# Additional Security Measures to Protect You Against Scams

As additional measures to bolster the security of digital banking services, we have implemented the following measures to prevent, detect and manage scam incidents.

**1) Suspend digital banking access through our hotline in the event of a scam or fraud**

**a) How do I suspend digital banking access through the hotline?**

Please call our hotline **1800-MAYBANK** (1800-629 2265) or **(65) 6533 5229** (Overseas) and press *1 or Option 4 in the main menu to suspend your Maybank2u online and mobile banking access immediately.

**b) Will I be able to access digital banking after suspension?**

No, you will no longer be able to access your Maybank2u online and mobile banking access after suspension.

**c) How do I re-activate my Maybank2u online and mobile banking access?**

To re-activate your Maybank2u online and mobile banking access, you will need to visit any of our Maybank Singapore branches with your NRIC or passport.

**2) No clickable links in emails or SMSes sent to retail customers**

**a) How can I tell if the emails or SMSes are sent by Maybank?**

There are no clickable links in our email and SMS notifications.

You may access your bank account(s) via Maybank2u SG app, or key in https://www.maybank2u.com.sg directly into the browser.

When in doubt, call **1800-MAYBANK** (1800-629 2265) or **(65) 6533 5229** (Overseas) to verify the authenticity of the emails or SMSes.

**3) Default threshold to receive transaction notifications is revised to $100**

**a) Can I change the default transaction threshold to receive the alerts?**

Yes, you may log into Maybank Online Banking (www.maybank2u.com.sg) to change the default transaction threshold to receive the alerts.

**E-Payment Alerts**
Log in to Maybank Online banking > 'Settings' > 'Manage E-Payments Alerts' to make the changes.

**Account Related Alerts**
Log in to Online banking > 'Settings' > 'SMART Alerts' to make the changes.*

**This option is not available on Maybank2u SG app.*

**b) How do I update my contact details to receive the transaction notifications?**

Steps to update your contact details:

1. Log in to Maybank2u Online Banking or Maybank2u SG app.

2. Select 'Settings' to check if your contact details are up-to-date.
3. Select 'Update Details' and follow the on-screen instructions.
4. Allow 3 business days for your details to be updated.

Do ensure that your contact details are updated so that you will not miss out on any transaction alerts and important notifications from us.

**4) Delay of at least 12 hours to activate a new Secure2u digital token on a mobile device**

**a) Why is there a need to delay the activation of a new Secure2u digital token?**

As a security measure, you can only use Secure2u to authenticate transactions at least 12 hours after registration. You will be able to use the physical token to complete your transactions in the meantime.

**b) Is it safe to use Secure2u digital token?**

Yes, it is safe to use Secure2u digital token as it is built with global security standards as part of our multi-layered authentication (e.g. phone lock, banking User ID and PIN).

**c) Can I still use my physical token instead of Secure2u digital token?**

Yes, you can continue using your physical token for your online transactions.

**5) Notifications will be sent to existing registered mobile number and/or email address for update of customer's contact details**

**a) Why do you send notification to my old mobile number or email address when I update the contact details?**

This is a security measure to verify that you have given the instruction to the bank to update your contact details.

**6) Additional security protection on transactions**

**a) What are the additional protection that Maybank has in place for fraud prevention and detection?**

Maybank has introduced a cooling period to perform selected payment transactions after a new payee has been added. This is a security measure to deter illicit transactions by providing some time for our customers to reconsider or seek advice before they perform funds transfer to the new payee.

The bank also triggers email alert to customers when there is a new browser login to their Maybank Online Banking. This is to notify customers in case of any unauthorised logins to Maybank Online Banking.

Maybank's advanced monitoring and surveillance systems help to detect potentially fraudulent activities in your account(s), providing a seamless banking experience without compromising your security. We have 24/7 monitoring of suspicious transactions that may be potentially fraudulent by our surveillance team. In the event of any abnormal activity in your account(s), we may contact you to confirm if the transactions are legitimate. There may be instances where we may freeze your account(s) in order to prevent any further potential fraudulent transactions in your account.

**7) Dedicated customer service teams to assist you with fraud and scam related matters**

**a) Who can I approach to report a fraud/scam incident?**

**If you suspect that you have fallen prey to a scam or if you have any suspicious activity on your Maybank accounts, cards or other products related to Maybank**

1. Suspend your digital banking access via 'Kill Switch', and
2. Call our hotline at 1800-MAYBANK (1800-629 2265) or (65) 6533 5229 (Overseas) and press *1 or
3. Visit our branches for assistance

**If you would like to report or check on any non-Maybank related scam cases***

1. Call and check with the 24/7 ScamShield Helpline at 1799

**For example, government officials or police impersonation, legitimacy of government SMSes, ecommerce scams*

**8) Timely and regular scam education alerts**

**a) How can I check for the latest updates on scams?**

We provide timely and regular updates on scam alerts on our website and social media accounts. These include information on new scams and security tips via Maybank2U SG website > Security > New Scam Alerts.

Our official social media accounts are:

Facebook: https://www.facebook.com/MaybankSingapore
Instagram: https://www.instagram.com/MaybankSG

**9) What can I do to protect myself?**

Scams can happen to anyone. It is important to remain vigilant as scammers are quick to adapt in targeting unsuspecting consumers. To avoid falling for online banking scams, you must:

- Never transfer money to people you do not know;
- Never click on links provided in unsolicited SMSes or emails;
- Verify unsolicited SMSes or emails received by calling the bank directly on the hotline listed on its official website;
- Always check that you are at the bank's official website before making any transaction or transact through the bank's official mobile application;
- Never divulge internet banking credentials or passwords to anyone;
- Secure your device with a strong password, PIN or a relevant mechanism to prevent unauthorised use; *TIP: A strong password is one that is difficult to guess and contains a mix of letters, numbers or symbols. You can use this on top of your device's biometric security feature (if available).*
- Use a different PIN or password for web-based services such as email, online shopping or subscription services; and
- Monitor transaction notifications closely so that any unauthorised payments are reported as soon as possible to increase the chances of recovery.

Remember, we will never request for your password or security information via phone, email or SMS.
As a Maybank customer, you have the option of suspending your digital banking access or changing your password in the event of a scam or fraud.

You may call our hotline at **1800-MAYBANK** (1800-629 2265) or **(65) 6533 5229** (Overseas) and press 1* or Option 4 in the main menu to suspend your Maybank2u online and mobile banking access immediately. Alternatively, you may login to Maybank2u online banking and select 'Settings' > 'Security' tab > 'Password' to change your password.