

## Malaysia Cyber Fraud Prevention Application: Features and Functions

### Aplikasi Pencegahan Penipuan Siber Malaysia: Ciri-Ciri dan Fungsi

Looi Xue Ying<sup>1</sup>, Azana Hafizah Mohd Aman<sup>1\*</sup>, Mohamad Sirajuddin Jalil<sup>2</sup>, Taha Mohd Omar<sup>3</sup>, Zainab S. Attarbashi<sup>4</sup>, Mustafa Ali Abuzaraida<sup>5</sup>

<sup>1</sup>Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia,

<sup>2</sup>Malaysia Cyber Consumer Association, Petaling Jaya, Selangor, Malaysia

<sup>3</sup>CODAM Protocol Sdn. Bhd., Kuala Lumpur, Malaysia

<sup>4</sup>Faculty of Information and Communication Technology,  
International Islamic University Malaysia, Gombak, Selangor, Malaysia

<sup>5</sup>Computer Science Department, Faculty of Information Technology,  
Misurata University, Libya

\*Corresponding author: [azana@ukm.edu.my](mailto:azana@ukm.edu.my)

Received 15 September 2023

Accepted 2 November 2023, Available online 1 December 2023

#### ABSTRACT

The advent of technological advancements in the era of globalization has given significant advantages upon developing nations. However, it has also led to certain drawbacks, notably the increase of cybercrimes such as Internet fraud (commonly known as scams). Among the contributing factors to this issue in Malaysia are the low level of public awareness and knowledge regarding cyber fraud prevention and Malaysia's cyber laws. Hence it is crucial to have a medium that can spread the knowledge and at the same time increase the awareness. To support this, an app is developed, named as National Fraud Prevention Centre (NFPC) application. The NFPC application used methods across diverse platforms, including laptops, smartphones, and tablets, using software such as Android Studio and Firebase. In addition, the Agile Methodology is adopted for the app's development, as it facilitates rapid adaptation to changes, fosters customer involvement, and prioritizes the delivery of high-quality software within tight timeframes. The primary objective of the application is to enhance public awareness regarding various forms of fraudulent activities. Users of the application are also provided with detailed information about the modus operandi of the scam, the types of fraud, and the preventive actions to be taken. With a broader knowledge of these crimes, the public will be able to recognize the early signs of fraud and avoid becoming a victim. Furthermore, the application will serve as a user-friendly reporting channel for individuals encountering suspicious or fraudulent activities. This streamlined reporting process will enable swift intervention by authorities, reducing the incidence of fraud and safeguarding the community against unnecessary financial losses.

**Keywords:** Cyber fraud awareness, cyber fraud prevention, cyber security

## ABSTRAK

Kemunculan kemajuan teknologi dalam era globalisasi memberikan kelebihan yang signifikan kepada negara-negara membangun. Walau bagaimanapun, ia juga telah menyebabkan beberapa kelemahan, terutamanya peningkatan jenayah siber seperti penipuan Internet (biasanya dikenali sebagai scam). Antara faktor penyumbang kepada isu ini di Malaysia adalah tahap kesedaran dan pengetahuan am yang rendah mengenai pencegahan penipuan siber dan undang-undang siber Malaysia. Oleh itu, adalah penting untuk mempunyai medium yang boleh memberikan pengetahuan dan pada masa yang sama meningkatkan kesedaran. Bagi menyokong perkara ini, sebuah aplikasi telah dibangunkan, dikenali sebagai National Fraud Prevention Centre (NFPC). Aplikasi NFPC menyediakan kaedah penggunaan pelbagai platform termasuk laptop, telefon pintar, dan tablet, berdasarkan perisian seperti Android Studio dan Firebase. Selain itu, Metodologi Agile digunapakai untuk pembangunan aplikasi ini, kerana ia merangkumi penyesuaian efisien kepada perubahan, menggalakkan penyertaan pengguna, dan memberi keutamaan kepada penyampaian perisian berkualiti tinggi dalam jangka masa yang ditentukan. Objektif utama aplikasi ini adalah untuk meningkatkan kesedaran awam mengenai pelbagai bentuk aktiviti penipuan. Pengguna aplikasi juga diberikan maklumat terperinci tentang modus operandi penipuan, jenis-jenis penipuan, dan tindakan pencegahan yang perlu diambil. Dengan pengetahuan yang lebih luas tentang jenayah ini, orang awam akan dapat mengenali tanda-tanda awal penipuan dan mengelakkan menjadi mangsa. Selain itu, aplikasi ini berfungsi sebagai saluran pelaporan yang mesra pengguna bagi individu yang terkesan dengan aktiviti yang mencurigakan atau penipuan. Proses pelaporan yang efisien ini akan membolehkan campur tangan pantas pihak berkuasa, mengurangkan insiden penipuan dan melindungi masyarakat daripada kerugian kewangan.

**Kata Kunci:** Kesedaran penipuan siber, pencegahan penipuan siber, keselamatan siber

## INTRODUCTION

In the current age of globalization, internet fraud is more frequent and costs victims' various losses (Monica 2018; Chen et al. 2021; Kemp et al. 2022; Chhabra et al. 2023). Internet scams are becoming increasingly common in Malaysia, with various modus operandi, where victims have lost thousands or millions (Aida 2023; Alisha 2021). Older adults are also the target of many scams since they are more susceptible to them and less technologically literate (Alexander 2022). Cyber-hackers are now targeting not only professional groups, the vulnerable, and older adults but also teens (Sinar Harian 2021; Smita 2022). The general public should, therefore, be aware of the most recent cybercrime trend containing "Scam" elements or scams that can result in victim losses of tens of thousands of ringgits (Astro Awani 2020).

The lack of awareness of fraud prevention and lack of knowledge about Malaysia's cyber laws are problems that need to be overcome (MCMC 2023; Majlis Keselamatan Negara 2023). Hence, it is necessary to raise public awareness of the modus operandi of fraud and the importance of cyber laws to protect against cybercrime (Lau 2020; Mohd 2022). Almost every day, cases of Internet fraud involving the general public are featured in newspapers and television shows (Berita Harian 2022; mStar 2022). Cybercrime statistics show a high percentage of instances, particularly in the fraud category, which is on the rise. 4,207 incidences of online fraud have been reported in Malaysia as of October 2022, according to information from the Malaysia Computer Emergency Response Team (MyCert) website for CyberSecurity Malaysia (CyberSecurity Malaysia 2022). Statistics show that more and more Malaysians are becoming victims of online fraud (Nurul 2019; Bernama 2020; Kumara 2022).

Therefore, in line with the government's efforts to tackle and prevent telecommunication network fraud, the paper aims to develop features for a fraud prevention mobile application for the community called the National Fraud Prevention Centre (NFPC).

This fraud prevention application aims to make the public aware of being victims and continuously falling for online scammers. Its goals include spreading awareness of cyber laws, educating people about the most recent fraud techniques, and evaluating public approval of these applications. Additionally, the application acts as a fraud technology where users are urged to report any questionable content, bank accounts, or phone numbers in order to assist law enforcement in preventing crime before it happens. Through the application, users may also verify the phone numbers or bank accounts of anyone who may be involved in similar scams. More than that, this mobile application also provides news-reading function, quizzes for testing knowledge, and forums for uploading images and texts through forums. The Malaysian public is also given early exposure and information of the "Scammer" criminal cases so they can learn about the most recent fraud techniques. Through the use of this comprehensive fraud protection program, the government can make sure that everyone is informed of how to protect themselves from falling victim to the increasingly aggressive scammers and always using their fraud methods. The learning process in this application makes use of information from resources, including the Check Mule app, the CCID Portal by PDRM, and an important Malaysian news network.

The structure of this article starts with the introduction followed by the highlights on the existing related applications. The next section is the methodology of the application development, followed by the determinant of the selected features and functions. The later section introduces the features of the NFPC, and the final section is the conclusion of the article.

#### LITERATURE ON EXISTING APPLICATIONS

This article compares three existing applications, Check Scammers CCID (Royal Malaysia Police 2021), Fraud Magazine (ACFE 2019; Google Play Store), and Fraudster (App Store), to develop fraud prevention mobile applications among the Malaysian community. These existing applications differ in features and functions. Check Scammers CCID is a system that allows people to check suspicious bank accounts and phone numbers through public portals on their website. Fraud Magazine developed by the Association of Certified Fraud Examiners (ACFE) provides information about fraud and fraudulent exam techniques. Ninja Alert (Google Play Store) application allows users to report fraud online and includes evidence to help law enforcement agencies catch cybercriminals.

Check Scammers CCID is an application developed in Malaysia. It provides a platform for reporting fraud and tracking call numbers or even reported accounts that the other two apps do not have. Through this system, the user will know that either the call number or the given bank account number has ever been used in criminal fraud operations in Malaysia. Additionally, the Fraud Magazine and Fraudster apps are more focused on education on fraud issues. Both apps provide knowledge of current scams and steps to protect themselves from becoming a victim of fraud. The purpose of the application is to raise public awareness due to the fact that the community is still in negligence and lacks of knowledge of online fraud, which leads to an increase in criminal cases.

In comparison to past studies, the NFPC offers several advantages. NFPC is a more thorough and relevant cyber fraud prevention app, with a focus on Malaysian society. The app offers a variety of useful functions, including reporting scams, checking scams, reading news, testing

knowledge through quizzes, and uploading photos and text through forums. In addition, NFPC offers elements of learning tips to boost users' confidence and morale in the face of cybercrime and cyber fraud. Moreover, NFPC offers more comprehensive functionalities to fulfill the needs and preferences of the Malaysian people, in comparison to existing apps that have been investigated, which only offer a limited number of specific functions. The app also places a strong emphasis on user interaction and the sharing of in-depth knowledge regarding online fraud and cybercrime. Therefore, it is anticipated that NFPC applications will be a successful instrument for increasing public awareness and shielding them against online fraud. Table 1 shows the application criteria comparison, including the NFPC.

TABLE 1. Applications Criteria Comparison

Criteria	Application			
	Check Scammers CCID	Fraud Magazine	Fraudster	NFPC
Platform	Android	Android & iOS	Android & iOS	Android
Version	1.1.5	2.2	1.0	1.0
Fee	Free	Free	Free	Free
Language	Malay	English	English	English
Size (approx.)	2MB	47MB	18MB	5MB
GUI	Not user friendly & less attractive	Not user friendly & attractive	Not user friendly & less attractive	User friendly & attractive
Fraud Reporting Feature	Yes	No	No	Yes
Fraud Detection Feature	Yes	No	No	Yes
Recent Fraud News Feature	No	Yes	Yes	Yes
Fraud Mitigation Awareness	No	Yes	Yes	Yes
Educate Users on Type of Fraud	Yes	No	No	Yes

In conclusion, the existing fraud prevention applications in Malaysia are less robust and not comprehensive in curbing and controlling the spread of online fraud cases. Not only that, there are also many applications whose functions are similar and focused on one functionality. In addition, lack of knowledge on the issue of fraud and low level of awareness are also issues that need to be addressed as public awareness is essential to protect oneself and family (Nurul 2022). As Internet users, we need to be smarter and more aware of every offering, link and any transaction we want to make (Nurulatiq 2019). Therefore, the crime of online fraud can be controlled and curbed by the enforcement authorities more effectively in collaboration with the Malaysian community (Salleh 2020; TheStar 2021).

## METHODOLOGY

The selection and development of the appropriate features involves the Agile methodology, as shown in Fig. 1. The Agile methodology was used since it allows customization according to the needs of the user with a short development cycle. Basically, there are five standard Agile

phases, namely, planning, analysis, design, development, and testing. Each brief cycle ends with users' comments, allowing the application to be improved and changed. Additionally, the agile methodology allows users direct input in the application development process and decreases risks with repeated development cycles.

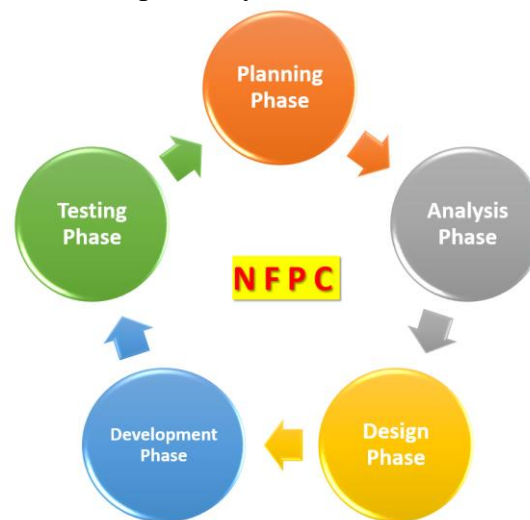


FIGURE 1. Methodology cycles

The Planning Phase is important in the development of the Fraud Prevention Mobile Application among the Malaysian community. Studies are conducted to identify the scope and solution of the problems discussed. The title, objectives, scope, and method of application development are also determined in this phase. It is basically to make sure that the developed application is more comprehensive and effective. The background of the problem is studied, and existing applications are also compared to understand the needs of the system.

The analysis phase is important to evaluate the development needs of NFPC applications and identify the weaknesses of existing applications. Studies are made on existing mobile applications to compare the pros and cons as well as select the appropriate functionality for NFPC applications. The purpose of this study is to develop applications that meet the needs of consumers and consider the popularity of Android as a widely used smartphone operating system. In addition, minimum requirements for the user's smartphone operating system are also set and usage specifications for each function were discussed.

In the design phase, NFPC applications is highlighted in detail, especially on the specifications and features required (MySQA 2022), including screen layout, system flow (John 2023), and how to use it. Data and analysis from the previous phase are used as a reference to build on the initial design of NFPC applications by focusing on ease of use. The initial design of the application used the High-Fidelity model for testing and user feedback to improve application usability. This High-Fidelity model carried an application interface that is very similar to a real representative. Android Studio software is used to develop the system interface and database, while the application interface is built using the Figma application. A review is conducted to get feedback from users to ensure the app interface is easy to understand and user-friendly.

The development phase involved the use of mobile application development software, namely the Android Studio and Firebase. The construction of the application functions involves coding and the user interface followed the pre-built design. The app is developed on Firebase as a database to add features, reach more users, generate revenue, and analyze app usage. Users can

create reviews, reports, and view cyber fraud prevention content. The programming languages used are Java and Kotlin in the development of this application.

The Test and Assessment phase is the last phase before the application is handed over to the customer. In this phase, the application features are tested according to the specified requirements (Jerry 2022). This phase aimed to detect any defects that may exist in the application features and ensure the application works as planned. The NFPC test involved 30 randomly selected adolescents aged from 17 years to 40 years. They tested the functionality of the application and provided feedback on the design and functionality of the application. Tests are also carried out to ensure there are no problems or errors during use. The feedback collected is used to improve and enhance the NFPC application as needed. Cronbach's Alpha statistical analysis method is also used to measure data reliability. This method of analysis is used to measure the effectiveness of the features.

#### DETERMINATION OF THE PRIMACY OF CRITERIA AND FEATURES

A survey of questionnaires has been conducted to obtain and understand the current features and function necessities (Jacqueline et al. 2018; Cassandra 2019; Abroshan et al. 2021; Elles 2021; Foring-IT 2022). This survey is also carried out to study the level of awareness and public knowledge on the issue of cyber fraud (Muhammad et al. 2019). This survey gets responses from 60 random individuals who responded through Google Forms online. In addition, the results obtained were also analyzed after obtaining respondents who no more. The Prevention Mobile Application Usage questionnaire and result is shown in Table 2.

TABLE 2. Questionnaire percentage

No.	Question	Percentage % (Agree)
Q1	Do you know the meaning of cyber fraud or online fraud?	75
Q2	Are you aware that online scams are on the rise since lately?	91.7
Q3	Do you know the level of awareness of online fraud prevention in Malaysia is very low?	93.3
Q4	Do the Malaysian society need education about the online fraud?	98.3
Q5	Do you know the cause of a person being deceived in online fraud?	68.3
Q6	Are you aware of the main reason a person is deceived but does not call the police?	70
Q7	Do you know what to do after suffering a loss from a online scam?	50
Q8	If you are offered a certain amount of money by a party as payment for the use of your identification for the opening of the party's bank account, do you agree?	63.3
Q9	If a friend recommends an online investment with a low credit but highly profitable, will you invest?	8.3
Q10	Have you receive any fraud prevention publicity through any channels?	81
Q11	Do you think the level of anti-fraud publicity methods in Malaysia is low?	63.3
Q12	Do you think application method should be used for anti-fraud publicity to be more awareness effective in the future?	80
Q13	If there is a comprehensive cyber fraud prevention application and focus on the Malaysian community, will you introduce it to your friends?	100

Of the 60 respondents, 36.7% of the 22 were citizens male, and 63.3% of 38 are female citizens. Table 3.1 shows the gender demographics of respondents based on the results of a survey involving 60 Malaysian. In addition, respondents aged 18 – 30 years showed the highest percentage of 56.7% compared to others. Next, 25 percent of respondents were aged 31 – 40. The under-18s and those aged 41 – 60 recorded 6.7%, which is 4 each. Meanwhile, those aged 60 and above showed the lowest percentage compared to the others. Table 3.2 shows the age demographic of respondents based on the results of the survey involving 60 Malaysian citizens. In addition, 6 respondents obtained a certificate of either Sijil Pelajaran Malaysia (SPM) or Sijil Tinggi Persekolahan Malaysia (STPM) while only 11 respondents received diplomas. Then, the number of respondents who received a Master's or Doctor of Philosophy degree was the lowest with 3.3% and 2 people only. From the survey results, a total of 61.7% of the 37 respondents at the bachelor's degree level recorded the highest number. Table 3.4 shows the demographics of the highest level of education achieved by respondents based on the results of the survey involving 60 Malaysian citizens.

TABLE 3. Age Record

Age (years)	Quantity	Percentage (%)
Under 18	4	6.7
18 - 30	34	56.7
31 - 40	15	25
41 - 60	4	6.7
60 and above	3	5

TABLE 4. Employment Record

Employment	Quantity	Percentage (%)
Government	8	13.3
Servant		
Private	15	25
Students	32	53.3
Miscellaneous	5	8.3

TABLE 5. Education Level Record

Education level	Quantity	Percentage (%)
Diploma and below	17	28.3
Degree	37	61.7
Master and above	2	3.3
Miscellaneous	4	6.7

## RESULTS: APPLICATION FEATURES

The application features is finally carried out based on predetermined complete Agile phases, requirements and design. Some features provided by Google Firebase are also used such as Firebase Authentication, and Storage. To facilitate user log-in, Google Sign-In is also used. The results of the study are discussed based on the identified features and functions, as follows:

1. **User Registration and Login feature:** In this application, user authentication is carried out through two methods, namely using an email account and password, as well as through Google Sign-In. Users who wish to register will need to fill in personal information, such as username, email address, phone number and password. After successfully registered, they can use that email address and password to log into the app. Once the user successfully logs in, each user will be assigned a unique User ID known as UID. This UID will be used to identify each user in the application and facilitate the management of user information in the system. Also, the app can manage situations when a user forgets his password. Users can press the forget password link to recover their password via email. The app also works to check the email address and password fields to make sure they meet the required requirements before implementing the login process. If there are any errors in the field, an error message will be displayed, and the login will not be executed. The interface for this feature is shown in Fig. 2 and Figure 3.

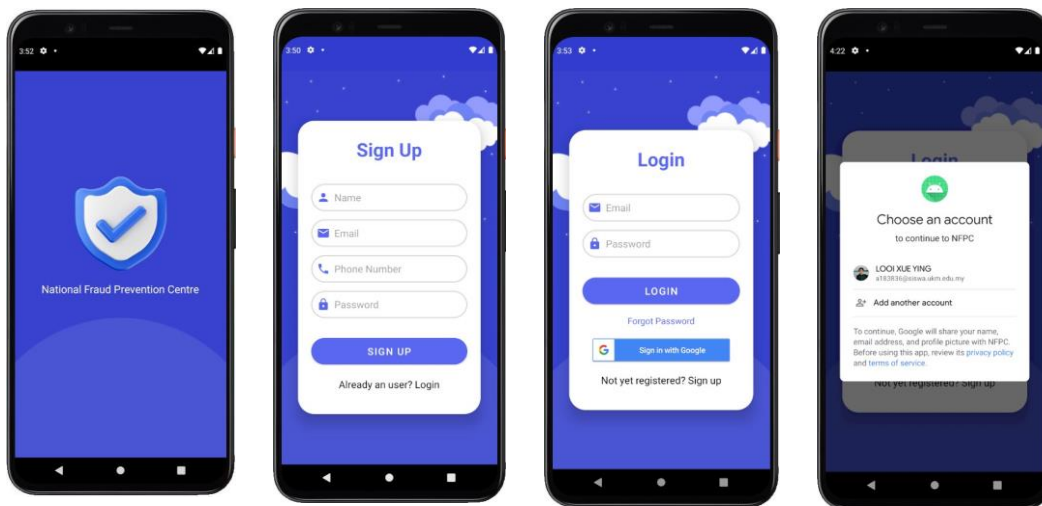


FIGURE 2. User Registration and Login Interface

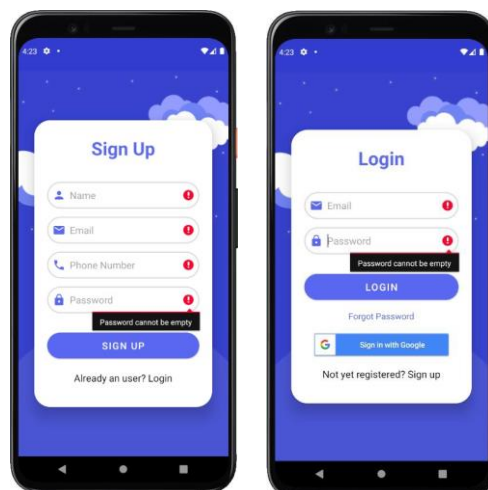


FIGURE 3. User Input Verification Interface



2. Home Screen Display feature: To provide a more seamless and enjoyable user experience, the development of a home screen display for cybersecurity education applications aims to produce an intuitive, practical, and user-friendly user interface. The "NFPC" home screen display has the following options: "Home," "News," "Help," and "Profile.". The interface for this feature is shown in Figure 4.

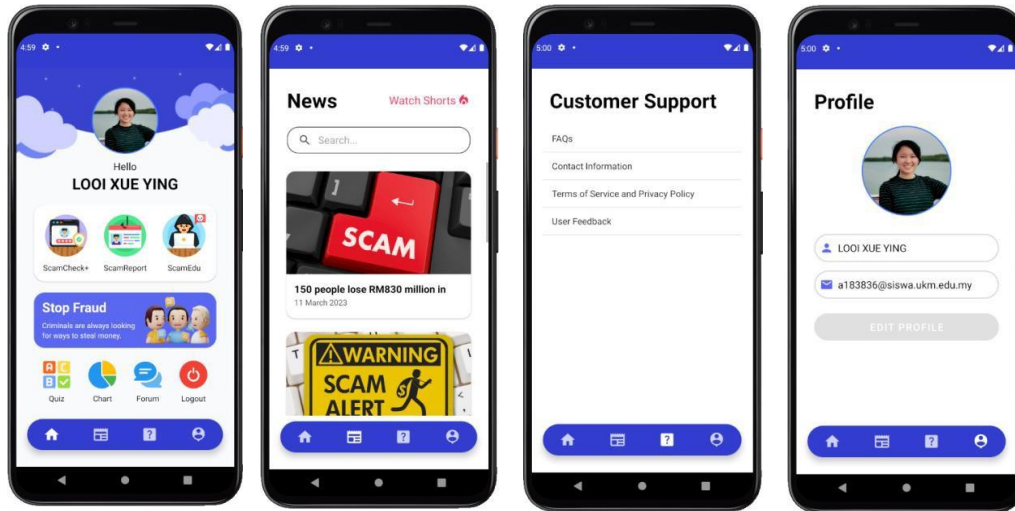


FIGURE 4. Home Screen Interface and Navigation Activities Interface

3. Function of Checking Online Fraud feature: The function of checking fraud is aimed at checking the information of users with a database of scammers. Scammer data is stored on Firebase. This function compares user information with a list of scammers for match. If there is a match, the user will be warned about scammers and preventive measures. The interface for this feature is shown in Figure 5.

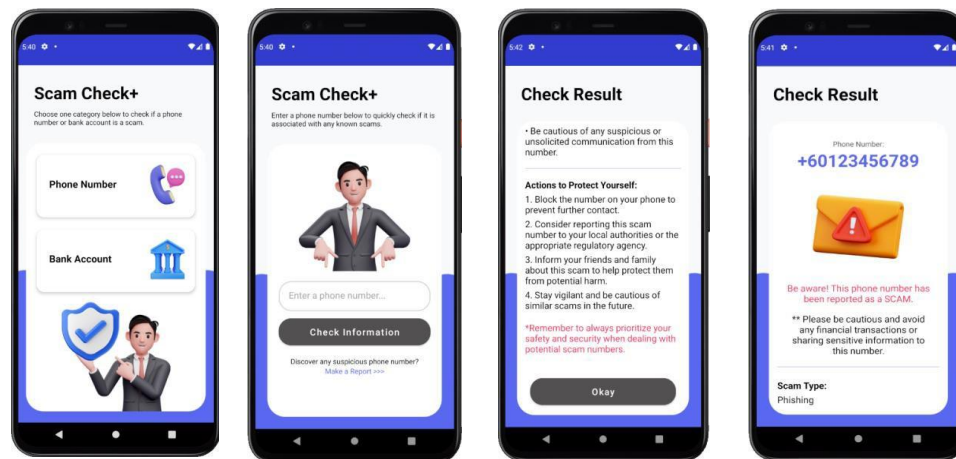


FIGURE 5. Interface of Checking Phone Numbers and Bank Accounts

4. Function of Accessing Cyber Fraud Information feature: The Fraud Information Access function helps users understand the different types of fraud and related laws. Each type of fraud will be accompanied by descriptions, common examples, prevention tips, steps to take if you are a victim and related YouTube videos. The legal part provides a brief description of the relevant legal aspects, provides an opportunity to gain in-depth knowledge of fraud and legal protection from it. The interface for this feature is shown in Figure 6.

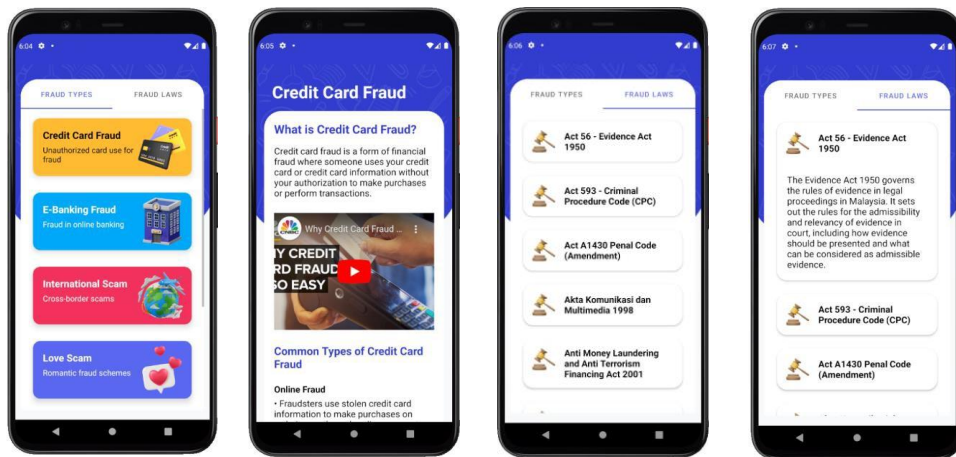


FIGURE 6. Interface Accessing Fraud Information

5. Cyber Fraud Quiz feature: The purpose of the scam quiz is to test users' familiarity with different frauds and available defenses. Users will be given options for answers when they take this quiz. By clicking the given answer button for each question, the user can choose one of the preferred answers. The interface for this feature is shown in Figure 7.

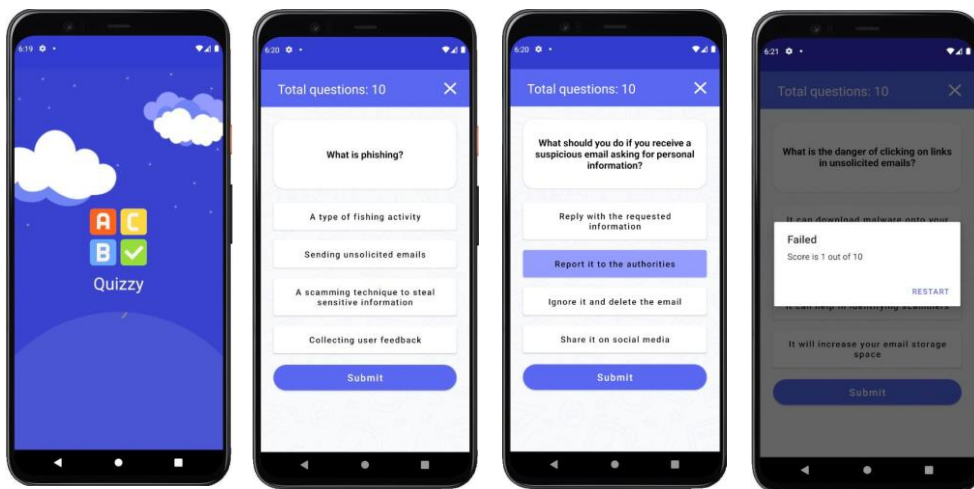


FIGURE 7. Fraud Quiz Interface

6. Function of Accessing Cyber Fraud Charts feature: The development of functions to access charts involves processing data and visual display of data in the form of graphs or charts. This function helps present data in an understandable and interactive manner to users. The interface for this feature is shown in Figure 8.



FIGURE 8. Interface Accessing Fraud Charts

7. News Surfing feature: News about cyber fraud plays an important role in raising awareness. This feature provides up-to-date information, preventing fraud and assisting authorities in tackling and countering cyber fraud activities. With access to provided link of the latest news related to cyber fraud, people can play an active role in protecting themselves and their communities from growing cyber threats. The interface for this feature is shown in Figure 9.

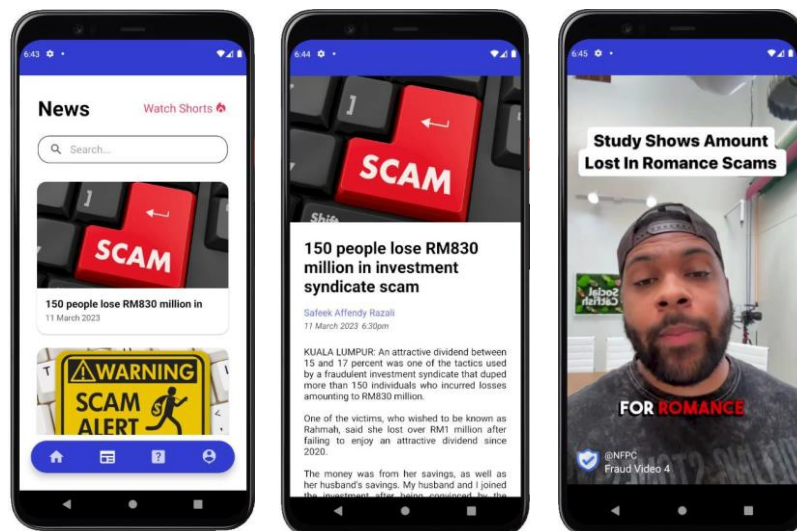


FIGURE 9. News Surfing Interface

8. Forum Browsing feature: The browsing forums promotes the interaction and sharing of information related to fraud between users of the application. This function allows users to access to the provided forums (existing social media forums) and view content that has been shared by other users. The interface for this feature is shown in Figure 10.

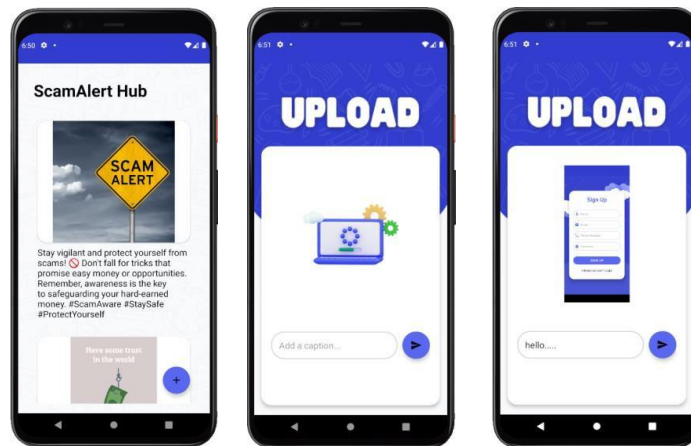


FIGURE 10. Forum Surfing Interface

9. **User Help feature:** The functionality of in-app User Assistance includes FAQs, Contact Us, Terms of Service and Privacy Policy, and User Feedback. FAQs help find answers, Contact Us interacts with support, Terms of Service and Privacy Policy explain the terms and privacy, and User Feedback responds and reports problems. The interface for this feature is shown in Figure 11.

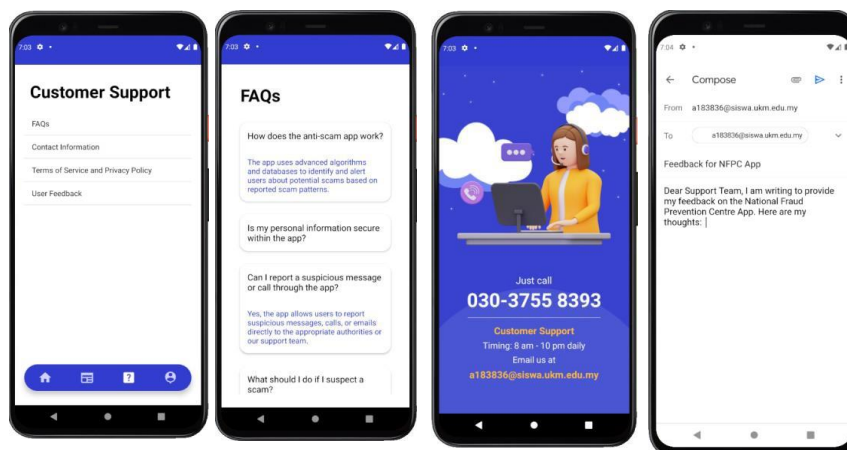


FIGURE 11. User Assistance Function Interface

10. **Browsing and Updating Profile feature:** The Profile Navigation and Update function allows users to access and manage their profiles within the app. Users can view their profile information, such as name, email address, phone number and profile picture. In addition, users can also update their profile data, such as changing their profile photo, changing their name, or updating their phone number. The interface for this feature is shown in Figure 12.

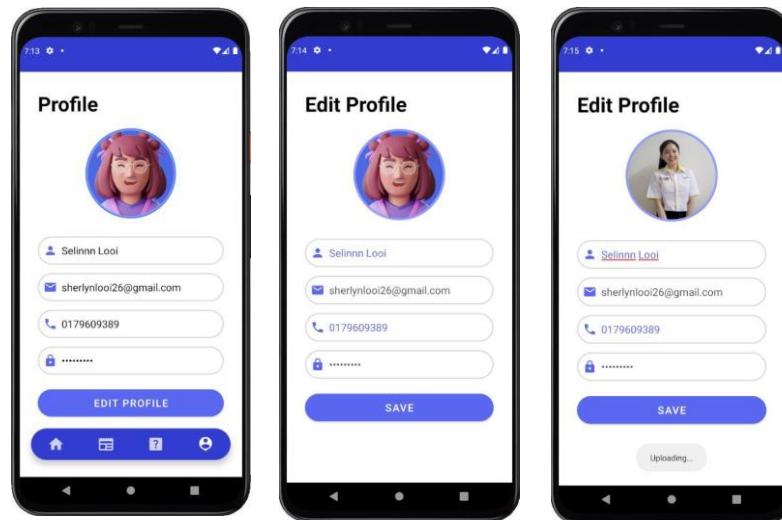


FIGURE 12. Interface Browsing and Updating Profiles

The results of this study have significant implications for the field of fraud prevention and cyber security. The development of the National Fraud Prevention Centre (NFPC) mobile app will increase public awareness of the modus operandi of fraud and cyber laws, as well as provide an easy reporting channel for enforcement actions. This will help reduce the number of victims and financial losses due to online fraud, as well as contribute to the development of cyber security technology in Malaysia.

## CONCLUSION

In conclusion, the fraud prevention mobile application features in this article promise great potential to increase awareness and prevention of fraud among the Malaysian community. By providing detailed information on the modus operandi of fraud and the preventive measures to take, the app can help people recognize the first signs of fraud and protect themselves from becoming victims. In addition, the app also offers additional functions such as reading news, knowledge quizzes, and forums for users to interact with. With the implementation of the Agile method, this application can be continuously updated and adapted to the needs of society and current cyber laws. This application is expected to be an important channel in efforts to overcome the issue of cyber fraud and increase public awareness and understanding of cyber laws in Malaysia. Future research for NFPC applications can consist of evaluations of the efficiency of preventive measures, sustainability studies, awareness measurements that included application use, interface optimization for user comfort, and application impact studies on community awareness. and application maintenance to ensure that the application remains relevant and effective.

## ACKNOWLEDGEMENT

This research is supported by Malaysia Cyber Consumer Association (MCCA) and Codam Protocol Sdn. Bhd. (CODAM) under research grant TT-2022-005.

## REFERENCE

- Abroshan J. Devos G. Poels and E. Laermans. 2021. Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process, *IEEE Access*, vol. 9, pp. 44928-44949, 2021, doi: 10.1109/ACCESS.2021.3066383.
- Aida Aziz. 2023. Macau Scam: Warga emas kerugian RM140,000 diperdaya ‘Puan Rohani’. *Astro Awani*, 17 Januari. <https://www.astroawani.com/berita-malaysia/macau-scam-warga-emas-kerugian-rm140000-diperdaya-puan-rohani-402352> [19 April 2023]
- Alexander. 2022. Penipuan dalam talian catat aduan tertinggi KPDNHEP. *Berita Harian*, 4 Ogos. <https://www.bharian.com.my/berita/nasional/2022/08/984189/penipuan-dalam-talian-catat-aduan-tertinggi-kpdnhep-alexander> [6 November 2022]
- Alisha Natasha. 2021. Tiga ditipu skim pelaburan Gold Hub International.com. *Journal Malaysia*, 1 November. <https://www.journalmalaysia.com/2021/10/01/tiga-ditipu-skim-pelaburan-gold-hub-international-com/> [29 November 2022]
- Astro Awani. 2022. Masyarakat perlu waspada trend terkini jenayah siber – Polis. *Astro Awani*, 24 Januari. <https://www.astroawani.com/berita-malaysia/masyarakat-perlu-waspada-trend-terkini-jenayah-siber-polis-343268> [9 November 2022]
- Association of Certified Fraud Examiners. 2019. *Fraud Magazine (ACFE)*. <https://play.google.com/store/apps/details?id=com.fraudmagazine.acfe&hl=id&gl=MY> [1 November 2022]
- Association of Certified Fraud Examiners. 2022. <https://www.acfe.com/> [25 November 2022]
- Berita Harian*. 2022. Malaysia perlukan transformasi digital inklusif. *Berita Harian*, 25 Mei. <https://www.bharian.com.my/bisnes/lain-lain/2022/05/959216/malaysia-perlukan-transformasi-digital-inklusif> [14 November 2022]
- Berita Harian*. 2022. Penipuan maya meningkat mendadak. *Berita Harian*, 9 Februari. <https://www.beritaharian.sg/setempat/penipuan-maya-meningkat-mendadak> [8 November 2022]
- Bernama. 2020. CyberSecurity rekod 5,697 kes penipuan. *Harian Metro*, 9 September. <https://www.hmetro.com.my/bisnes/2020/09/618608/cybersecurity-rekod-5697-kes-penipuan> [29 November 2022]
- Cassandra Cross. 2019. Online Fraud. *Criminology And Criminal Justice*, 25 Januari. <https://oxfordre.com/criminology/criminology/abstract/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-488> [27 November 2022]
- Chen, Shuai, Chundong Gao, Dong Jiang, Mengmeng Hao, Fangyu Ding, Tian Ma, Shize Zhang, and Shunde Li. 2021. "The Spatiotemporal Pattern and Driving Factors of Cyber Fraud Crime in China" *ISPRS International Journal of Geo-Information* 10, no. 12: 802. <https://doi-org.eresourcesptsl.ukm.remotexs.co/10.3390/ijgi10120802> [ 3 Mac 2023 ]
- Chhabra Roy, N. and Prabhakaran, S. 2023, "Internal-led cyber frauds in Indian banks: an effective machine learning-based defense system to fraud detection, prioritization and prevention", *Aslib Journal of Information Management*, Vol. 75 No. 2, pp. 246-296. <https://doi-org.eresourcesptsl.ukm.remotexs.co/10.1108/AJIM-11-2021-0339>
- CyberSecurity Malaysia. 2021. *Landskap Keselamatan Siber Malaysia 2020: Apakah Persiapan Menghadapi Cabaran Keselamatan Siber Mendatang?* [https://www.cybersecurity.my/data/content\\_files/26/2150.pdf](https://www.cybersecurity.my/data/content_files/26/2150.pdf) [1 November 2022]
- CyberSecurity Malaysia. 2022. *Incident Statistics: Reported Incidents based on General Incident Classification Statistics 2022*. <https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=00d34a6a-4a5e-4833-95bf-5e08b8c57fed> [7 November 2022]

- Elles Houweling. 2021. Chinese ‘anti-fraud centre’ becomes most downloaded app. VERDICT, 7 September. <https://www.verdict.co.uk/chinese-anti-fraud-centre-becomes-most-downloaded-app/> [29 November 2022]
- Fraudster. Mobile Application. <https://apps.apple.com/ca/app/fraudster/id1614776876> [ 1 November 2022]
- Fraud Magazine. Mobile Application. <https://www.fraud-magazine.com/twocolumn.aspx?pageid=4294973108&terms=mobile%20app> [ 1 November 2022]
- Foring-IT. 2022. SIA - Scammer Information App.
- Jacqueline M Drew & Lucy Farrell (2018) Online victimization risk and self-protective strategies: developing police-led cyber fraud prevention programs, *Police Practice and Research*, 19:6, 537-549, DOI: 10.1080/15614263.2018.1507890
- Jerry Virgo. 2022. Mengatasi Cabaran dengan Menguji Aplikasi Mudah Alih. Aptude. <https://aptude.com/ms/blog/kemasukan/mengatasi-cabaran-dengan-menguji-aplikasi-mudah-alih/> [9 November 2022]
- John Stephens. 2023. Apakah Perbezaan antara Carta Alir Sistem dan Carta Alir Program? STREPHONSAYS, 10 Januari. <https://ms.strephonsays.com/what-is-the-difference-between-system-flowchart-and-program-flowchart> [6 Januari 2023]
- Kemp, S., Miró-Llinares, F. & Moneva, A. The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain. *Eur J Crim Policy Res* 26, 293–312 (2020). <https://doi-org.eresourcesptsl.ukm.remotexs.co/10.1007/s10610-020-09439-2>
- Kumara Sabapatty. 2022. Orang Melayu paling ramai jadi mangsa scammer. *MalaysiaGazette*, 22 Jun. <https://malaysiagazette.com/2022/06/22/orang-melayu-paling-ramai-jadi-mangsa-scammer/> [9 November 2022]
- Kumara Sabapatty. 2022. PDRM sasar 10 peratus penurunan kes penipuan online setahun – KPN. *MalaysiaGazette*, 13 September. <https://malaysiagazette.com/2022/09/13/pdrm-sasar-10-peratus-penurunan-kes-penipuan-online-setahun-kpn/> [9 November 2022]
- Lau Lee Keng. 2020. Vulnerability Assessment In Malaysia Government Web-Based Application. Universiti Tunku Abdul Rahman. 19 Mei. [http://eprints.utar.edu.my/4991/1/LAU\\_LEE\\_KENG.pdf](http://eprints.utar.edu.my/4991/1/LAU_LEE_KENG.pdf) [26 April 2023]
- MCMC. 2023. Apa itu Phishing? MCMC. 19 April. <https://www.mcmc.gov.my/ms/faqs/phishing-attack/1-what-is-phishing> [19 April 2023]
- Majlis Keselamatan Negara. 2023. Jenis Penipuan Atas Talian! Majlis Keselamatan Negara, 28 Mac. <https://www.mkn.gov.my/web/ms/2023/03/28/jenis-penipuan-atas-talian/> [10 April 2023]
- Mineshwara. 2022. Jangan Terpedaya! Waspada Strategi Penipuan Maya @ Scam. Nadi Bangi, 11 Julai. <https://www.nadibangiukm.com/post/jangan-terpedaya-waspada-strategi-penipuan-maya-scam> [18 April 2023]
- Mohd Zaky Zainudin. 2022. Jenayah kewangan rentas sempadan semakin sukar dikesan. *Berita Harian*, 14 November. <https://www.bharian.com.my/bisnes/lain-lain/2022/11/1025580/jenayah-kewangan-rentas-sempadan-semakin-sukar-dikesan> [27 November 2022]
- Monica T Whitty. 2018. 419 – It's just a Game: Pathways to Cyber-Fraud Criminality emanating from West Africa. *International Journal of Cyber Criminology*, 12(1), 97–114. <https://doi-org.eresourcesptsl.ukm.remotexs.co/10.5281/zenodo.1467848>
- mStar. 2022. Labur sedikit, dipaksa tukar pakej mahal... ada yang sampai tangguh kahwin! Ramai miskin selepas ‘bantu’ scammer jadi kaya. *mStar*, 1 Oktober. <https://www.mstar.com.my/lokal/viral/2022/09/30/labur-sedikit-dipaksa-tukar-pakej->

- mahal-ada-yang-sampai-tanggung-kahwin-ramai-miskin-selepas-bantu-scammer-jadi-kaya [19 April 2023]
- Muhammad Adnan Pitchan dan Siti Zobidah Omar. 2019. Dasar Keselamatan Siber Malaysia: Tinjauan Terhadap Kesedaran Netizen dan Undang-Undang. *Malaysian Journal of Communication*, Jilid 35(1) 2019: 103-119. <http://journalarticle.ukm.my/13171/1/30796-98936-1-PB.pdf>
- MySQA. 2022. BUKU PANDUAN KRISA. <https://sqa.mampu.gov.my/index.php/en/4-8-reka-bentuk-antaramuka-pengguna-f3-4> [6 Januari 2023]
- Nurulatiq Ahmad Bandi. 2019. Ancaman jenayah scam. *Sinar Harian*, 9 Jun. <https://m.sinarharian.com.my/mobile-article?articleid=71853> [25 Oktober 2022]
- Nurul Hidayah Bahaudin. 2022. Masih ramai individu jadi mangsa penipuan dalam talian. *Harian Metro*, 10 Mac. <https://www.hmetro.com.my/mutakhir/2022/03/819330/masih-ramai-individu-jadi-mangsa-penipuan-dalam-talian> [23 November 2022]
- Royal Malaysia Police, CCID. 2021. Semak Mule CCID. <https://play.google.com/store/apps/details?id=com.ccid.ccis2020&hl=id&gl=MY> [13 November 2022]
- Salleh Buang. 2020. Strategi banteras jenayah scammer. *Sinar Harian*, 18 Oktober. <https://www.sinarharian.com.my/article/105778/khas/pendapat/strategi-banteras-jenayah-scammer> [9 November 2022]
- Smita Tripathi. 2022. A Review of Literature Based Online Fraud in India. *ADHYAYAN* Volume 12, Issue 1. <https://smsjournals.com/index.php/Adhyayan/article/download/2770/1251> [29 November 2022]
- TheStar. 2021. Campaign to raise awareness about online scams. *TheStar*, 21 September. <https://www.thestar.com.my/metro/metro-news/2021/09/21/campaign-to-raise-awareness-about-online-scams> [27 November 2022]
- Tretyakov, V., & Golyatina, S. 2022. Applying Big Data technologies to counter cyber fraud. *Amazonia Investiga*, 11(49), 9-16. <https://doi.org/10.34069/AI/2022.49.01.1>