On the first day of Christmas the scammer said to me …

Scammers operate year-round, but Christmas offers a greater opportunity for them to sneak under the radar of busy, often frazzled consumers.* Update *has identified some of the most common Christmas scams so you can be armed and ready

Holiday and flight bookings online: Whether you are planning to holiday in Australia or overseas, scammers have ways to try separating you from your money and personal details. Always check travel and accommodation offers are legitimate before you sign up. Before buying accommodation vouchers, check with the hotel that they will be honoured at the time of year you are planning on travelling.

Also be cautious when deciding to buy cheap airfares online. Scammers set up fake but convincing sites and offer fake tickets. Check that the ABN quoted on a flight booking website is genuinely registered to the trader. You can look up an ABN at www.business.gov.au.

Beware of costly scam travel and accommodation clubs which don't deliver on what is promised. Never give your credit card details to someone you don't know or trust.

Online shopping: Buying online can be cheaper, but if you get caught by a scammer you will lose your money and never receive the item you thought you were buying. Scammers post fake classified ads, auction listings and run bogus websites for everything from pets and electronics to fridges, cars and boats.

Avoid any arrangement with a stranger that asks for an up-front payment via money order or wire transfer—scammers will try to encourage you to pay outside of the website's official payment systems. Some scammers will send you emails that appear to be from official payment systems requesting payment, others will try to direct you to a fake payment website which looks genuine but has a slightly different URL.

Parcel delivery: If you have shopped online or are expecting a parcel from family or friends—beware. Scammers may call or email pretending to be from a logistics or parcel-delivery service, claiming that a parcel could not be delivered to you. They will offer to redeliver the non-existent parcel in exchange for a fee and may also ask for personal or credit card details.

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

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

Gift vouchers: Gift vouchers make handy gifts, but always buy them from an official source. Recent scams have involved fake gift vouchers and 'free products' being offered through social networking sites.

Scammers will ask you to give personal details via surveys in return for vouchers and products which either never arrive or are not honoured. Scammers commonly use these surveys to steal your personal information.

Again, if you doubt the authenticity of a free offer, contact the company on their official customer service number to verify it.

Charities: Many legitimate charities appeal for donations of money, food, clothing and children's gifts at Christmas. Not surprisingly, scammers take advantage of people's generosity at this time of year and may try to disguise themselves as genuine charities. Approach charity organisations directly if you want to make a donation or offer support.

Weight loss: The classic New Year's resolution. You may be looking to shed unwanted Christmas kilos, but watch out for scammers offering 'miracle' weight loss pills and potions. These scams may promise weight loss for little effort or may involve restrictive diets, 'revolutionary' exercise or fat-busting devices or other products. These products may not produce the results that are promised.

Full details about how these scams operate and how to protect yourself are available at **www.SCAMwatch.gov.au**. To stay one step ahead of scammers, follow @SCAMwatch_gov on Twitter or visit **http://twitter.com/SCAMwatch_gov**.

The Australian Government has established the Stay Smart Online website, which provides information on the simple steps internet users can take to protect their personal and financial information. Visit **www.staysmartonline.gov.au**.

As well, *Protecting Yourself Online—What Everyone Needs to Know* is a publication that combines information and advice on internet security from a range of Australian Government agencies.

*The booklet and brochure are available at **www.ag.gov.au/cybersecurity.** You can request printed copies by emailing **cybersecurity@ag.gov.au.***