Vol. 4 Special Issue. 1
International Journal of Data Science and Advanced Analytics (ISSN: 2563-4429)

Preventing Malicious Keyloggers using Anti-keyloggerIntegrated Keyboard in Mobile Banking Applications

Chow Wen Xuan[1], Intan Farahama Binti Kamsin[2], Salmiah Amin[3] and Nur Khairunnisha Zainal[4]
[1] '2Asia Pacific University of Technology and Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia.
[1]TP059581@mail.apu.edu.my, [2]intan.farahana@staffemail.apu.edu.my, [3]salmiah@staffemail.apu.edu.my,
[4]khairunnisha.zainal@staffemail.apu.edu.my

***Abstract*—** In current mobile banking applications, users will need to have an account to access the banking services. Every time accessing mobile banking applications, users are required to login using their credentials. This will lead to a chance that cyber-attackers perform malicious keylogging activities. Although the implementation of Multi-Factor Authentication can strengthen the authentication process, there are still restrictions in certain cases. In this research paper, a new keyboard system is suggested to overcome this issue. The proposed system is trusted and verified by the bank companies and prevents users from being threatened by malicious keyloggers. This research will be using quantitative study via survey to review to gather information from respondents. The target respondents will be 300 respondents who are using mobile-banking applications regularly around Malaysia. The sampling method applied is proportionate stratified sampling. In conclusion, this study will cover the limitations in the current keyboard system and propose a new system to fulfill the gap. The recommendation for future researchers is to develop a system that could identify the nature of a keylogger, so that the keylogger used for supervising will not be removed.

***Index Terms*—** Anti-keylogger, Keyboard application, Keylogger, Mobile Banking Application

1.0 Introduction

Banking services have changed significantly in the recent decades following the rapid development in the information technology industry. Commonly, major bank companies will not only provide the banking services physically to their customers, but also online banking systems that allow customers to utilize the banking services via the Internet. The banking services provided included checking account balance, funds transfer, paying utility bills and so forth, which are similar to the services provided physically. [10] Anyone with an account created for the online banking system can use the banking services provided remotely with their electronic devices such as laptops, tablets and mobile phones. In consequence, this boosts up the whole financial transaction process and efficiency when people use bank services.

Mobile banking, which can refer as m-banking, is a subset of online banking systems which allow the users to use the banking services via mobile devices. As for the growing usage of mobile devices nowadays, the usage of m-banking has increased rapidly as well. According to DataProt, there are around 5.22 billion active mobile device users globally by year 2021 while the total mobile payments made reached 503 billion USD in 2020. [14] In another study from Statista, active online banking users around the world is approximately 1903.2 million in 2020 and predicted that the users will keep growing until around 2551.8 million in 2025. [17]

In current mobile banking applications, users require an account to utilize the banking services provided. Every time accessing the online banking applications, users are required to login using their credentials which causes the cyber-attackers stand a chance to perform malicious activities such as using keylogger to capture the keystrokes from users. The keystrokes captured might include the credentials or other confidential data which can grant access to mobile banking applications. Consequently, this will increase the possibility of fraud transactions. From the study of DataProt, mobile applications fraud transactions have grown by more than 600% since 2015 while most of the fraud transactions occur due to account takeover. [14]

The focus of this research paper is to resolve the malicious keylogger issue by proposing a new system that is secured and keeps users aware of the keyloggers to prevent the user credentials and other confidential data being stolen by the attackers easily.

2.0 Literature Review

2.1 Keylogger

Keylogger is basically a neutral term that describes a program that can perform keystroke logging. The main purpose of this function is to record the keystrokes that input by the user on a specific device without the user's knowledge. There is legitimate keylogger software that is widely used to monitor and keep track of the activity of the users. For example, employers monitor their employees to prevent them using company computers for non-working-related purposes; parental control to ensure their children surf the Internet securely and appropriately. [15] However, there is a chance for people using keylogger software for malicious purposes, such as stealing credentials from user input, and capturing privacy information.

Keylogger can be classified into two main categories: Software keyloggers and Hardware keyloggers. The two types of keyloggers are performing the same way, but still have their own pros and cons. [8]

For software keylogger, it is usually installed on the hard drive of a device, which will capture the data transmitted from keyboard to the operating system (keystroke event), then the captured data will be stored in a remote location before sending them to the person that installed the software keylogger. The ways that sending the captured data can be via predefined email or uploading them to FTP server which the person installed the keylogger can access. [29] Software keylogger can be undetectable if the users do not perform virus scanning on the machine because software keylogger will only run in the background.

In terms of hardware keylogger, it is usually being implemented between the input device and the machine (For example on USB ports or PS/2 ports). Another way of implementing hardware keylogger is to directly install the keylogger circuit into the keyboard. [1] Hardware keylogger can be further classified as active hardware keylogger and passive hardware keylogger. The most significant difference between these two is active hardware keylogger is connected in series between the input device and computer while passive hardware keylogger is connected parallelly. An Active hardware keylogger will directly involve in the transmission of the data while passive hardware keylogger will just observe the data transmitted between input device and computer. [8] In modern way, the data collected will be stored in a temporary storage (a tiny memory chip on hardware keylogger), then the person installed the keylogger can access the stored data via some specific software. [29] Or else, by using the traditional method, the person must detach the hardware keylogger from the target machine to read the data stored. [8]

Figure 1. A Hardware keylogger on USB port
Source: https://www.pinterest.com/chamoo007/hardware-keylogger/

The two types of keylogger can be implemented based on different scenarios. For instance, software keyloggers can be easily detected by antivirus software while hardware keyloggers are impossible to be detected using antivirus software. In this case, the hardware keylogger will become the ideal choice to stay stealthy from the virus scanning process. But then, the installation of hardware keyloggers can be challenging if the person wants to install the hardware keylogger without others knowing as the only way to install a hardware keylogger is via physical access to the target machine. Furthermore, since hardware keyloggers can only be installed physically, the users can realize the existence of hardware keyloggers easily when they inspect the I/O ports of the machine.

Regarding the study, the focus will be on the software keylogger as the implementation of hardware keylogger on mobile devices is nearly impossible to achieve. Software keylogger on mobile devices can be crucial because nowadays the usage of mobile devices is increasing rapidly and most of the tasks can be done via mobile devices. For example, daily schedules can be recorded on the phone, fund transactions via online banking applications, and chat with friends via social media applications. [21] These can be the starting points for an attacker to capture the privacy data and personal information. Thus, the attacker can take this chance to grant access to one's account and take control of the account by changing the user password.

2.2 Anti-keylogger

Anti-keylogger is a software that is specifically designed to counter the keylogger software. It can detect the existence of any keylogger software on the system. (Anti Keylogger, 2019) With this technology, the users can be protected from the malicious keylogging activities that are trying to capture the confidential data. However, the shortage for this technology is it will prevent any type of keyloggers, including those being used for supervising purposes. [5]

In real life, some organizations will adopt anti-keylogger to strengthen the endpoint protection as we know that end devices in enterprises usually are the weakest point to be exploited by the cyber-attackers. The staff who lack cyber security awareness might accidentally click on some phishing emails, unknown websites, then cause malicious software installed on the system. [11] Hence, aside from giving security awareness training to employees, the organization can install anti-keylogger on their system for additional security.

Anti-keylogger works basically based on two functions, Signature-Based Detection and Behavioral Detection. [9] For signature-based detection, it will inspect the signature of the files entering the system. If the signature matches any signature of an existing keylogger, the file will be tagged as a threat. However, if the signature of keylogger could not be recognized, it can bypass this detection as well. For behavioral detection, it will observe and identify the behavior of the files to see if they are trying to perform any suspicious activities. Once the keylogger activity is detected, it will be terminated instantly to prevent the keystrokes being captured. [5] This function works similarly to behavioral detection for physical security, observing, communicating, and evaluating to see if a person is trying to carry out criminal activities. [2]

Related to this study, anti-keylogger could be implemented to detect the existence of keyloggers on mobile devices. As

mentioned in Section 2.1, software keylogger on mobile devices is an issue to be seriously concerned. The integration of anti-keylogger together with a keyboard application could improve the protection of confidential data whenever users give inputs to mobile applications by keeping them away from malicious keyloggers. In the proposed system, once the keylogger is detected, it will alert the users whether their keystrokes are being captured or not affected and remove the keylogger immediately to avoid further damage.

2.3 Mobile banking application

Mobile banking (can be referred as m-banking) is defined as "A product or service offered by a bank or a microfinance institute (bank-led model) or MNO (non-bank-led model) for conducting financial and non-financial transactions using a mobile device, namely a mobile phone, smartphone, or tablet" by Shaikh and Karjaluoto. [23] The first m-banking can be traced back to the late 90's Germany, in which a company named Paybox cooperated with Deutsche Bank to implement this service. [23] Initially, m-banking was only established in the European region, utilizing SMS banking for the banking services. After a few years of technology development, some new approaches to access m-banking services were released, for instance like mobile-banking applications, mobile-banking websites, and tablet m-banking applications. [10] In this study, this focal point will be on mobile-banking applications.

M-banking applications are specifically designed for smartphones. Before the year 2010, people owning a mobile phone could only perform some simple tasks, such as phone calls, text messaging, take photos and videos. Only few of them offer Internet surfing service, unlike the smartphones nowadays. Therefore, the two common ways to access m-banking services are through SMS banking and m-banking websites. [10] M-banking applications started emerging together with the evolution of smartphones. [24] Smartphones provide much better and broader functionalities to the users, including installing the m-banking applications on the system and accessing the banking services in a simpler way.

In Malaysia, m-banking applications are supported by most of the banking companies. For example, Maybank2U from Maybank, CimbClicks from CIMB bank, AmOnline from AmBank are some m-banking applications that are often being used by Malaysians. [13] These applications provide convenience and enhance the overall effectiveness and efficiency where people can check the financial balance, making funds transfer, utility bill payment, investment at anytime, anywhere with internet access. Especially during the Covid-19 pandemic, the adoption of m-banking applications in Malaysia has grown significantly due the Movement Control Order In general, the m-banking applications are well-design from the perspective of user-friendly and security to ensure users can access banking services while at the same time their confidential data and asset can be protected. [26]

Although the m-banking applications are well designed for data security, the attackers are still capable of exploiting the system from the user's side using technology like keylogger. As there is limited research on preventing keylogger on m-banking applications, this study will consider mitigating the threat by deploying a new system that can cover this aspect.

2.4 Keyboard application

Keyboard applications come along with the evolution of smartphones. It is obvious that smartphones these days operate in touch screen mode hence, they rely on keyboard applications to receive the input from the users. By default, every smartphone will include a built-in keyboard application for the users.

However, various types of keyboard applications are also available on the Play Store/App Store, with different functionalities and appearance settings provided. Users will usually install those third-party keyboard applications based on their preference on the devices instead of using the built-in keyboard. The reason for this is because some users prefer to have a more personalized and customizable keyboard application on their own devices. [22]

Still, there is an existing risk in these third-party keyboard applications that might cause users' privacy information being threatened. According to [27], most of the third-party keyboard applications collect the data from the users when they are using their keyboard, which will then store into their own server. In addition, the keystrokes will also be captured by these keyboard applications. Even the original intention of doing this is to provide better services to the users, but anyhow there is still a chance that their server will be attacked, and all this information will be stolen.

In this study, we are focusing on preventing the users of m-banking applications to be threatened when they are using a third-party keyboard to access. Therefore, the proposed system will overcome the issue mentioned above while keeping the same functionalities provided by these third-party keyboard applications.

2.5 Similar Systems

2.5.1 GO Keyboard

GO keyboard is a keyboard application that can be installed without any charge from Google Play Store but not available in iOS devices. This application allows users to create cartoon avatars using their own photos and customize their own sticker packs. Apart from that, GO keyboard provides more than 1000 keyboard themes and emojis, 100 font styles, GIFs together with more than 800 emoticons. Furthermore, it supports more than 60 languages so users can customize the keyboard based on their demand. [22]

The screenshots of GO keyboard systems are provided as below:

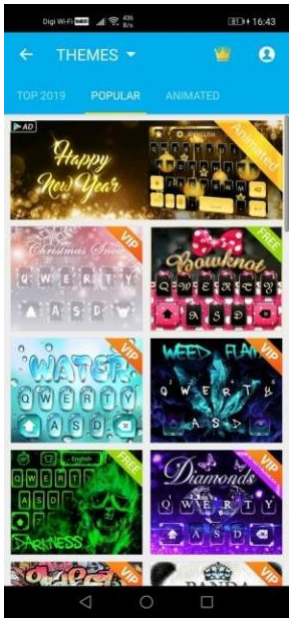

Figure 2.0 Themes available for GO Keyboard

Figure 3.0 Avatar Design for GO Keyboard

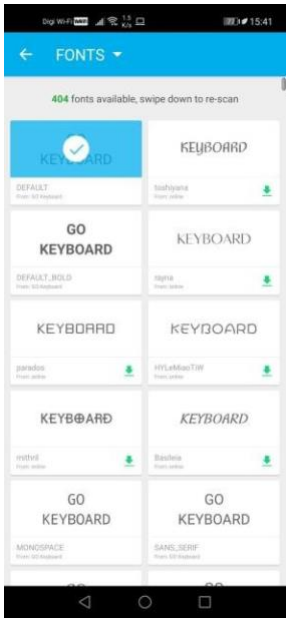

Figure 4.0 Font styles available for GO Keyboard

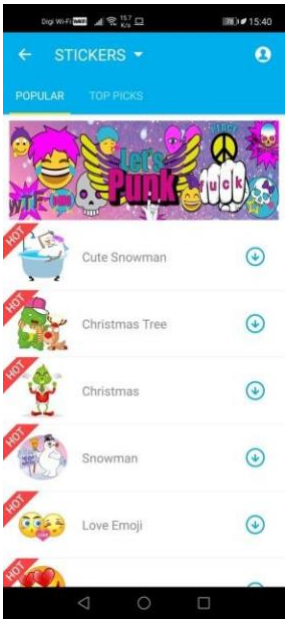

Figure 5.0 Stickers available for GO Keyboard

Figure 6.1 Languages available for GO keyboard

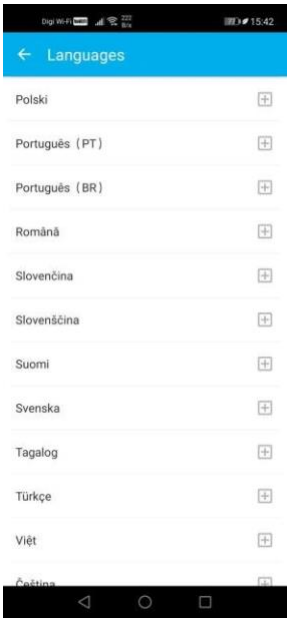

Figure 6.2 Languages available for GO keyboard

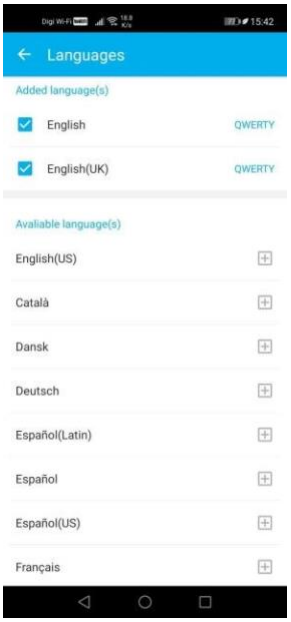

Figure 6.3 Languages available for GO keyboard

2.5.2 Sogou Input

Sogou Input is a keyboard application developed by Chinese company, Sogou. This application mainly aims for the users who are using Chinese as their main communication language. However, this application is only available in the Apple App Store for iOS users but not Android users. It offers similar functionalities as other keyboard applications do, such as attractive keyboard themes, customized emojis, GIFs, multiple languages. Also, it provides the feature of text prediction and auto-correction which could benefit the users by saving their time. [28]

The screenshots of Sogou Input are provided as below:

Figure 7.0 Themes available for Sogou Input

Figure 8.0 Font Styles available for Sogou Input

Figure 9.0 Stickers available for Sogou Input

Figure 10.1 Languages available for Sogou Input

Figure 10.2 Languages available for Sogou Input

Figure 10.3 Languages available for Sogou Input

2.5.3 Compare and Contrast Table

Criteria/System	GO Keyboard	Sogou Input
Free to install	/	/
Available on Google Play Store	/	
Available on Apple App Store		/
Trusted by the m-banking applications	/	/
Keylogger detection		
Anti-keylogger feature		

Table 1.0 Compare and Contrast Table for Similar Systems

From Table 1.0, we realize that GO Keyboard is free to install from Google Play Store on Android phones, and it can be used to access m-banking applications without being blocked. For Sogou Input, it is also free to install from Apple App Store and used in m-banking applications. Nevertheless, both applications do not support keylogger detection and anti-keylogger features that can be used to enhance the security level when users accessing m-banking applications. For this reason, the new proposed system from this study will include all the features that existed in both applications, together with additional features which are keylogger detection and anti-keylogger function.

3.0 Problem Statement

According to [8], a major issue in user authentication methods by providing username and password inputs is the chance of the keystrokes being captured by malicious keylogging applications. A keylogger is not an emerging technology but as the usage of mobile devices has kept growing in recent years, the threat from keyloggers has caught the sight of the public. Nowadays, mobile devices have multiple functions, for instance surfing the Internet or social media, making transactions via online banking applications, making phone calls, writing emails, playing games. These bring a lot of convenience to our daily life, however in other words that most of the users' privacy and personal information can be found inside the mobile devices. In consequence, the mobile devices will become the target of many cyberattacks, which included keylogging attacks.

As mentioned by [21], the mobile banking applications utilize the username and password inputs for the login authentication, thus an attacker will try to implement a keylogger software on the user's device to capture the keystrokes and then gain access to the user's bank account. [8] This has caused a serious issue for the users while accessing a banking application using their phones. It is difficult for the users to realize the existence of keylogger software as most mobile device users will have their own preferred/customized third-party keyboard applications which may contain hidden keylogger software. [21] In this situation, the bank company can only force the users to use a virtual built-in keyboard when entering their credentials, however there is still a chance for the attacker to deploy a keylogger inside the built-in keyboard.

There is another way to make the authentication process more effective, which is utilizing the Multi-Factor Authentication (MFA) together with entering the credentials. Applying MFA will not only protect the users against keylogger attacks but too can increase the overall security of the authentication method. However, with this method, a user will sometimes require another device or feature as part of the authentication process. In real life, not all users have additional devices or the function on the device to perform the authentication process hence this method might not be applicable in some certain scenarios. [8] Users might have to purchase additional devices just to utilize MFA which is not reasonable from every point of view.

4.0 Aim and Objectives

4.1 Aim

The main aim of this research is to provide users a safer environment when using the online banking application and prevent users threatened by illegal keylogger activities.

4.2 Objectives

1. To develop a keyboard application that is secured, trusted and verified by the banking companies that can be deployed on their own online banking application.

2. To notify users and ask them to change the credentials (username or password) immediately when detected malicious keylogging applications.

5.0 Research Significance

The outcome of this study could benefit the users of mobile banking applications, bank companies that provide mobile banking applications to their customers. The proposed solution can be implemented into the mobile banking applications to prevent attackers stealing the credentials from users' keystrokes easily even when the users do not realize the menace of this cyber-attack. Apart from that,by looking from the perspective of bank companies, they can perform a quickerrecovery and mitigate the possible assets loss that might be caused by the attack with current implementation. Not only that, dueto the Covid-19 pandemic in recent years, the usage of mobile banking applications has also increased significantly which stated thatpeople nowadays will rely more on online banking applications to perform their fund transactions. Thus, the proposed solution could enhance the mobile banking applications to become more reliable and trusted by the customers and the bank companies could maintain their good reputation when they could provide secured services to their customers.

6.0 Research Methodology

6.1 Target Respondents

In this study, the target respondents of the survey will be 350 mobile-banking application users from every age group, different states in Malaysia, which are also frequently using m-banking applications in their daily life. Reason for this is to ensure that the results gathered have the value to be taken as reference.

6.2 Sampling method

The sampling method will be applied in this study is stratified sampling. After the surveys are collected, we will use stratified sampling to choose the sample to represent a population and analyze the data. This type of sampling method will categorize the respondents based on specific criteria into strata, then randomly choose the response from each stratum. By the way, it can produce a result that is highly precise as the selection bias will be eliminated.

Regarding our study, since we are applying quantitative research, stratified sampling is suitable when doing sampling. There are two ways of doing the stratified sampling, which are proportionate stratified random sampling and disproportionate stratified random sampling. In the formal case, the respondents can be categorized into stratum in a proportionate manner, for example 100 respondents in each stratum, then the sample will be selected randomly. However, in the latter case, the respondents will be categorized based on certain attributes which might make the stratum contain unequal members. This will cause the result acquired to be less accurate rather than disproportionate stratified random sampling. [20] Hence, we will be using disproportionate stratified random sampling in our study to get a more precise outcome.

6.3 Data collection method

The data collection method decided to be used in this study is quantitative research via survey. Quantitative research will be useful when we are dealing with large amounts of data required for the research without going in-depth. In addition, the results can be quantified using a graph, table, chart and so forth thus researchers can understand the data easily. [18] Survey is a widely used method to collect data from the population due to its cost-effectiveness and efficiency. Surveys can be distributed to the population via online platforms such as email, Google form and online polls, which saves a lot of time instead of distributing the survey to the respondents physically. [25] Moreover, particularly in the current Covid-19 pandemic situation, survey via online is a more ideal option to gather data from a large population.

The survey for this study will be designed with closed ended questions regarding the awareness and concern on the security aspect when respondents are using mobile banking applications and gather the opinion from respondents on the new proposed system to see if it fulfills the expectation from user's point of view.

7.0 Proposed System Overview

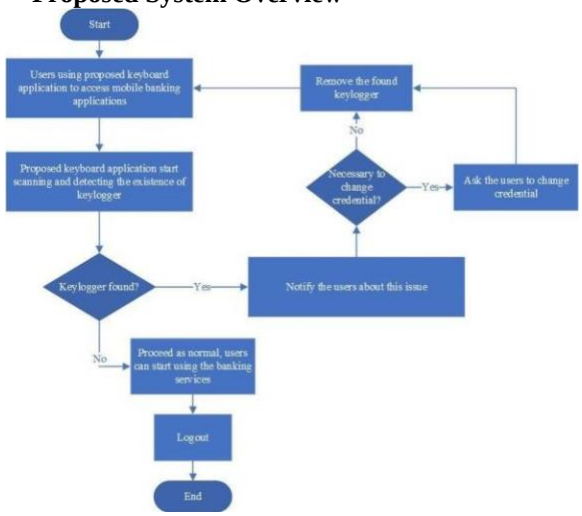

Figure 11.0 System flow of the proposed system

This flowchart shows that the operation of the proposed keyboard integrated with anti-keylogging features.When a user is using the keyboard to access m-banking applications, it will automaticallyscan and detect if there is any keyloggerexisting in the system. If any keylogger is found after the scanning and detectingprocess, the proposed keyboard application will notify the users about the issue, remove the keylogger instantly and check if the keystrokes are captured by the keylogger. If yes, there might be a chance that the user's credential is being captured as well so it willask the user to change the credential. After that, users can proceed to login again.

8.0 Conclusion

The integration of anti-keylogger and keyboard applications will enhance the security level to an advanced level whileusers are utilizing mobile banking services. With the increasing usage of mobile banking services in recent years, this issue will become a serious concern for the whole society around the world. Although there are some security features implemented to secure the system, for instance fingerprintauthentication, face recognition and PIN, there are still spaces for the attackers to launch their attack. Hence, the advent of the proposed system will fulfill the gap and make the overall security environment robust.

9.0 References

[1] Abukar, Y., Maarof, M., Fuad, M., Hassan, & Sugow Mohamed, (2017). *Survey of Keylogger Technologies A Conceptual Scheme for Ransomware Background Knowledge Construction View project Efficient Anomaly Detection Model for Wireless Sensor Networks View project*.

[2] *Advanced Security & Risk Solutions*. (2022). Advanced Security & Risk Solutions. http://advancedsecurityandrisksolutions.ie/what-is-behaviour-detection/

[3] Aloul, F., El-Hajj, W., Zahidi, S., & El-Hajj, W. (2009). Multi Factor Authentication Using Mobile Phones Wireless Security View project OMA: Opinion Mining in Arabic View project Multi Factor Authentication Using Mobile Phones. *International Journal of Mathematics and Computer Science*, *4*(2), 65–80.

[4] Anti Keylogger. (2019, April 30). *What is Anti Keylogger? | How Does a Keylogger Detector Work?* Comodo Enterprise. https://enterprise.comodo.com/anti-keylogger.php

[5] *Anti-keylogger - GeeksforGeeks*. (2021, March). GeeksforGeeks. https://www.geeksforgeeks.org/anti-keylogger/

[6] Ariff, D. (2022). *A Study on User Interface, Mobile Services and Effectiveness of Mobile Banking Application in Malaysia*. Academia.edu. https://www.academia.edu/9348352/A_Study_on_User_Interface_Mobile_Services_and_Effectiveness_of_Mobile_Banking_Application_in_Malaysia

[7] *Awareness of cyberattacks and cybersecurity may be lacking among workers*. (2021, July). TechRepublic; TechRepublic. https://www.techrepublic.com/article/awareness-of-cyberattacks-and-cybersecurity-may-be-lacking-among-workers/

[8] Blåfield, T. (2020). *DIFFERENT TYPES OF KEYLOGGERS Mitigation and risk relevancy in modern society*. https://trepo.tuni.fi/bitstream/handle/10024/122479/Bl%c3%a5fieldToni.pdf?sequence=2&isAllowed=y

[9] *Chinese keyboard apps on the spot over suspicion of privacy violation - Global Times*. (2021). Globaltimes.cn. https://www.globaltimes.cn/page/202101/1214202.shtml

[10] Corporate Finance Institute. (2020, July 14). *Mobile Banking*. Corporate Finance Institute; Corporate Finance Institute. https://corporatefinanceinstitute.com/resources/knowledge/finance/mobile-banking/

[11] *Endpoint Security*. (2022, January 4). Comodo News for Enterprise Security. https://enterprise.comodo.com/blog/what-is-endpoint-security/?af=7639

[12] Kim, J.-J., & Hong, S.-P. (2011). A Method of Risk Assessment for Multi-Factor Authentication. *Journal of Information Processing Systems*, *7*(1), 187–198. https://doi.org/10.3745/jips.2011.7.1.187

[13] Krishnan, G. (2019, March 18). *Best Mobile Banking Apps in Malaysia*. IMoney Malaysia. https://www.imoney.my/articles/mobile-banking-apps-review

[14] *Mobile Banking Statistics That Show Wallets Are a Thing of the Past*. (2021, March 17). DataProt. https://dataprot.net/statistics/mobile-banking-statistics/#:~:text=In%202021%2C%20there%20are%205.22,are%20due%20to%20account%20takeovers.

[15] Nikolay Grebennikov. (2007, March 29). *Keyloggers: How they work and how to detect them (Part 1)*. Securelist.com; Kaspersky. https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/

[16] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), https://doi.org/10.3390/cryptography2010001

[17] *Online banking users worldwide by region 2020 | Statista*. (2020). Statista; Statista. https://www.statista.com/statistics/1228757/online-banking-users-worldwide/

[18] *Quantitative Research: Definition, Methods, Types and Examples | QuestionPro*. (2018, April 12). QuestionPro.

https://www.questionpro.com/blog/quantitative-research/

[19] Pousttchi, K., & Schurig, M. (2019). Assessment of Today's Mobile Banking Applications from the View of Customer Requirements - Munich Personal RePEc Archive. *Uni-Muenchen.de*. https://doi.org/https://mpra.ub.uni-muenchen.de/2913/1/MPRA_paper_2913.pdf

[20] Research-Methodology. (2020). *Stratified Sampling - Research Methodology*. Research-Methodology. https://research-methodology.net/sampling-in-primary-data-collection/stratified-sampling/

[21] Rubel, Rahaman, M., & Dhaka. (2019). *KEY-LOGGING THREAT TO THE ANDROID MOBILE BANKING APPS*. http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/5188/P14917%20%2815_%29CSE.pdf?sequence=1&isAllowed=y

[22] Rudra, N. R. (2022, January 31). *9 Best Mobile Keyboard Apps*. Geekflare. https://geekflare.com/mobile-keyboard-apps/

[23] Shaikh, A. A., & Karjaluoto, H. (2015). Mobile banking adoption: A literature review. *Telematics and Informatics*, *32*(1), 129–142. https://doi.org/10.1016/j.tele.2014.05.003

[24] Sharma, S. K., & Sharma, M. (2019). Examining the role of trust and quality dimensions in the actual usage of mobile banking services: An empirical investigation. *International Journal of Information Management*, *44*(Feb), 65–75. https://doi.org/10.1016/j.ijinfomgt.2018.09.013

[25] *Survey Research and Questionnaires | Research Connections*. (2014). Researchconnections.org. https://www.researchconnections.org/research-tools/data-collection/survey-research-and-questionnaires

[26] *The future of banking is shaped by mobile banking*. (2020, November 22). The Edge Markets. https://www.theedgemarkets.com/content/advertise/the-future-of-banking-is-shaped-by-mobile-banking

[27] Third-Party Keyboards Give Mobile Users More Options (Published 2016). (2022). *The New York Times*. https://www.nytimes.com/2016/06/30/technology/personaltech/third-party-keyboards-give-mobile-users-more-options.html

[28] Uptodown Technologies SL. (2019, June 29). *Sogou Input (Android)*. Uptodown.com. https://sogou-input.en.uptodown.com/android#:~:text=Sogou%20Input%20(%E6%90%9C%20%E7%8B%97%20%E8%BE%93%E5%85%A5,Chinese%20keyboard%20for%20mobile%20devices.&text=Sogou%20Input%20is%20an%20excellent,want%20to%20input%20characters%20manually

[29] *What's the Difference Between Hardware Keylogger and Keylogger Software*. (2012). Easemon.com. https://www.easemon.com/whats-the-differences-between-hardware-keylogger-and-keylogger-software.html

[30] *When to Use Qualitative vs. Quantitative Research*. (2010, March17). Alchemer. https://www.alchemer.com/resources/blog/quantitative-qualitative-research/