Cyber Security

Preventive Measures

Staying safe and secured in the digital world

We all love convenience. With digitalisation, we can now perform banking transactions at our fingertips.

But it also comes with a price. With online threats such as phishing, man-in-the-middle attacks, and malware, we at MBSB Bank have the responsibility to provide solutions to combat these threats and prevent our customers from being victims.

In this booklet, you will learn how to safeguard your banking and personal information while staying updated on the latest cyber security features.

Practice Safe Banking

Secure your data when performing transactions online. Here are some steps to ensure the safety of your accounts.

Check Your URL Address

Always make sure you enter the correct web address in your internet browser bar.

Verify Security Image and Phrase

Always verify **SECURITY IMAGE AND PHRASE** displayed on the login page before entering your password. If it does not match yours, click the **"Not Me"** button.

Enter the Correct TAC Number

Ensure the TAC number entered is the same as the one in your SMS.

Unique Password and Username

Avoid creating passwords and username that are similar to your security phrase.

Devices

Secure your computer and keep it updated.

Unsolicited E-mail

Avoid clicking link through e-mails.

Location

Access your accounts from a secured location. Do not access from a public WiFi.

Log Out

Always log out when you are done.

Protect Your Card Info

Keep your card safe and do not reveal the 16-digit debit card number and ATM Pin.

Username, Password and TAC MUST be protected.
Scammers would not stand a chance if you take precautionary measures.

Password-security Attack

Password-security attack is a trial and error scam. The scammer will try to guess the username and password of your internet banking.

Strengthen Your Username

Avoid using combinations of name and your year or date of birth.

Avoid using the same username similar to your social media.

Don't Share Your TAC

Do not forward or reveal your TAC to anyone.

Strengthen Your Security Phrase

Do not set your security phrase similar/same to your password or vice versa.

Strengthen Your Password

This usually happens to those who have short or easy passwords. Use alphanumeric passwords that are not related to you, your background and account information.

Avoid using the same password for all your online accounts (e-mail, social media).

Phishing

If it's too good to be true, it might be a fraud.

If you receive any emails claiming that your bank account has been blocked/ dormant/ under maintenance, do not click the link and report to the Bank.

Phishing is not limited to email but also include sms, WhatsApp or other social communication tools.

Inspect the full URL, phishing website might look like MB5B.COM where S is replaced with 5 which resemble the actual URL.

Do not click on any links from third party sources to download app. Never login to your internet banking from any links you received either via SMS, WhatsApp, e-mail etc.

Practice Safe Browsing

Ensure browser padlock icon is locked

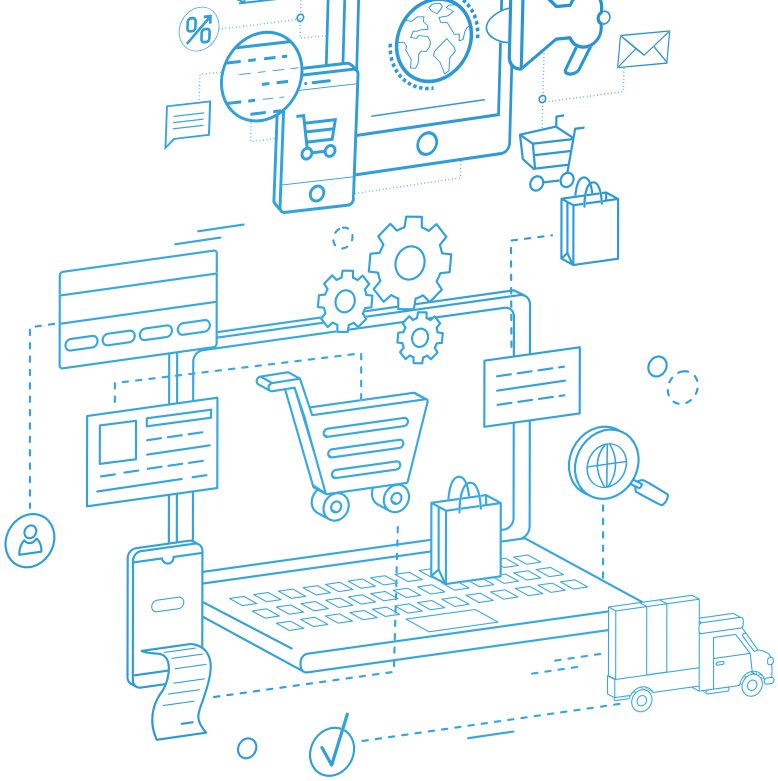
Always key in the full URL rather than from external link.

If you're a victim:

Change your compromised password immediately.

Disconnect from your network (computer or device that have been infected with malware).

This requires more than just unplugging your device power source and deleting the e-mail. It will not stop any damage the attack may have caused.



Online Business Scam

Online transactions are meant to make our lives easier but they do pose certain risks. Here are some scam types and prevention tips.

Seller Scams

Fraud

When payment is made for the product but it is not delivered.

Hidden Charges

When the buyer is asked to pay for unnecessary tax or asked to refund after making purchase.

Parcel Scams

When you receive an unknown parcel from an unknown address.

False Pricing

If the price is “Too Good To Be True” - don’t buy.

Online Threats

If you have been pressured or threatened by a seller/ buyer - don't proceed with the business.

Buyer Scams

Upfront Payment

If you are a seller, do not make any form of payment (tax/custom clearance) on your buyer's behalf.

Cash on Delivery (COD) Scams

When someone claims to be a delivery person and asks for cash on delivery when no order or purchase has been made.

Scan to watch

Spot The Scam: Fake Merchants

Call Scams - Prohibited Parcel

Prohibited parcel scam is an act where scammers will claim that the victim had ordered/ received/ sent prohibited parcels. They will threaten victims by impersonating the police and force victims to transfer money, reveal TAC number and internet banking credentials.

Modus Operandi

1

Scammers will call victim as POS Malaysia personnel claiming that the victim had ordered/ sent/ received prohibited parcels and then ask for the victim's IC & debit/ credit card details.

2

If the victim stays on the line, the call will be transferred to another line, supposedly to be the police.

3

The scammer impersonating the police accuses the victim of a crime.

4

They will offer to help, but the victim must follow their orders.

5

They will ask the victim to transfer money or request for TAC and internet banking credentials for the purpose of investigation.

6

Victim transfers money or reveals TAC and internet banking credentials. Victim only realises they have been scammed after receiving SMS notification on the amount transferred.

TAC Scams

Transaction Authorisation Code (TAC) is a six digit code that is used for online transactions. It is usually sent offline to your phone as a second layer of security.

Scan to watch

Defend Your Data: TAC Scam

Last 4-Digit Account Number

Ensure account number.

Beneficiary Name

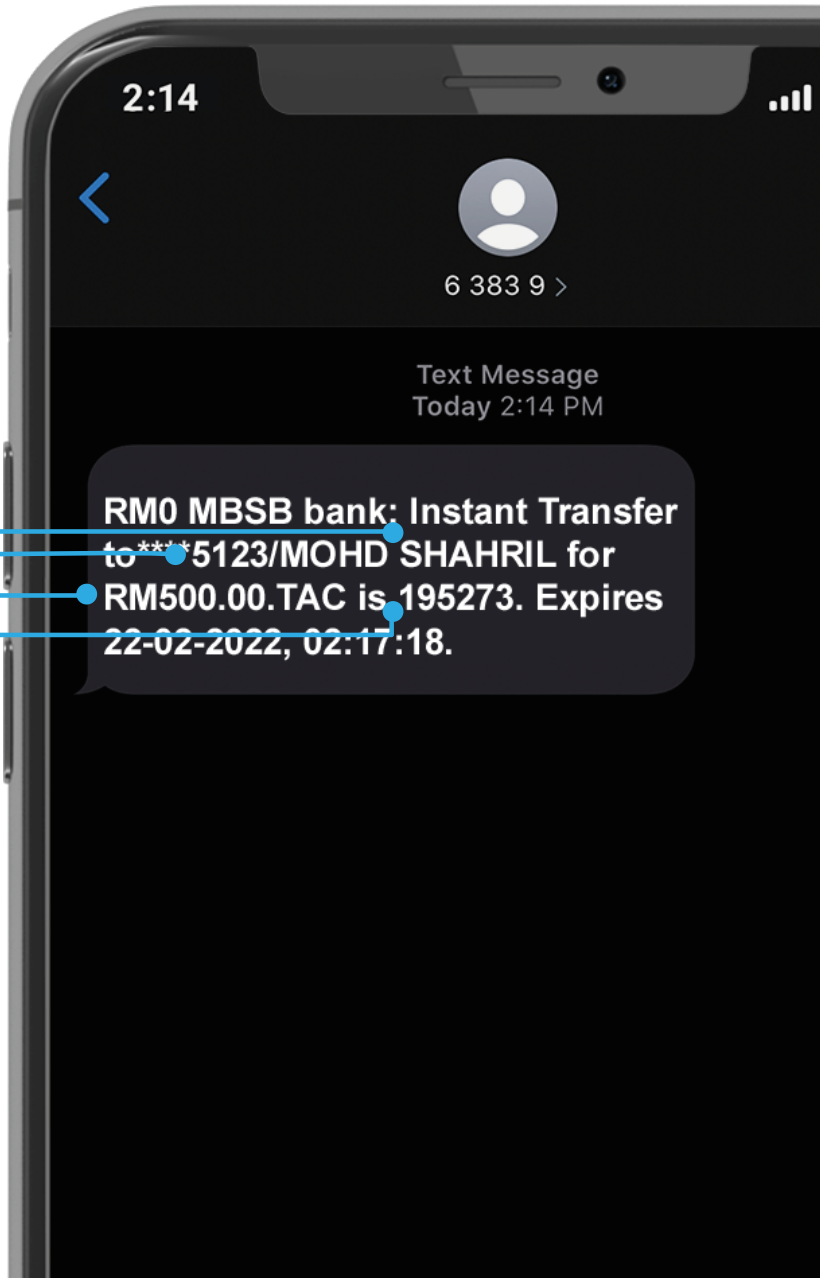
The name in the SMS should be the same as the one stated in online/ mobile banking.

Transfer Amount

Ensure the amount that is being transacted is the same in the SMS received.

Transaction Authorisation Code (TAC)

Ensure you key in the TAC code correctly.



Mule Accounts

Mule accounts are savings/current accounts that belong to individuals who are recruited by a scam syndicate.
Mule accounts are usually created to perform illicit activities.

Who Is a Target?

Recruiters from scam syndicate will hire vulnerable individuals (fresh graduates, housewives, elderly) who are desperate to earn quick money. However, there are also cases of fully employed individuals who are mule account owners.

How Does It Work?

Once an account is opened, the individual will provide scammers with the account information and the account will be used to transfer money for illicit activities.

What Are the Incentives?

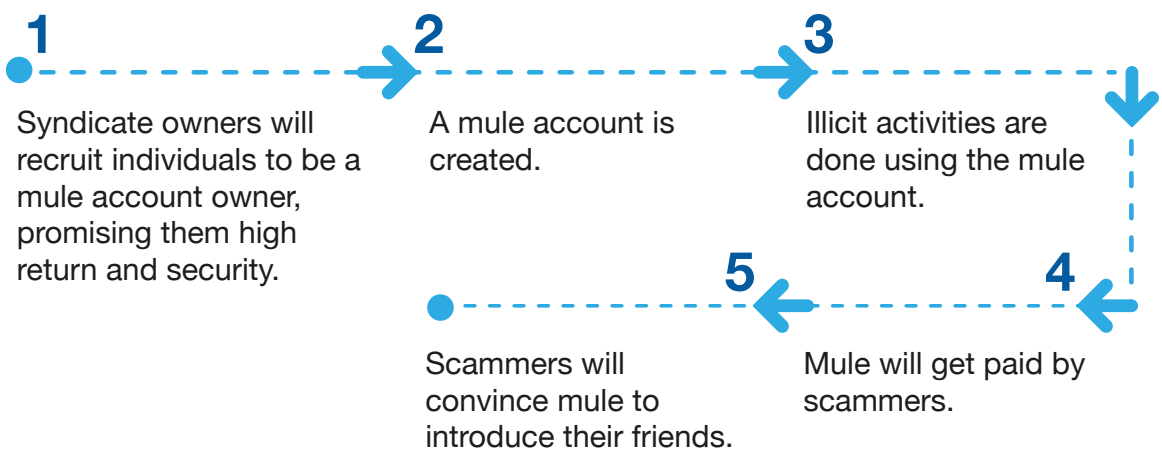
Victims are often blinded by the short term incentives given to them (usually monetary). They are either given monthly payments or commissions for being a mule account owner. This is how they continue to be a syndicate accomplice.

Imprisonment for up to 5 years, or fine, or both

It is an offence to 'rent out' your bank accounts; scammers use the account to launder illegal funds.

Money mules can be charged under Section 424 of the Penal Code for fraudulently concealing monies and Section 29 (1) of the Minor Offences Act 1955 for being in possession of stolen goods.

The Mule Process



Fraudulent Financing Syndicate

A syndicate claiming to offer financing services to potential victims ends up as fraud. This type of syndicate will ask their victims to make upfront processing payment upon financing application approval.

Modus Operandi

1. Syndicate approaches victim via various telephone channels (Messenger/ WhatsApp/ Line etc) and offers financing application.
2. Victim accepts the offer for financing
3. Syndicate requests upfront payment from victim to process the financing application such as legal fee, stamp duty, deposit, insurance
4. Victim makes payment to the syndicate's bank account
5. Victim realizes the scam when he/she does not receive the 'approved' financing

Make sure you deal with officers appointed by financial institutions.

Scan to watch

Defend Your Data: Personal Financing Scam

Malvertising

What is Malvertising?

Attacks where malicious code is being injected into the legitimate online advertising networks such as YAHOO, Facebook, Google, etc.

How Does It Work?

The malicious code redirect the victims to the malicious websites to install malware into victim's computer without being noticed by the victim.

Through which channel?

Attacker purchased online advertising service from legitimate advertising networks and advertised ads which consists of malicious code.

Who is the victim?

Below were the reported platform for malicious activities:
BBC News, The New York Times, MSN, Spotify, AOL.

How to identify Malicious Web

- Ads that do not look like they were made by a professional graphic designer.
- Ads that have spelling errors.
- Ads that promise giveaways, miraculous cures which sounds too good to be true.

How to Prevent Malvertising

1. Enable "Pop-up Blocker"

For Chrome User:
Go to Settings -> Privacy and security -> Site settings -> Pop-ups and redirects -> Don't allow sites to send pop-ups or use redirects

For Internet Explorer:
Select the Tools button -> Internet options -> Privacy tab, under Pop-up Blocker, Turn on Pop-up Blocker check box, and then select OK.

For Microsoft Edge:
Go to Settings -> Cookies and site permissions - > Pop-ups and redirects - > Toggle on for Block (recommended)

2. Uninstall browser plug-ins not used and set the rest to "click-to-play"

For Chrome User:
Go to Settings -> Privacy and security -> Site settings

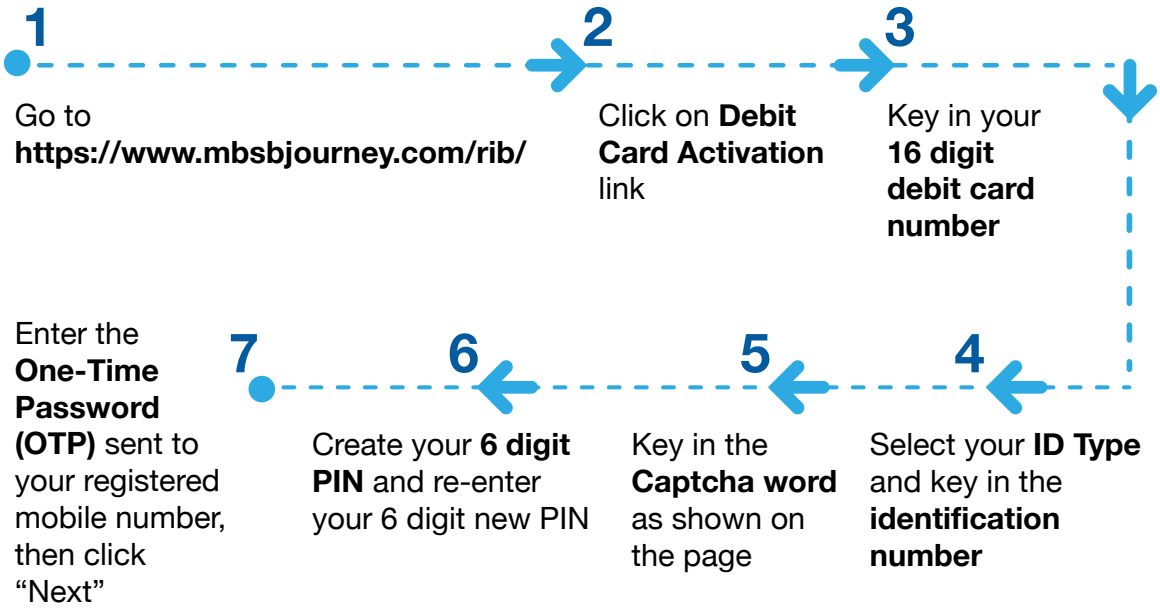
For Internet Explorer:
Select the Tools button -> Manage add-ons-> Toolbars and Extensions

For Microsoft Edge:
Go to Settings -> Cookies and site permissions

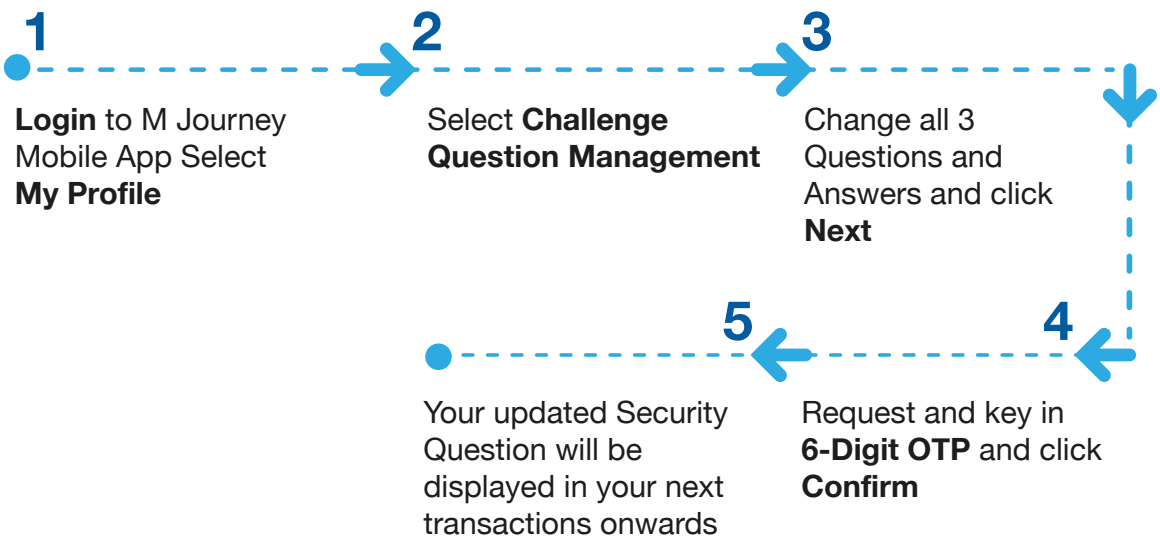
3. Do not click any online advertisement on the website

4. Ensure your antivirus, browser, Operating System patches are up to date.

Debit Card Activation



How do I change my Security Questions & Answers?



What should I do if I forget the answer to the challenge question?
You may call our Customer Service Centre at +603-2096 3000 for further assistance.

What is the purpose of the challenge question?
To authenticate the user when an activity is determined to be high risk.

M Journey Key

M Journey Key is a safer and convenient way to authorise transactions using Secure Token (one-slide approval). This feature is an alternative to the SMS TAC.

- The mobile device can only be tied to your M Journey Individual Online Banking access (i.e. username(s)) and protected by a secured login procedure using security image and phrase.
- Approve your transactions using M Journey Key from your registered mobile device.
- Only one login session is allowed per M Journey Individual Online Banking access. If the same M Journey Individual Online Banking access is used to login from another device, the current session will be terminated when trying to perform a monetary transaction.

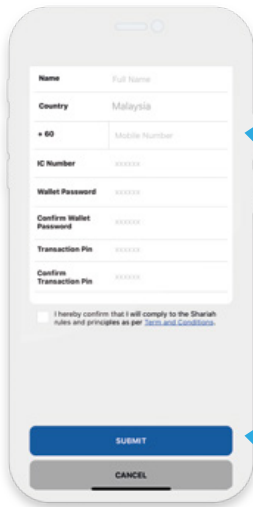
MBSB BANK
e-wallet

Download on the App Store

GET IT ON Google Play

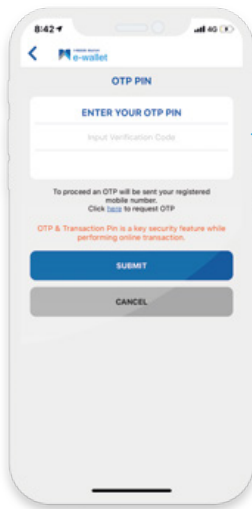
How to register

Click **Sign Up.**

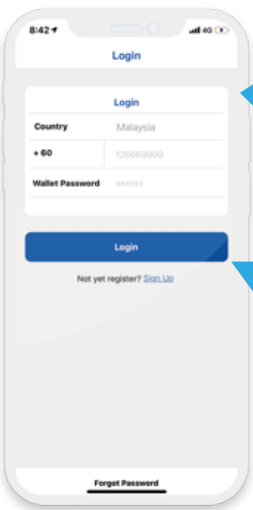


Key in your **details.**

Then click **Submit.**



Request for **OTP PIN** and key in the field once received from SMS. Then click **Submit.**



Key in your **details.**

Then click **Login.**

Scam Modus Operandi

There are many types of scam modus operandi (MO). These are some of the famous MO:

Scammers forcing victims to withdraw cash

Scammer will request victim cash and ask victim to surrender their debit card.

Scammers offers help for settlement

Victim is asked for a huge amount of cash in order to be released from a criminal charge and allegation of wrongdoing.

Scammers pose as a police officer

Victim will receive a call from fake police officers who will request payment from the victim to pay some amount to settle their case.

Claiming you are involved in money laundering

Victim will received a call claiming to be from any government agency and then the call will be transferred to a fake police officer.

Scammers asking victims to leave valuables at a secret spot

Victim withdraws the cash and surrenders all the debit card to scammer at the appointed place, date and time.

Posing as a friend on WhatsApp

Scammers are continuing to target WhatsApp users and hijack their accounts by posing as a friend and asking for SMS TAC or cash financing.

Scammers will pretend having a problem or in crisis situation and ask your friends and family in your contact list for money or TAC.

Scammers pose as a police officers, bank officers, BNM officers and court officers

Bank officers or any authorities will never ask for your internet banking username and password, credit/debit card number, ATM PIN or ask you to transfer payment to a personal account.

Scammers impersonating as insurers or well-known insurance company, alleged victim on the accident claim insurance on your vehicles number

Scammers will pretend to help you by transferring the call to PDRM to report that someone has misused your identification to make a false claim.

BNM fake app

Scammer will contact victim and instruct to download and install APK file, containing a fake application on their mobile phone via WhatsApp. The app will then take over the existing SMS system (TAC).

How Does Debit Card Fraud Happen?

Hackers

Beware while using public WiFi networks. Hackers might use a keylogging software to capture everything you type, including your name, debit card account number and PIN.

Phishing

Be cautious of unknown email / SMS messages asking your account information. It can look like its from a valid source. Please avoid from clicking on to an unknown link and avoid from revealing your personal information to an unknown 3rd party.

Spying

Fraudsters may simply look over your shoulder as you take out your card and enter your PIN. They can also pretend to be good Samaritans, offering to help you remove a stuck card from an ATM slot.

DOs

Be Alert When Using Your Card in ATM

Look out for unstable parts and faulty screens as these may indicate presence of a card skimmer. Contact MBSB Bank Customer Careline immediately if you found anything suspicious.

Keep Card Details to Yourself

If you frequently make card payments over the phone, it is important do it privately.

Read the Fine Print

Double check the URL and e-mail addresses. Make sure there are no extra commas or other unusual characters. Fraudsters may impersonate brands and individuals URL / e-mail addresses.

DON'Ts

Make Transactions on Public Networks

Public WiFi networks are an easy target for fraudsters to access your banking or personal information. It's best to avoid these types of unsecured networks where possible.

Don't Leave Your Card Unattended

Fraudsters are always waiting for opportunities to take your debit card away from you.

Avoid Posting Images of Your Debit Card

Once an image is posted in social media site or forum, it may remains on the internet. Fraudsters may able to figure out your debit card details (Social Engineering).

MBSB Bank Visa Debit Card-i Benefits

Quick and Convenient

- One card with dual function, its an ATM and Payment card.
- Enjoy the convenience of paying directly from your account.
- Cash withdrawal at any VISA PLUS and MEPS ATM network worldwide.

Contactless Transaction

- Simple and fast payment by just tapping your MBSB Bank Visa Card-i on Contactless reader machine.
- Maximum of RM250 per transaction, cumulative total of RM750 per day*

*The Bank may revise these limits from time to time

Purchase (Point-of-sales transaction)

- You can shop using your MBSB Bank Visa Debit Card-i at any outlet that accepts MyDebit of Visa nationwide.
- Pay with your MBSB Bank Visa Debit Card-i and the amount spent will be deducted from your link Savings or Current Account-i.
- Sign on transaction slip or key in your PIN for verification.

Card-not-present (CNP) Transaction

- CNP transactions include online tracsactions, mail order and telephone order transactions.
- Call our Call Centre at +603-20963000 for one time activation. Alternatively you may also activate your card at any nearest MBSB Bank branch.

Overseas Transaction

- Call our Call Centre at +603-20963000 for Overseas Purchase & Cash Withdrawal activation. Alternatively you may also activate your card at any nearest MBSB Bank branch.

Security and Fraud Transaction

- Receive instant SMS alerts on your MBSB Bank Visa Debit Card-i transactions to help you monitor your account activity and safeguard yourself against unauthorized transaction.
- These SMS alerts are sent at no extra cost to you.
- This feature provides you with security protection on your purchases using our debit card especially on online purchases.

Visa Debit Card-i

Exclusively for MBSB Bank Debit Card-i Cardholders

Effective from 1 February 2022, a RM1 fee will be charged to other banks' cardholders for each interbank cash withdrawal at any MBSB Bank ATMs. MBSB Bank Debit Card-i cardholders can still perform interbank cash withdrawals at any other banks' ATM nationwide at NO FEE or CHARGES.

	MBSB Bank Debit Card-i	Other Banks' Debit Card
Other Bank ATMs	NO FEE	RM1 FEE
MBSB Bank ATMs	NO FEE	RM1 FEE

Promotion extended until 31 December 2022

Terms and Conditions apply

Learn more about our fraud awareness and cyber security

Scan the QR code to watch the campaign video.

Spot The Scam: Online Contest

Spot The Scam: Fake Merchants

Defend Your Data: TAC Scam

Defend Your Data: Personal Financing Scam

Defend Your Data: Macau Scam

Scan to learn more about fraud awareness

MBSB BANK

PERBANKAN ISLAM

03-2096 3000

www.mbsbbank.com

MBSB Bank

MBSB Bank Berhad
Registration No.
200501033981
(716122-P)