

Your well being is important to us at AIA. With the increase of cyber crimes this festive season, here are some tips on how you can protect yourself against scammers.

Step 1: Spot the red flags



Fake Online Stores



Scammers on Legitimate Websites

Criminals create fake online stores that mimic the look of authentic sites or use the names of well- known stores or brands. When you search for the best online deals, you may find yourself at one of these fake sites. By purchasing from such websites, you can end up with counterfeit or stolen items, or your purchases may never be delivered.

Keep your guard up even when shopping at trusted websites. Online stores often offer products sold by third parties that may have fraudulent intentions. Such online stores are like retail shops, where some sellers are more trustworthy than others.



ADS S

Be suspicious of advertisements or promotions on search engines and social media with prices that are significantly lower than those you see at the established online stores. If a deal sounds too good to be true, it may be a scam. When in doubt, purchase items from the official flagship store.

Check the URL of the website before any purchase and make sure the spelling of the website you are shopping from is legitimate.

CONTACT US

XXXX

Be careful with websites that have no contact details, uses broken contact forms or provides personal email addresses.

4

Perform a reputation check on the website by typing the name of the online store or its web address into a search engine to see what others have said about it. Look for terms like "fraud," "scam," "never again," and "fake".

5

Protect your online accounts by using a unique and strong password for each of your accounts. You may consider storing your passwords in a password manager if you are unable to remember them.

××

Avoid using NRIC, FIN, or passport number as your username as it is a unique identifier issued primarily for public administration purposes and to facilitate transactions with the government.

7

Avoid websites that require obscure payment methods such as accepting payment only in cryptocurrency. Use electronic payment services or e-wallets which is a safer option for online purchases as disclosing your credit card number is not required.

Choose to shop online with stores that provide access management security methods such as multi-factor authentication (MFA) and enable this for your accounts. AIA's website – www.aia.com.sg – is equipped with MFA capabilities.

9

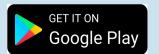
Regularly review your credit card statements to identify suspicious charges. Enable notifications via email or text when charges are made. If you find any suspicious activity, report it to your credit card company immediately.

Bookmark and purchase from reputable online stores that you are familiar with.

Here's wishing you and your family a Merry Christmas and a blessed new year. We look forward to continually being your trusted partner to enable you and your loved ones to live Healthier, Longer, Better Lives!

Download the My AIA SG app to view and manage your policies today!





Copyright© 2022, 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.

FOLLOW US









Privacy Statement