Security Tips

Golden Rules

Be alert and protect yourself when banking online or on mobile

At RHB Bank, security is our top priority. Stay safe with us by practicing the following Golden Rules with RHB Now Internet & Mobile Banking.

Protect yourself from cyber frauds

Online security is important when you do internet banking. It is always a good idea to take necessary precautions to improve the security of your devices. Here's how to stay safe online:

TIP #1: THE RIGHT ACCESS

Internet Banking

Ensure you're in the correct URL

- RHB Group Website: http://www.rhbgroup.com
- RHB Now Login Page: https://logon.rhb.com.my

Ensure that a padlock 🔒 RHB Bank Berhad [MY] is seen in the address bar and confirm that the URL is highlighted in green. This would mean the website is secured.

Mobile Banking

Ensure you install RHB Now Mobile Banking App from a legitimate app store only.

TIP #2: YOUR SECRET WORD

Always check your Secret Word upon entering your username. Proceed to enter your password only if it matches.

TIP #3: ONE-TIME PASSWORD (OTP)

Always reconfirm your transaction details using your one-time password (OTP) SMS. This is a security feature which is sent to your mobile phone to ensure that the transaction is performed by yourself.

TIP #4: WHEN IN DOUBT, CALL US.

If any doubt arises, you need to call us. Kindly contact our Call Centre at 03-9206 8228 should you require any clarification.

More tips on identity theft and fraud prevention coming your way or visit www.rhbgroup.com for more information.

RHB Group @RHBGroup RHB Group RHBGroup

Bank Berhad (6171-M)

Your Role

Be alert and protect yourself when banking online or on mobile

We urge that you play your role to stay safe in using Internet and Mobile Banking services too. Here are the top security tips that you should do.

Protect your computer from malicious programs

Besides destroying important information on your computer, some viruses and malicious programmes such as Trojan Horse may capture your password without your knowledge. These programmes are often disguised as normal files. To avoid getting infected, you should:

1. Never download any file from questionable websites (programmes, games, pictures, etc) or people (e.g. email attachments)
2. Never use features in your programs that automatically get or preview files
3. Install a personal firewall and virus detection software. You should also update your software frequently
4. Disable the preview mode in your email programs

Don't save your Login Username and Password on computers

Sometimes, when you enter Login information on websites, you will be prompted whether to store your Login Username and Password for convenience sake. Do not tick the "Remember username or password" setting it at all times. Someone who uses the same computer might use your account for malicious activities.

If you have stored your Login information on your browsers, clear it immediately from your browsers' setting. 'Uncheck' all settings to remember usernames and passwords.

Keep your Login ID and password confidential

Never share or reveal your Login Username or Password to anyone just like how confidential are you with your Email or Facebook account. It's the same concept when you bank online.

Here are some tips on how you can keep safe of your Login information:

1. Do not write down your Login Username and Password or use it when someone can see it
2. Do not choose a Login password that is easy to guess such as your Login Username, telephone number, identification number or birth date. Password should be alpha numeric i.e. Bookmark38
3. Do not use the same password on Internet banking as telephone banking
4. Change your Login password often. You can easily change it online at RHB Now Internet Banking site
5. If you suspect your Login Password has been compromised, change it as soon as possible
6. Clear your cache (temporary storage in a computer) and delete your cookies each time you log out

How to clear your cache memory

Internet Explorer

1. Click "Tools"
2. Select "Internet Options"
3. Click "General"
4. Select "Temporary Internet Files" and click "Delete Files"
5. Click on "OK" to save your settings

Mozilla Firefox

1. Click "Tools"
2. Select "Options"
3. Click "Advanced" menu
4. Click "Network"
5. At the "Offline Storage" box, click "Clear Now"

Learn to spot spoof emails and fake websites

Criminals use spoof emails and fake website to phish information. Yes, 'phishing' is the term coined towards cyber crime of stealing information. They may create a fake banking site with same design as the real site and ask you to enter your financial details. Therefore, you need to be alert whenever you read emails and access the banking site to perform any transaction.

Learn to spot spoof emails and fake RHB Now website before you login based on the following:

1. **Email Sender's Address** - RHB's official email address only ends with @rhbgroup.com only. In fake email, the sender of the email usually is not from RHB's official email address
2. **Links in the email** - The link in the fake email may not match with the URL of the site it takes you to
3. **Website URL address** – The official RHB Now Internet Banking address is https://logon.rhb.com.my. Always check the URL address first before entering any information on the site. Do not continue to transact if the URL is not the official URL
4. **Secret Wor**d – Secret Word is a mutual authentication used by RHB to verify that the login page is from a genuine RHB Now site. Before you submit your password, make sure the Secret Word appeared is the word you have registered with RHB Now
5. **RHB Obligation** - RHB will not ask you to perform or verify any transaction or change personal information via email

Protect your mobile phone

Mobile phone may be the closest device that is always with you, which you will use it for banking or online shopping. Some of you may even store your important personal information such as username and password like a diary. Be extra careful on this.

We recommend that you should:

1. Set and use security PIN code on your phone. Never allow anyone to use your phone easily
2. Adjust your phone setting to lock the phone automatically if you did not use it for five or ten minutes
3. Never store your username, password or any sensitive personal information that is easily understood by anyone

4. Be cautious about any voicemail and text message scams. Never respond immediately. If you are doubtful, call us at 016 988 288 to check if the bank has such promotion/offer, change of banking processes or account problems
5. Be cautious on MMS you received too. Some MMS may be attached with malware. Once click, some viruses or malicious software may be installed. Always check the sender and content details before you click. If you are doubtful, do not respond

Download RHB Now Mobile Banking App from genuine source only

For mobile banking users, always download your RHB Now mobile banking application from iTunes® AppStore (for iPhone/iPad users) and Google Play (for Android users) only. Remember the same guide above to prevent downloading the application from any malicious application provider.

For mobile banking users, always download your RHB Now mobile banking application from iTunes® AppStore (for iPhone/iPad users) and Google Play (for Android users) only. Remember the same guide above to prevent downloading the application from any malicious application provider.

Our Role

Be alert and protect yourself when banking online or on mobile

We know security is the utmost important measures to protect you, our customers.

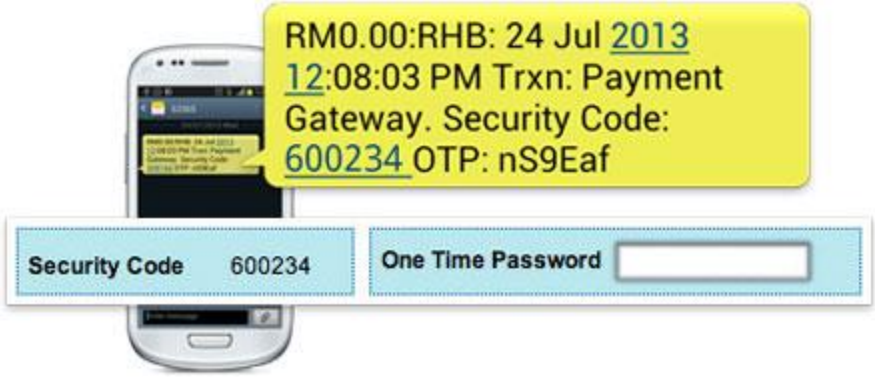
Unique Username and Password

Username and password created must be unique and only tied to your account information. This is the first level authentication to confirm your identity and to ensure the privacy of your Internet & Mobile Banking session.

Secret Word for Genuine Site Verification

Before you enter your password, you will see your Secret Word. Secret Word is a mutual authentication used by RHB to verify that the login page is from a genuine RHB site. You will be asked to register your Secret Word when you first register to use RHB Now. Thereafter, your Secret Word will appear on your Internet or Mobile Banking whenever you login. Always check that the Secret Word is the same as the one you have registered.

One-time Password (OTP) with Security Code for Secured Transactions



RM0.00:RHB: 24 Jul 2013 12:08:03 PM Trxn: Payment Gateway. Security Code: 600234 OTP: nS9Eaf

Security Code 600234

One Time Password

As the name depicts, OTP is only valid for one transaction. This is the second level protection to authenticate your transaction. It will be sent together with Security Code via SMS to your registered mobile number. It is given randomly in alphanumeric code. No one can determine what OTP number to be generated.

Reminder: You have to make sure that the Security Code displayed on the Confirmation page of your transaction is an exact match with the Security Code sent via SMS before entering your OTP to complete the transaction.

RHB Now Site is Secured by Entrust SSL

We use Secure Socket Layer (SSL) to encrypt data going between your Web browser and RHB Now website. The communication of your private information from any address beginning with "https" is encrypted and secured using SSL.

We use Secure Socket Layer (SSL) to encrypt data going between your Web browser and RHB Now website. The communication of your private information from any address beginning with "https" is encrypted and secured using SSL.

Protected with Secure Network Firewall

Our Internet and Mobile Banking system is protected with secure network Firewall to prevent our programs from any unauthorized or malicious intrusion.

Report A Problem

Be alert and protect yourself when banking online or on mobile

When should you report a problem?

Receiving a suspicious email

Suspicious email requesting for your login information? Request to change password or account activation? Respond to cancellation of transaction? Stop. Never respond to these emails. As mentioned, the bank will not request for your personal banking information via email. Report this suspicious email to us by forwarding it to ibanksupport.kh@rhbgroup.com. Please do not remove the original subject line or change the email in any ways when you forward it to us for our investigation.

The web URL seems wrong

Can't see the web URL on the page? The web URL is not https://rhbnow.rhbgroup.com/kh? Stop. Do not key in any information. Report this suspicious website to us by sending us the link and attach the print screen image of the suspicious website to ibanksupport.kh@rhbgroup.com. Please do not alter the image before sending it to us for our investigation.

Did Not Make a Payment

Did not make a payment but it appeared in your transaction record? Call us immediately at 016 988 288 to check. We put our best effort to investigate the activity.