

# eSafety with Be Connected

## Safer online shopping - Christmas edition

### 5 steps to a safer online shopping experience

#### 1. Only shop on secure sites

Look out for the 'https' in the address bar and the closed padlock icon – they indicate the page you're on is safe and secure.

#### 2. Before you pay, know who you're buying from

Do your research: read the 'About Us' section and type the retailer's name into Google to check for reviews. Look for a physical address and/or a phone number and try calling it to see if somebody answers.

#### ✓ Tip

Avoid using public Wi-Fi when entering personal information such as bank account and credit card details, or usernames and passwords.

#### ✓ Tip

Stay alert when shopping on social media sites such as Facebook and Instagram.

#### 3. Look for detailed terms and conditions

Familiarise yourself with the retailer's cancellation and returns policy. How long do you have to return the item, and who pays for the return shipping? Do you get a full refund or a store credit? If they only offer a store credit, are you likely to buy from their product range again?

#### 4. Use a secure payment method

PayPal and credit cards are the safest way to pay for goods online because they offer extra protection and make it easier to get your money back should anything go wrong. Always check your statements and keep confirmation emails of your online purchases.

#### 5. Keep your computer secure and up-to-date

Use strong passwords and make sure automatic updates are enabled on your device. 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.



## If your online shopping experience doesn't go as planned:

1. Try resolving the problem directly with the online retailer or seller first.
2. Contact your bank, PayPal or credit card company.

### ✓ Tip

Know your consumer rights. When you buy products online, you're covered by Australian Consumer Law. If a product or service you buy fails to meet a consumer guarantee, you have the right to ask for a repair, replacement or refund.

Go to: [www.consumerlaw.gov.au](http://www.consumerlaw.gov.au)

If you've received an unsafe product, you can contact the ACCC or your local consumer protection agency.

Go to: [www.productsafety.gov.au/reportanunsafeproduct](http://www.productsafety.gov.au/reportanunsafeproduct)



## Scams to watch out for around Christmas

While there are scams that are more popular at certain times throughout the year, online safety advice remains the same all year round.

### Missed parcel delivery scam

- You receive an email, text or call from what appears to be a legitimate parcel delivery service like Australia Post or FedEx, saying you've missed a delivery. In some cases, the email may even include your name and address.
- You're asked 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.

### Stay ahead of the scammers:

- 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.
- 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 scams

Travel scams come in many forms, but the common theme is a message that arrives out of the blue saying you've won a free holiday or scored a great deal on a holiday. It can be a pop-up message that appears while you're browsing the internet or a message received after filling out an online survey.

### Remember

You can't win a prize if you haven't entered the draw.

### Do not:

-  Provide your bank account or credit card details, driver's licence or passport information to somebody who has called you out of the blue claiming you've won a prize.
-  Click on pop-up messages on the internet saying you've won a holiday or any other prize. Ignore them!
-  Make any payments to claim a prize.
-  Fall for high pressure tactics – if something doesn't feel right, hang up or tell them you need time to think about it.

### Tip

If you see a well-known product or brand advertised at a considerably discounted price, it's very likely to be fake or second-hand, or does not exist at all.


**Do your research before you buy.**

## Fake online deals and websites

### Some tell-tale signs of a dodgy website

- Web address. Carefully read the website address and look for missing or extra letters in the brand name, or words like "deals", "sales" or "discounts" as part of the address. For example, [webberbbqdiscounts.com.au](http://webberbbqdiscounts.com.au) is a fake site, the official site is [weberbbq.com.au](http://weberbbq.com.au).
- Method of payment. They may ask for payment via non-secure forms such as money order, gift card, bitcoin, wire transfer, etc.
- Websites that don't provide adequate contact details like a phone number or a physical street address and instead only have an email address or PO Box.
- Vague details in the 'About Us' section or in their returns policy, if they even have one.

### Stay ahead of the scammers

- Stick to reputable retailers you know.
- If the deal looks too good to be true, type in the seller or website's name into Google to check for reviews. For example, if the web address is [www.myoffer.com](http://www.myoffer.com), type in: myoffer reviews.
- Remember to look for the 'https' in the web address and the locked padlock symbol. 
- If it's an Australian site, you can check if the ABN is legitimate at: <http://abr.business.gov.au>

## Help! I think I've been scammed

1. Contact your bank immediately to stop any future payments or ask to have payments reversed.
2. Contact iDcare if you think your identity has been compromised:  
**1300 432 273** or [www.idcare.org](http://www.idcare.org)
3. Report the scam to Scamwatch to help warn the community:  
[www.scamwatch.gov.au/report-a-scam](http://www.scamwatch.gov.au/report-a-scam)
4. Change your online passwords.
5. Counselling and support services are also available:  
Lifeline **13 11 44**  
Beyondblue **1300 22 4636**  
MensLine **1300 78 99 78**

## Five things to remember

1. Do your research.
2. Make payments via secure methods such as PayPal or credit card.
3. If you're unsure about a message you've received, ask somebody or call the company direct - don't use the contact details in the message.
4. Slow down and carefully re-read messages. What are they asking you to do? Does it sound right to you? Don't click on links or open attachments.
5. Help is always available when you need it.

### ✓ Tip

Stay up-to-date with the latest scams by subscribing to the **Scamwatch** alert service. You can also follow them on Facebook or Twitter.

[www.scamwatch.gov.au/news/subscribe-to-scam-alert-emails](http://www.scamwatch.gov.au/news/subscribe-to-scam-alert-emails)

### i Take the time to discover Be Connected

Find out more hints and tips on how to stay safer online, plus there are fun hobbies you can learn to do online like research your family history and discover the amazing Google Earth from the comfort of your own home. For registered users, there's a free eBook you can download that'll show you how to build your own family tree.

Take a look today:

<https://beconnected.esafety.gov.au>

