The 1st Saizu International Conference on Islamic Philantrophy
"Fundrising in Digital Era for Sustainable Community Development"
UIN Prof. K.H. Saifuddin Zuhri Purwokerto
July 3, 2023
Volume 1, July 2023

# Optimizing Financial Technology Literacy in Minimizing Phishing Threats (Case Study of Indonesian Sharia Bank Customers)

Andriani[1,*], Bambang Hermantoro[2]

Corresponding Author. Email: andriani@iainkediri.ac.id

[1]IAIN Kediri
[2]Postgraduate IAIN Kediri

**Abstract**

The rapid growth of technology has made people switch to making non-cash payments, and banks have made many breakthroughs in improving digital financial services/Financial Technology. Technological advances have both positive and negative impacts. Many technological crimes / Cybercrimes have emerged and continue to increase yearly in line with advances in Fintech, especially Phishing. Phishing comes from the word fishing, which lures victims into providing sensitive data, draining the victim's balance. Bank BSI is a Sharia Bank with the best assets and services in Indonesia, and one of its customers is affected by Phishing. The research method uses qualitative discrete, obtaining data from books, journals, and related issues. Digital financial Literacy combines financial and digital Literacy and manages finances appropriately using current technology. Digital financial attacks include Phishing, Whaling, Covert direct, Spear Phishing, and Clone. In May 2023, one of BSI's customers was affected by Phishing, draining a balance of Rp. 378 million, there was no compensation because it was not the fault of the BSI system. Digital financial Literacy continues to be improved by BSI. In opening accounts, customers are constantly reminded to keep sensitive data confidential. Corporate insights are also provided online via email, SMS, website, and social media, and BSI staff go directly to the field. Optimizing digital financial Literacy must be embedded from an early age considering that the target is the Customer. BSI is also working with the OJK, Bareskrim Polri, and Kominfo. So that the ITE Law will ensnare the Phisers and not disturb the Indonesian people.

**Keywords: Literation, Fintech, Phising**

## 1. Introduction

The development of information technology is now experiencing a rapid increase. Previously, information technology was only used on social media and presenting company biographical information. But now, almost all companies use this technology, one of which is to transact using the Internet. Starting from selling goods or trading what we know as E-

commerce (Tokopedia, Shoppe, Lazada, Bukalapak, FB Marketplace, etc.), in the field of transactions, there are already e-wallets (Gopay, OVO, LinkAja, Funds, I Pocket, etc.) in the world. Transportation (Gojek, Go Car, Grab bike, Grab Car, KAI Access, Traveloka, Tiket.Com, etc.).

Bank and non-bank financial institutions also warmly welcome the latest information technology. Many previously offline services have become online for cash deposit and withdrawal transactions, consulting with customer service, even though they are all online. The Bank continues providing offline services, especially for clueless and Premier customers. Financial Technology is a financial transaction service that fully uses technology. Referring to Bank Indonesia regulation Number 19/12/PBI/2017 concerning the implementation of financial technology, financial technology is the use of technology in the financial system that produces new products, services, technology, or business models and can have an impact on monetary stability, financial system stability or efficiency., smoothness, security, and completion of the payment system.

The progress of Financial Technology is prolific growth in Indonesian society, especially among millennials who know the use of technology, which facilitates and helps many things, can reach remote areas. (Finance, 2019) Technology has caused Indonesians to switch payments using non-cash in daily transactions.

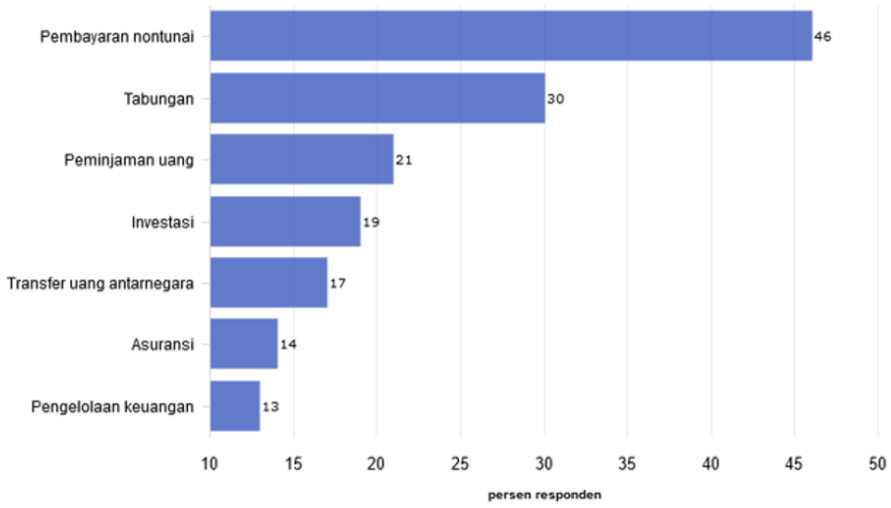
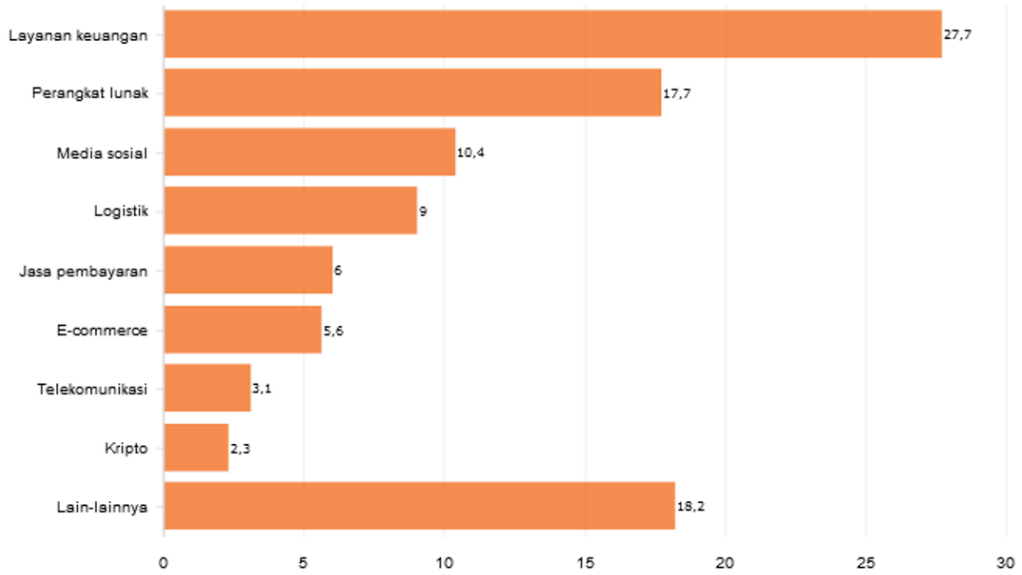



Diagram of digital financial services frequently used by ASEAN Residents in 2022

Based on databoks, from 2022, financial technology is experiencing significant growth. Fintech is more widely used for non-cash payments. On average, millennials aged 25-35 years, in terms of very modern technological advances, will bring up people with bad intentions who want to take advantage of technology, benefit from Fintech users, and become victims. (Winarsih, 2022) ) Technological progress, apart from bringing good, also brings negative sides. As sophisticated as technology must have weaknesses. Many smart people have bad traits that want to hack the system. Cybercrime is a crime carried out through today's technology. Before the advent of Phishing, which was more familiar with skimming (ATM duplication), skimming incidents have been known since the invention of the ATM. With so

many transactions without using an ATM, Phishing (stealing the victim's data) emerged. Phishing in Indonesia has claimed many victims, and the impact of Phishing has greatly disturbed the community.




Global Phishing Attacks Proportion Chart by Industry Sector 2022

Launch databoks.co.id phishing attacks topped the highest in the financial sector, mentioning phishing attacks reached 4.7 million reports. Databoks, "The Trend of Phishing Attacks Continues to Increase, Reaches Record Highs in 2022," 2023, https://databoks.katadata.co.id/datapublish/2023/05/17/tren-serangan-Phising-terusmeningkat-achievement- record-high-in-2022. In the third quarter of 2022, there have been 7,988 cases. The business and government sectors are the main targets. As reported by Republika.com OJK, at the end of the period January 1, 2022, to December 16, 2022, there were 7,104 complaints, and 6,896 from the Non-Bank Financial Industry (INKBI) sector and 88 from the capital market sector. These Phisers continue to target victims from E-Commerce and Fintech, remembering that in transactions and making payments as well as payments, all use today's technology. (REPUBLIKA, 2022)

With the very fertile growth of Fintech, Pisher's growth is also growing rapidly. Phishing is stealing customer data without hacking systems owned by Fintech or banking. Phishers steal data to get into the fintech system and drain victims' balances on a large scale. Considering that 86.9% of Indonesia's population is Muslim, around 237.53 million people are Muslim. (Databox, 2023) Fintech Syariah took steps to introduce how Indonesian people can stay alert to phishing activities. So that phishing reports do not increase yearly, many people are unfamiliar with the advantages and disadvantages of this technology. Then a re-literacy is needed about financial technology / digital finance.

Digital Financial Literacy combines Financial Literacy and Digital Literacy. Financial Literacy is managing or allocating finances appropriately. (Arianti, 2021) Digital Literacy is knowledge in utilizing digital media, communication tools, and networks. Digital Literacy includes Digital Skills, Digital Ethics, Digital Safety, and Digital Culture. (Ministry of Communication and Informatics, 2021) Digital Financial Literacy The ability of the public to

utilize digital financial services includes all products, services, technology, and infrastructure that allow individuals or companies access to payment, savings, and credit facilities boldly without the need to visit a bank office or deal directly with financial service providers. (Financial Services Authority, 2021) With Digital Financial Literacy, it is hoped that the Indonesian people can find out about earlier, Phishing attacks (Cybercrime).

Cybercrime involves hackers/hacking systems and data theft (Phishing, pharming, sniffing, money mule, and social engineering). Cyber Crime is a crime that uses computer and network technology. With criminal motives to damage the victim's reputation, creating physical and mental harm by utilizing the Internet, chatrooms, email, and mobile phones (SMS/MMS). Technology fraud aims to obtain information, passwords, and identities that we are more familiar with Phishing. Phishing is a digital technology crime aiming to retrieve information about victims via email, websites, social media, and text messages. In carrying out Phishing all activities using computers and internet networks, proficiency in computers and operating systems is the capital of Phishing, which includes Phishing Emails, Phishing Websites, and Phishing Malware. The program is implanted into the victim's computer without the victim's knowledge by tricking the victim into downloading an application or file on the Internet and observing the victim's habits. Without the victim's knowledge, Phishing can control the computer remotely. What you want can all be obtained.[12]

Standard of the Indonesian Ulema Council Number 117/DSN-MUI/II/2018 Regarding Information Technology-Based Financing Services Based on Sharia Principles. (Com, 2019) Sharia principles, free from prohibited transactions, products according to Sharia contracts, maintaining adab-adab (morals) in muamalah. Sharia Digital Bank, POJK Number 12/POJK.03/2021, in the legal umbrella, explains that a bank fully utilizes current technology or electronic channels in carrying out its operations. It no longer opens branch offices (physically) except for the head office, which is in the capital city. Looking at Sharia Economic Law, a bank is a trust which is obliged to maintain the security of data and funds that have been given to the public, which has been explained in Allah's word:

……فَإِنۡ أَمِنَ بَعۡضُكُم بَعۡضٗا فَلۡيُؤَدِّ ٱلَّذِي ٱؤۡتُمِنَ أَمَٰنَتَهُۥ وَلۡيَتَّقِ ٱللَّهَ رَبَّهُۥۗ …….

Meaning: …. If some of you trust others, then let those who are trusted carry out their mandate and let them fear Allah….

A bank's job is always to maintain the confidentiality of customer data and including public funds. (Hasanatul Munawarah, 2022) Financial Technology, owned by BSI, combines financial and technology services. All activities can be carried out without coming to the BSI office directly.

| Uralan | 2022 | 2021 | 2020* |
|---|---|---|---|
| Kas | 4.951.469 | 4.119.903 | 3.180.739 |
| Giro dan Penempatan pada Bank Indonesia | 31.778.458 | 20.563.580 | 21.527.933 |
| Giro dan penempatan pada Bank Lain-Neto | 2.475.917 | 1.841.551 | 8.695.805 |
| Investasi pada Surat Berharga-Neto | 57.841.271 | 67.579.070 | 49.105.637 |
| Tagihan Akseptasi-Neto | 476.589 | 159.880 | 292.789 |
| Piutang-Neto | 120.701.979 | 98.336.983 | 86.589.188 |
| Pinjaman *Qardh*- Neto | 8.867.013 | 9.081.400 | 9.054.373 |
| Pembiayaan *Mudharabah*-Neto | 1.001.957 | 1.592.314 | 2.598.787 |
| Pembiayaan *Musyarakah*-Neto | 66.450.946 | 53.903.123 | 50.896.175 |
| Aset yang Diperoleh Untuk *Ijarah* - Neto | 1.484.573 | 901.565 | 1.509.461 |
| Aset Tetap dan Aset Hak Guna - Neto | 5.654.698 | 4.055.953 | 3.397.075 |
| Aset Pajak Tangguhan | 1.675.103 | 1.445.324 | 1.109.281 |
| Aset Lain-lain-Neto | 2.367.465 | 1.708.435 | 1.624.281 |
| JUMLAH ASET | 305.727.438 | 265.289.081 | 239.581.524 |

* Disajikan kembali

Indonesian Sharia Bank Financial Report

PT Bank Syariah Indonesia Tbk is a merger of three Islamic banks in Indonesia. BSI assets have continued to increase every year. In line with digital financial services, BSI is the largest Sharia-based banking in Indonesia, occupying number 6 after Commercial Banks, becoming Islamic bank number 14 worldwide. (C. Indonesia, 2023) Even though it is the best regarding assets and services, it cannot be separated from phishing attacks.

## 2. Research Methods

The research study used the descriptive-analytical method with a qualitative approach. The researcher gets to try to explain the subjects and objects to be studied in the form of events/phenomena/symptoms from various sources of electronic print media and related information sites. Whereas secondary data is obtained from various sources published or shared on official websites, such as statistical data and fintech reports, identifying this information is related to problems (electronic media). (Zuchri Abdussamad, 2021) Source -sources of analysis data in journals, scientific papers, articles, reference books, and various other sources. The literature results can provide readers insight into phishing attacks in Indonesia, especially using financial technology services in banking.

## 3. Results and Discussion

### 3.1 Financial Tecnology Literacy

Financial Technology Literacy consists of Financial Literacy and Digital Literacy. Financial Literacy positively influences a person's financial behavior, such as properly managing or allocating their finances. Financial management, which includes financial planning, management, and control activities, is crucial for achieving financial well-being. (Arianti, 2021) Digital Literacy has the knowledge and ability of users to utilize digital media, communication tools, internet networks, and so on. Digital Literacy includes:

*3.1.1Digital Skill*

The ability to sort files on the Internet before downloading and find information whether it is true or false. In accessing and downloading files, you have to be careful whether they include dangerous files or not, official or illegal sites. Each file contains a virus.

On the fake site, an inducement tells you to download the file. After opening the file, you accidentally detect a *Trojan Horse Virus*, *a Trojan running* without the computer owner's knowledge, which damages the system and hacks the computer system. Usually, the computer will feel that it is running slowly and slowly disconnects itself. This is of utmost concern, especially on devices frequently used for digital financial transactions, so they are more careful downloading files. Various efforts and government companies to use legal applications and continue to remind the antivirus to be updated regularly.

*3.1.2 Digital Ethics*

Invite people not to comment negatively, share screenshots on social media, or share accident information directly. It is stated that hoax spreaders will be subject to the Criminal Code, Law No. 11 of 2008, concerning Information and Electronic Transactions (ITE). Whereas actions whose truth is uncertain are prohibited from spreading false news, inciting, inciting hatred, such as by mentioning race and ethnicity, which results in conflict, while in the financial world don't be affected by uncertain issues, such as issues regarding banking, that Bank X is going bankrupt and failed to pay. Hence, customers flocked to withdraw all their savings. Before reading, visit a legal site with a trusted source.

3.1.3 Digital Safety.

Create a secure password using a combination of letters, numbers, and punctuation marks, the ability to distinguish emails containing spam/viruses/Malware. Digital safety is more about maintaining the confidentiality of sensitive data such as PIN, OTP, Password, Username, and KTP.

Users of technology services to be more careful, especially Malware (*Malicious and Software*), software that is distributed via the internet network. Malware, including Sabotage and Extortion, is a crime with a damaging internet network. Malware can move on computers and cell phones. The 2021 Digital Literacy National Movement in Bandung explained that Malware is an application without a permit, moving freely without the owner's knowledge. The Malware aims to obtain sensitive data information and gain access to main computers in the financial world, draining company customer balances by asking for very high imbalances.

*3.1.4 Digital Culture.*

Write names when reposting, reconsider when reposting, and do not mention ethnicity, religion, and bad words that cause conflict. (Ministry of Communication and Informatics, 2021) In hate speech mentioning ethnicity or community, as

experienced by Yogja students, when queuing in one BBM, complaining on social media, Twitter indirectly insults Yogja residents. In the end, the student was sanctioned by Yogja residents. Meanwhile, financial services complain about Bank X's services and provide commentary on social media status that offends companies and customers.

### 3.2 Optimizing Financial Technology Literacy in Minimizing Phishing Threats

Financial Technology Literacy, is an expertise in organizing, managing, and allocating the right finances that is also safe, using high digital technology. To facilitate all activities of the customer. Financial technology cannot be said to be safe from cybercrime, even though the system owned by customers already has high protection, but customers are still negligent in making transactions by visiting illegal sites, resulting in sensitive data leaks (Phishing Attacks), Phishing, namely stealing data without destroying the existing system , various ways to trick customers via website, sms, email, telephone. The following digital literacy about phishing includes:

*3,2.1 Whaling & Covert direct*

*Whaling* is similar to spear phishing but has a different goal of targeting victims with a high position or position in an organization, such as subpoenaing courts, etc. Whereas Covert Direct, this technique is smoother, almost like the original, using a similar official site with creative pop-ups. When the victim uses more of the website, it isn't easy to distinguish, so they don't understand the original information.

On January 30, 2023, Phishing began to take its toll. Phishers chose the Bali DPRD organization from the PDIP (*Phising Whaling*) party, which drained balances of up to Rp. 654 million, which started on social media Facebook and found links on behalf of banks related to saving savings (*Phising Covert direct*), make transactions with mobile banking. The Head of Public Relations of the Bali Police presented the explanation.

*3.2.2 Spear Phising & Clone Phising*

*In Spear Phishing*, perpetrators who target their victims have clear characteristics and specifications, Spear/spear. This spear is aimed at only a few people. The success rate is also very high. And Clone Phishing is a way of tricking victims by using email, SMS, Whatsaap Chat, telephone in the form of valid messages as the original by changing the file to be different from the email.

On May 31, 2022, the victim's balance was drained of up to Rp. 1.1 billion for phishing incidents that chose to focus more on one married couple living in Padang, West Sumatra (*Spear Phishing*). The way to send a message in the WhatsApp chat acts as a bank call center (*Clone Phishing*) to quickly update the data. Phishers send the form via a link. If not done, a transaction fee of IDR 150,000 will be charged. Explained by the West Sumatra Regional Police

On December 25, 2021, Phishers targeted their victims at recitation organizations that have communities. Phishers act as a call center *(Clone Phishing)*, which provides information on getting prizes, promos, and bonuses to respond immediately. They will be given another

(Clone Phishing) if they don't respond. After purchasing, almost all study groups get the message, then the day they complain about receiving inflated bills on online loans, purchase transaction history on e-commerce Bukalapak. Traced by related parties, Phiser got the contact from Facebook.

The Bank and the Government have made efforts to eradicate Phishing. Here the Bank directly cooperates with Kominfo and Cyber Bareskrim Polri. Kominfo blocks sites/websites and contacts that are detrimental to society. Bareskrim acts to prosecute Phisers under the ITE Law, which fines and criminalizes according to charged action.

Banks and financial institutions, in dealing with Phishing, have been carried out since the beginning of opening accounts so that they remain aware of sensitive data owned by account holders and are smart and careful in every transaction, especially online. Continuous efforts by sending SMS, email, official website, and advertisements on ATM screens, and 24-hour customer service is ready to help if there is a suspicious transaction.

## 3.1 Optimizing Financial Technology Literacy in Minimizing Phishing Threats to Indonesian Sharia Bank Customers

### *3.3.1* Phishing on Indonesian Sharia Bank Customers

Phishing is the crime of stealing sensitive data, especially from bank account holders. The goal of phishers is to get account balances, many reports are obtained, and every year it continues to increase. Those who are more numerous in the Spear Spising community have high success.

BSI was not spared from phishing attacks, as reported by voi.id BSI Semarang media that one of BSI's customers was identified as Phishing. The Customer complained of losing his balance of IDR 300 million in April 2023. Here, there is no connection/relationship with the problem system they have by BSI. It is known that the details are IDR 378 million. This information was obtained from social media Twitter, with the upload of proof of transaction, from an Islamic bank (BSI). (Voi. id, 2023)

PT Bank Syariah Indonesia Tbk, Describes the incident experienced by a friend who became a victim of Phishing which suddenly drained a balance of IDR 378.25 million in April 2023. It has nothing to do with the system owned by BSI and explains to always be vigilant in every transaction. (Instagram, 2023) From the explanation above, Phishing is no compensation from Fintech and banking, banking/fintech can only help trace transactions and file documents/evidence to the obligatory party. As reported by IDX Chanel, with the recent rise of Phishing in Indonesia, customers who are victims of Phishing will not receive compensation. The error is not in the banking and fintech systems. Who is the secretary of the BUMN Bank company. (Channel, 2022)

### 3.3.2 Financial Technology Literacy for Indonesian Sharia Bank Customers

The Indonesian Syariah Fintech Association (AFSI) is a fintech organization in Indonesia that has legal entity number AHU-0001911.AH.01.07 of 2018, which the Minister of Law and Human Rights issued. AFSI was formed by identifying the strengths of Sharia fintech in Indonesia, which provide riba-free services, in addition to advocating for fintech start-ups in conveying

aspirations and supporting the development of Sharia fintech. Members consist of various Islamic banks and other Islamic financial institutions, members of BSI, Muamalat, Aladin, Brk Syariah, Aminin, Arah Muslim, etc. (AFSI, 2023)

PT Bank Syariah Indonesia Tbk is a Sharia-based state-owned bank ranked number 6 as one of the largest banks in Indonesia. in terms of assets, services, and security systems.

As for the efforts provided by BSI, what I got at a BSI branch is that before obtaining an ATM PIN and activating mobile banking, the ATM PIN is packaged securely and confidentially. Those who can open it alone may not be represented. While the Customer himself makes all mobile banking, customer service only guides us when experiencing problems. Customer service always reminds us to stay alert for every transaction, checks transactions periodically, and strictly prohibits giving sensitive data (PIN, User ID, transaction Password, and OTP).

Apart from the customer service providing direct explanations, the company does not stop reminding via, Not forgetting, offers from the Bank to activate direct SMS from BSI when a customer transacts more than a certain nominal value. If you do not make a transaction, immediately contact the call center to complete the account. The company also continues to remind customers through social media, as reported by Facebook media, to make transactions safely.

Always protect all sensitive/personal data, starting from PIN, Password, User Id, and OTP.

a. Suggest changing your PIN and Password periodically.
b. To periodically check transactions, if there are suspicious transactions, immediately contact the call center.
c. Activate sms and email notifications.
d. Avoid VPN apps and free Wifi. (Facebook, 2021)

Facebook also posts frequently and reminds phishing alerts to be careful when surfing the Internet and unknown apps. (Facebook, 2022)

Launching the BSI Instagram account, there is a way to discover phishing attacks earlier, so customers can quickly discover whether this is phishing. (Facebook, 2022)

a. Prohibit visiting sites that are not clear on behalf of BSI, as well as explain that the BSI site is only one www.bankbsi.co.id besides that to ignore.
b. The second explains sensitive data, so it is forbidden to give it to anyone, even if an officer claims to be a BSI employee. That BSI has never done this.
c. To be careful about accepting any offers, double-check most of these offers via WhatsApp and social media chat. (Instagram, 2022)

The banking sector also went straight to the field by introducing the importance of managing digital finance and maintaining the confidentiality of sensitive data owned by customers, by holding seminars on campus and in the community. Such as the recitation of mothers and the environment of Islamic boarding schools, the contents of campus seminars, etc

### 3.3.3. Optimizing Financial Technology Literacy for BSI Customers

Digital financial Literacy is the client's ability to manage financial levels further by using Smartphone and Computer digital devices, the client's analytical ability to understand, access, evaluate and use information effectively before using the technology. Low digital financial Literacy makes patients unable to identify whether the information is correct. Low digital financial Literacy makes patients easily influenced and unable to identify and catch false information. To overcome this problem, it is very important to increase digital financial Literacy, seeing that the current era is all digital-based:

a. Learn from trusted sources.

In obtaining information that already has good accreditation, ensure the source has a reputation and accurate information. Many fake sites resemble the original, from the appearance to the writing of almost perfect words. The way to find out earlier is by looking at the brochure provided by BSI Customer Service or on the baleho on the streets that the official website address must be included. The second is that BSI only has a website address https: www.bankbsi.co.id/. At the end of the site, there is …..co.id/, which is a company-owned paid domain site, when downloading the Mobile Banking application. If you can't tell the original one, use the barcode on the BSI bank brochure or ask for help directly from the nearest branch, Customer Service, Call Center 24, and Chatroom on the official website. For secure transactions or shopping, use e-commerce with a good track record in Indonesia, such as Tokopedia, Shoppe, Traveloka, Tiket.com, etc.

b. Improve information-seeking skills

Improving sustainable online skills, learning by searching for information effectively and efficiently, and obtaining accurate and fast information. This allows BSI customers to have valid information, such as knowledge about security in managing sensitive data regularly and the latest insights about BSI, usually posted on website pages and social media. BSI customers are advised to visit the official website https://ir.bankbsi.co .id/ or on social media, Facebook, Instagram, and Twitter. What distinguishes fake social media from not is looking at their followers. Real social media routinely posts activities and knows if there is still confusion at the nearest branch of Customer Service, Call Center 24, and Chatroom on the official website.

c. Improve analytical skills

Analytical ability is the most important factor, recognizing the truth of information sources and knowing the intent and purpose of these sources. The ability of BSI customers to analyze information that must be able to differentiate, such as SMS Banking, Whatsapp, Email, and connecting telephones. How to find out fake SMS Banking, Email, and Telephone, fake SMS senders always include a cellphone number. In contrast, the original SMS is not a direct cellphone number. The name of Bank BSI does not provide a number, and it cannot reply to the SMS. The sending conversation is carried out by the system automatically. A prepaid,

original email seen by email address can be seen directly as BankBSI@bsi.co.id, which indicates the original email ….@bsi.co.id is a paid company email. Whatsapp is almost the same as BSI's direct name. Chatroom is provided on the official BSI website only if something else is fake. The last is a telephone. BSI call centers always use office telephones to contact their customers. We know that office telephones pay higher than regular telephones. The telephone number first with the area code and fewer digits like 021…. It is the Jakarta area code.

d. Cyber Increase understanding of Cyber security

Cybersecurity capabilities, being alert to Malware, Phishing, and hacking attacks. Devices used by BSI customers are expected to have high security and licenses before using cell phones, laptops, and computers. For one of the Production Devices owned by the USA, namely Apple, which has a different Algorithm system than other devices, if another device enters, it cannot run without going through their license. The Android system has the best hardware for other Windows original devices that can update automatically. The best device is one way to prevent other applications from entering without our knowledge. These applications, such as ransomware and Trojans, can run and be controlled remotely without our knowledge. With a good device system owned by BSI customers, BSI customers remain vigilant, such as visiting websites and opening an email linked to a website address, a good security system for hackers to have trouble hacking, one of which is how to send an illegal website. The website invites the Customer to write sensitive data, which we are more familiar with Phishing. Maybe a good and safe device has a special price, but seeing the incident, BSI Semarang customers were hit by phishing attacks, draining hundreds of millions of balances. Maybe you can reconsider this special device.

e. Get involved in online communities.

Joining an online or technology community is a discussion forum to find out other people's experiences in dealing with a problem, share knowledge, get more information, and build a network. In addition to information and insights obtained by BSI customers, information obtained from others is very important, considering our limited knowledge. Sometimes people know first, while we don't know, such as the https://ifsoc.id/ community, discussion forums that discuss the development of Fintech in Indonesia, https://fintech.id/id activities about recent fintech collaboration and innovation, UNS fintech which is held by students about insights into the use of Fintech.

f. Keep learning and updating your knowledge.

Because technology continues to develop rapidly, knowledge of digital financial management is needed, starting from reading books, articles, and courses on topics regarding the development of digital financial technology. BSI customers continue to update information regularly. Many digital financial literacy books are now easy to obtain, can be downloaded anytime, and are constantly updated. Because the government now sees low digital financial Literacy, free books have been distributed on the Internet.

POJK Consumer Protection Number 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector. As for the points in POJK Number 77/POJK.01/2016, it also regulates consumer protection, General.

a. Pasal 24, Explanation that a Virtual Account is a technology-based service providing facilities for borrowers.
b. Pasal 29 explains that all lending and borrowing activities must be fair, transparent, open, and without conflict resulting in unilateral harm.
c. Pasal 30 - 32, In lending and borrowing transactions, all must be easily understood using polite Indonesian accepted by all groups. The explanation is clear, without any words that are difficult to understand.
d. Pasal 34, In the service, the criteria given must follow the portion of the candidate bids.
e. Pasal 35 products must have a license supervised by OJK.
f. Pasal 36, the lender must provide a clear and standard agreement based on the established law.
g. Pasal 38 An operational activity already has Pindar standards, which already has a permit from the OJK and complies with applicable laws. Starting from transaction activities and grouping electronic documents.
h. Pasal 40, organizers, accommodated user complaints, are required to make periodic reports to the Customer submits a response or report, it must be prepared periodically and regularly which will be forwarded to the OJK.[8]

3.3.4 Financial Literacy and Inclusion

Pasal 33, all activities in the context of increasing financial Literacy and inclusion are required to hold socialization 12 times in different cities and provinces, six on the island of Java, and six outside Java. Maintain the confidentiality of the disclosure of client personal data with the approval determined according to the applicable law, and notify in the event of a failure or delay in writing.

3.3.5 Confidential Data and Personal Data

a. Pasal 26 Explanation in managing customer data, confidentiality must be kept because it concerns personal data, all transactions must be stored securely, and data must be destroyed at certain times.
b. Pasal 39, Organizer, explains the prohibition of providing data to any party to users or third parties.

Phishing is an activity outside of fintech and banking financial managers. This is the confidentiality of data owned by customers that is provided and used by other parties. There are no data leaks and system damage to related banks and Fintech. Like the father's account book, the transaction password and user-id were also written there because he put them carelessly. His nephew finally found it and, at the same time, endangered the balance. While Phishing uses network and electronic media, the victim accesses website info from email, SMS, social media, etc., which can resemble the original website. Victims unintentionally provide personal and sensitive data.

The banking sector has provided much insight into Phishing, from the official website, SMS appeals, introduction to email insights, and social media.

The effort provided is in addition to protecting customers so that they continue to be vigilant every time they visit websites and information. You have to be observant and thorough in checking email, sms, and live chat, whether social media is an official account or not, keeping everything confidential regarding PIN, OTP, CVV (*Credit Card*) banking data, and especially personal data, the latter often changing your PIN regularly. (Facebook) , 2021)

Victims launching databoks.com data are known to have a lot of difficulties distinguishing whether this is phishing or not. If you are still confused about this, it is advisable to immediately contact the call center / live chat on the official fintech and banking websites, usually listed in the passbook or fintech/banking brochure. Besides being favored to be more careful surfing in cyberspace, if you have already turned off your cellphone and laptop as soon as possible so that it doesn't recover anywhere, it is recommended that the system used by customers has the most advanced system, which has a data protection license that is always maintained. Like Apple for Android and original Windows, antivirus is always updated regularly. The last is about the user id, OTP, and transaction password. Fintech and banking have never asked for this sensitive data, so if someone asks, report directly to the Bank so that the Bank will follow up with the Interpol authorities (UU ITE) to carry out a permanent blocking if Phishing (Cybercrime) is identified. OJK, Kominfo, and Cyber Criminal Investigation Police continue to fight Phishing. It's not just digital financial institutions that are detrimental to government institutions that are also affected.

## 4. **Conclusion**

Digital financial Literacy is a combination of financial Literacy and digital Literacy, which aims to manage finances properly using high technology, which is easier. What must be considered is to avoid Phishing. Phishing is the theft of data owned by consumers. First, whaling targets more victims who have positions or officials. Both Covert direct by using a website that resembles the original so that victims fill out the form. Spear Phishing has high success because it focuses on only one criterion. Finally, Clone Phishing tricks victims with direct calls, WhatsApp chat, social media chat, SMS, and telephone.

Bank Syariah Indonesia is the largest Bank in Indonesia regarding assets and services implementing sharia. One of the customers cannot be separated from Phishing. In April 2023, the Customer's balance was drained by up to IDR 378.25 million. The Bank did not provide compensation because the fault was not the banking system. Efforts by Bank Syariah Indonesia to continue to increase vigilance. Commemorating Phishing continues to increase every year. In opening accounts, customers are constantly reminded to keep sensitive data confidential. Companies continue to provide insight online via email, SMS, website, and social media. The Bank went directly to the field, bypassing invitations from universities, communities, and community organizations. In addition to bank literacy, optimizing customer financial literacy must be improved and instilled from the start considering that the target is direct customers, not banks. The Bank also cooperates with OJK, Bareskrim Polri, and Kominfo. So that the ITE Law will ensnare the Phisers.

**References**

AFSI. (2023). *Asosiasi Fintech Syariah Indonesia*. https://fintechsyariah.id/id/members

Arianti, B. F. (2021). *Literasi Keuangan* (W. Kurniawan (ed.)). CV. PENA PERSADA.

Channel, I. (2022). *Hati-hati Phising, Berikut Penjelasan Bank soal Ganti Rugi*. https://www.idxchannel.com/banking/hati-hati-phising-berikut-penjelasan-bank-soal-ganti-rugi

Com, T. (2019). *Dorong Akses Keuangan Syariah, Ma'ruf Amin Bicara Fintech*. https://bisnis.tempo.co/read/1175257/dorong-akses-keuangan-syariah-maruf-amin-bicara-fintech

databoks. (2023). *Jumlah Populasi Muslim di Kawasan ASEAN (2023)*. https://databoks.katadata.co.id/datapublish/2023/03/28/ini-jumlah-populasi-muslim-di-kawasan-asean-indonesia-terbanyak#:~:text=Laporan The Royal Islamic Strategic,mencapai 237%2C55 juta jiwa.

Databoks. (2023). *Tren Serangan Phishing Terus Meningkat, Capai Rekor Tertinggi pada 2022*. https://databoks.katadata.co.id/datapublish/2023/05/17/tren-serangan-phishing-terus-meningkat-capai-rekor-tertinggi-pada-2022

Facebook. (2021). *Bank Syariah Indonesia*. https://www.facebook.com/bankBSI.ID/posts/maraknya-modus-penipuan-dan-phising-via-mobile-banking-pasti-bikin-kita-semakin-/10161857662782501/

Facebook. (2022). *Waspada Terhadap Modus Phising BSI Net Banking*. https://www.facebook.com/bankBSI.ID/photos/a.10152398373472501/10162600746162501/?type=3

Hasanatul Munawarah, M. Y. (2022). *Bank Digital Syariah Analisis* (P. Komarudin (ed.)). PT. Borneo Development Project Anggota.

Indonesia, C. (2023). *Mantap! BSI Melesat Jadi Bank Terbesar ke-6 di Indonesia*. https://www.cnbcindonesia.com/market/20230222112734-17-415955/mantap-bsi-melesat-jadi-bank-terbesar-ke-6-di-indonesia#:~:text=Saat ini BSI berada di peringkat 14 bank syariah di seluruh dunia.

Indonesia, F. S. (n.d.). *PT Bank Syariah Indonesia Tbk*. https://fintechsyariah.id/id/members/25857a60-9dee-11ec-8853-4135bf146558

Instagram. (2022). *Tips Agar Sahabat Semua Nggak Jadi Korban Phising*. https://www.instagram.com/p/CY--WiSLIij/?id=phising_okt22.jpeg

Instagram. (2023). *Nasabah Lapor Simpanan Rp 378 Juta Tiba-tiba Raib, BSI Buka Suara*. https://www.instagram.com/p/CsNwPntp4rN/

Kementerian Komunikasi dan Informatika. (2021). *Status Literasi Digital di Indonesia 2021* (S. L. V. Zabkie (ed.)). KOMINFO.

Keuangan, O. J. (2019). *Lembaga Jasa Keuangan Lainnya (Seri Literasi Keuangan)*. https://sikapiuangmu.ojk.go.id/FrontEnd/LiterasiPerguruanTinggi/assets/pdf/Buku 7 - Lembaga Jasa Keuangan Lainnya.pdf

Liputan6. (2023). *Daftar Terbaru 10 Bank Terbaik di Indonesia Versi Forbes*. https://www.liputan6.com/bisnis/read/5259051/daftar-terbaru-10-bank-terbaik-di-

indonesia-versi-forbes

Otoritas Jasa Keuangan. (2021). *Strategi Nasional Literasi Keuangan Indonesia 2021 - 2025 1*. OJK.

REPUBLIKA. (2022). *OJK Ingatkan Waspadai Kejahatan Skimming, Phising hingga Soceng*. https://ekonomi.republika.co.id/berita//rni0gd383/ojk-ingatkan-waspadai-kejahatan-skimming-phising-hingga-soceng?

Voi. id. (2023). *Nasabah Kehilangan Rp300 Juta, BSI Sebut Ada Indikasi Phising*. https://voi.id/ekonomi/279806/nasabah-kehilangan-rp300-juta-bsi-sebut-ada-indikasi-phising

Winarsih, T. (2022). *Memaknai Perkembangan Fintech Syariah melalui Sistem Akad Syariah*. *1*(3), 130–142.

Zuchri Abdussamad. (2021). *Metode Penelitian Kualitatif* (P. Rapanna (ed.); 1st ed.). syakir Media Press. https;//repository.ung.ac.id