

Introduction

Online shopping has made the shopping experience more efficient and accessible for purchasing goods and services, but not every website or seller is legitimate. Online shopping scams may take payment for products that never arrive, request unnecessary identity documents, or direct you to potentially unsafe payment methods.

This fact sheet will provide some tips on how to shop online safely and steps you can take if something goes wrong.

Protecting yourself online

- ☐ Research the website or seller before buying. Checking independent reviews and comments from other buyers can help you assess whether the seller is legitimate.
- ☐ Use secure third-party payment methods like PayPal where possible. Be cautious of sellers who push for direct bank transfers, prepaid cards, or gift cards.
- ☐ Avoid clicking on pop-ups or links in advertisements. Go directly to the retailer's official website.
- ☐ Be cautious if a seller requests identity documents or personal information that is not reasonably required for the purchase. Where a copy is genuinely necessary, redact information that is not required, especially document numbers.
- ☐ Keep records of seller communications and keep track of order confirmations, receipts, reference numbers, and shipping information for each purchase.
- ☐ Treat prices that are significantly lower than everywhere else as a warning sign, particularly for popular products.
- ☐ Use caution if the seller asks to continue the conversation outside the original platform as this can be an attempt to remove certain buyer protections.

Common online shopping scams

- ☐ **Fake retailer websites:** Scammers set up websites that look like genuine retailers. The websites may advertise the same products as legitimate sites but at reduced prices.
- ☐ **De-platforming:** Sellers may attempt to make a deal outside of the original website or platform to trick you into giving them money or personal information. Since these transactions happen outside of a legitimate website, it is unlikely you will recover funds sent.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document,

IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Common online shopping scams cont.

- ☐ **Buyer fraud:** Criminals may also pose as buyers to try to get you to refund money they have purportedly sent or pay advance fees for shipping.
- ☐ **Online marketplaces:** Scammers may pose as legitimate sellers using fake listings and then disappear once payment has been made. They may provide a fraudulent link for payment that impersonates a legitimate payment platform. In some cases, the scammer may request identity information or share previously stolen identity documents to appear more credible.

Response checklist

If you suspect your identity has been compromised, or if you have sent money to a scammer, there are steps you can take to limit damages:

- ☐ If you've sent money or banking details, contact your bank or card provider immediately.
- ☐ Stop all contact with the suspected scammer and do not send any further money, including fees they claim are required to release or deliver the order. Identify any personal or identity documents that were exposed. Contact the organisation that issued each document, such as your state or territory driver licensing authority or the Australian Passport Office and follow its advice about securing or replacing the document.
- ☐ Be cautious of anyone who contacts you unexpectedly and promises to recover your money for an upfront payment. This may be a second scam targeting previous scam victims.
- ☐ Report online shopping fraud to [Report Cyber](#) (in Australia) or contact New Zealand police by calling 105 or [online](#)

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 160 (Aus) | 0800 121 068 (NZ)

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.