RHB MULE PUBLIC AWARENESS 2026

Protect Yourself from Mule Account Scams. Don't Let Your Bank Account Be Used for Criminal Activities.

If you suspect you have been scammed, immediately call National Scam Response Centre (NSRC) at 997 (24 hours/7 days a week) or RHB's 24/7 Hotline at 03-9206 8118.

[Warning] If someone asks you to receive money into your account and transfer it to another person or account, **STOP** immediately. This may be a money mule scam. Criminals use mule accounts to move illicit funds and conceal their identities.

Whenever in doubt, always check **https://semakmule.rmp.gov.my**. You may use the *Semak Mule* portal to check whether a bank account or phone number has been linked to reports lodged with the Royal Malaysia Police (PDRM). However, a "No Record Found" result does not guarantee that an account is free from fraud-related activities.

What is a Mule Account?	• A mule account is a bank account that is used to receive, transfer or move money on behalf of criminals to conceal the source or destination of illegally obtained funds. • It may belong to an individual who knowingly or unknowingly allows their account to be used for illegal activities.
How is a mule account typically used by scammers?	• **Recruit individuals.** Scammers may contact individuals or victims through email, social media, websites, or messaging apps or offer fake job advertisements. • **Offer incentives.** They may offer rewards, commissions or easy money in exchange for allowing the use of a bank account or ATM/debit card. • **Use the account to receive funds.** Scammers transfer funds into accounts under their control or into accounts belonging to individuals who knowingly or unknowingly allow their accounts to be used. The individuals or victims are then told to transfer the money to another account. • **Move funds through accounts to conceal the criminals' identities.** The transferred funds are then withdrawn, transferred multiple times, or moved to other accounts to make it harder for authorities to trace the criminals.
Do not be a victim	• Never let anyone else use your bank account. • Never share your banking details, passwords, PINs, ATM card, or TAC with anyone. • Never receive or transfer money on behalf of someone you do not know or trust.

How can you identify a mule account?	• Check the *Semak Mule* portal at **https://semakmule.rmp.gov.my**. The portal allows users to check whether a bank account or phone number has been linked to reports lodged with the Royal Malaysia Police (PDRM). You may also report suspected scam-related accounts through the portal. • Always exercise caution when dealing with unknown parties, especially if they request payments, transfers, or banking information.
What are the consequences of being a mule account holder?	Anyone involved with a mule account may face: • Criminal investigation and prosecution under applicable laws, including Section 424B of the Penal Code (Act 574). Upon conviction, individuals who allow their bank accounts, ATM/debit cards or online banking credentials to be used by others without lawful authority may face a fine of RM10,000 to RM100,000, imprisonment of between 1 and 7 years, or both. • The Bank may restrict, suspend or close banking facilities in accordance with applicable laws and regulatory requirements. • Restrictions on opening future bank accounts with RHB.
How should you respond to a suspicious offer?	• Check the recipient's account number on the *Semak Mule* website **(https://semakmule.rmp.gov.my)** before making any payment. • Report to the police immediately if you suspect that scammers have compromised your bank account.
How Scammers Recruit Mule Accounts: 4 Common Methods	Be cautious if someone: • Offers easy money or commissions for using your bank account. • Asks you to receive money and transfer it to another person or account. • Requests your ATM card, debit card, online banking credentials, passwords, PINs or TAC. • Claims they cannot use their own bank account and asks to use yours instead. • Asks you to open a new bank account on their behalf. • Sends money into your account and instructs you to transfer it elsewhere. • Pressures you to act quickly or keep the arrangement secret. Common recruitment methods include: • **Fake job advertisements** - If you see a job ad that is too good to be true, it could be a scam! Many scammers set up fake job postings on social media or they may approach you via chats to get you to give them your ATM card or banking details for fake salary processing. DO NOT fall for it! • **Loan sharks** - Loan sharks usually prey on their victims with quick and easy cash loans. In return, they will ask for your ATM card and banking information to 'check on your money in the bank'. They will then use your account to transfer illegal money and keep their identities hidden.

	• **Bank account rentals** - Renting, selling or allowing others to use your bank account is prohibited and may result in your account being used for criminal activities, including scams and money laundering. Scammers will offer you payment for your ATM card and online banking details so they can use your bank account to funnel illegal funds and hide their real identity. • **Family & friends** - Never allow anyone, including family members or friends, to use your bank account, ATM card, online banking credentials or security authentication methods on your behalf. More often than not, the reason given is to help them receive and/or transfer funds to third parties using your bank account.
Think you've been scammed?	• Immediately call National Scam Response Centre at 997 (24 hours/7 days a week) or RHB Bank 24/7 Fraud Hotline at 03-9206 8118. • Activate the ***Kill Switch** immediately if you suspect that you have fallen victim to a scam. The feature temporarily suspends access to your online banking, bank accounts, and cards, helping to minimise the risk of further unauthorised transactions and financial losses. (***Kill Switch** refers to a security feature (Lock Account) provided by banks that enables customers to immediately suspend or block access to their bank accounts, cards, or online banking when fraudulent activity or compromised banking credentials are suspected.).

Need Further Assistance?
• Please visit your nearest RHB branch to learn more about the terms and conditions. • Former RHB accountholders whose accounts have been closed due to confirmed mule account involvement may submit an appeal for consideration under products approved by the Bank, subject to applicable requirements and the Bank's discretion.

IMPORTANT CONTACT DETAILS – BE SAFE !

	Organization	**Contact Details**
Have you noticed a transaction you don't recognize or suspect someone is using your account?	RHB Bank Berhad	Contact us at 03-9206 8118 or email via customer.service@rhbgroup.com
Have you been a victim of a scam and would like to lodge a report?	National Scam Response Centre (NSRC)	Contact NSRC speed dial at 997

Are you intending to verify whether any of your bank accounts or the accounts you wish to transact with have been linked to criminal activities?	Commercial Crime Investigation Department, Polis Diraja Malaysia (PDRM)	Verify via https://semakmule.rmp.gov.my/
Do you wish to verify information, online content or messages that may be false, misleading or related to scams?	Malaysia Communications and Multimedia Commissions (MCMC)	Verify via https://sebenarnya.my/
		You may lodge a complaint through the MCMC portal at: https://aduan.skmm.gov.my Or Email to MCMC via aduanskmm@mcmc.gov.my Or Contact MCMC via WhatsApp at 016-220 6262