Maybank

Maybank heightens online banking security; to fully migrate from SMS OTP to Secure2u

- Bank welcomes new measures by Bank Negara Malaysia and will continue to step up efforts to combat financial scams to protect its customers

Maybank will fully migrate to a more secured authentication method via Secure2u by June 2023 for online activities or transactions relating to account opening, fund transfers and payments as well as changes to personal information and account settings. This is in line with Bank Negara's steer for Banks to migrate from SMS One Time Passwords (OTP) to a more secure authentication for these transactions.

Currently, Maybank only allows one Secure2u device per account holder (per customer) to minimise the possibility of a customer's online banking details being compromised or used by any third party. As an added security measure, Maybank alerts a customer via SMS, a push notification and an email when Secure2u is registered on a new device.

Dato' Khairussaleh Ramli, Group President & CEO of Maybank said this is in line with the Bank's effort to prioritise at all times the safety and security of its customers' funds and online banking transactions.

"We remain highly committed in helping our customers to avoid being scammed by fraudsters. This is done through existing security measures that are already in place and as we progressively rollout more measures that can help deter or minimise the likelihood of customers falling prey to financial scams," he said.

"We are also supportive of Bank Negara Malaysia's announcement on 26 September 2022 in relation to the five measures to be adopted by banks in Malaysia to ensure higher standards of security, especially for Internet and mobile banking services. The banking industry is committed to working together to combat financial scams which are increasingly prevalent in today's digitalised environment."

Maybank will also introduce a cooling-off period when customers enable Secure2u on a different device to help prevent unauthorised Secure2u approvals by the fourth quarter of 2022. The cooling-off period before the activation of Secure2u on a new mobile device will provide sufficient time for customers to verify and report to the Bank in case of any unauthorised registration. The Bank introduced the usage of Secure2u in April 2017 as a safer and more convenient way for Maybank customers to authorise Maybank2u and MAE transactions, using

Secure Verification (one-tap approval) and Secure transaction activation codes (a six-digit TAC number generated on the mobile app). This feature is an alternative to SMS TAC.

The introduction of the cooling-off period for first time enrolment of Secure2u or when a new device is registered on Secure2u is an added measure that the Bank will implement in an attempt to mitigate the rise in financial scams seen nationwide and in an effort to continuously safeguard Maybank's customers' account details and funds.

In term of tightening fraud detection rules and triggers for blocking suspicious transactions, Maybank has a fraud detection and monitoring system with customised rules and additional risk parameters. Besides that, the Bank has in place a call back verification process to alert customers of suspicious transactions.

Maybank already has a dedicated 24/7 hotline for customers to report financial scam incidents. Customers are urged to contact the fraud hotline at +603 5891 4744 immediately if they suspect their banking details have been compromised or that a suspicious transaction has taken place or even if they would like to suspend their bank account swiftly. Alternatively, customers can contact Maybank Customer Care Hotline at 1 300 88 6688 on the above. This will enable the Bank to promptly assist customers in preventing further losses immediately.

Meanwhile, the Bank also would like remind its customers on some useful tips to protect themselves when using online platforms:

- Avoid installing/downloading apps/Android Package Kit (APK) files or clicking on suspicious links sent via chat messages such as SMS, WhatsApp, Messenger or other similar services.
- Do not provide permission for any app to send or view your SMSes.
- Do not ignore any warnings from your devices, especially when downloading or installing a new file.
- Do not enter your banking details, especially username or password, in any suspicious apps or websites.
- Always keep your antivirus software updated for constant protection.
- Only download apps from the genuine app stores such as Apple App Store, Google Play Store or Huawei AppGallery and not from a link.
- Be alert if you are being prompted to download a file that is not compatible with your device i.e.: iPhone/iPad device being asked to use an Android device to download a file.
- Always look out for your online banking security image and phrase (i.e.: Maybank2u security image and phrase), to ensure the website and app are legitimate.
- Do not root or jailbreak your device.
- Update your mobile device's operating system (OS) and apps regularly.

Maybank continuously shares informative content on its Maybank2u website and on Facebook and Instagram, in an effort to remind and create awareness among customers on the dangers of scams. Customers should regularly pay attention to these reminders so that they will be made aware of latest scam methods to protect themselves.

Customers are also reminded to continuously protect themselves by ensuring their online banking details are kept safe and never shared with a third party, either knowingly or unknowingly through any scam attempts.

****