Security of Internet Banking Services in Malaysia: A Survey of Current Practices

Nor Naematul Saadah Ismail
Awang Had Salleh Graduate School
School of Computing, Universiti Utara Malaysia
06010 Sintok, Kedah, Malaysia

Mohd Khairudin Kasiran
School of Computing
School of Computing, Universiti Utara Malaysia
06010 Sintok, Kedah, Malaysia

ABSTRACT
Internet banking has become increasingly popular in Malaysia, but the risk of fraud has also increased. This article examines the security implementation on Internet banking sector in Malaysia. The article begins by discussing the growing problem of banking fraud in Malaysia, and then reviews the security measures that are currently in place. The article then will compare the security implementations of selected banks in Malaysia. The article concludes by discussing potential fixes and upcoming advancements in Internet banking security. The article's findings are that there are several security measures in place to protect users of Internet banking in Malaysia. However, there are also some areas where security could be improved. The article recommends that banks continue to invest in security measures, and that users of Internet banking should be aware of the risks and take steps to protect themselves.

Keywords
Internet banking, online banking, security measure

1. INTRODUCTION
In Malaysia, banking fraud is a getting serious. The risk of becoming a victim of financial crime increases as more people use Internet banking services for day-to-day convenience. Among financial crime that committed in Malaysia are online and cyber fraud, banking fraud and identity theft. The problem has escalated due to the rise in internet-based and digital payments usage [1].

According to [2], there are several data breaches in Malaysia for the year 2022, such as 13 million voters details were copied illegally from the Election Commission and being posted on a popular online marketplace database. The same report also mention about the safety of MyKad numbers and addresses as well as mobile numbers for Maybank and Astro Malaysia customers were also being compromise. In addition, according to [3], there are 13, 703 reported cases regarding online scam with loss worth RM 590 million in year 2019. Meanwhile, in 2020, the cases increased to 17, 227 cases reported to the Royal Malaysian Police (RMP) make the losses of RM 511.2 million and in the year 2021, 20,701 cases reported with loss worth RM 560.8 million and the number are on rise. According to Tan Sri Acryl Sani Abdullah Sani, the Inspector General of Police, the scammer usually targeted youths as their victim.

Not only that, as reported by [4], phishing incidents increased tremendously in South-east Asia targeted the users in Malaysia, Philippines, and Vietnam in the first half of 2022. In a phishing attack, a false website is used to imitate a real website to trick visitors into visiting the fake website, where their personal information, including usernames, passwords, and credit card information, is stolen. Phishing incidents typically occur while performing Internet banking or shopping [5]. Thus, this research is purposely to analyze the security implementation on Internet banking sector in Malaysia. This article will examine the present state of Internet banking security implementation, including the difficulties and worries experienced by users and the steps taken by banks to address these problems. We'll also talk about potential fixes and upcoming advancements in Internet banking security. Meanwhile, this research will be motivated by these research questions:

Research Question 1: What security measures are implemented by Internet banking industries to ensure the identity of the user is always authenticated?

Research Question 2: How do the security implementations of selected banks in Malaysia compare?

2. LITERATURE REVIEW
Due to the rapid pace of technological development, the usage of cutting-edge technology, and the internet's unprecedently rapid expansion, many businesses are now taking the technological initiative to make their goods and services easily accessible to clients online. For example, the banking industry has embraced cutting-edge technology and incorporated it into its operations. With the advent of web-based information systems, such as interactive web sites and/or portals and by making online transactions automatic for users, banking has been transformed from the traditional delivery method. For financial institutions, cost savings and meeting customer needs are two possible advantages of the click and mortar approach [6]. Internet banking can be characterized as a secure website provided by the bank to conduct commercial or financial transactions as well as other financial services. Internet banking can be used to access the activity from a laptop, desktop computer, or mobile device. The proliferation of technology, fierce competition among banking institutions, and the globalization of the economy have compelled banks to look for new markets and cutting-edge financial services. Routine banking activities are now conducted online thanks to the banking industry's use of the Internet as an online business tool [7].

The banking industry is crucial to Malaysia's economy because it makes it easier for people to transact money, supports businesses, and gives them access to basic services. The Malaysian banking sector's deployment of robust security has become a top priority due to the rapid advancement of technology and the rising prevalence of cyber threats. This introduction establishes the groundwork for a research study that concentrates on the security measures and difficulties faced by Malaysian banks with the goal of identifying efficient methods to protect customer data, reduce risks, and preserve the integrity of the financial system.

The ability to make financial transactions from any location at

any time thanks to Internet banking has revolutionized the way individuals handle their money. However, as Internet banking becomes more popular, it becomes more important than ever to take strong security precautions to safeguard consumers' private data and avoid fraud. To protect the privacy and security of their clients' online transactions, banks have put in place several security measures.

Even though Internet banking has become the convenient way for customers to perform most of their transactions, there are several security threats that have occurred such as phishing and identity theft. Various phishing techniques have been launched by the attackers to attack Internet banking users. In phishing technique, phisher usually will post a link that seems so legit and make users tend to click the bait [8].

Internet banking has completely changed how individuals handle their money because it offers a quick and easy way to execute transactions and have access to financial data. However, as Internet banking becomes more popular, there is a greater need for effective security measures to deter fraud and online crime. Major banks in Malaysia have put in place a variety of security and authentication systems to protect their clients' data and money. Despite these initiatives, both banks and customers are still concerned about the security of Internet banking. This literature review seeks to present a summary of the status of study on the deployment of Internet banking security in Malaysia. This review will fill in any gaps in the literature by critically analyzing current studies and guide future investigation into this crucial subject.

According to researchers in [9], they claimed that as society steadily enters the modern era, the number of tech-savvy consumers has been increasing tremendously. Such patterns would eventually lead to a rise in customer demand for services connected to the digital realm, such Internet banking. Therefore, the demand for Internet banking services is projected to rise as the number of tech-savvy consumers grows. In Malaysia, the report examines seven variables that affect consumer intentions to use Internet banking. These elements include perceived credibility, perceived usefulness, perceived ease of use, perceived risk, perceived social impact, accessibility, and perceived facilitating conditions.

[6] in their research explained that web security measures on web-based system sites, such as authentication, secure socket layers, encryption, and other security standards, show the company is serious about lowering the risk connected with the web-based channels. Organizations can aid consumers in comprehending the security mechanism and improving their perception of security by doing this. Therefore, by increasing users' trust and confidence in the security of the system, web security plays a critical role in influencing the adoption of Internet banking systems.

By deploying Internet banking, security features should be considered as well. Thus, researchers in this paper [10] mentioned about common security risks that might arise such as security gaps in every innovation, phishing attacks, malware attacks, identify theft and unauthorized access to legitimate account. Therefore, the researchers suggest some security measure that can be implemented by the financing services provider such as bank to upgrade the Secure Socket Layer (SSL) certificates, daily login logging information, encrypt the certificate, two-factor authentication, using firewalls and antivirus software. Not forgetting to educate Internet banking users about safe Internet banking practices.

However, this paper will only focus on the security implementation that the customer wants to pass through based on the following situation. To access online banking accounts, customers need to have an online banking account with the bank. After login credentials have been obtained, they can login into the system. The system will grant access to customers if the login credentials are given correctly. They can perform activities such as fund transfers, balance inquiries, pay bill online and more [11]. Nowadays most of the online banking systems provide additional security measures to protect customers' accounts. User ID and transaction passwords, one-time passwords, grid authority cards, QR codes, biometric systems, security questions, and E-tokens are a few examples of typical security precautions. Additionally, to ensure that client data is sent securely and consistently, banks should adopt "best of breed" systems to authenticate users' identities [12]. Therefore, author in [13] propose an Internet banking security software to overcome and control the illegal access to the Internet banking.

3. METHODOLOGY

This research has been performed using content analysis and experimental testing. The security implementation information of Internet banking service on five major banks in Malaysia will be gathered. There are almost 177 banks in Malaysia, including commercial banks, Islamic banks, and Investment banks. Lots of services provided by these banks [14]. The selection of five major banks in the category of consumer banking in Malaysia are based on the authors account which involved Public Bank Berhad, Agro Bank, CIMB Bank, Maybank Berhad, and RHB Bank. Data is collected from the websites and Internet banking portals of these banks, with a focus on the information provided about Internet banking security and the steps involved in logging in to their Internet banking portals. To ensure the reliability of the results, a coding scheme is used to categorize the data and multiple coders are used to ensure all activities and data recording can be done accordingly and produce a reliability of the results. The data is systematically analyzed to identify patterns and draw conclusions about the security measures implemented by these banks and their approaches to Internet banking security. The results of the analysis will be used to improve the understanding of internet banking security and to develop recommendations for improving the security of internet banking systems.

The steps taken involved these coding scheme so that the security implementation of these five major banks can be differentiated by using these parameters which are:

1. Authentication methods: This category includes data related to the different methods used by banks to authenticate users when they log in to their Internet banking portals. Examples of authentication methods could include passwords, security questions, one-time passwords (OTPs), or biometric authentication.
2. Security features: This category includes data related to additional security features implemented by banks to protect their customers' information and transactions. Examples of security features could include encryption, firewalls, or intrusion detection systems.

The collected data from the websites and Internet banking portals of the five major banks would be assigned to one of these categories based on its content and relevance. The data within each category could then be analyzed to identify patterns and draw conclusions about the security measures implemented by these banks. The main selected Internet banking in Malaysia

will be randomly mentioned as Bank A, Bank B, Bank C, Bank D, and Bank E afterwards in this research.

4. RESULTS

This section will describe and discuss three schemes or processes that have been carried out to gather the data. The researchers had carried out the process and collected all relevant data based on the experimental testing on how each bank handles the following process.

4.1 Authorization

Bank A will ask the customer to key in the User ID, after the next button is clicked, it will display the personal login phrase, customer needs to verify the phase either yes or no. If the customer clicks no, it will return to the login screen again and the customer needs to key in the User ID again. By clicking yes, then the customer will have to key in the password. For extra security, this bank provides an on-screen keyboard. This will prevent the key logger from sniffing the customer's password. If a customer keyed in the wrong password, it will return to the login screen.

For Bank B login screen, it will prompt safety and precaution windows to make sure customers are aware of possible threats. To login into its Internet banking account, the customer needs to key in the username and press the login button. After that, it will display the chosen security image with security phrase. If both security parameters are correct, then the user needs to verify that. After verification has been done, then the password field will be activated, after that then customer can key in the password and click submit to get logon to the Internet account.

As for Bank C, the customer needs to enter the User ID, click login button then secureword will be displayed. To login, the customer will key in the password after verifying the secureword. If the customer entered the wrong password, it would display an alert.

Bank D will straight away display the login menu if we directly type the correct URL. Customer will key in the username. Right away after clicking the login button, a small welcoming menu will be displayed. It displays the security image together with the security phrase. If both security parameters are correct, the customer will click the yes button, the password field will be provided. Then the customer can input the password and login.

Lastly, for Bank E, it will ask permission to collect location information before it displays its login screen. The customer will need to key in the Username then the login button will be activated. Then the customer will need to confirm SecureWord. After that the Password field will be displayed. After the correct password has been keyed in, the customer will be logged into the account.

Table 1 below shows the summary of security parameters that have been used by the authors bank preferences.

Table 1. Security parameters associated with the bank preferences

Bank	Security parameters
A	Secure phrase
B	Security image, security phrase
C	Secure word
D	Security image, security phrase
E	Secure word

Table 2 below shows the summary of each bank authentication process flow.

Table 2. Authentication process flow

Bank	Security parameters
A	User ID➔ Personal Login Phrase ➔ Password
B	Username➔Security Image&Phrase➔Password
C	User ID ➔ Secureword ➔ Password
D	Username➔Security Image&Phrase➔Password
E	Username➔Location Permission➔SecureWord ➔ Password

4.2 Transaction

This section compares the fund transfer methods of five different banks in Malaysia: Bank A, Bank B, Bank C, Bank D, and Bank E. To transfer funds using Bank A, customers must choose the DuitNow menu and select their ID type as account number. They also must choose whether they are transferring funds to the same bank or another bank. For other banks, they can use either DuitNow or IBG options. To complete the fund transfer, they must use the SecureSign option on Bank A's mobile app. For Bank B, customers can choose from various options such as DUITNOW, own transfer account, third party, and other account. They can also select the payment mode as now, later, or recurring payment. They need a key activation from the mobile app to make the fund transfer successful. For Bank C, customers can choose DUITNOW/transfer from the menu and enter the account number and the transfer method. If they are transferring funds to another bank, they must select the bank name from a list. They need a SecureTAC from the mobile app to finish the fund transfer on the website. For Bank D, customers must choose the DUITNOW option and then select the transfer type such as another bank, oversea account, mobile number, or ASNB. They have to verify the transaction using the mobile app. For Bank E, customers can choose DUITNOW and then select the transfer type such as bank account, mobile number, NRIC, Army/Police ID, passport, or business registration number. If they choose an account number, they must select the bank name from a list. They also need a mobile app authorization for Bank E.

4.3 Bill payment

Bank A's customers will need to choose their favorite bill if there is any other bill, or multiple bill payment. Bank B does not classify the payee code which refers to the corporation code. There are almost one hundred and twenty corporations code that can be selected including all the telecommunication companies (telcos), utilities provider, insurance company, financial services as well as ~~PBT~~. Before using the multiple bill payment options, customers need to add the bill into favorite first.

For bank B bill payment option, customers can choose from these four options which are education financing, online shopping, telecommunication companies (telcos) and utilities. There is only one option for education financing and online shopping which is PTPTN and its corresponding partner. While there are only four telcos and seventeen utilities available for the bill payment.

For customers at Bank C, they can choose from the pay&transfer option, and then choose the pay bills option. Customers can enter a new biller name or code; or can just select from their favorite biller.

Customers at Bank D can choose to pay and select the payee from the list either payee or JomPAY. If there is no favourite account on the list, they can choose from the dropdown list provided by Bank D. There are lots of options available at Bank D compared to previous banks.
Lastly, for Bank E, there is only one option available for bill payment which is by using JomPAY option. With this option, customers need to know the biller code that can be found in the account statement.

Table 3 below shows the summarization of bill payment process for each bank.

Table 3. Bill payment process for each bank

Bank	Bill Payment Process
A	Favorite Bill / Multiple Bill Payment
B	Education Financing / Online Shopping / Telcos / Utilities
C	Pay & Transfer ➔ Pay Bills ➔ Select Biller
D	Pay & Transfer ➔ Payee / JomPAY
E	JomPAY Option

As a conclusion for this section, all processes that have been performed must be authenticated using each bank's mobile application that has been installed on a registered device. Each bank only allows one application to be registered on a device.

5. DISCUSSIONS

As mentioned at the beginning of the paper, there are two research questions that need to be answered before the paper concludes. As stated at RQ1, to identify the security measures that have been implemented by each bank. For the authentication mechanism that is being performed by al five banks, it showed that all five banks have implemented various security measures to protect their customers' accounts. These measures include the use of personal login phrases, security images and phrases, on-screen keyboards, and alerts for incorrect password attempts. Bank A asks for a User ID and displays a personal login phrase for verification. Bank B prompts a safety and precaution window and displays a security image and phrase. Bank C requires the entry of a User ID and verification of a secureword. Bank D displays a security image and phrase after the entry of a username. Bank E asks for permission to collect location information before displaying its login screen.

Generally, all banks implemented similar security measures such as username and password for authentication with additional either security image, security phrases or secure word. For other processes such as fund transfer and bill payment, all banks protect the customers by requiring customers to approve the desired processes using application that has been installed on a registered device.

Meanwhile as RQ2, as to compare the security implementations of selected banks, the five banks that were chosen to have put in place a variety of security measures to safeguard their customers' accounts. All five banks offer the DuitNow option for financial transfers, and all five banks demand some sort of mobile app authorization to accomplish fund transfers. However, each bank employs a different set of authentication methods. While Bank B prompts a safety and precaution window and displays a security image and word, Bank A requests a User ID and displays a personal login phrase for verification. Bank D displays a security image and phrase after entering a username, while Bank C requests the input of a User ID and the confirmation of a secureword. Before presenting its login screen, Bank E requests consent to collect location data. Customers have other choices for paying their bills as well. Customers of Bank A can choose their favorite bill to pay or pay numerous bills at once, whereas Bank B offers a variety of transfer and payment methods. Customers of Bank C can select the transfer method and the destination bank from a list when transferring to another bank, while Bank D offers a variety of transfer options and requires mobile app authentication. Customers must have the biller code, which can be found on the account statement, in order to use Bank E's single bill payment option, which is the JomPAY option.

6. CONCLUSIONS

The researchers found that all five selected bank implemented similar security level as simplified in Figure 1 below. At level 1, customers need to provide username and password to login. Additionally, all these five banks provided extra security measures, either security phrase, security image or secure word to get customers authenticated. After login credentials successfully validated using the banking system database, then customers can get log into the banking system. To perform services such as fund transfers, balance inquiries, and so on, customers will be authorized to perform the processes or services after approving using the processes credentials using mobile application that has been installed on a device that has been registered during the application installation process.

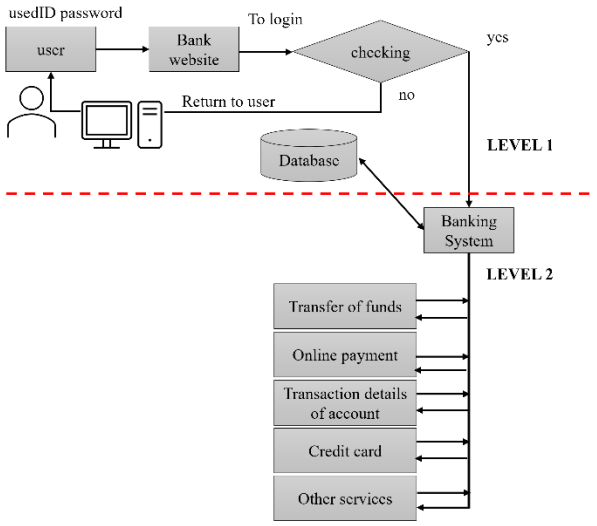

Fig 1 : Authorization Level in Internet Banking Service

All banks have already implemented security measures accordingly to protect the customers' data and account. Meanwhile, customers also need to be aware about the cyber security threats while using online banking services and keep up to date to the bank's security awareness program.

7. ACKNOWLEDGEMENT

The authors would like to thank all School of Computing members who were involved in this study. This study was conducted for the purpose of Online Business, Financial Technology & Cybersecurity Research Project. This work was supported by Universiti Utara Malaysia.

8. REFERENCES

[1] Blogmalaysia.com, "Online Banking Fraud Cases In Malaysia," 2023. [Online]. Available: https://blogmalaysia.com/online-banking-fraud-cases-malaysia/.

[2] R. Loheswar, "Major data breaches in Malaysia in the past 24 months," *Malay Mail*, 31-Dec-2022. [Online]. Available: https://www.malaymail.com/news/malaysia/2022/12/31/major-data-breaches-in-malaysia-in-the-past-24-months/47722.

[3] M. Basyir and H. N. Harun, "Online scam cases increasing in Malaysia," *New Straits Times*, 26-Sep-2022. [Online]. Available: https://www.nst.com.my/news/nation/2022/09/834531/online-scam-cases-increasing-malaysia.

[4] MalayMail, "Kaspersky: Phishing attacks on the rise in Malaysia, SE Asia," *Malay Mail Sdn. Bhd*, 11-Oct-2022. [Online]. Available: https://www.malaymail.com/news/malaysia/2022/10/11/kaspersky-phishing-attacks-on-the-rise-in-malaysia-se-asia/32996.

[5] S. R. Mohd Kassim, "Measuring the Effectiveness of Phishing Detection Tool: Comparative Study on Pattern Matching and User Rating Technique," *J. Comput.*, vol. 14, no. 4, pp. 302–310, 2019.

[6] F. H. Chandio, Z. Irani, A. M. Zeki, A. Shah, and S. C. Shah, "Online Banking Information Systems Acceptance: An Empirical Examination of System Characteristics and Web Security," *Inf. Syst. Manag.*, vol. 34, no. 1, pp. 50–64, 2017.

[7] S. R. Omar Ali, W. N. K. Wan Marzuki, N. S. Mohd Said, S. M. Abdul Manaf, and N. D. Adenan, "Perceived Ease of Use and Trust Towards Intention to Use Online Banking in Malaysia," *J. Intelek*, vol. 15, no. 1, pp. 107–114, 2020.

[8] S. Manoharan, N. Katuk, S. Hassan, and R. Ahmad, "To click or not to click the link: the factors influencing internet banking users' intention in responding to phishing emails," *Inf. Comput. Secur.*, vol. 30, no. 1, pp. 37–62, 2022.

[9] A. P. Khan, S. Khan, and I. A. R. Xiang, "Factors Influencing Consumer Intentions to Adopt Online Banking in Malaysia," *Bus. Econ. Rev.*, vol. 9, no. 2, pp. 101–134, 2017.

[10] N. Yildirim and A. Varol, "A research on security vulnerabilities in online and mobile banking systems," *7th Int. Symp. Digit. Forensics Secur. ISDFS 2019*, pp. 1–5, 2019.

[11] D. Ghelani, T. Kian Hua, S. Kumar, and R. Koduru, "A Model-Driven Approach for Online Banking Application Using AngularJS Framework," *Am. J. Inf. Sci. Technol.*, vol. 6, no. 3, pp. 52–63, 2022.

[12] S. PAKOJWAR and D. N. J. UKE, "Security in Online Banking Services – A Comparative Study," *Int. J. Innov. Res. Sci. Eng. Technol.*, vol. 03, no. 10, pp. 16850–16857, 2014.

[13] M. D. Bhosale, "' Internet Banking Security Software ' Proposed Model," *Int. J. Res. Publ. Res. J. Sci. IT Manag.*, vol. 4, no. 7, pp. 54–74, 2015.

[14] B. N. Malaysia, "Financial Sector Participants Directory," 2023. [Online]. Available: https://www.bnm.gov.my/regulations/fsp-directory.