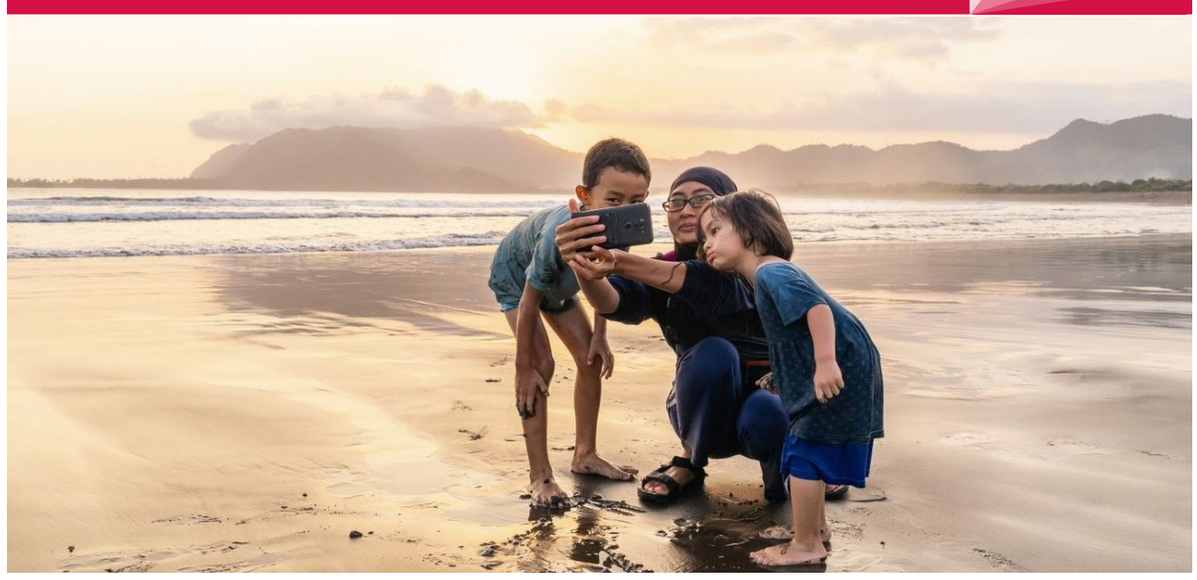
Important Travel Safety Tips You Need to Know If you cannot read this email, click here.

HEALTHIER, LONGER, BETTER LIVES



Dear Valued Customer,

Now that travel has resumed, we'll like to share security travel tips to keep your information and devices secure while you travel overseas.

1. Secure your information

Only use secure devices
Computers made available for general usage at public places such as cafes, hotel lobbies or airports may not be appropriately secured. Avoid using devices from public places to key in personal information or access sensitive data or services.

Think before you post
Do not post sensitive information such as images of your boarding pass or passport on social media as this allows your contact information or identification details to be exposed online.

Update your software
Update your devices with the latest versions of operating systems and software to ensure your devices are protected with the latest security features.

2. Secure your devices

Set up "Find my device"
This will help you to locate your phone or devices and allow you to remotely wipe data from the disabled device if it falls into the wrong hands.

Password protect all your devices
Set up your devices (e.g. mobile phones, tablets, and laptops) with strong passwords or personal identification number (PIN) to keep them secure.

Strong passwords typically include a mix of alphanumeric characters and special characters with minimal character repetitions. Avoid the usage of PINs that are easy to guess, such as your/family members' birth dates, vehicle numbers and phone numbers.

Back up files
Keep a recent back up of your devices that you intend to bring overseas like your phone or laptop in case your device is lost, stolen or broken.
Always ensure your backup is kept in a secured storage to minimise the risks of data being compromised.

3. Secure your connection

Set up "Actively manage your location services"
Turn off location services when not in use as these can expose your geographic location and alert others of your absence at home.

Disable auto connection
Disable remote connectivity and Bluetooth connection if not required as this stops your devices from automatically seeking and connecting to available public wireless networks.

Only use secure internet access
Do not use public Wi-Fi to access services like company emails, personal emails and

accounts or banking transactions. In the absence of a secured Wi-Fi, a more secure approach is to use a VPN (Virtual Private Network) or use your phone as a personal hotspot to access the internet.

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.