

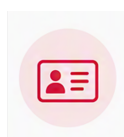


Scammers may pose as trusted organisations to trick you into sharing your personal information. They may approach you through social media, dating platforms, or even messaging apps. Remember, not everyone online is who they claim to be.

Learn how to spot the warning signs and protect yourself.

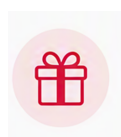
Spot the red flags

Be cautious if someone:



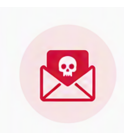
Requests for your personal information

E.g., your NRIC number, passport details, passwords or OTPs.



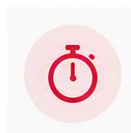
Promises guaranteed returns or rewards

Offers that seem too good to be true often are not.



Sends suspicious links or attachments

These may lead to fake websites or malware.



Creates urgency or pressure

Scammers often rush victims into making quick decisions.

Simple ways to protect yourself



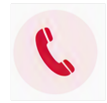
Never share your passwords or OTPs

AIA will never ask for your passwords or one-time passwords.



Use official websites and apps

Only access your insurance information through official AIA platforms.



Verify through official channels

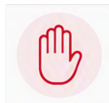
Take a moment to confirm that any request or contact details are legitimate.



Never click suspicious links

Be cautious of unexpected links sent via social media platforms.

Think you've encountered a scam?



Stop all communication

Do not click any links, share information or make payments.



Report the scam

Report suspicious messages or websites via ScamShield.



Stay alert. Stay safe.

Scammers continuously evolve their tactics, but knowing the warning signs can help you protect yourself and your loved ones.

Need help? Contact us



<https://www.aia.com.sg/en/help-support/contact-us>



1800 248 8000

Follow Us



Copyright© 2026, 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.

[AIA Personal Data Policy](#)