AFIA

Australian Finance Industry Association Limited
ABN 13 000 493 907
L11, 130 Pitt Street Sydney NSW 2000
T: 02 9231 5877
www.afia.asn.au

22 December 2021

FINANCIAL SAFETY TIPS FOR THE HOLIDAYS

While we're all looking forward to relaxing during the holiday break, we know scammers do not rest and they're becoming more sophisticated every day.

Many of us are doing the bulk of our Christmas shopping online and with Boxing Day sales coming up. Many of us are also looking to take a holiday and will be booking flights, accommodation and car rental online.

Now is not the time to let your guard down. Christmas scammers are relying on you being a bit distracted, so watch out for these tricks:

Fake holiday accommodation

Look out for fake accommodation vouchers, scam travel clubs and scammers asking you to pay upfront deposits for properties which aren't actually available for rent. Always check holiday or accommodation vouchers or travel offers are legitimate before you sign up, check the validity period, and search the wording of the offer or the company name on the website as many scams can be identified this way.

Fake flight or car rental bookings

Scammers set up fake websites to make you believe you are booking a real car rental or flight ticket. Be cautious when deciding to purchase very cheap car deals or airfares – if it looks too good to be true, it may be a scam. Always book through a legitimate travel agent, airline, accommodation, or car website or contact centre. You can check the ABN quoted is genuinely registered to the trader named on the site on the Australian Government's business.gov.au website.

Real car or holiday rental booking – Telephone scam

You may be asked by phone to make a separate new deposit or pay to update to your car rental or holiday accommodation booking. If you're not sure whether a call is a scam you can check by

independently using official contact details. Always contact the company directly. Never use phone numbers or email addresses provided by the caller.

Real parcel or booking – Fake confirmation

If you're expecting a parcel or have made a car rental booking and receive an SMS or email with a link to track your delivery or update your preferences, don't automatically click the link (especially if the parcel has already been delivered!). This may install software on your device to steal your personal and financial information.

Fake parcel – Fee for delivery

Scammers may also call or email pretending to be from a logistics or parcel delivery service (i.e. Australia Post or Amazon) and claiming a non-existent parcel could not be delivered. They will offer to redeliver the parcel in exchange for a fee and may also ask for personal and financial details. Don't make any commitments. Take their name and number and hang up. Call the company directly using their official customer service number from their website to verify the offer is genuine. Never use contact details provided by the caller or in an email.

Real or Fake parcel – Refund alert

If you receive an SMS notifying you've made a purchase and can receive a refund because the goods are not available, don't click on the click or call until you have checked your recent transactions, or called your bank from the number listed on the retailer's website to find out if the transaction is legitimate.

Fake online advertisements, auction listings, and websites

If the advertised price of an item online looks unusually low, be cautious. Scam ads quote items at much lower prices than similar items on the same or other sites, but the business and item don't actually exist. Avoid any arrangement with a stranger that asks for up-front payment via money order or international wire transfer. Scammers will ask you to pay outside of a website's official payment systems. Be especially cautious when buying pets, smartphones and tablet devices, motor bikes, cars and boats – these are common scam targets.

Real purchase – Fake payment information

Beware, some scammers will send scam emails which appear to be from official payment companies requesting payment, others will direct you to fake payment websites which look genuine but have a different URL.

Real or Fake Christmas e-card – with bonus malware

At this time of year it's not uncommon to be sent emails containing links to Christmas e-cards. These emails will often come from colleagues, friends and family, but they may have unknowingly forwarded on attachments containing hidden malware or links to scam websites. The emails may contain animations, pictures, videos, or links which when opened, download malicious software onto your computer or phone. Malware can be used to steal sensitive personal and financial information stored on the computer or device to record your keystrokes when you enter usernames and passwords online.

Never open unsolicited emails, delete them immediately! And as fun as they may look, exercise caution when opening Christmas e-cards even if they've come from someone you know. Never click on any links or open any attachments in these emails.

Finally…

There are a few sensible things you can do to maximise your financial safety from Christmas scammers:

- Never provide your credit card details and other personal and financial information to someone you don't know or trust.
- Always think before you click. A financial services provider will never ask for sensitive information like passwords or bank account numbers or ask you to click on a link.
- Take a few minutes to check a request out. The time it takes to check whether an SMS or email sent from your supplier is valid is significantly less than the time it takes to try and remedy financial loss to a scammer.

And here are some precautions you should consider taking at any time of the year:

- Keep your computer updated with the latest anti-virus and anti-spy ware software. Also, use a good firewall and regularly back up your data.
- Change your security settings to enable multi-factor authentication—a second step to verify who you are, like a text with a code—for accounts that support it.
- Change any compromised passwords right away and do not reuse those passwords for other accounts.

- Use a cloud-based account, such as Google Drive or Microsoft OneDrive, that can allow you to restore your data if your computer is comprised.
- If you think you have provided your bank account, credit card, or other personal and financial details to a scammer, contact your financial institution **immediately**.

Stay safe and happy holidays from AFIA!

NB: Thank you to our vigilant friends at Scamwatch for some of this content. For more information, check out Scamwatch's 12 Scams of Christmas.

Regards
Diane Tate
Chief Executive Officer