Beware of Impersonation Scams

If you cannot read this email, click here.

AIA HEALTHIER, LONGER, BETTER LIVES

Dear Valued Customer,

Impersonation scams are on the rise with scammers contacting victims pretending to be persons of authority such as employees or representatives from a financial institution. We have put together some samples of common impersonation scams and the tactics scammers use for your reference.

TECH SUPPORT SCAM

Unsolicited calls, supposedly from your internet service provider, claiming that your Wi-Fi network has been compromised by hackers.

Pop-up alerts on the internet browser claiming that your computer has been compromised. The alert message will solicit you to call the number on display for assistance, leading victims to believe it is legitimate.

GOVERNMENT OFFICIAL IMPERSONATION SCAM

Unsolicited emails from tax authority claiming inconsistencies in submitted tax returns and instructing recipients to click on a fraudulent link to make payment. Please refer to a sample screenshot of the scam email.

From: Income Tax Audit <TaxServices@secure-datalink.org>
Sent: Wednesday, 11 May 2022 11:50 PM
To: [redacted]
Subject: Income Tax Changes

Hi [redacted]

We are proposing changes to your 2022 IRAS Form 6A tax return.

Proposed amount due: $1,818

We received information from third parties, such as employers or financial institutions that doesn't match the information you reported on your tax return. This notice:

- Proposes a change to your tax payments and credits (such as federal withholding tax, earned income credit, etc.) that you originally reported,
- Provides you with an opportunity to agree or disagree with the proposed changes.

If our information is correct, you will owe $1,818 (including interest), which you need to pay immediately.

Click here to view details and complete payment.

If we don't hear from you

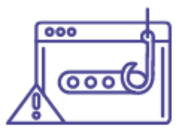
If we don't receive your response within 30 days, we'll send you a Statutory Notice of Deficiency followed by a final bill for the proposed amount due. During this time, interest will continue to accrue and penalties may apply.

SCAM

Unsolicited calls from scammers pretending to be a policeman and instructing victims to transfer monies to assist with investigation.

Unsolicited calls or emails from scammers pretending to be an employee of a financial institution claiming that your identity has been used for illegal activities.

HOW TO PROTECT YOURSELF



Never reveal log-in credentials, bank account details, credit card details or personal information to anyone. AIA Singapore insurance representatives and staff will never ask you for your personal log-in credentials such as password, one-time PIN (OTP), security token, unlock code, etc.

Never authorise a transaction or log-in unless you know its purpose.

Should you receive an unsolicited call, always verify the identity of the caller and its intent by calling the official contact number of the organisation.

Scammers can target any one and scams can occur at any time with potentially devastating consequences. Always stay vigilant when performing online transactions and do not divulge log-in credentials to anyone or perform suspicious online transactions.

Contact the organisation immediately when unsure of the details or intent of an unsolicited request.

For more information on how to protect yourself from scams, please visit AIA Singapore's security webpage using the QR code.

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!

GET IT ON Google Play

Google Play and the Google Play logo are trademarks of Google LLC.

Download on the App Store

FOLLOW US

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