

BANK RAKYAT CREDIT CARD-i AND DEBIT CARD-i SAFETY TIPS



Have you detected fraudulent transactions on your card?
Follow these steps and prevention tips to keep your account safe.

Step 1 - Block your card

1. Call the number on the back of your card. Our customer service representatives will assist you to block* the card as needed.

or

1. Log in to iRakyat or Bank Rakyat Mobile Banking Application.
2. Choose the card you want to block*.

Note:

* This is a temporary restriction. Transactions including standing instructions, recurring payments (such as utility payments and installment plans), refunds, fees and charges will be unaffected.

Step 2 - Report suspicious transactions and obtain a new replacement card.

1. Immediately call 03-2693 6880.
2. Your new replacement card will be mailed to your registered mailing address within 14 business days.
3. Lodge a police report to ease the investigation.

What can you do to reduce the risk of unauthorized transactions?

1. Please notify Bank Rakyat if your contact information changes. This will allow us to reach you promptly.
2. Pay attention to your SMS alerts and transaction statements. Please notify Bank Rakyat if there is any discrepancy.
3. Please be aware of your surroundings when entering the PIN number at the electronic payment terminals.
4. Avoid lending out your card to others.
5. Report your lost card to Bank Rakyat immediately to avoid any unauthorized transactions.



Here are some simple tips to protect your online banking.

1) Phishing or Scam Alert

- Fraudsters will send a legitimate e-mail requesting bank account information, passwords, and other personal information. **DO NOT REPLY, PROVIDE ANY PERSONAL INFORMATION OR CLICK ON THE LINK IN THE EMAIL.**

2) Password

- Create a password with a **COMBINATION** of alphanumeric and special characters.
- Use your own computer, tablet, or smartphone to change the password.

3) Internet browser

- Avoid using public Wi-Fi.
- Do not access your bank account on a shared computer.
- Sign out of your bank account and do not leave the browser unattended.
- Delete all cache memories and browsing history.

4) Smartphones or Personal Devices

- Do not save your personal information or passwords on your phone.
- Do not click links, URLs or download applications that are sent via unknown SMS, WhatsApp, and other messaging services.
- Do not install any application or Android Package Kit (APK) file from unknown sources.
- If your phone is lost or stolen, contact your Telco's customer service (mobile connection providers, such as Maxis, Celcom, and Digi) and request them to block your number.

5) General Security

- Please ensure that the antivirus software on your computer, tablet or smartphone is up to date with the most recent virus definitions and security updates.



PROTECT YOUR BANK RAKYAT CREDIT CARD-i/DEBIT CARD-i DATA

✓

- PAY ATTENTION to your transaction alerts.
- CHECK your account activities regularly.
- ONLY call the number on the back of your Bank Rakyat Credit Card-i or Debit Card-i.
- ALWAYS refer to Bank Rakyat website "contact us" page.
- CHECK the url of a website before making any purchase.
- ENSURE the "lock" icon or "https" appears on the website address bar.
- ALWAYS make sure the online merchant is genuine.

✗

- Give personal information to strangers.
- Apply for Bank Rakyat Credit Card-i or Debit Card-i through unverified links or individuals.
- Take instructions from anyone to change the mobile number in Bank Rakyat records.
- Continue with an online purchase with a suspicious merchant.

KEMENTERIAN PEMBANGUNAN USAHA RAKYAT DAN KOPERASI

PERSEKUTUAN

BNK 2030



REMINDER

- Avoid falling prey to fraud and phishing.
- Remember that Bank Rakyat, Police, Government Agencies or other law enforcement agencies will never call and ask you to transfer funds to unidentified third-party accounts under the guise of an investigation.
- Bank Rakyat will never send you an SMS notification that includes a link to your Internet Banking.
- Please contact Bank Rakyat if you have any inquiries regarding a suspicious message you have received.
- Never share your Internet Banking ID, password, PIN or OTP (One-time password) with anyone.
- You should regularly change your passwords and PIN.
- Follow the *Amaran Scam* Facebook page and join over 50,000 followers to get the latest information on financial scams in Malaysia.



For further assistance or inquiries, you may reach us at:

- ✓ 24/7: Card Centre at 03-2693 6880 (Malaysia/ International) Card Centre is available 24 hours a day, 7 days a week at +60326936880 (Malaysia/International).
- ✓ 24/7: Call Centre at 1300805454 or +60355269000 (international)
- ✓ Email: aduan@bankrakyat.com.my or telerakyat@bankrakyat.com.my