Press Release **16 June 2022**

Maybank reminds customers to remain vigilant when online

Bank provides online safety tips to help customers protect themselves

Online fraudsters continue to find new ways to scam unsuspecting users, especially given the recent rise in e-commerce activity spurred by the COVID-19 pandemic. As more consumers opt to transact online today, scammers are finding opportunities to trick consumers using new and sophisticated scam tactics.

On top of developing fake banking websites or applications (apps) to lure or phish customers, scammers have now incorporated malware components in fake law enforcement apps and fake retail e-commerce websites or apps to gain access to customers' online banking information such as their user names and passwords.

A common scam that customers might fall prey to begins with them coming across an unbelievably cheap deal or advertisement on a social media website. The customer then contacts the third party service provider/ seller (which is the fraudster) for further information. The fraudster provides the customer with a link and tells the customer to download an app to participate in the cheap deal. When installing the app, the customer will be prompted to allow the app to be the default SMS service provider. By approving this request, the customer has effectively provided the fraudster access to the customer's banking TACs in the future.

After installing the app, the customer will be directed to register with the app commonly requesting for information such as name, identification card number, email address and phone number, among others. Subsequently, the app will direct the customer to a fake payment gateway (fake FPX page) during the checkout stage or finalisation of purchase. Once the customer keys in the username and password in this page based on the customer's bank selection, the page will subsequently show an error message that the payment was unsuccessful i.e.: unexpected error occurred while connecting to the bank server.

In actual fact, these steps have effectively compromised the customer's online banking account details as the fraudster now has access to the customer's username and password, and can also view all TACs inbound into the customer's device. Soon after the fraudster has gained access to these details, the fraudster will start transferring funds out of the customer's bank account and the customer will not be aware as he/she has given permission to the fraudster to receive all his/her SMS messages when installing the earlier fake app.

Some useful tips customers can follow to protect themselves when using online platforms include:

- Avoid installing/downloading apps/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 App Store, 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.

If a customer suspects that his/her online banking account details have been compromised, remove the app and scan the device with an antivirus software. Next, change your online banking account password and contact Maybank's fraud hotline at +60358914744 for further assistance.

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 malware scams. Customers should regularly pay attention to these reminders so that they will be made aware of latest scam methods to protect themselves.

At the same time, the Bank wishes to remind customers to continue to remain vigilant about other scam tactics such as phishing scams via SMS/emails, telephone calls alleging customers have committed some kind of offence, payment for parcels and so on, all of which aim to obtain customers' banking details or induce them to transfer their funds to the fraudsters.

The Bank would also like to reaffirm that the safety and security of its customers' funds and online banking transactions are prioritised at all times. Maybank's online banking platforms and apps are secure, safe and employ strong security controls to combat cyber threat.

However, customers are reminded to do their part in continuously protecting themselves by ensuring their online banking details are kept safe and never shared with a third party, either knowingly or unknowingly through malware or any phishing attempts.

Do contact our fraud hotline at +60358914744 immediately if you suspect your banking details have been compromised, as it is a 24/7 hotline service and the Bank can assist you in preventing further losses immediately.

****