FAQ – Enhanced Security Measures Against Malware Scams

1) What are the control measures Maybank has in place to combat scams including malware scams?

To bolster the security of our digital banking services, Maybank has implemented a holistic approach to prevent, detect and manage scam incidents, including:

i. Restricted or disablement of mobile banking app when suspicious applications are detected
ii. Notifications will be sent to existing registered mobile number and/or email address if there is a request to update customer's contact details
iii. Additional security protection on transactions such as a cooling period to perform selected payment transactions after a new payee has been added
iv. Advanced monitoring and surveillance systems help to detect potentially fraudulent activities in customers' account(s)

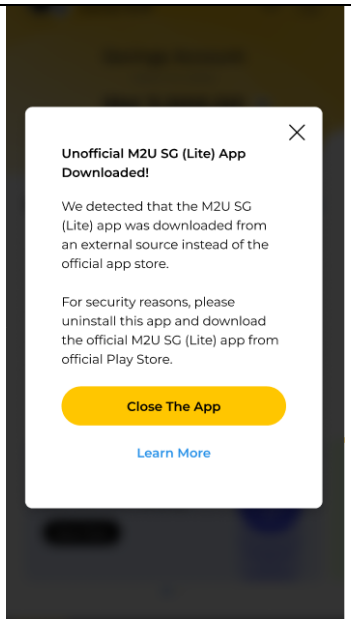
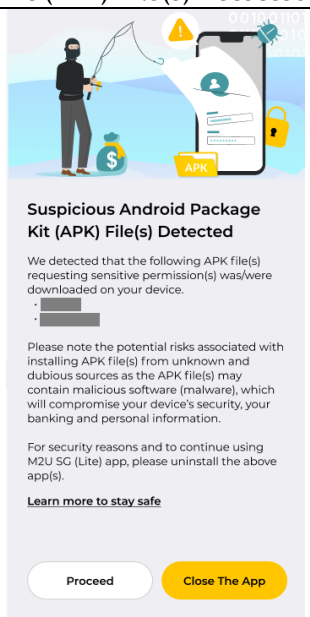
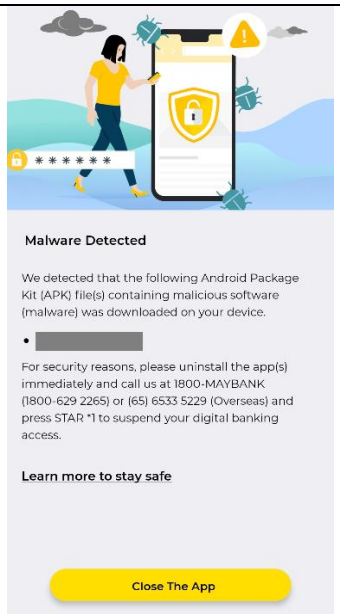
As part of our roadmap to combat cybercrime and to enhance the security of our digital banking app, Maybank will continuously be rolling out additional security measures in our digital banking apps to protect our customers from malware scams.

2) Why is there a need for banks to have anti-malware security features?

Over S$300 million has been lost to scammers from January to June 2023, according to the Singapore Police Force. As the number of scam cases rise, the prevalence of malware-enabled scams involving Android device users in particular have become a key area of concern.

As such, the development and enhancement of anti-malware security features are necessary to protect customers from the serious threat that malware scams pose to them.

3) What message(s) will I see on my Maybank app if my phone contains potentially harmful apps?

Unofficial M2U SG (Lite) App Downloaded!	Suspicious Android Package Kit (APK) File(s) Detected	Malware Detected
		

4) **How do I ensure I am up to date with any enhanced security features?**

You may refer to the Maybank2u website under 'Security Alerts' to keep up to date with the latest security measures, scam advisories and tips on scam prevention.

Customers will also be kept informed on any enhanced security features in advance via Maybank's various communication platforms such as our mobile applications, website, social media pages and e-mail.

5) **Why am I not encouraged to use applications downloaded from unofficial sources?**

Apps downloaded from official app store have gone through security checks to ensure the safety of users' devices. On the other hand, unofficial sources may not implement such stringent security checks, which may potentially expose unsuspecting users to malware threats.

6) **Am I able to disable the anti-malware measure and continue using the unofficial Maybank app or blacklisted malware application?**

These measures are necessary for enhanced security to mitigate the dangers and limit your exposure to malware scams. You will need to uninstall for the mentioned apps shown on the error message in order to continue to use Maybank app.

7) **Is it safe to disregard the pop-up warning message for suspicious APK file?**

To minimise the risk of a malware attack from these apps, the recommended course of action is to uninstall any apps mentioned in the warning. However, if you are confident that the listed APK files are safe and accept that it may compromise your device's security, your banking and personal information, you may proceed to use the Maybank app.

8) **If I can still access the Maybank app, does that mean I am completely safe from malware?**

While the anti-malware security measure is capable of detecting malware or malicious apps, no security measure is entirely foolproof. As scammers continually refine their tactics and grow more sophisticated, we strongly recommend our customer to stay vigilant as you remain the best defence against scams.

9) **How does the bank determine which apps are installed on my device?**

Our security measures check is performed on device level. Maybank will neither monitor nor engage in any form of surveillance on customers' mobile devices, and we do not gather or retain any personal data.

10) **Why was I not prompted to uninstall the app previously?**

As part of our ongoing effort to fight evolving malware scams, we are constantly updating our security measures.

11) **How else can I safeguard myself against Malware Scams?**

For more information on how to protect yourself, please visit our Tips to Staying Safe.