



Dear Valued Customers,

Your well-being matters to us. SMS phishing scams targeting customers of financial institutions (FI) are on the rise. In recent incidents, scammers may impersonate FI to target victims via SMS links, which were used to trick victims into clicking on a malicious link and entering their credentials on a fraudulent website. At AIA, we are committed to protecting you and your data from phishing scams.

How to avoid becoming a victim of SMS phishing?

01

DO NOT click on links or "shortcuts" from unknown or suspicious senders provided in SMS messages or emails without verifying the authenticity of the message first. A safer alternative would be manually typing a website URL directly into the browser address bar.

Tips

Pay attention to the domain name in the URL provided. For example, a legitimate URL would look like this:

<https://www.aia.com.sg/en/index.html> ✓

Whereas a spoofed URL could look like this:

<https://www.aia-alert.com.sg/en/index.html> ✗



Notice that the legitimate domain name of AIA Singapore has been spoofed by threat actors. The spoofed link contains the aia acronym to trick unsuspecting users into believing it to be authentic.

02

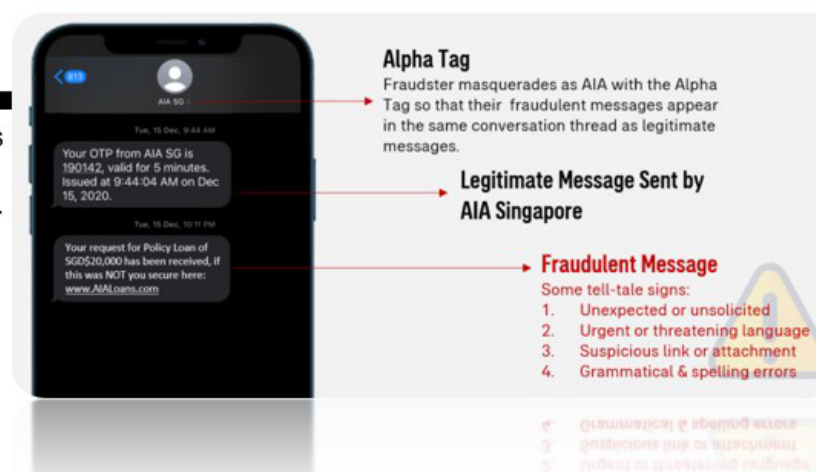
DO NOT divulge confidential information such as user ID, passwords, PINs or OTPs to anyone.

03

DO NOT act on the instructions of a message without verifying the legitimacy of the sender. Scammers often use either the threat of penalty or enticement of reward to create a sense of urgency to induce users to do something quickly. Always **STOP**, **THINK** and **ASSESS** before you respond.

04

DO NOT assume that messages sent in the same conversation thread are from the same sender. Scammers can masquerade as legitimate senders by using the Alpha Tag method to include the sender ID rather than from an anonymous number.



05

- **DO** download the ScamShield app which is developed by Singapore authorities to block unsolicited messages and calls (only available on iOS devices). Please visit <https://www.scamshield.org.sg/> to find out more.
- **DO** visit <https://www.aia.com.sg/en/help-support/security-advisory-tips.html> to learn more and protect yourself.
- **DO** find out more in the advisory issued by the Monetary Authority of Singapore (MAS) and the Association of Banks in Singapore (ABS) below: <https://www.mas.gov.sg/news/media-releases/2022/mas-and-abs-announce-measures-to-bolster-the-security-of-digital-banking>.

Contact us at 1800 248 8000 or (65) 6248 8000 from overseas, Mondays to Fridays between 8:45am and 5:30pm should you suspect any fraudulent transaction or unauthorised access to your account.

THE ONE-STOP APP FOR YOUR INSURANCE AND HEALTH NEEDS

Download the My AIA SG app and enjoy greater convenience today!



FOLLOW US

A row of four social media icons: Facebook (blue circle with white 'f'), YouTube (red circle with white play button), Instagram (purple and pink camera icon), and LinkedIn (blue square with white 'in').

Copyright© 2020, AIA Group Limited and its subsidiaries. All rights reserved.

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

Privacy Statement