The 12 Scams of the Holidays

The following cams occur all year round, but scammers prey on people's generosity and vulnerabilities at this time of year.

1. Holiday accommodation scams

Time for a holiday? Whether you're relaxing in Australia or travelling overseas this festive season, scammers may try to get hold of your money and personal details. 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.

Protect yourself

Always check travel offers are legitimate before you sign up, search the wording of the offer or the company name on the web as many scams can be identified this way.

Before buying holiday or accommodation vouchers check with the hotel that they are genuine and will be honoured during the period that you intend on using them.

Never provide your credit card details and other personal information to someone you don't know or trust.

2. Flight booking scams

Scammers set up fake websites which look genuine and make you believe you are purchasing an authentic flight ticket. When you arrive at the airport you may find your booking was a fake.

Protect yourself

Always book flights through a legitimate travel agent, airline, flight booking or travel website.

Be cautious when deciding to purchase very cheap airfares – if it looks too good to be true it may be a scam.

Check that the ABN quoted on a flight booking website is genuinely registered to the trader named on the site. You can look up an ABN on the Australian Government's business.gov.au website.

3. Charity scams

At Christmas many legitimate charities appeal for donations of money, food, clothing and children's gifts. Unfortunately scammers also try to get your money by camouflaging themselves as genuine charities.

Protect yourself

Beware that scam charity emails and websites may use official-looking logos and words which make them look genuine. Always check that a website is legitimate before donating.

Approach legitimate charity organisations directly to make a donation or offer support.

Don't rely on any phone number or website address given by the person who first called, visited or emailed you. Independently search for the charity name online as many scams can be identified this way.

4. Online shopping scams

Found that perfect gift online? Beware, scammers post fake classified ads, auction listings, and run bogus websites. If you get caught by a scammer you will not only lose your money but will also never receive the item you were trying to purchase!

Protect yourself

Be cautious if the advertised price of an item online looks unusually low. Scam ads quote goods at much lower prices than similar items on the same or other sites.

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 the website's official payment systems.

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.

Be especially cautious when buying pets and pedigree puppies, smartphones and tablet devices, horses and saddles, motor bikes, cars and boats. These are common scam targets.

5. Parcel delivery scams

Australians are predicted to send and receive millions of parcels at Christmas time. If you are expecting a parcel from family or friends, it's important to be aware of scams involving parcel collection. Scammers may call or email pretending to be from a logistics or parcel delivery service such as Australia Post, claiming that a non-existent parcel could not be delivered to you. They will offer to redeliver the parcel in exchange for a fee and may also ask for personal details.

Protect yourself

If you are in doubt about the authenticity of a parcel delivery call or email, don't commit to anything. Call the company directly using their official customer service number to verify that it is genuine. Never use contact details provided by the caller or in an email.

If you think you have provided your banking or credit card details to a scammer contact your bank or financial institution immediately.

6. Social media gift voucher and free product scams

Gift vouchers make handy presents when someone is hard to buy for, but always buy them from an official source to avoid being scammed. Recent scams have involved fake gift vouchers and "free products" being offered via social networking sites. Scam offers will ask victims to give

personal details via survey in return for vouchers and products which either never arrive or are not honoured.

Protect yourself

Never click on suspicious links on social networking sites – even if they are from your friends. Remember if an offer seems too good to be true it probably is!

Be very wary when filling in surveys linked to via social networking posts and pages. Scammers commonly use these surveys to steal your valuable personal information.

If in doubt about the authenticity of a free offer always contact the company on their official customer service number to verify that it is genuine. You can also search the internet using the exact wording of the offer as many social media scams can be identified this way.

If you think you have provided your banking or credit card details to a scammer contact your bank or financial institution immediately.

7. Door-to-door scams

Lots of legitimate traders sell products and services door-to-door over the holiday season. Unfortunately scammers also approach their victims this way trying to sell poor quality products that don't do what is promised. If you fall victim, you will not get value for your money and money-back guarantees will turn out to be useless.

Protect yourself

If someone comes to your door, ask to see their identification. You do not have to let them in, and they must leave if you ask them to.

Do not agree to offers or deals straight away: tell the person that you are not interested or that you want to get some independent advice before making a decision.

Carry out a web search on the trader to see if there are other consumers who have commented on the quality of their product or service.

8. Telephone scams

If you are taking time off work over the Christmas and New Year period, you may find you receive scam calls on your home landline telephone. These scams have been prominent over 2011 with scam callers claiming that your computer is infected with a virus, offering fake government grants/compensation or seeking bank details in order to process a bank fee or tax refund.

Protect yourself

Be cautious if you are contacted out of the blue by someone claiming to be from a government department, a business or private organisation requesting personal information or payment for various services or fees. If you're not sure that a call is a scam you can check by independently using official contact details, never use phone numbers or email addresses provided by the caller.

NEVER provide or confirm your personal, credit card or online account details over the phone unless you made the call using details you found yourself and you trust the other party.

9. Christmas e-card scams

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

Protect yourself

Never open unsolicited emails, delete them immediately!

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

Keep your computer updated with the latest anti-virus and anti-spy ware software. Also, use a good firewall.

10. Romance scams

Online dating scams are very common and last year cost Australians more than $15 million. If you are looking for that special someone online be cautious. Scammers post fake profiles on legitimate online dating websites and will give various excuses to ask you to send them money via international wire transfer.

Protect yourself

Be wary of anyone who you have not personally met who asks you to send them money, gifts or your banking and credit card details.

Be very careful about how much personal information you share on social network and dating sites.

11. Weight loss Scams

Many of us make resolutions to loose weight over the Summer holidays, but watch out for scammers offering 'miracle' weight loss pills and potions. These scams may promise weight loss for little or no effort or may involve unusual or restrictive diets, 'revolutionary' exercise or fat-busting devices, or products such as pills, patches, or creams. Also watch out for 'free trials' that may sign you up to unexpected payments.

Protect yourself

Remember, there are no magic pills for rapid weight loss, instead speak with your GP about healthy and safe weight loss options.

Be very careful about offers for medicines, supplements or other treatments: always seek the advice of your health care professional.

12. Lottery scams

There are many legitimate lottery jackpots, competitions and sweepstakes throughout the festive season, however lottery scams also circulate at this time of year. These scams will often use the names of legitimate overseas lotteries or carry the name of a well known company, event or person. You will usually be asked to pay various ongoing fees to release your winnings but you will lose all the money you pay and won't receive anything in return.

Protect yourself

If you receive a letter, email or SMS out of the blue claiming you have won a lottery which you never entered it's most likely a scam – ignore it.

Ask yourself why you are being asked to pay fees when these could come out of the winnings. Genuine lotteries don't operate this way.

Report

You can report scams to the FCC, your state's Attorney general or local police.

Happ Holidays.