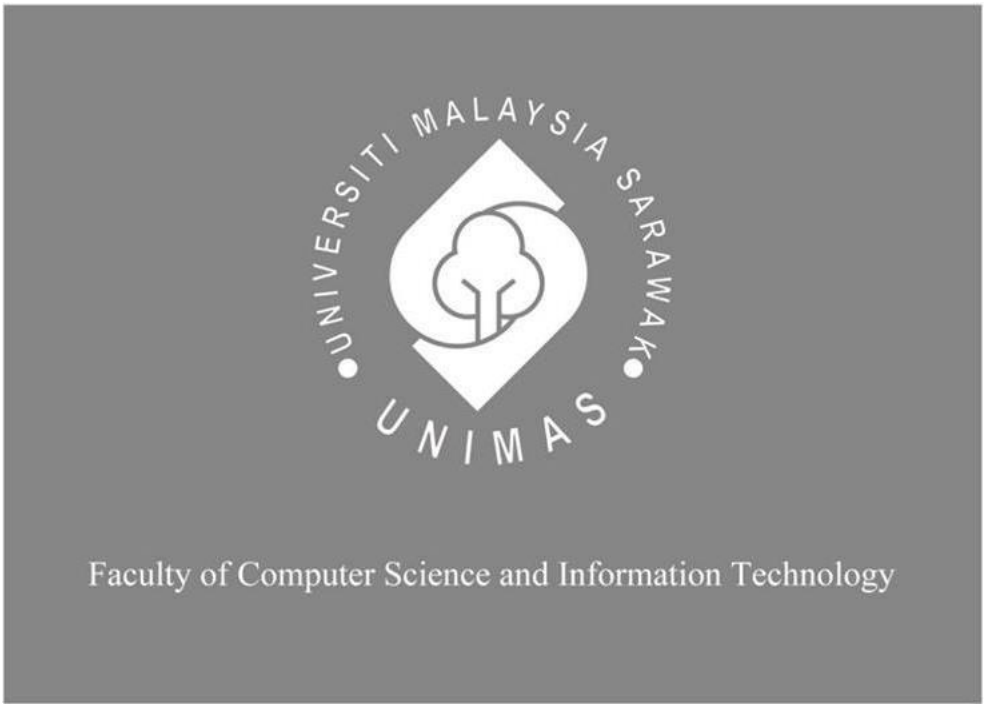

EDUSECURE: EDUCATIONAL APP FOR CYBER SECURITY

NUR BAQIYAH BINTI HAIDIR

(72520)

BACHELOR OF COMPUTER SCIENCE WITH HONOURS

(NETWORK COMPUTING)

2023

EDUSECURE: EDUCATIONAL APP FOR CYBER SECURITY

NUR BAQIYAH BINTI HAIDIR

This project is submitted in partial fulfilment

of the requirements for the degree of

Bachelor of Computer Science with Honours

(Network Computing)

Faculty of Computer Science and Information Technology

UNIVERSITI MALAYSIA SARAWAK

2023

EDUSECURE: APLIKASI PENDIDIKAN KESELAMATAN SIBER

NUR BAQIYAH BINTI HAIDIR

Projek ini merupakan salah satu keperluan untuk

Ijazah Sarjana Muda Sains Komputer dengan Kepujian

(Pengkomputeran Rangkaian)

Fakulti Sains Komputer dan Teknologi Maklumat

UNIVERSITI MALAYSIA SARAWAK

2023

DECLARATION

I hereby declare that this project has been composed solely by myself and that the work contained herein is my own except where explicitly stated otherwise in the text. I have not copied from any other student's work, nor has any part that had been written for me by another person.

_____

Nur Baqiyah Binti Haidir (72520)

Network Computing
Faculty of Science Computer and Information Technology
Universiti Malaysia Sarawak
Date:

UNIVERSITI MALAYSIA SARAWAK

THESIS STATUS ENDORSEMENT FORM

TITLE: EDUSECURE: EDUCATIONAL APP FOR CYBER SECURITY

ACADEMIC SESSION: 2022/2023

NUR BAQIYAH BINTI HAIDIR
(CAPITAL LETTERS)

hereby agree that this Thesis* shall be kept at the Centre for Academic Information Services, Universiti Malaysia Sarawak, subject to the following terms and conditions:

1. The Thesis is solely owned by Universiti Malaysia Sarawak
2. The Centre for Academic Information Services is given full rights to produce copies for educational purposes only
3. The Centre for Academic Information Services is given full rights to do digitization in order to develop local content database
4. The Centre for Academic Information Services is given full rights to produce copies of this Thesis as part of its exchange item program between Higher Learning Institutions [or for the purpose of interlibrary loan between HLI]
5. ** Please tick (√)

☐	CONFIDENTIAL	(Contains classified information bounded by the OFFICIAL SECRETS ACT 1972)
☐	RESTRICTED	(Contains restricted information as dictated by the body or organization where the research was conducted)
√	UNRESTRICTED	

Validated by

(AUTHOR'S SIGNATURE)

(SUPERVISOR'S SIGNATURE)

Permanent Address

284, Jalan Saadon,
Kampung Lintang, Petra Jaya,
93050, Kuching, Sarawak

Date: 31/07/2023

Date: 31/07/2023

Note * Thesis refers to PhD, Master, and Bachelor Degree
** For Confidential or Restricted materials, please attach relevant documents from relevant organizations / authorities

ACKNOWLEDGEMENT

Firstly, praises and thanks to God, the Almighty, for His blessings for the completion of this project. Hereby, I would like to express my special thanks of gratitude to my supervisor, Dr Chiu Po Chan for her guidance throughout this project as well as my examiner, Associate Professor Dr Johari bin Abdullah for his comment on my project. In addition, I would like to express my gratitude and a special thank you to my parents, Mr Haidir and Madam Hasmah for their support and encouragement during rough times are much appreciated. Not to forget, I would also like to thank my family members and my friends. It was a great comfort and relief to have them while completing this project. Lastly, I appreciated everyone that involved indirectly in this project and that helped me to complete my final year project.

ABSTRACT

In today's digital age, almost everyone especially college students rely on technology and the Internet. As a result, the unexpectedly rapid growth of cyber users creates the need for healthy cyber habits and awareness. This is due to the increasing number of cyber security incidents recorded. The increase in cyber security incidents shows that cyber security awareness may still be insufficient among cyber users. Some cyber security incidents occurred because of social engineering, poor password practices, and malicious mobile applications. Therefore, from these incidents and the data collected through the questionnaire, an educational app called EduSecure is proposed to assist in cyber security education and awareness among UNIMAS students. As the proposed system is a mobile application, it can be the easiest and the best way to reach cyber users. EduSecure, the educational app for cyber security will provide learning topics regarding password practices, social engineering, and mobile applications. Quiz games are also included for the user to test their understanding after completing the learning topics. EduSecure focuses on promoting gamification practices and implementing threat escape room concept in cyber security. The use of the threat escape room in cyber security increases motivation and promotes cyber security awareness learning. Therefore, the threat escape room has greater potential than a traditional learning methodology about cyber security. The usability testing reveals that EduSecure demonstrates good usability and effectively enhancing users' understanding of cyber security. The app empowers users by providing valuable insights that contribute to their improved knowledge of cyber security. Furthermore, the findings of this work also demonstrated the effectiveness of employing gamification techniques and threat escape rooms as a cyber security learning tool.

ABSTRAK

Pada zaman digitalisasi ini, hampir semua orang terutamanya pelajar kolej bergantung pada teknologi dan Internet. Akibatnya, pertumbuhan pengguna siber yang tidak dijangka pesat mewujudkan keperluan untuk tabiat dan kesedaran siber yang sihat. Ini disebabkan oleh peningkatan jumlah insiden keselamatan siber yang direkodkan. Peningkatan insiden keselamatan siber menunjukkan bahawa kesedaran keselamatan siber mungkin masih tidak mencukupi di kalangan pengguna siber. Beberapa insiden keselamatan siber berlaku kerana kejuruteraan sosial, amalan kata laluan yang lemah, dan aplikasi mudah alih yang berniat jahat. Oleh itu, dari insiden ini dan data yang dikumpulkan melalui soal selidik, aplikasi pendidikan yang dinamakan EduSecure dicadangkan untuk membantu dalam pendidikan dan kesedaran keselamatan siber di kalangan pelajar UNIMAS. Oleh kerana sistem yang dicadangkan adalah aplikasi mudah alih, ini boleh menjadi kaedah termudah dan terbaik untuk menjangkau pengguna siber. EduSecure, aplikasi pendidikan untuk keselamatan siber akan menyediakan topik pembelajaran mengenai amalan kata laluan, kejuruteraan sosial, dan aplikasi mudah alih. Permainan kuiz juga disertakan untuk pengguna menguji pemahaman mereka setelah menyelesaikan topik pembelajaran. EduSecure memberi tumpuan kepada mempromosikan amalan gamifikasi dan melaksanakan konsep bilik pelarian ancaman dalam keselamatan siber. Penggunaan ruang pelarian ancaman dalam keselamatan siber meningkatkan motivasi dan mempromosikan pembelajaran kesedaran keselamatan siber. Oleh itu, ruang pelarian ancaman mempunyai potensi yang lebih besar daripada metodologi pembelajaran tradisional mengenai keselamatan siber. Ujian kebolehgunaan menunjukkan bahawa EduSecure menunjukkan kebolehgunaan yang baik dan berkesan meningkatkan pemahaman pengguna mengenai keselamatan siber. Aplikasi ini memberi peluang kepada pengguna dengan memberikan pandangan berharga yang menyumbang kepada peningkatan pengetahuan mereka mengenai keselamatan siber.

Selain itu, penemuan kerja ini juga menunjukkan keberkesanan menggunakan teknik gamifikasi dan bilik pelarian ancaman sebagai alat pembelajaran keselamatan siber.

Table of Contents

List of Tables

List of Figures

CHAPTER 1: INTRODUCTION

1.1 Background

Cyber security awareness is a continuous process to educate cyber users on cyber threats and the practice of protecting cyberspace in the event of security incidents. Cyber security awareness involves being aware of daily online activities and situations. In this digital era, despite the Internet's importance and its educational influence among students, cyber security threats are said to be becoming increasingly complex and deteriorating regularly (O'Brien, 2014). To overcome cyber security threats, it is crucial to spread awareness among college students, as they are the digital generation. In addition, according to Jawad and Tout (2020), people have become so used to the daily use of social media that more awareness about cyber security is important to avoid people falling victim to cyber-attacks. Furthermore, with the increased usage of mobile devices, a mobile application is said to be the best way to reach cyber users.

According to The Sun Daily, cyber-crimes have shown an upward trend in Malaysia, of which 6,512 cyber security incidents were recorded in 2020. Some cybercrimes are committed through social engineering, poor password practices, and malicious mobile applications. Social engineering is one of the critical issues, as the attacker uses psychological manipulation to trick the target into making security mistakes or giving away sensitive information. There are many types of social engineering that can be covered such as baiting, phishing, and tailgating. These cyber threats are the top encountered threat in Malaysia based on Kaspersky's survey ("M'sians Encounter Most Social Engineered Scams," 2022). According to a poll created by Google, over 90% of respondents surveyed admitted to poor online habits, which include sharing, reusing, and using a guessable password ("Serious data breaches experienced amidst poor password

practices: Google", 2021). Therefore, this is a must-cover topic, especially for college students who are likely to practice this habit for their social and educational accounts. Moreover, the number of mobile applications increased with great functionality, causing people to rely on mobile devices even more, but they did not realise that because of the heavy reliance on mobile devices, attackers used this platform to attack the target. According to the New Straits Times (2022), Malaysia was ranked 10th among the top 10 countries in the world with a 27.36 per cent share of users targeted by mobile malware in 2019. In addition, Yeo Siang Tiong, Kaspersky's general manager of Southeast Asia, said that the malicious apps are masked under the guise of legitimate apps, that can be downloaded from the official app stores, so it is difficult to notice these hidden malicious apps.

As with the aforementioned issues, this project, called EduSecure, is a mobile application that assists in cyber security education and awareness among UNIMAS students with varying levels of knowledge about cyber security. It will include the cyber security issues (password, mobile app, and social engineering). Furthermore, three levels of quiz games-Level 1, Level 2, and Level 3—are designed to assess the user's understanding.

1.2 Problem Statement

Due to the growing reliance on digital technology, the need to create healthy cyber habits and cyber security awareness has become important (Garba et al., 2020). Because of the unexpectedly rapid growth in cyber users, users may be unaware of or behind on cyber threats (Peker et al., 2016). As a result, college students, who are also the biggest population in the cyber world, may be unaware of their personal information and safety risks through the use of the Internet (Garba et al., 2020). The increase in cyber security cases shows that cyber security awareness is still insufficient among cyber users.

Several studies have been conducted to assess college students' awareness of cyber security issues. A study has been conducted among academic staff, researchers, employees, and college students in the education sector in the Middle East (Al-Janabi & Al-Shourbaji, 2016). The findings indicate that participants lack the necessary knowledge and understanding of the significance of cyber security practices in their daily life. A finding also indicates that the major issue with security awareness is not a lack of security knowledge, but rather how students apply that knowledge in real-world situations (Moallem, 2019). Another study has taken part among 295 Malaysian undergraduate students regarding social networking sites (SNSs) risk awareness (Kirwan et al., 2018). According to this study, more than one-third of participants had fallen victim to SNS scams. Moallem (2019) surveyed 247 students and found that 60% of respondents were familiar with cyber security, whereas the other 40% were unaware of cyber security. Although the percentage can be regarded as favourable, the assumption that college students have greater knowledge of computers is significant. The study also found that 16% of respondents admitted to not knowing about cyber security.

College students are the future leaders and workforce. As a result, developing healthy cyber habits and increasing cyber security awareness are critical. Although the organization provides cyber security training to their employees, the majority of technology users, such as college students, only have access to the limited cyber security information available online. Therefore, the student needs to be educated on cyber security awareness.

1.3 Scope

The scope of this project is:

- The target user for this application are college students, specifically UNIMAS students.
- This application will use English language as the application language.

- This EduSecure application contains educational content and quizzes to allow UNIMAS students learn about cyber security.

1.4 Aims and Objectives

The main objectives of this project are:

1. To study and analyse existing mobile cyber security educational apps.
2. To develop a mobile cyber security educational app that enhances the security awareness of cyber users.
3. To evaluate the usability of the proposed cyber security educational app.

1.5 Significance of Project

This mobile application is significant to college students for cyber security education as college students always use technology and the Internet for education and socialising, making them a high-risk group. With this mobile application, students can learn through real-life situations and the information and quizzes provided. Moreover, they can always refer to this mobile application instead of looking it up online, as it can be overwhelming with many sources to be referred to, and this can save their time. The topics covered in this mobile application will help them be aware of and practice healthy cyber habits to avoid any possible cyber threat. As a result, this mobile application can help and guide students on cyber security.

1.6 Project Schedule

Figure 1.1 shows the project schedule for Final Year Project 1 and Final Year Project 2, and Figure 1.2 is the Gantt Chart.

Task Name	Start Date	End Date	Duration
Prepare Brief Project Description	21/10/2022	24/10/2022	3
Submit Brief Project Description to Supervisor	25/10/2022	25/10/2022	0
Feedback from Supervisor	25/10/2022	25/10/2022	0
Brief Project Description Amendment	25/10/2022	27/10/2022	2
Submit Brief Project Description to FYP System	28/10/2022	28/10/2022	0
Prepare Full Proposal	08/11/2022	14/11/2022	6
Submit Full Proposal	14/11/2022	14/11/2022	0
Chapter 1: Introduction	15/11/2022	21/11/2022	6
Chapter 2: Background/Literature Review/State of Art	22/11/2022	09/12/2022	17
Chapter 3: Methodology/Requirement Analysis and Design	12/12/2022	30/12/2022	18
Submit FYP1 Final Report and Paper for Assessment	12/01/2023	12/01/2023	0
FYP Amendment and Modification	17/01/2023	10/02/2023	24
Submit Final FYP1 Report	10/02/2023	19/02/2023	9
Submission of proposed structure of FYP report, Title and gantt chart	05/04/2023	07/04/2023	2
Prototype	01/04/2023	30/04/2023	29
Testing (Functional and Usability Testing)	01/05/2023	15/05/2023	14
Submission of First Draft for Chapter 4	30/04/2023	15/05/2023	15
Submission of First Draft for Chapter 5,6 & Abstract for Paper	16/05/2023	29/05/2023	13
Submission of First Draft for FYP 2 Full Report and Paper	10/06/2023	10/06/2023	0
Submission of Final Report, source code, installation kits, user manual and Paper for Assessment	24/06/2023	01/07/2023	7
Submission of Pre-recorded Video and Presentation Slides	01/07/2023	03/07/2023	2
Submission of Final Report	30/07/2023	30/07/2023	0

Figure 1.1 Project Schedule Table

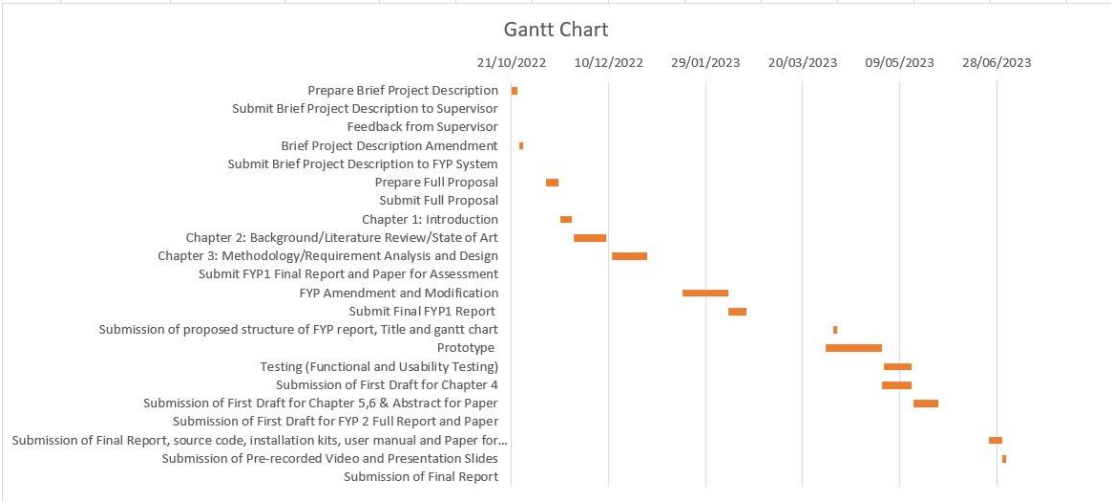

Figure 1.2 Gantt Chart

1.7 Expected Outcome

This mobile app is expected to assist in educating and raising awareness among UNIMAS students with varying levels of knowledge about cyber security. They are expected to learn and practice healthy cyber habits in their daily online activities and be able to overcome the situation if they are ever at risk of a cyberattack. There will be a quiz game for the user to test their knowledge after reading the topic provided.

1.8 Project Report Outline

Chapter 1: Introduction

The project title, background, problem statement, scope, aims and objectives, a brief methodology, the significance of the project, the project schedule, and the expected outcome were all included in this chapter to provide a complete picture of the project. The background section discussed the project's objective, scope, and literature review. The problem statement defined the issues that arise that make this project possible. The limitations of the project were defined in the scope, with aims and objectives defining the goal that this project must achieve. Following that, a brief methodology explained the methodology used to develop and launch this entire project. In the project schedule section, a Gantt chart and project schedule table listed the activities to be followed and to ensure the project followed the timeline for smooth progress. Lastly, the expected outcome is the expected result of the project.

Chapter 2: Background/Literature Review/State of Art

This chapter focused on the literature review of existing mobile applications with cyber security topics that are similar and related to this project. There will be four existing mobile applications that serve a similar purpose as the proposed project will be reviewed and compared to be reflected on the proposed project.

Chapter 3: Methodology/Requirement Analysis and Design

This chapter discussed the requirement planning and prototype phase of the Rapid Application Development (RAD) methodology in more detail. Requirement planning will include the user requirements based on data that will be collected through a questionnaire. In addition, project objectives, and scope along with hardware and software requirements are also included during this phase. However, the prototype cycle will include a logical design where Unified Modeling Language (UML) is used which includes Use Case diagrams with their descriptions, Sequence

diagram, Activity diagram and lastly, Class diagram. The physical design which is the User Interface design is also included.

Chapter 4: Implementation

This chapter emphasised the implementation phases of the proposed application. The implementation phase involves turning the design and specifications into a functional application. It includes coding and refining the app's features to ensure it meets the intended requirements and delivers a seamless user experience.

Chapter 5: Testing

This chapter emphasised the testing phases of the proposed application. The testing phase ensures its usability and follows all the requirements and objectives.

Chapter 6: Conclusion and Future Works

This chapter describes the conclusion of the project after every phase is completed. In addition, this chapter will go over potential future work that could be done to enhance the application.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

The purpose of this chapter is to review and compare the features of the existing mobile applications that have a similar purpose to the proposed project. Reviewing and comparing these apps can reflect the features that will be implemented in the proposed project. There will also be a summary of the chapter and its findings at the end of this chapter.

In this chapter, four existing mobile applications will be reviewed and compared. These four existing apps aim to educate users about cyber security. They are the Cyber Security App (2017), Learn Computer Security (2021), Learn Cyber Security (2022), and Ethical Hacking University App (2022). The Cyber Security App is an informational app that helps people understand the importance of cyber security by providing knowledge of cyber security and its importance, various types of cybercrime, and ways to prevent becoming a victim of cybercrime. Correspondingly, Learn Computer Security provides knowledge on the practice of protecting systems, networks, and programs from digital attacks. Meanwhile, Learn Cyber Security provides lessons for beginners to enhance their understanding and skills in cyber security. Lastly, Ethical Hacking University App enlightens the user with the knowledge of basics and advanced skills of Cyber Security and Hacking.

2.1.1 Learning Cyber Security Through Mobile Applications

According to Sakshi Gupta (2020), approximately 50% of internet traffic comes from mobile devices, which is probably a factor in the increase in mobile app downloads; meanwhile, desktop and laptop usage continue to decline. A study by Nitin Deshdeep (2022, April 28) states that users prefer mobile apps more than mobile websites. The statement may be a solid reason for the author to create mobile apps that can reach out to potential users. Furthermore, a well-designed mobile app performs faster than a mobile website. In contrast to websites, which

typically use web servers, apps typically store their data locally on mobile devices. Although relatively mobile learning is a new phenomenon, it has numerous benefits for high-quality education and the learning process (Kearney et al., 2012). Qureshi et al. (2020) conducted a study regarding learning through mobile applications and found them effective. Users can learn at their own pace as mobile applications allow users to access information instantly, regardless of location. Users are also able to use the apps according to their needs and share their ideas and views with other users about the applications. The proliferation of educational mobile apps and technological advancements provide opportunities for users to gain new skills. Recent days have seen a tremendous increase in the development of smartphones, which is directly related to the daily release of new applications for various devices as well as the field of cyber security. In light of this, the author has decided to implement an educational mobile application for cyber security.

2.1.2 Gamification Element in Educational Apps

According to Mindy Jackson (2016), gamification is the application of game-playing elements to another type of activity. Since it gained popularity in the early 2010s, gamification—the design strategy of utilising gameful design in various contexts for inducing familiar experiences with games to support different activities and behaviours—has remained a hot topic in both industry and academia (Huotari & Hamari, 2017). According to Landers (2014), game-based learning, serious games, edugames, and more recently, gamification are some of the terms used to describe the long history and variety of ways that gameful interactions can be incorporated into educational contexts. Gamification in education is a technique that incorporates game design dynamics into the educational environment to engage students and has direct interactions with them, helping them to significantly improve their academic, cognitive, and social skills (Manzano-León et al., 2021). According to Alsawaier (2018), gamification utilises strategies to get people interested, spur them to action, and encourage learning and problem-solving.

Some examples of gamification elements are points, timers, badges, and leaderboards. Gamification in learning activities is believed to boost learner motivation, engagement, and enjoyment. Therefore, gamification has been addressed and applied in the education field, where sustaining and maintaining user engagement is a continuous challenge. The implementation of gamification elements in educational applications allows users to engage with the apps as well as be motivated to complete all the courses and quizzes available. The author hopes that the implementation of gamification elements in the proposed mobile application will help the user be engaged with the content and motivated to learn cyber security.

2.2 Review on Similar Existing System

Four existing apps will be reviewed and explained in this section.

2.2.1 Cyber Security App

An educational app, the Cyber Security App seeks to make users aware of the significance of cyber security. The developer launched this app to sensitise people to cybercrimes such as hacking, and identity theft has become more common. The apps include knowledge of cyber security and its importance, the various types of cybercrimes, how to prevent them, and what to do if the user becomes a victim of cybercrime. The developer has updated the app with tips on how to remain safe on social platforms like Facebook, WhatsApp, and online shopping. A forum has also been added for users to talk about their problems with cyber experts. This app also includes a quiz to test the user's knowledge. Given that a link to the quiz is already provided, users are free to take it whenever they want, either before or after reading all the content. The user has the option of testing their understanding before or after the content is finished. Figure 2.2 shows the list of contents available in the app and the link to the forum page and the quiz. This app includes the topic of Cyber Security, Cyber Crimes, Types of Cyber Crimes, Protection from Cyber Crime, if you become a victim..., Facebook Tips, WhatsApp Tips and Online