CYBERTIPS: A LEARNING APPLICATION ON IMPROVING CYBERSECURITY KNOWLEDGE OF SENIOR HIGH SCHOOL STUDENT AND EMPLOYEES OF FORT BONIFACIO HIGH SCHOOL

A Capstone Project Proposal
Presented to
The Faculty of the College of Computer and Information Sciences
UNIVERSITY OF MAKATI
Makati City

In Partial Fulfillment
of the Requirements for the Degree
BACHELOR OF SCIENCE IN FORMATION TECHNOLOGY MAJOR IN
INFORMATION AND NETWORK SECURITY

Laorden, John Rey A.

Onzaga, Aldrick C.

Rañopa, John Ishmael V.

Engr. Edgardo Tan Cruz

January 2023

Contents

CHAPTER I

The Project and Its Background

Introduction

The state of cybersecurity in the Philippines is terrible due to the fact that Filipinos are experiencing it. According to the Daily Guardian (2019), a publishing firm and media outfit in Ilo-Ilo, the Philippines is the biggest attack originator for both automated and human-driven cyberattacks. The majority of cyber threats, such as phishing, malware smuggling, credential stuffing, social media account takeovers, etc., were therefore carried out in the Philippines.

The engagement of Filipino students and employees with online learning technology has several advantages for both students and teachers in terms of creating and delivering lesson plans and helping students with their homework and research. However, it is also an opportunity for attackers to steal from and exploit the Filipino students and employees. According to Catalina Ricci S. Madarang of Interaksyon under Philstar Global (2020), Angel Redoblethe, chief information security officer and first vice president at PLDT, ePLDT, and Smart, stated that attacks against workers who are working from home have been seen by cyber threat intelligence operators. Given the aforementioned circumstances, the goal of this research is to raise awareness among students and employees of Fort Bonifacio High School through the development and application of cybersecurity.

Project Background

Nowadays, as the number of people who use the internet is increasing, so do the threats that they will encounter. Browsing on the internet with no awareness of danger can lead to invading privacy, having data stolen, and more.

Cybersecurity awareness is the knowledge of security hazards and responsible behavior to reduce risks. In the Philippines, cybercrime is one of the most dangerous threats on the internet. It can lead to chaos and destruction of the computer system if the threats do not seek prevention. Ignorance of cyber awareness is one of the problems in the Philippines. Ignoring the threats that can harm the computer and also possible data loss or stolen due to the threats that can be encountered. Being aware can help to avoid threats to the computer and privacy of the users. (De Ramos & Esponilla II, 2022).

The researchers conducted a preliminary investigation at Fort Bonifacio High School. The researchers are given a chance to talk about how they manage to inform their senior high school students about cybersecurity. The assistant principal, Jolivelle Magadia, stated that the school hosts an event called "ICT Month," during which senior students who specialize in ICT compete and have fun while also raising awareness about cybersecurity. When the researchers asked the assistant principal if the other senior students were aware of this event, the answer was that the other students, who specialize in other education tracks, either knew or did not know about this event.

Due to the researchers experience with learning applications and other online learning materials, the researchers decided to create a learning application. The learning application will create convenience for the students and employees. The learning application can be installed on mobile devices for mobility and flexibility. Because of this, students and employees who will use this learning application have their own time to learn.

The app will be built on Android Studio with Java and XML for the front end, and for the back end, Firebase, a serverless backend-as-a-service. Once the design for the app is finished using

Figma, the researchers will start on back end. The back end has databases, managed hosting and also analytics. The security of the app will also come from Firebase's Firestore database. The Firestore database can provide a set of security rules that researchers can manage, such as authenticated users only and 2-way factory authentication.

The purpose of this project is to improve the cybersecurity knowledge of senior students and employees. Students should be aware of the cybersecurity awareness program at all times, rather than just once a month, to raise awareness in every educational track, not only for ICT's students but also for employees too.

Objectives of the Project

General Objectives

The general objective of this study is to develop a learning application on improving cybersecurity knowledge of senior high school students and employees of Fort Bonifacio high school.

Specific Objectives

- To design a learning application that has following features and cybersecurity application:
    1. Features:
        - **Learning modules and tools -** educational materials for the user to improve their awareness of cyber security.
        - **User dashboard** – this is where users can find the modules that they can read and download, as well as video links for the modules that they want to study.

        - **Administrator dashboard** - this will provide shortcuts for common management tasks like account monitoring, update modules, and system announcements for admins.
        - **Authentication protocols -** the protocols for this will serve as a layer for the security of the user and also for the data.
        - **Push notification -** sending a notification about cybersecurity and also providing tips.
        - **Data analytics -** data from the user to determine their cybersecurity awareness.
    2. Cybersecurity applications:
        - **Cybersecurity Disaster Recovery Plan -** Cybersecurity applications to ensure the continuity and protections of the data regarding natural disasters, attacks, and other factors.

- To develop a learning application using the following technologies:
    1. Android studio - The official IDE (Integrated Development Environment) for Android app development. This technology will be used to develop the features and also the User Interface (UI) of CyberTips.
    2. JAVA - A general-purpose programming language. Java will be used for this development to proper functioning of features.
    3. XML - XML or Extensible Markup Language is a markup language to developed the UI of the project.
    4. Firebase - This technology will be the back end of the CyberTips. The researchers will configure the database for the data of the users and also the security of the data.

- To test the features of learning application.
- To evaluate the Functionality, Reliability, Usability, and Efficiency of the application.

Scope and Limitations

CyberTips will provide modules and tools to help people learn more about cyber security. The modules can be categorized into levels such as beginner, moderate, and intermediate. The modules will contain various tips, information, and learning materials. CyberTips will provide tools such as a password generator and text encryption. CyberTips will have separate page for users and administrator. The user page will only show the modules and tools. The administrator page will show the system management, where the admin can add, update, and delete a user. The authentication protocols will be configured on Firebase, where CyberTips' databases are. The authentication protocols ensure the security of the data collected by CyberTips during account processing.

The development of CyberTips will be used by the senior students and employees of Fort Bonifacio High School. Fort Bonifacio High School manages senior and junior students separately; the employees who manage the senior students are the only ones considered for the system's evaluation, while other employees with no connections to the senior students are not considered. This study will only be a way to improve the knowledge of the senior students and employees of Fort Bonifacio High School.

Significance of the Study

This educational research aims to develop a learning application for improving cybersecurity knowledge of senior high school students and employees of Fort Bonifacio High School. They are the people who will benefit for this development:

Senior high school students

The senior high school students will benefit from this development by enhancing their knowledge and their curiosity. The students can explore the applications to learn what they want to learn and, at the same time, learn how to protect themselves.

Senior high school employees

The senior high school employees will benefit from this development by improving their knowledge and seeing things differently than the others. The employees can use this development to enhance their teaching.

CHAPTER II

Review of Related Literature and Studies

This chapter present the review of related of literature, journal and studies underlying the framework of the study. It includes the conceptual model of the study and the operational definition of terms.

Foreign Literature

The Importance of Cybersecurity Education in School

According to Milos Tisma and Jasmina Andric (2021), the worldwide society's routine used of ICTs, which was accelerated by the COVID-19 viral pandemic, has resulted in a sharp rise in the amount of cyberattacks, scams, and other security concerns in cyberspace. Lack of cyber security professionals, poor awareness of hazards in cyberspace and the depths of the internet, and a lack of efficient methods for obtaining cyber security intelligence and alerting the public to threats have all been problems for society as a whole.

According to Timothy Brittan et al (2018), studies looking at the impacts of technology exposure starting at age 0 show that children are getting exposed to more technology than ever before and at younger ages. According to research from the Joint Research Centre of the European Commission (2017), children today will have used more technology by the time they graduate from school than any of the current generations of working adults have.

Improving students' cybersecurity awareness is important because it makes them aware of the risks associated with the internet. Using social media, online tools, and online gaming can harm students. According to Nurul Amirah Abdul Rahman et al. (2020), lack of teacher knowledge, skills, funding, and resources can be challenges to cybersecurity education. The challenges can

hinder the students' ability to learn about cybersecurity; therefore, it is best to utilize what resources can be used to provide for the students.

Mobile learning application

According to Kadir Demir and Ercan Akpinar (2018), quick information access, studying at any time and from anywhere, interacting with friends, and supporting learning are considered some of the major benefits of mobile learning. The study emphasizes that the mobile learning applications increase the effect of learning and enhance the process of learning. Furthermore, the study emphasizes how mobile learning can help students meet their academic requirements.

According to Jonathan O. Etcuban and Leocineza D. Pantinople (2018), mobile learning improved students' knowledge and achievement. Also, in line with their education, the administrator of the school should enforce and include the use of mobile learning to maximize the learning experience of the students. Maximizing the use of mobile learning can significantly increase and benefit students' self-education.

According to a study made by Ahmad Althunibat et al (2021), the recent appearance of the COVID-19 has resulted in a significant acceleration of the utilization of mobile learning applications in education and learning. Both students and teachers can benefit from mobile learning technology's convenience, engagement, and ability to conduct instruction at any time and from any location. Many instructors and lecturers are interested in mobile learning courses to improve student learning outcomes, especially in universities, because mobile learning technology makes online learning more flexible.

Cybersecurity

One of the most crucial challenges in recent years has emerged is the cyber security of information systems and infrastructure. Children and adults alike frequently access computer networks that are connected via the Internet using portable devices like smartphones and tablets in their daily lives. However, because using the internet involves using a lot of shared tools, such as navigation, information access, social media trends, news content, entertainment, and office tools like e-mail, calendar, etc. It has also turned into a place where risks like user identity theft, privacy sabotage, malicious code, cyberbullying, and others can occur (Zwilling, et al, 2019).

Local Literature

Local Literature

Cyber awareness

According to Amparo Pamela H. Fabe and Ella Zarcilla-Genecela (2021), the government is still managing cybersecurity despite the lack of employees, skills, and education regarding this topic. This include both external and internal challenges that the government is facing. The government's external challenges include a lack of awareness of cybersecurity among Filipinos. Internal challenges are the means by which the government raises Filipinos' awareness of cybersecurity and security against cybercrime.

Distance learning

The impact of the pandemic in the Philippines empowers distance learning. Distance education has many forms, such as radio, television, mobile devices, and computers. Using distance learning in this pandemic allows students and employees to learn without having to meet

face-to-face. Electronic learning (E-learning) is one of the forms of distance education that can be used by students and employees. The employees can use this e-learning to empower or enhance their knowledge, and the students can use e-learning to understand what they want to know (Joaquin et al., 2020).

Review of Related Studies

Foreign studies

Mobile learning application

According to Business Partner Magazine (2021), nearly half of college students use their mobile devices for learning, and 86% of them own a smart device. Research has shown that mobile devices, such as smartphones and tablets, are the most popular tools for accessing online information, making up more than 50% of all browsing activities worldwide. The use of mobile learning has become a great way to give college students more flexibility and a sense of control over their education.

In the past few years, mobile learning applications have increasingly become popular forms of education. Additionally, as technology advances, students will have access to a variety of new gadgets that can be used to greatly simplify and facilitate their academic pursuits. Students from all over the world will be at the center of mobile learning, sharing educational materials through tools and apps like Pedagogue (Lynch, Matthew, 2021).

Cybersecurity

The bad news is that when it comes to information technology and cyber security, the education sector still has a long way to go, and significant data loss instances are occurring

everywhere. Attackers can target industries of all shapes and sizes, and as more businesses move crucial data to the cloud, cyber security risks have increased significantly. Attackers can target the education sector for the students and employee's data to make quick money (Sander, Alexa, 2020).

Cyber awareness

According to Corey Nachreiner (2022), cybersecurity work isn't getting any simpler. Intelligent attackers increasingly prioritize attacking people over systems. An "all hands-on deck" culture of cybersecurity knowledge and accountability is necessary to be really safe in this setting. Everyone should be aware of their obligations and ability to change things, regardless of their position.

Threats that affect teachers and staff can be the main focus of a school's security awareness training program. But they require a different approach for kids, particularly those who attend K–12 institutions. They should encourage their kids' digital hygiene in the same way that they grow their language, reading, writing, and other skills. The classroom, whether physical or virtual, shouldn't be the only place where cybersecurity is taught. It is crucial to learn individually and always act responsibly online (Bisson, David, 2021).

Local studies

Cyber awareness

In this era of modern technology, it is very vital for everyday people to make their lives easier when they use the internet. It is readily accessible anytime and everywhere for the students, also, threats are everywhere on the internet. The increasing popularity of technology, such as mobile phones and the internet, has an impact on society in terms of individual needs and the

economy, and the expansion of the internet can lead to multiple cybercrimes. According to Ben Fermin Q. Abuda et al, (2020) the majority of users of mobile devices and the internet have a lack of knowledge about cybercrime. The students use their own knowledge on how to interact with the internet without awareness of threats and vulnerabilities.

Everybody has a duty to protect themselves online. The capacity of the individual is to secure or protect the use of cyberspace from cyberattacks. The combination of knowledge and action to protect one's assets or personal information is known as cyber security awareness. In the Philippines, there is a continuing increase in reports about cyberattacks that can be alarming for innocent users who do not know how to use the internet without knowledge of cyber threats. According to a study conducted at Occidental Mindoro State College (OMSC) in the Philippines, the results suggest that most students and teachers had passing scores or higher in terms of their knowledge of cyber security, however over 50% had scores that were below passing. To increase the security level of the devices utilized, practices call for teachers and students to become more knowledgeable about system and browser updates. Proper program education and training are strongly advisable to gain knowledge and give the students awareness of cybercrimes. More than half of IT students are aware of the fundamental cyber security procedures, but there is a sizable portion of non-IT students that needs to be taken into programs for cyber awareness. The need to improve student awareness of appropriate social media etiquette is critical. To prevent being a victim of cybercrime, increase basic cyber security awareness training for all students and teachers (Ailen B. Garcia et al., 2022).

According to Challiz D. Omorog and Ruji P. Medina (2018), 60 million Filipinos used the Internet in January 2017, making the Philippines the country with the highest Internet usage. The

attackers' expansion rates show no signs of slowing down in the Philippines, and there are still more reports about data breaches, exploiting data, scams, and other attacks from which the hacker can benefit. This growth has evolved into the launch pad for the government to begin and grow its online operations, influencing a wide range of fields like business, academics, and health.

Cybersecurity

Today, information and communications technology are a significant contributor to both our daily lives and the overall economy. However, given the difficulties posed by global connection, it is essential to comprehend cybersecurity, the dangers and threats it faces, how to reduce those risks, the best security practices, and how to respond to security incidents. According to the May S. Hermogeno (2018), successful phishing attacks account for 42% of all attacks. The cybersecurity defense of any organization is weakest where people are involved. As a result, the uninformed about cybercrime, especially students and users of the internet, are frequently the first victims of cyberattacks. People are easier to compromise, especially if they haven't received the correct instruction in fundamental security procedures.

According to Michael Francis M. Aquino and Marvin I. Noroña (2021), there are many different types of cybercrimes that are committed by cybercriminals. These crimes include cracking into other people's computers, bypassing passwords, and removing license restrictions; hacking into systems to steal, alter, and destroy data. Cyberterrorists who utilize the Internet to advance their political and ideological viewpoints. Cyberbullies who harass people online, Salami attackers who carry out minor to large-scale attacks, cause a denial of service, mine bitcoins, and steal an imperceptible sum of money from bank systems are just a few ways they utilize the Internet to spread fear and devastation.

According to Noly M. De Ramos and Francisco Dente Esponilla II (2022), in particular at a research institution, the cybersecurity dilemma poses a threat to the intellectual capital of students as well as the theft of sensitive data and financial loss. The current study is a multiple-case study of cybersecurity threats and problems at selected Philippine State Universities and Colleges in the National Capital Region. Information technology professionals from a variety of state colleges and universities were specifically chosen as sample participants. Threats were investigated in the study primarily using a structured interview. Identifying active and proactive strategies for creating a model framework for security resources in separate academic institutions requires evaluating the risks and difficulties of cybersecurity.

Conceptual Model of the Study

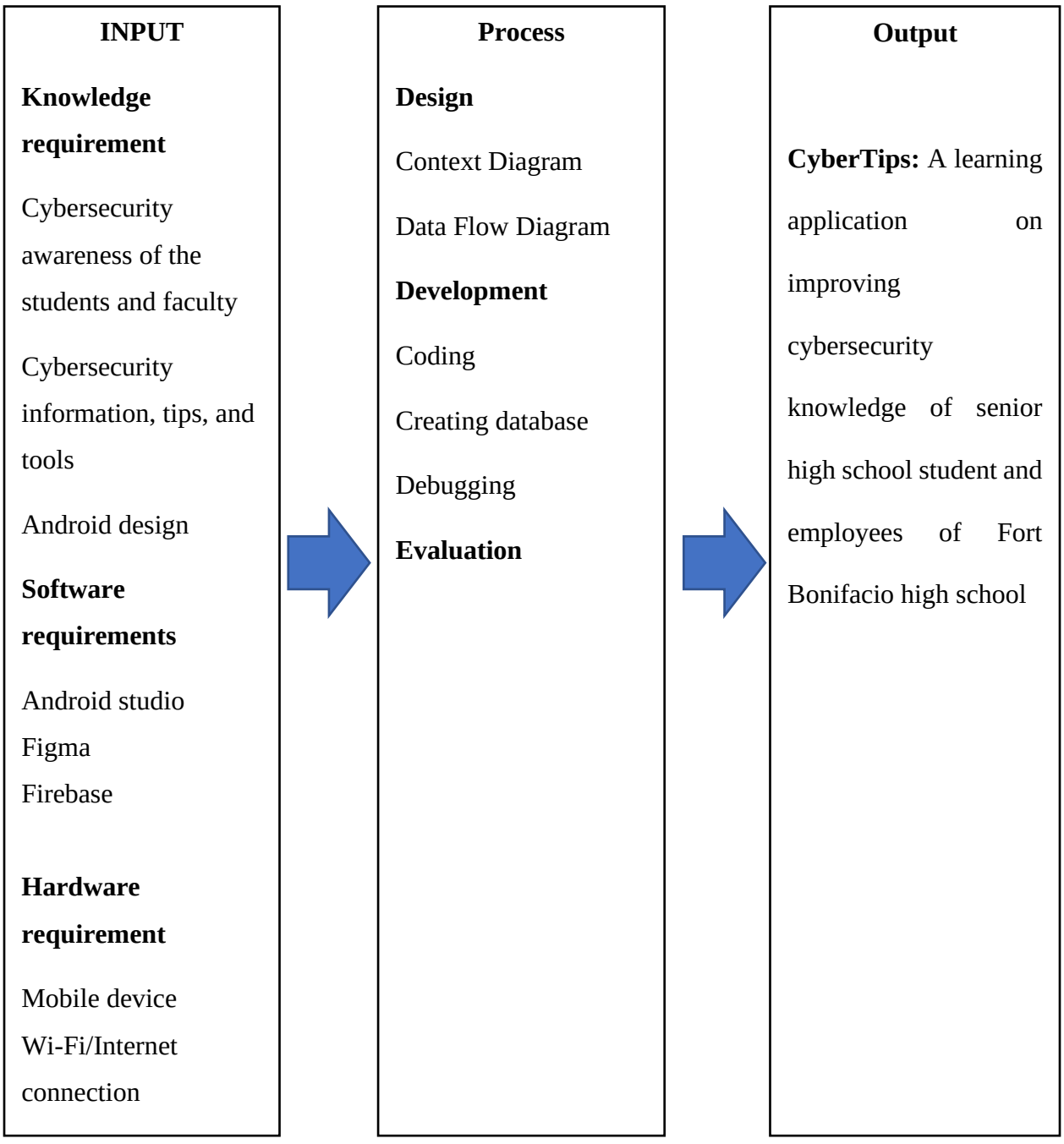

Figure 1. Conceptual Model

A system is portrayed in a conceptual model. It consists of ideas that aid in knowing, comprehending, or simulating the subject the model portrays. The diagram consists of three sections:

input, processing, and output. In the input, it contains three requirements. First, the researcher needs to survey the respondents for the knowledge scale about cybersecurity awareness for the knowledge requirements. After doing the survey and getting the results, the researcher will input the modules needed about cybersecurity awareness for the students and employees of Fort Bonifacio High School. For coding, design, and the database, the researcher will use Android Studio, Figma, and Firebase for software requirements. Mobile devices with a Wi-Fi connection are the final input requirement. This hardware requirement does not necessitate a large number of device specifications. After the input section, the researcher needs to process the design, development, and evaluation. This part is very important for the researcher and the users. For the development of this system, the entire system will rely on programmers and designers for the functionality and usability of the system. After integrating the components of the system, the researcher will create a prototype of the system for the evaluation process. This evaluation process can show how the system will work. Lastly, after the output of the two sections is completed, the system's development is fully complete, and it can be accessed by the students and employees of Fort Bonifacio High School.

Knowledge requirements

The researchers must know the knowledge of the students and employees on cybersecurity to create the necessary modules. The researcher will conduct interviews and surveys with Fort Bonifacio High School senior high school students and employees. The interview and survey will form the basis for creating modules, tips, and tools necessary for the students and employee's improvement in cyber awareness.

Software requirements

For the development of the learning application, the researchers will use Android Studio. The programming language that will be used by the researchers is Java. The researchers will use Figma, an interface design web application, to create a graphical user interface to make the learning application appealing from the user's perspective. After the researchers create a design in Figma, they will integrate the design into the Android Studio. To collect the data from the user, the researchers will use Firebase as the database.

Hardware requirements

The user can access the learning application through mobile devices that can connect to the internet. The internet connection will connect the user to the database to collect the data. The data that researchers collect will provide information for cybersecurity.

Design

The context diagram will show how students and employees interact with the learning application. The interactions that the students and employees on the application will assume are shown in the diagram.

The data flow diagram will show how the data of the students and employees flows from the application to the database. The data of the students and employees will be stored in the database, and the data will flow.

Development

The development phase will start with coding for the design and functionality of CyberTips, to collect the data of the students and employees, the developer will create a database to collect and store the data while also debugging and rechecking the functionality of CyberTips.

Evaluation

The evaluation will be performed by the Fort Bonifacio senior high school students, course adviser, and technical adviser to ensure functionality and reality.

Operational definition of terms

CyberTips - This technology will provide knowledge and awareness about cybersecurity for the senior students and employees of Fort Bonifacio High school.

Log in and sign in form - This module is for the authentication and also registration for the senior high school students and employees.

User dashboard - Within the user dashboard is the learning modules, tools and also the announcement board.

Administrator dashboard - Within the administrator dashboard is the information of user and announcement board.

Learning modules - All of learning modules about cybersecurity are in this page. Learning modules are about cybersecurity knowledge and awareness.

Tools - CyberTips also provides educational tools such as password generator and text encryption.

Announcement board - Users may see all announcements on CyberTips, and administrators can add new announcements.

CHAPTER III

Research Methodology

This chapter presents the sequence of project development. It includes the discussion of methods and actions in developing the project. It also includes some related information and development procedures.

The researchers conducted their research using descriptive and developmental methodologies. In contrast to exploratory research, descriptive research is conclusive in character. This means that descriptive research collects measurable data that may be used for data analysis to draw statistical conclusions about your target audience. As a result, this kind of research uses closed-ended questions, which reduces its capacity to offer original insights. However, when used appropriately, it can assist a company in more accurately defining and quantifying the importance of a particular aspect of a set of respondents and the community they represent. The survey, which comprises questionnaires, in-person interviews, phone surveys, and normative surveys, is the most popular descriptive research methodology. Research on development is also descriptive. Data that define the state of nature at a certain time are produced by descriptive study, which includes both qualitative and quantitative data. The numerous types of descriptive research are covered in this chapter along with some of their characteristics and fundamental methods.

Project design

This is how the proposed application is presented in a diagram. This will display the context diagram and logical data flow diagram for the proposed application. This covers every step of the application's process and all relevant data.

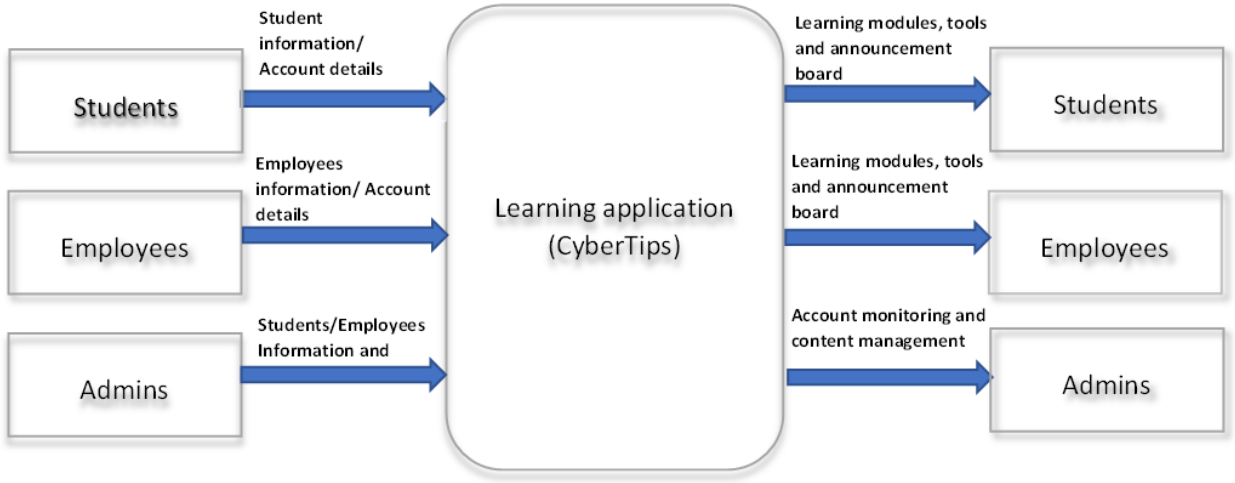

Figure 2. The context diagram of the study

This is the context diagram of this study this shows the three factors consist of students, admin, and employees. The diagram shows how the users will interact with this system it shows the relationship between the users and the learning application. The pointed arrow that goes to the learning application will be the input and output of the system. The students and employees will go through the registration page to create their secure accounts to gain access to this system. The admin will monitor the account database in this system so that in case of complications with their account, the admin can check every account that has been input. Also, the admin can input and modify learning modules inside of this application, and after posting, the admin will maintain the modules for responsiveness.

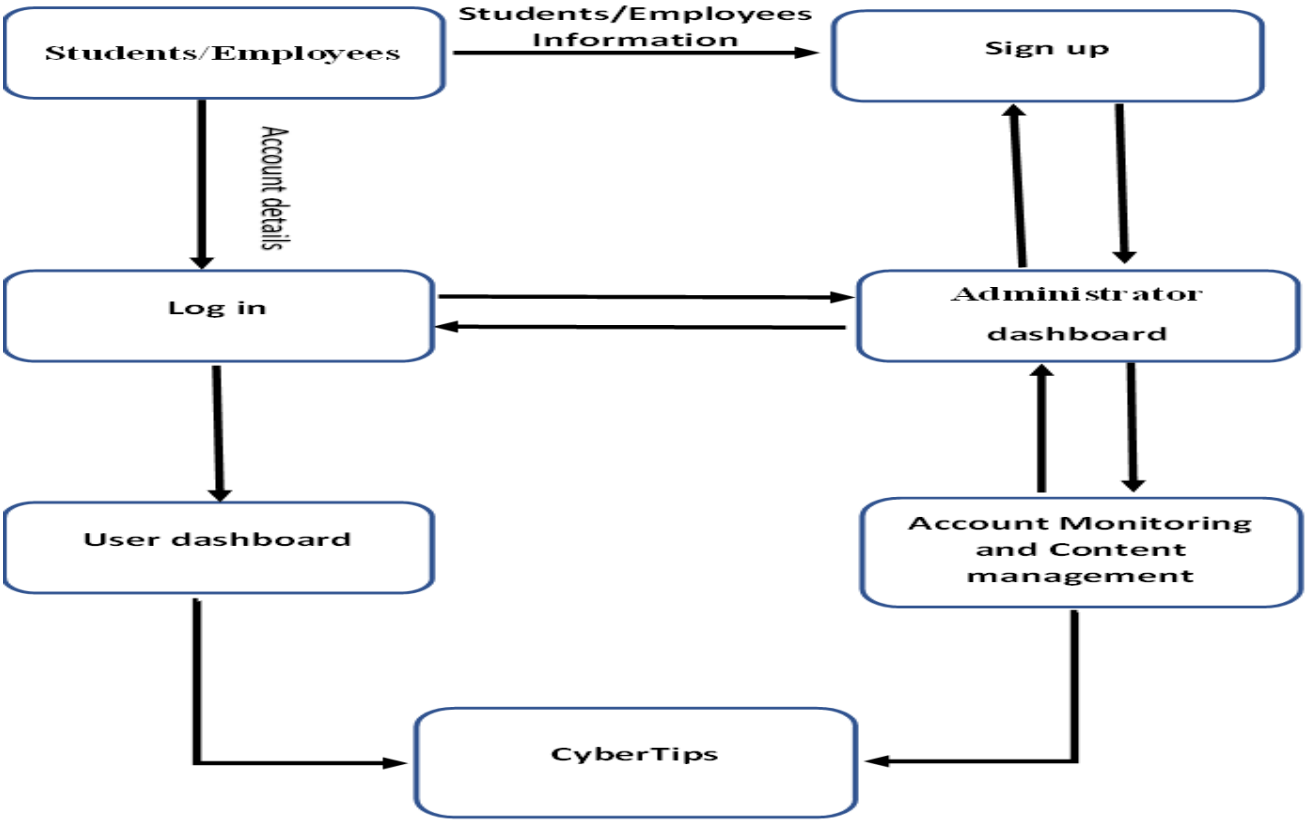

Figure 3. The data flow diagram of the study

This figure shows the logical data flow diagram of the application. This illustration depicts how users can interact with the application's components using the user categories of students, employees, and administrators. The students and employees should register first; after that their registered details will be processed in the database, and it will send to the student and employee that their registered account is processed and completed, after that, they will have a registered account from the database, and then they will go to the login page and input their username and password to gain access to the system. The admin will monitor the database of the students' and employees' accounts in account monitoring to ensure that all accounts are safe and also admin can update and delete their accounts in database. Admins can control the learning

modules for input, modification, deletion, and posting for the users of this application in the admin dashboard, and they can also put announcements for maintenance and updates so that the users are aware of the announcements. The students and employees can go directly to the user dashboard after logging in, and then they can choose the learning module that they want to study.

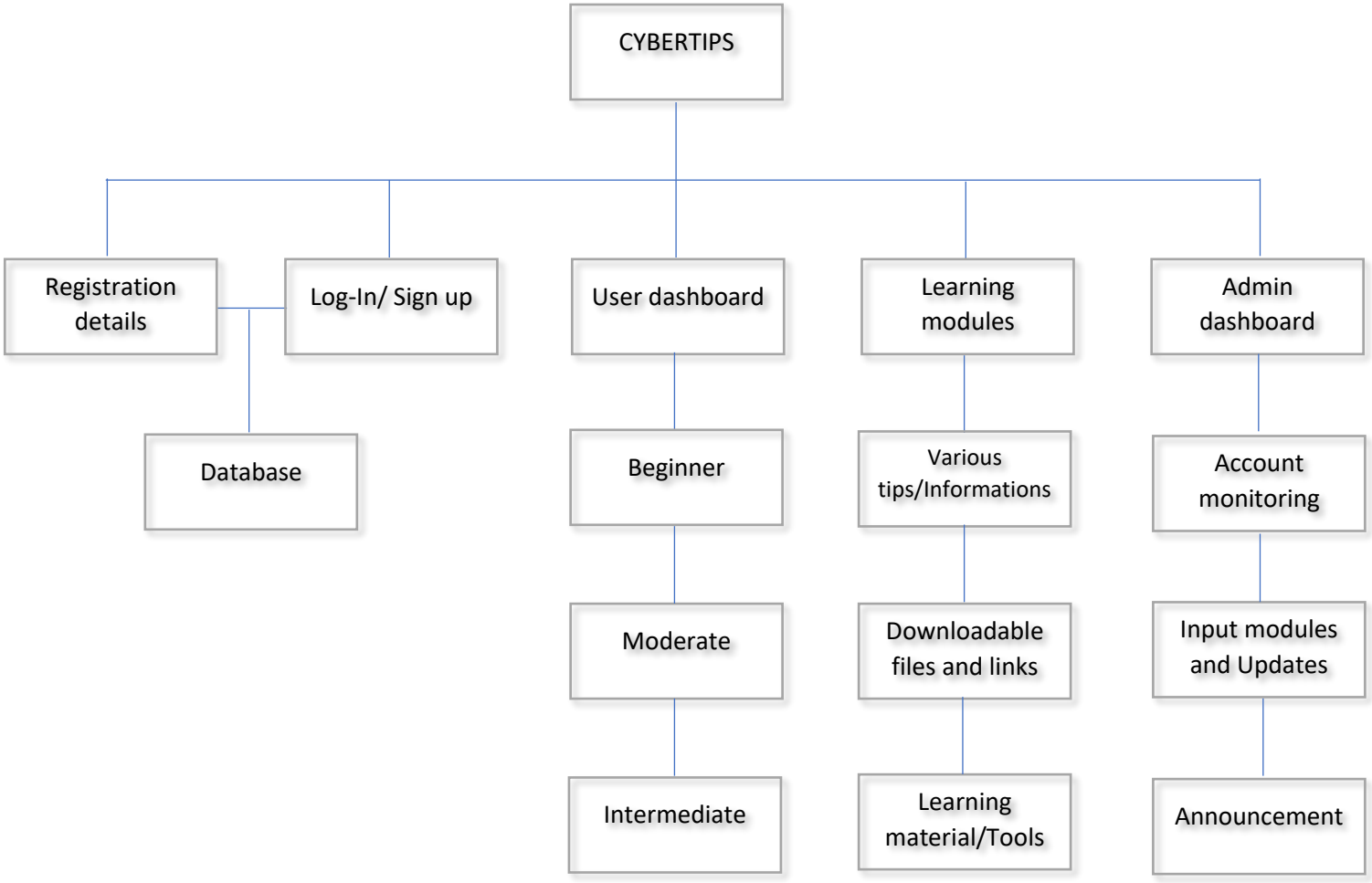

Figure 4. The hierarchical Input process output of the study

The HIPO diagram shows the system's module structure. Analysts utilize HIPO diagrams to get a high-level picture of system functions since they hierarchically break down functions into their component parts. It illustrates how the system operates.

The learning application has five main functions for interacting with this system: registration details, login/sign up, user dashboard, learning modules, and administrator dashboard. Each main function is accompanied by a subfunction. After a user creates an account, the database will process it, and all accounts will be registered. They can then go to the system to access it. Then the user will go to the next main function, which is the user dashboard, and then the user can select the levels of learning, which is a subfunction of the system. The levels are beginner, moderate, and intermediate. This procedure will help the user determine the level before beginning the learning process. After they choose the level, the learning module will be displayed, and the subfunctions are: various tips and information for beginners; downloadable files and links; deep learning about cyber security for moderate users; and lastly, the learning materials and tools for intermediate users. The last main function is the admin dashboard. This function is very important in this system. The administrator dashboard allows them to control all the components of the system; they can modify, input, maintain, and update the whole system. This main function has three subfunctions: account monitoring, input modules, and updates and announcements.

Project development

For the capstone project, the researcher will use Joint Application Development (JAD) to represent how the Android application will develop. It is a strategy for assuring accuracy between the project scope definition and delivery through ongoing stakeholder participation. The JAD development process and lifetime are centered around these interactions. It is a contemporary method of gathering and examining application requirements, which are talked about in a series of meetings and workshops between the business and technical teams (*Stephen, Olalekan, 2017*).

According to Olalekan Stephen (2017), the Joint Application Development is meant for the process of development of the system, but it can also be applicable to other types of development. Joint Application Development (JAD) is more agile in delivering environments in which agreements between the commercial and technical stakeholders on what is known as the minimum viable product (MVP) constitute the basis for the rapid development and delivery of software solutions.

The advantages of joint application development are: to develop systems from a customer perspective; to remove all risk by cooperating between researchers and organizations; to progress faster.

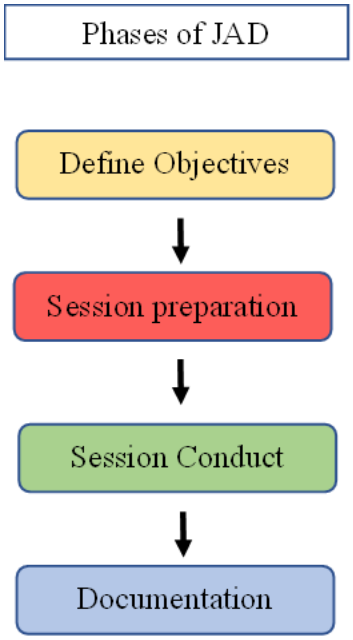

Figure 5. The Phases of the JAD Model

Define Objectives

Defining the objectives is the first stage of developing a joint application. The project's aims and goals were established at this phase of collaboration between the researchers and the end users. The project's objectives cover its scope, its expected outcome, and the people involved in creating the application.

Session preparation

The second phase of JAD is the preparation for conducting meetings with the assistant principal of Fort Bonifacio High School and other faculty members to provide them with information on the project. The meetings will be virtual to provide them with comfort and a flexible schedule. After several meetings, the researchers will have clearer objectives, scope, and limitations for their project. The researchers must be confident enough to facilitate ideas and discuss their project with the end users.

In this session, the researchers should present a wireframe of the project to the assistant professor and other faculty members. The researchers present the features of such things as learning modules and tools, user dashboards, administrator dashboards, authentication protocols, and data analytics. The feedback will be used for development. This process will repeat until the desired goal is achieved.

The researchers also present the application of cybersecurity toTo ensure the continuity of operations and protection of the data regarding natural disasters, attacks, and other factors, the researchers will come up with a plan for cybersecurity disaster recovery.

Session conduct

Another virtual conference will be held during this phase for the researchers to demonstrate the built system to the study participants and get their feedback on any flaws or concerns. The researchers will be able to assess the requirements' completeness, accuracy, coherence, and viability thanks to this. The gathered requirements will also be condensed to address the demands of the participants. Once everything has been accomplished, the stakeholders will be asked for their consent before the system may be used to carry out the researcher's objective.

User acceptance testing and evaluation

The system will go through a number of tests when it has been fully designed before being put into use. Before the user acceptability assessment, the researchers will do a number of tests, including system, integration, and unit testing.

The objectives and features of the CYBERTIPS; A LEARNING APPLICATION ON IMPROVING THE CYBERSECURITY KNOWLEDGE OF SENIOR HIGH SCHOOL STUDENTS AND EMPLOYEES OF FORT BONIFACIO HIGH SCHOOL will be assessed, and selected users will determine if the system under test recognizes legitimate inputs.

Documentation

The facilitators and the selected "documentation head" must make sure that no significant material is missed during the conversations in order to produce well-explained papers, which is the final phase in Joint Application Development (JAD).

During this phase, the researchers will request user approval and record every session that takes place. Following the collection procedure, the papers will be preserved in both local and cloud storage. This will assist researchers in gaining the following information: a.) Information that is useful in the project's ongoing development; b.) Evaluations of the project's actual process; and c.) Preparation for the capstone's next stage of development.

The users' responses on the evaluation form that was distributed when the system was being tested will be used by the researchers to calculate the efficacy of the system. The researchers will be able to ascertain whether the system achieved the users' goals and whether faculty members support its use.

Conceptual Process of the System

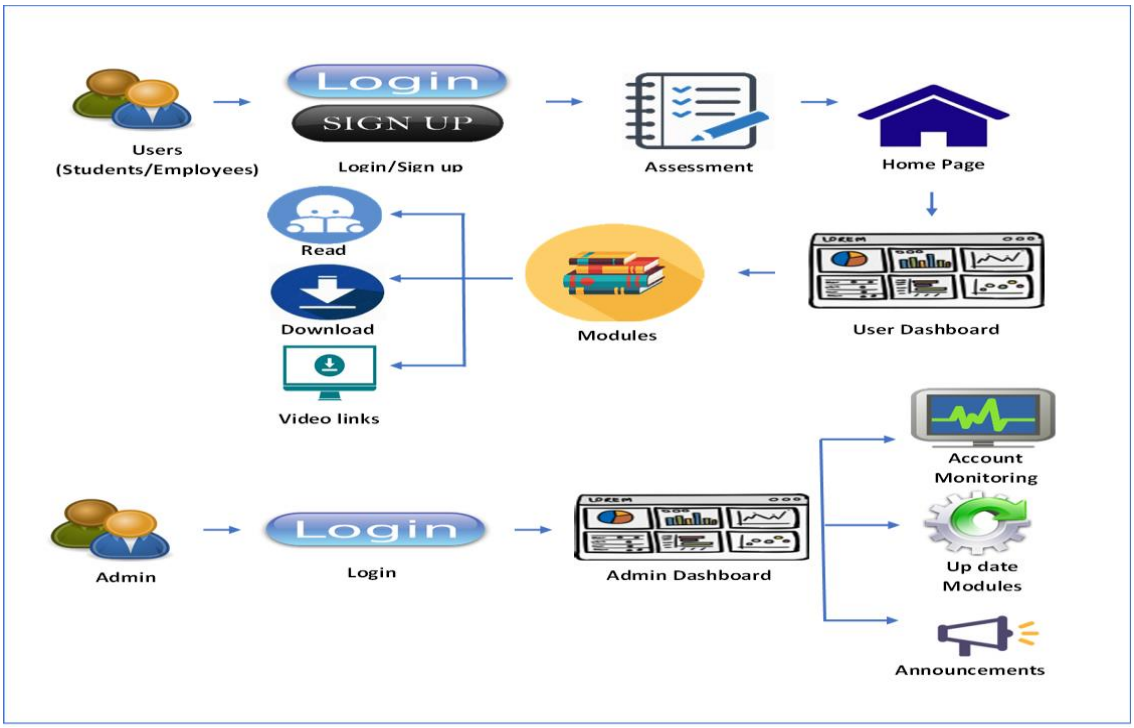

Figure 6. Conceptual process of the system

The process of what the system can achieve is depicted in the above figure. For Students and Employee users, the system will make them create an account or login to it if they already

have an account. New users will have to answer an assessment on their knowledge and awareness on cybersecurity, and if they are a student or an employee. And on the home page, users will see a user dashboard which will lead to modules that they can read and download, as well as video links for the modules that they want to study. For the Admin users, the system will make them login to their account and it will lead them to the home page. In the home page, they will see an Admin Dashboard that provides shortcuts for common management tasks like account monitoring, update modules, and system announcements.

Testing and Operating Procedures

The figures display the main functionality of the application for the senior students and employees of Fort Bonifacio High School. The application could be used with the following process.

Testing procedure

The main purpose of this phase of system development before its implementation is to test the functionality, reliability, usability, and efficiency so that the senior students and employees meet their expectations.

Table 1. Tests that will be conducted for the testing procedures

System features	Test conducted
Learning modules and tools	a. The modules and tools should be usable.
User dashboard	a. The system must show the users information. b. The system must show the progress of learning.

	c. The system must show the modules and tools.
Administrator dashboard	a. The system must show the user's information. b. The admin will maintain the user's information. c. The admin can add, edit, update and delete profile. d. The admin can manage the system. e. The admin can manage content.
Security protocols	a. The security protocol of the system should work
Push notification	a. The system must send a notification on user
Data analytics	a. The system must show data about the level of awareness among Fort Bonifacio High School senior students.

Evaluation Procedure

The researcher will create a prototype of this system in order to evaluate the designs and user interface of the learning application and each module; this procedure will assist the researcher in creating the system's designs and interfaces. This procedure will be followed for a demonstration on how to use and navigate all components and interfaces of this application and how it works. The researcher will conduct a survey for the evaluation of this application.

The researchers will gather respondents by means of random sampling in order to assess the system. The Fort Bonifacio high schools' 25 senior students with ICT specialization and 25 senior students with non-ICT specialization, and 10 teachers will be requested to take part in the project evaluation by the researchers.

All respondents can participate in the evaluation procedure for the development of this application since all of them have mobile devices to gain access to it. It is easy to navigate and test this application for beta testing.

Evaluation Criteria

A survey will be sent to the chosen students and employees in order to evaluate the project's performance. The following criteria will be used for this study's ISO 9241 for human interaction and ISO/IEC 9126 for software quality evaluation: functional appropriateness, usability, reliability, maintainability, and portability.

1. Functional Suitability - This characteristic indicates the degree to which a product or system provides functions that meet explicit and implicit requirements when used under specific conditions.

2. Usability - The extent to which a user can utilize a system or application to accomplish a particular objective in a certain usage context effectively, efficiently, and successfully.

3. Reliability - The extent to which a system, product, or component performs a specific function under specific conditions and within a specific period of time.

4. Maintainability - This feature describes how effectively and efficiently a product or system may be adjusted to enhance, modify, or adapt to changes in the environment or needs.

5. Portability - The flexibility by which a framework, service, or resource may be moved from one operating system, software, or another environment to another.

Table 2. Rating, Range, Interpretation

Rating	Range	Interpretation
5	**4.50 - 5.00**	**Strongly Agree**
4	**3.51 - 4.50**	**Agree**
3	**2.51 - 3.50**	**Neutral**
2	**1.51 - 2.50**	**Disagree**
1	**1.00 - 1.50**	**Strongly Disagree**

Treatment of data

The ratings of "CyberTips: A Learning Application for Cyber Awareness and Threats" will be evaluated using the provided criteria by calculating the mean. The researchers will utilize it to calculate the mean, also referred to as the average.

using the formula:

$$\overline{X} = \frac{\sum X}{N}$$

Where:

$\overline{X}$ = Mean

$\sum X$ = The sum of the Respondent's ratings

N = Total number of respondents

Figure 11. Statistical Formula

Research instrument

CyberTips: Improving the Cybersecurity Knowledge of Senior High School Students and Employees at Fort Bonifacio High School (Employees only)

Researchers collected data entered by respondents to evaluate a learning application, "CyberTips: Improving the Cybersecurity Knowledge of Senior High School Students and Employees at Fort Bonifacio High School." Rest assured that all information about the study is stored and strictly excluded from outside sources, and only the researchers know the data collected. Researchers keep the data they collect private and delete it after a year. Thanks for your cooperation.

The purpose of this study is to develop a learning application to improve the cybersecurity knowledge and awareness of senior students and employees.Answering the following surveys will take about 5-8 minutes. Thank you very much for your candid responses. All responses are retained for research purposes only. For more information, please contact: aonzaga.k11720977@umak.edu.ph

Rating Grade:

1- Strongly Disagree
2- Disagree
3- Neutral
4- Agree
5- Strongly Agree

Name

Your answer

Age

Your answer

Email

Your answer

Functionality

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
User can create and log in in his/her own account.	○	○	○	○	○
The system let user choose between student and employee.	○	○	○	○	○
The user can view his/her own information and learning progress	○	○	○	○	○
The user can see the modules and tools	○	○	○	○	○

Reliability

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The modules are downloadable	○	○	○	○	○
The user's profile display the user's information precisely.	○	○	○	○	○

Usability

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The system can be easily learned by any user.	○	○	○	○	○
The system is understandable.	○	○	○	○	○
The system can be accessed via mobile devices.	○	○	○	○	○

Efficiency

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The system is available at all times.	○	○	○	○	○
The modules and tools available.	○	○	○	○	○

Maintainability

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Data security for users was guaranteed by the system.	○	○	○	○	○
The admin can edit, update, add and delete profile	○	○	○	○	○
The administration can see the informations of the users	○	○	○	○	○

Portability

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The system can be installed on any mobile device.	○	○	○	○	○
The application is portable and can be used at any time.	○	○	○	○	○

Comment/suggestions

Your answer

Get link

CyberTips: Improving the Cybersecurity Knowledge of Senior High School Students and Employees at Fort Bonifacio High School (Students only)

Researchers collected data entered by respondents to evaluate a learning application, "CyberTips: Improving the Cybersecurity Knowledge of Senior High School Students and Employees at Fort Bonifacio High School." Rest assured that all information about the study is stored and strictly excluded from outside sources, and only the researchers know the data collected. Researchers keep the data they collect private and delete it after a year. Thanks for your cooperation.

The purpose of this study is to develop a learning application to improve the cybersecurity knowledge and awareness of senior students and employees.Answering the following surveys will take about 5-8 minutes. Thank you very much for your candid responses. All responses are retained for research purposes only. For more information, please contact: aonzaga.k11720977@umak.edu.ph
Rating Grade:
1- Strongly Disagree
2- Disagree
3- Neutral
4- Agree
5- Strongly Agree

Name

Your answer

Age

Your answer

Email

Your answer

Functionality

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
User can create and log in in his/her own account.	○	○	○	○	○
The system let user choose between student and employee.	○	○	○	○	○
The user can view his/her own information and learning progress	○	○	○	○	○
The user can see the modules and tools	○	○	○	○	○

Reliability

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The modules are downloadable	○	○	○	○	○
The user's profile display the user's information precisely.	○	○	○	○	○

Usability

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The system can be easily learned by any user.	○	○	○	○	○
The system is understandable.	○	○	○	○	○
The system can be accessed via mobile devices.	○	○	○	○	○

Efficiency

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The system is available at all times.	○	○	○	○	○
The modules and tools available.	○	○	○	○	○

Maintainability

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Data security for users was guaranteed by the system.	○	○	○	○	○

Portability

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The system can be installed on any mobile device.	○	○	○	○	○
The application is portable and can be used at any time.	○	○	○	○	○

Comment/suggestions

Your answer

References

Abuda, B. F., Rivera, K. D., & Noroña, R. V. (2020). Predictive Validity of a Cybercrime Awareness Tool: The Case of Senior High School Students in a Philippine Secondary School. *International Journal in Information Technology in Governance, Education and Business*, 18-26. Retrieved from https://ssrn.com/abstract=4007646

Althunibat, A., Almaiah, M. A., & Altarawneh, F. (2021). Examining the Factors Influencing the Mobile Learning Applications Usage in Higher Education during the COVID-19 Pandemic. *Electronics*, 1-23. doi:10.3390/electronics10212676

Bisson, D. (2021, June 2). Retrieved from Security Intelligence: https://securityintelligence.com/articles/how-awareness-training-improves-school-cybersecurity/

Brittan, T., Jahankhani, H., & McCarthy, J. (2018). An Examination into the Effect of Early Education on Cyber Security Awareness Within the U.K. In H. Jahankhani (Ed.), *Cyber Criminology* (pp. 291-306). Springer International Publishing. doi:10.1007/978-3-319-97181-0_14

Business Partner Magazine. (2021, May 4). Retrieved from Business Partner Magazine: https://businesspartnermagazine.com/impact-mobile-learning-higher-education/

Clark, J. (n.d.). Retrieved from back4app: https://blog.back4app.com/firebase-vs-google-cloud/#Google_Cloud_vs_Firebase_Comparison

De Ramos, N. M., & Esponilla II, F. D. (2022, September). Cybersecurity program for Philippine higher education institutions: A multiple-case study. *International Journal of Evaluation and Research in Education (IJERE), 11*(3), 1198~1209. doi:10.11591/ijere.v11i3.22863

Demir, K., & Akpinar, E. (2018). The Effect of Mobile Learning Applications on Students' Academic Achievement and Attitudes toward Mobile Learning. *Malaysian Online Journal of Educational Technology, 6(2)*, 48-59. Retrieved from https://eric.ed.gov/?q=learning+application&ff1=dtySince_2018&pg=2&id=EJ1174817

Etcuban, J. O., & Pantinople, L. D. (2018). The Effects of Mobile Application in Teaching High School Mathematics. *International Electronic Journal of Mathematics Education,, 13(3)*, 249-259. Retrieved from https://doi.org/10.12973/iejme/3906

Garcia, A. B. (2022). A Cyber Security Cognizance among College Teachers and Students in Embracing Online Education. In *2022 8th International Conference on Information Management (ICIM)* (pp. 116-119). doi:10.1109/ICIM56520.2022.00028

Hermogeno, M. S. (2019, March). Assessment on the Cybersecurity Awareness in Academic Institutions. *International Journal of Engineering Science and Computing, 9*(3). Retrieved from https://ijesc.org/upload/cc84eddb2d8dc6f3e70575bf91a7e63f.Assessment%20on%20the%20Cybersecurity%20Awareness%20in%20Academic%20Institutions%20(1).pdf

Joaquin, J. J. (2020). The Philippine Higher Education Sector in the Time of COVID-19. *Frontiers in Education, 5*. doi:10.3389/feduc.2020.576371

Lynch, M. (2021, August 2021). Retrieved from The Tech Advocate: https://www.thetechedvocate.org/exploring-the-future-of-mobile-learning/

Madarang, C. R. (2020, September 11). *hobbies-interest: Filipino students, too, can be targets of cyber crime. How to keep crooks at bay*. Retrieved from interaksyon: https://interaksyon.philstar.com/hobbies-interests/2020/09/11/176688/students-cybercrime-victims/

Nachreiner, C. (2022, December 20). *Why a Culture of Awareness and Accountability Is Essential to Cybersecurity*. Retrieved from https://www.csoonline.com/article/3683789/why-a-culture-of-awareness-and-accountability-is-essential-to-cybersecurity.html

Noroña, M. F. (2021). Enhancing Cyber Security in the Philippine Academe: A Risk-Based IT Project Assessment Approach. *Proceedings of the 11th Annual International Conference on Industrial*

Engineering and Operations Management Singapore. Retrieved from https://www.ieomsociety.org/singapore2021/papers/878.pdf

Omorog, C. D., & Medina, R. P. (2017). Internet Security Awareness of Filipinos. *International Journal of Computing Sciences Research, 1(4)*, 14-26. doi:10.25147/ijcsr.2017.001.1.18

Rahman N. A. A, S. I. (2020, May). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology, 10*(5). Retrieved from http://www.ijiet.org/vol10/1393-JR419.pdf

Ruguru, J. (2021, October 1). Retrieved from Section: https://www.section.io/engineering-education/how-to-secure-firebase-apps-with-firebase-security-rules/

Sander, A. (2022, October 20). Retrieved from Security Boulevard: https://securityboulevard.com/2022/10/the-state-of-cyber-security-in-schools/

Stephen, O. (2017, December 25). *Joint Application Development: Definition, Phases & Methodology*. Retrieved from Study.com: https://study.com/academy/lesson/joint-application-development-definition-phases-methodology.ht.ml.

The Sorry State of Cybersecurity in the Philippines. (2019, September 4). Retrieved from DailyGuardian: https://www.dailyguardian.com.ph/the-sorry-state-of-cybersecurity-in-the-philippines/

Tisma, M., & Andric, J. (2021, December). Importance of cyber security awareness and e-learning motivation for cyber security in reshaping the education. *Journal of Information Systems & Operations Management, 15*(2), 284-296. Retrieved October 29, 2022, from https://www.proquest.com/openview/684afd2311d9e031a130e1768baacdf8/1?pq-origsite=gscholar&cbl=1216366

Zarcilla-Genecela, A. P. (2021). The Philippines' Cybersecurity Strategy: Strengthening partnerships to enhance cybersecurity capability. In M. M. Scott N. Romaniuk, *Routledge Companion to Global Cyber-Security Strategy* (pp. 315-324). Retrieved from https://doi.org/10.4324/9780429399718

Zwilling, M., Lesjak, D., Natek, S., Phusavat, K., & Anussornnitisarn, P. (2019). HOW TO DEAL WITH THE AWARENESS OF CYBER HAZARDS AND SECURITY IN (HIGHER) EDUCATION? *Thriving on Future Education, Industry, Business and Society; Proceedings of the MakeLearn and TIIM International Conference 2019* (pp. 433-439). Piran Slovenia: ToKnowPress. Retrieved from https://www.toknowpress.net/ISBN/978-961-6914-25-3/papers/ML19-130.pdf

Abuda, B. F., Rivera, K. D., & Noroña, R. V. (2020). Predictive Validity of a Cybercrime Awareness Tool: The Case of Senior High School Students in a Philippine Secondary School. *International Journal in Information Technology in Governance, Education and Business*, 18-26. Retrieved from https://ssrn.com/abstract=4007646

Althunibat, A., Almaiah, M. A., & Altarawneh, F. (2021). Examining the Factors Influencing the Mobile Learning Applications Usage in Higher Education during the COVID-19 Pandemic. *Electronics*, 1-23. doi:10.3390/electronics10212676

Bisson, D. (2021, June 2). Retrieved from Security Intelligence: https://securityintelligence.com/articles/how-awareness-training-improves-school-cybersecurity/

Brittan, T., Jahankhani, H., & McCarthy, J. (2018). An Examination into the Effect of Early Education on Cyber Security Awareness Within the U.K. In H. Jahankhani (Ed.), *Cyber Criminology* (pp. 291-306). Springer International Publishing. doi:10.1007/978-3-319-97181-0_14

Business Partner Magazine. (2021, May 4). Retrieved from Business Partner Magazine: https://businesspartnermagazine.com/impact-mobile-learning-higher-education/

Clark, J. (n.d.). Retrieved from back4app: https://blog.back4app.com/firebase-vs-google-cloud/#Google_Cloud_vs_Firebase_Comparison

De Ramos, N. M., & Esponilla II, F. D. (2022, September). Cybersecurity program for Philippine higher education institutions: A multiple-case study. *International Journal of Evaluation and Research in Education (IJERE), 11*(3), 1198~1209. doi:10.11591/ijere.v11i3.22863

Demir, K., & Akpinar, E. (2018). The Effect of Mobile Learning Applications on Students' Academic Achievement and Attitudes toward Mobile Learning. *Malaysian Online Journal of Educational Technology, 6(2)*, 48-59. Retrieved from https://eric.ed.gov/?q=learning+application&ff1=dtySince_2018&pg=2&id=EJ1174817

Etcuban, J. O., & Pantinople, L. D. (2018). The Effects of Mobile Application in Teaching High School Mathematics. *International Electronic Journal of Mathematics Education,, 13(3)*, 249-259. Retrieved from https://doi.org/10.12973/iejme/3906

Garcia, A. B. (2022). A Cyber Security Cognizance among College Teachers and Students in Embracing Online Education. In *2022 8th International Conference on Information Management (ICIM)* (pp. 116-119). doi:10.1109/ICIM56520.2022.00028

Hermogeno, M. S. (2019, March). Assessment on the Cybersecurity Awareness in Academic Institutions. *International Journal of Engineering Science and Computing, 9*(3). Retrieved from https://ijesc.org/upload/cc84eddb2d8dc6f3e70575bf91a7e63f.Assessment%20on%20the%20Cybersecurity%20Awareness%20in%20Academic%20Institutions%20(1).pdf

Joaquin, J. J. (2020). The Philippine Higher Education Sector in the Time of COVID-19. *Frontiers in Education, 5*. doi:10.3389/feduc.2020.576371

Lynch, M. (2021, August 2021). Retrieved from The Tech Advocate: https://www.thetechedvocate.org/exploring-the-future-of-mobile-learning/

Madarang, C. R. (2020, September 11). *hobbies-interest: Filipino students, too, can be targets of cyber crime. How to keep crooks at bay*. Retrieved from interaksyon: https://interaksyon.philstar.com/hobbies-interests/2020/09/11/176688/students-cybercrime-victims/

Nachreiner, C. (2022, December 20). *Why a Culture of Awareness and Accountability Is Essential to Cybersecurity*. Retrieved from https://www.csoonline.com/article/3683789/why-a-culture-of-awareness-and-accountability-is-essential-to-cybersecurity.html

Noroña, M. F. (2021). Enhancing Cyber Security in the Philippine Academe: A Risk-Based IT Project Assessment Approach. *Proceedings of the 11th Annual International Conference on Industrial Engineering and Operations Management Singapore.* Retrieved from https://www.ieomsociety.org/singapore2021/papers/878.pdf

Omorog, C. D., & Medina, R. P. (2017). Internet Security Awareness of Filipinos. *International Journal of Computing Sciences Research, 1(4)*, 14-26. doi:10.25147/ijcsr.2017.001.1.18

Rahman N. A. A, S. I. (2020, May). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology, 10*(5). Retrieved from http://www.ijiet.org/vol10/1393-JR419.pdf

Ruguru, J. (2021, October 1). Retrieved from Section: https://www.section.io/engineering-education/how-to-secure-firebase-apps-with-firebase-security-rules/

Sander, A. (2022, October 20). Retrieved from Security Boulevard: https://securityboulevard.com/2022/10/the-state-of-cyber-security-in-schools/

Stephen, O. (2017, December 25). *Joint Application Development: Definition, Phases & Methodology*. Retrieved from Study.com: https://study.com/academy/lesson/joint-application-development-definition-phases-methodology.ht.ml.

The Sorry State of Cybersecurity in the Philippines. (2019, September 4). Retrieved from DailyGuardian: https://www.dailyguardian.com.ph/the-sorry-state-of-cybersecurity-in-the-philippines/

Tisma, M., & Andric, J. (2021, December). Importance of cyber security awareness and e-learning motivation for cyber security in reshaping the education. *Journal of Information Systems & Operations Management, 15*(2), 284-296. Retrieved October 29, 2022, from https://www.proquest.com/openview/684afd2311d9e031a130e1768baacdf8/1?pq-origsite=gscholar&cbl=1216366

Zarcilla-Genecela, A. P. (2021). The Philippines' Cybersecurity Strategy: Strengthening partnerships to enhance cybersecurity capability. In M. M. Scott N. Romaniuk, *Routledge Companion to Global Cyber-Security Strategy* (pp. 315-324). Retrieved from https://doi.org/10.4324/9780429399718

Zwilling, M., Lesjak, D., Natek, S., Phusavat, K., & Anussornnitisarn, P. (2019). HOW TO DEAL WITH THE AWARENESS OF CYBER HAZARDS AND SECURITY IN (HIGHER) EDUCATION? *Thriving on Future Education, Industry, Business and Society; Proceedings of the MakeLearn and TIIM International Conference 2019* (pp. 433-439). Piran Slovenia: ToKnowPress. Retrieved from https://www.toknowpress.net/ISBN/978-961-6914-25-3/papers/ML19-130.pdf