdays, locations, school information, photographs, contact details, and other information through social media and other online platforms. If privacy settings are not properly managed, personal information may become accessible to unintended users.

A 2025 study involving students of a private college examined privacy awareness, perceived risks, and protection behavior on social media. The study reported relationships between privacy awareness and protective behavior. This supports the inclusion of privacy protection as one of the major areas in the present study.

Social Engineering Awareness

Social engineering focuses on manipulating people rather than directly attacking a computer system.

Attackers may pretend to be trusted individuals or organizations and attempt to convince users to

provide information or perform an action.

Students may encounter social engineering through fake account messages, impersonation, fraudulent offers, suspicious requests, and other deceptive communication.

Understanding social engineering is therefore important because students may encounter these threats during ordinary online activities.

Safe Browsing and Online Practices

Safe browsing involves carefully using websites and online services and avoiding suspicious links, downloads, and websites.

College students regularly browse the internet for research, entertainment, communication, and other activities. Because of this, safe browsing practices can help reduce exposure to malicious websites and online scams. Recent research involving BSIT students examined cybersecurity protection practices including phishing awareness, safe browsing, and device security. Therefore, safe browsing is included as one of the cybersecurity awareness areas in this study.

Cybersecurity Awareness and Protective Behavior

Awareness and behavior are related but are not necessarily the same. A student may know that a particular action is unsafe but may still perform that action.

A 2026 study among college students in the Philippines found high cybersecurity awareness but moderate data privacy skills and behavioral compliance. It also reported a significant but weak relationship between awareness and behavior.

Another 2026 study involving Filipino college students found relatively high cybersecurity awareness but weak associations between awareness and several protective behaviors. These findings support the focus of the present study on both awareness and protective online behavior.

Research Gap

Previous studies have examined cybersecurity awareness, password security, phishing, privacy, and online safety among students. However, there is still a need to examine how cybersecurity awareness relates to protective online behavior within a specific college setting.

The present study addresses this gap by assessing cybersecurity awareness across five areas:

Password Security

Phishing and Scam Awareness

Privacy Protection

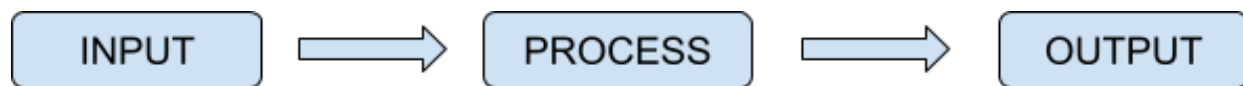
Social Engineering Awareness

Safe Browsing and Online Practices

The study will also identify areas that need improvement and use the findings as a basis for the proposed InfoShield cybersecurity awareness prototype.

2.3 Conceptual Framework

The study will use the Input–Process–Output (IPO) Model.



• Respondents' profile. • Cybersecurity awareness. • Password security. • Phishing/scam awareness. • Privacy protection. • Social engineering awareness. • Safe browsing and online practices. • Common cybersecurity risks. • Existing cybersecurity practices.	• Preparation of questionnaire. • Validation of research instrument. • Distribution of questionnaire. • Collection of responses. • Data tabulation. • Statistical analysis. • Interpretation of results. • Identification of areas needing improvement. • Development of InfoShield prototype.	• InfoShield Cybersecurity Awareness Prototype. • Cybersecurity learning materials. • Security tips. • Cybersecurity quiz. • Privacy checker. • Phishing awareness activities. • Awareness results. • Personalized recommendations.
--	--	--

2.4 Synthesis

The reviewed literature shows that cybersecurity awareness is an important factor in protecting students' personal information. Studies have discussed common cybersecurity concerns such as weak passwords, phishing, scams, privacy issues, unsafe browsing, and unsecured networks.

However, the reviewed studies also show that awareness does not always result in consistent protective behavior. Some students may understand cybersecurity risks but still practice unsafe behaviors such as reusing passwords or sharing personal information.

The present study therefore focuses on both cybersecurity awareness and protective online behavior. The results will be used as a basis for identifying areas that need improvement and developing the proposed InfoShield awareness prototype .

SECTION III — METHODOLOGY

3.1 Research Design

3.1 Research Design

This study will use a quantitative descriptive-correlational research design.

The descriptive approach will be used to determine the level of cybersecurity awareness and cybersecurity practices of college students. The correlational approach will be used to determine whether there is a relationship between cybersecurity awareness and protective online behaviors.

This approach is appropriate because similar studies involving college students have used quantitative and descriptive-correlational methods to examine cybersecurity awareness and practices.

3.2 System Development Methodology

For the development of the proposed InfoShield prototype, the researchers will use an Agile methodology.

Agile will allow the researchers to develop the prototype gradually and make improvements based on feedback from the researchers, adviser, and potential users.

The development may follow these stages:

1. **Planning** -The researchers will identify the main features and requirements of InfoShield based on the research objectives.
2. **Design** -The researchers will create the interface and user flow using Figma.
3. **Development** -The planned interface and functions will be developed into the proposed prototype.
4. **Testing** -The researchers will check the prototype for usability, functionality, and errors.
5. **Improvement** -Feedback from users and evaluators will be used to improve the prototype.
6. **Finalization** -The improved version of the InfoShield prototype will be presented as the proposed output of the study.

3.3 Requirement Specification and Analysis

Functional Requirements

The proposed InfoShield system should be able to:

- 1.Allow users to access the cybersecurity awareness dashboard.
- 2.Display cybersecurity learning materials.
- 3.Provide information about password security.
- 4.Provide information about phishing and scams.
- 5.Provide privacy protection tips.
- 6.Provide social engineering awareness materials.
- 7.Provide safe browsing recommendations.
- 8.Provide cybersecurity quizzes.
- 9.Calculate or display quiz results.
- 10.Provide recommendations based on identified areas of weakness.
- 11.Provide a privacy-checking activity.
- 12.Allow users to navigate between different cybersecurity topics.

Non-Functional Requirements

The system should have the following qualities:

Usability – The interface should be simple and easy for college students to understand.

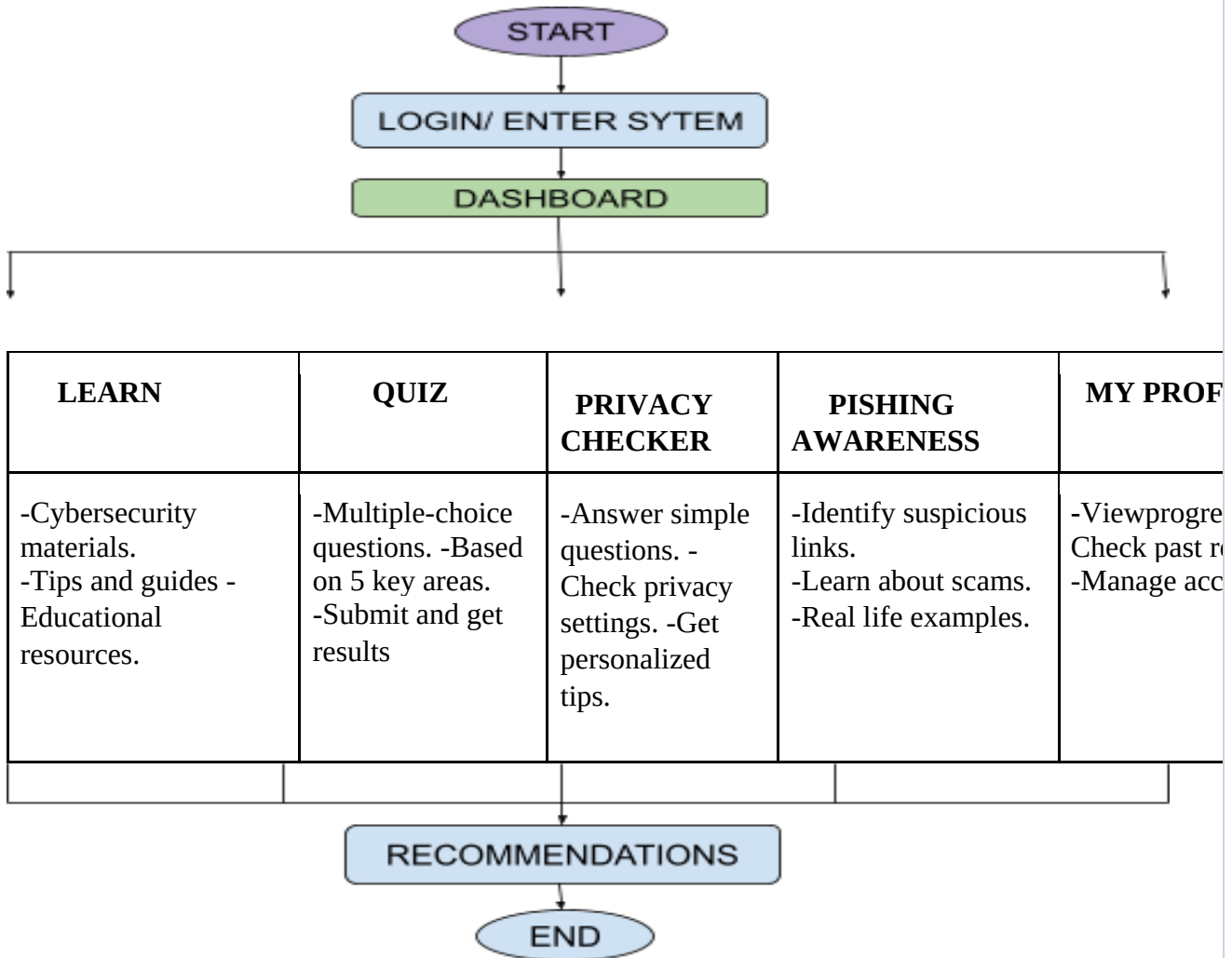
Performance – Pages and activities should load within a reasonable amount of time.

Security – The system should avoid collecting unnecessary sensitive information.

Accessibility – Information should be readable and easy to navigate.

Reliability – The main features should function

consistently. **Basic User Flow**

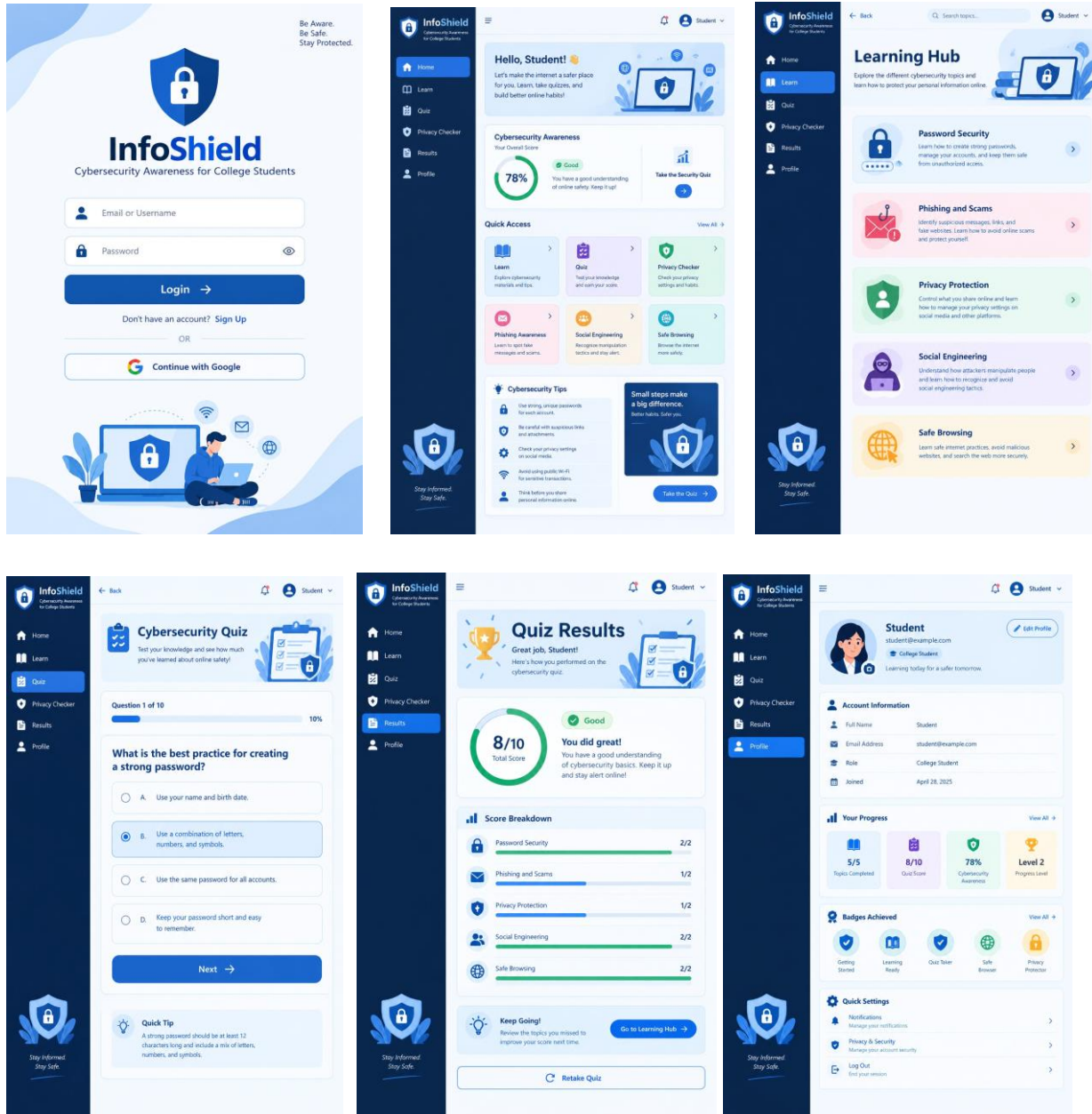


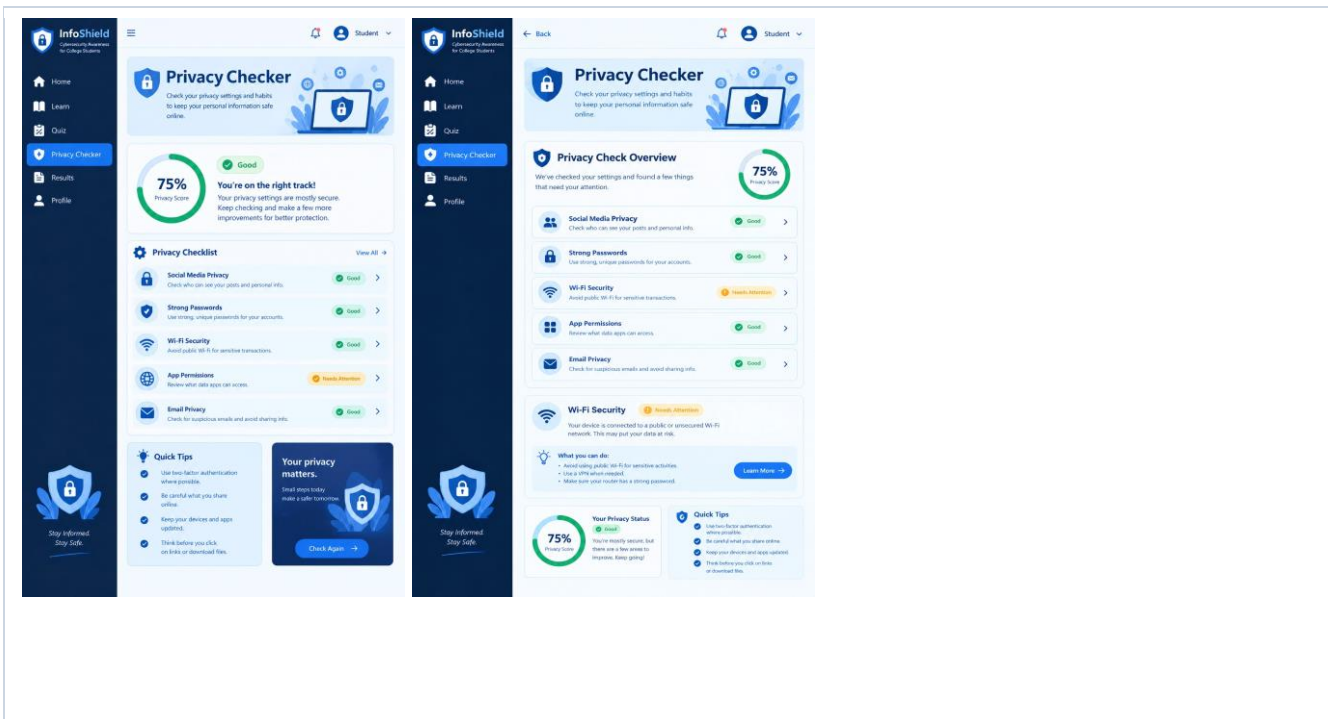
3.3 Requirement Specification and Analysis

- Functional decomposition, design criteria, and requirements models (DFDs, ERDs, System Flowcharts).

3.4 System Design Specification

The InfoShield interface will be designed using **Figma**. The design will focus on simplicity and ease of navigation because the intended users are college students. **Proposed Screens**





3.5 Implementation

The InfoShield prototype will be implemented based on the requirements and interface designed in Figma. The researchers will organize the system into different sections such as the dashboard, learning materials, quiz, privacy checker, results, and recommendations.

The development will focus on providing a simple and understandable interface for college students. The cybersecurity information will be based on the topics covered by the study and supported by appropriate references.

The system will avoid requesting sensitive information such as actual passwords, banking information, or private account credentials.

3.6 Testing and Evaluation

The proposed InfoShield prototype will undergo testing to determine whether its functions work properly and whether users can easily understand and navigate the system.

Functional Testing -The researchers will check whether the buttons, navigation, quiz, privacy checker, and other functions work properly.

Usability Testing -Selected users or evaluators may test the prototype to determine whether the interface is understandable and easy to navigate.

Content Evaluation -The cybersecurity information will be reviewed to ensure that the information presented is relevant to the research objectives.

User Evaluation

The prototype may be evaluated using criteria such as:

-Ease of use -Functionality -

Accessibility -Content quality -Interface design

-Overall usability **A 5-point Likert scale may be**

used:

SCALE	INTERPRETATION
5	Excellent
4	Very Good
3	Good
2	Fair
1	Poor

The exact evaluation criteria and scale should be finalized with your research adviser.

REFERENCES

Reference Guidelines

1. Alabab, B., et al. (2023). Cybersecurity awareness of college students in a private higher education institution. CGCI International Journal of Administration, Management, Education and Technology, 1(1), 51–57.
<https://doi.org/10.70059/1zw7x826>
2. Arances, J. A., et al. (2025). Cyber literacy and cyber risk mitigation program of one municipal college in the Philippines. Zenodo. <https://zenodo.org/records/16905221>
3. Dawkins, S., & Jacobs, J. (2023). Phishing with a net: The NIST Phish Scale and cybersecurity awareness. National Institute of Standards and Technology. <https://www.nist.gov/publications/phishing-net-nist-phish-scale-and-cybersecurity-awareness>
4. Florendo, R. B. B., et al. (2025). Examining cybersecurity awareness among college students across various year levels in the Province of Laguna. International Journal for Multidisciplinary Research, 7(3).
<https://doi.org/10.36948/ijfmr.2025.v07i03.41945>
5. National Institute of Standards and Technology. (2025). How do I create a good password?
<https://www.nist.gov/cybersecurity-and-privacy/how-do-i-create-good-password>
6. National Institute of Standards and Technology. (2025). Phishing.
<https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing>
7. Picardal, J. (2026). Cybersecurity awareness, data privacy practices, and behavioral compliance among college students in a provincial university in the Philippines.
<https://doi.org/10.13140/RG.2.2.25605.92647>
8. Rufino, J. R., & Moyao, J. (2025). Cybersecurity awareness and practices among criminal justice students in one higher educational institution in Cordillera. Technium Social Sciences Journal, 71(1). <https://doi.org/10.47577/tssj.v71i1.12703>
9. Ventura, I. J. S., et al. (2026). Level of awareness and susceptibility to phishing attacks among students of Quezon City University: A stratified survey study. International Journal of Latest Technology in Engineering, Management & Applied Science, 15(5), 1653–1666.
<https://ideas.repec.org/a/bjfl/ijitem/v15y2026i5a2560.html>
10. (2025). Investigating students' awareness of online privacy and cybersecurity: An empirical study with effective cybersecurity training framework. Global Knowledge, Memory and Communication. <https://doi.org/10.1108/GKMC-05-2024-0319>