Mobile Malware Threats targeting your banking credentials

Dear Valued Customer,

Recently, there is a surge in online scams involving mobile malware that have become more efficient at stealing banking credentials and carrying out fraudulent transactions. Enhance your awareness of cyber security to safeguard your financial and personal information.

WHAT ARE SOME TYPES OF MOBILE SCAMS?

QR Code Scams

QR codes lead you to websites to steal your credentials.

SMS Phishing

SMS with link directing you to websites to steal your credentials.

Voice Phishing

Scammers impersonate legitimate individuals or companies to urge you to take action and steal your information.

SOME EXAMPLES OF MOBILE MALWARE

1 CypherRat/SpyNote

A type of malware that monitors & control devices to gain access to banking information and execute fraudulent transactions.

2 Letscall

A type of malware that targets Android device users to conduct financial fraud by impersonating the victim to answer incoming calls from the bank or posing as bank staff to prevent the user from alerting the bank.

3 WebAPK

Android feature that allow users to install applications through websites without going through the official source (i.e.: Google Play Store). Scammers will send a SMS containing a link to redirect the user to download applications to steal your data and conduct fraudulent transactions.

TIPS TO PROTECT YOURSELF

Ensure that the operating system and the applications in your device are updated to the latest version.

Be cautious when clicking on links received through SMS. Access links from reputable sources to ensure its legitimacy.

Do not grant permission to persistent pop-ups that request access to your device's hardware or data.

Exercise caution when scanning QR codes in public areas, especially if the offer or promotion sounds too good to be true.

Only download applications from official stores like the Google Play Store and iOS App Store.

Your one stop app and portal for all your financial, health and wellness needs

Enjoy greater convenience with My AIA SG today!

GET IT ON Google Play

Download on the App Store

AIA is committed to protecting our customers from potential scams and addressing concerns over security issues when you conduct digital transactions with us. If you suspect any fraudulent transaction or unauthorised access to your account, please contact us at 1800 248 8000 or +65 6248 8000 (from overseas), Mondays to Fridays between 8:45am and 5:30pm.

Follow Us

This service communication is associated to your insurance/investment policies held with us. Please do not reply to this email.

AIA Personal Data Policy