Online presentation summary

Australian Government

Be Connected
Every Australian online.

Safer online shopping – Festive season edition

The festive season is a busy and often stressful period for many Australians, as people spend more time and money shopping and planning for festive activities online. It's also a busy time for scammers! Shop online with confidence by following our safety tips and enjoy the many benefits that the internet can provide.

Tips for safer online shopping

Use secure websites and payment methods

Before you enter personal or payment details online, check how secure the website is. Look for a padlock beside a website address in the address bar or a URL that starts with 'https' instead of 'http'. This can mean a site is more secure than other sites.

When making online payments, only pay for items using a secure payment method like PayPal, BPay or your credit card. Using credit cards can minimise risk when shopping online because they offer extra protection and make it easier to get your money back if anything goes wrong.

Never pay by direct bank deposits, money transfers or other methods (like a pre-loaded card or Bitcoin).

Use trusted sellers

Research online shopping websites before you buy and stick to well-known, trusted retailers. Search for reviews from other customers. Look for a physical address and/or a phone number and try calling it to see if somebody answers.

Read the terms and conditions

Before you buy, read the fine print including warranty, refund, complaints and handling. Familiarise yourself with the retailer's cancellation and returns policy and find out key information you may need like who pays for the return shipping, do you get a full refund or store credit and how long is the return period.

Keep your device secure and up to date

Use strong passwords and make sure automatic updates are enabled on your device. Use antivirus software such as McAfee or Norton. When prompted, install or agree to software updates for your operating system and browsers such as Chrome, Firefox and Safari. This helps to provide better protection against malware.

Be alert to online shopping scams

Online shopping scams involve scammers pretending to be legitimate online sellers, either with a fake website or a fake ad on a genuine retailer site. Keep in mind that scammers:

- often only accept payment in the form of money order, wire transfer, international funds transfer, pre-loaded card or electronic currency like Bitcoin
- don't provide contact details or have limited information about delivery and other policies
- are often selling goods at prices that are too good to be true
- are often a very new online store with very few reviews
- often have poor reviews.

The best way to detect a fake trader or social media online shopping scam is to search for reviews before purchasing.

Scams to watch out for

Scammers take advantage of busy times, so it pays to be alert and look for the signs of a scam.

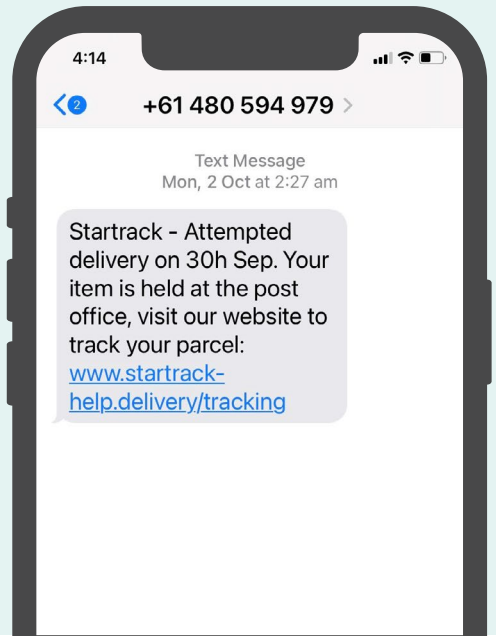
Missed parcel delivery scam

Missed parcel delivery scams are attempts by scammers to trick you into believing that they are from a trusted parcel delivery service organisation to get you to give out personal information such as your credit card details. You might receive an email, text or call from a scammer pretending to be from a service provider like Australia Post or FedEx, saying you've missed a delivery and that you need to pay a fee to have the parcel redelivered or held in their warehouse. Alternatively, they may ask you to click on an attachment or link, which will then download a virus to your computer.

How to protect yourself

- If you're unsure about a message you've received, call the delivery company. Look up their number - don't rely on the contact details provided in the message as they may be fake.
- Use the tracking number provided by the store to track your parcel, either through their site or directly via the courier's site.
- Don't click on links or download files, especially if they're executable (.exe) files or zip (.zip) files.

Remember: Parcel delivery services will put a notice in your letterbox if a package was undeliverable. They'll never ask for payment to hold or redeliver your parcel.



Travel prize scam

Travel prize scams involve an unexpected email, letter, text or a call from a scammer trying to trick you into believing that you have won a holiday or a great deal on a holiday even though you haven't entered a competition.

The scammer will then ask you to pay a fee or provide financial or identity details so you can claim your prize.

How to protect yourself

- Don't pay a fee to collect a prize or winnings. Legitimate lotteries don't ask you to do this.
- Never share your bank or credit card details or your identity documents to anyone you don't know or trust.
- Don't click on pop-up messages on the internet saying you've won a holiday or any other prize – ignore them.
- Don't fall for high pressure tactics – if something doesn't feel right, hang up or tell them you need time to think about it.

There's help when you need it

When things don't go as planned online, there's always somebody you can talk to.

1. First, contact the online seller or website.
2. If you can't resolve your problem directly with the online retailer, your local state or territory consumer protection agency (sometimes called 'consumer affairs' or 'fair trading') can provide you with information about your rights and options. They may also be able to help negotiate a resolution between you and the seller.
3. If you suspect you have been scammed:
   - Contact your bank or financial institution immediately to stop any further payments to the scammer.
   - If you have experienced cybercrime and lost money online, you can report it to the police via ReportCyber or visit: cyber.gov.au
   - If you are concerned that your personal information has been exposed and misused, contact Australia's national identity and cyber support service IDCARE on 1300 432 273 or idcare.org
   - Report the scam to the National Anti-Scam Centre at scamwatch.gov.au/report-a-scam. This helps to warn others about current scams, monitor trends and disrupt scams where possible.

Tip: the Australian Competition and Consumer Commission has a complaint letter tool you can use to help you draft a letter or email to the seller.

To keep up to date with the latest scams to avoid, subscribe to receive scam alert emails.

Take the time to discover Be Connected

Be Connected is a comprehensive website with free resources specifically designed to support older Australians to connect online safely and navigate the digital world confidently. The site is also useful for families and community organisations who want to help older community members access all the benefits of the internet.

visit beconnected.esafety.gov.au

Australian Government | eSafety Commissioner

This program has been developed by eSafety as part of the Be Connected initiative.