



# Buy/sell scams



Buy/sell scams are typically seen within the online retail sector, with scammers setting up fake websites or profiles on legitimate retailer sites. Online marketplaces have also become a target for scams, with scammers posing as both online buyer and sellers.

## How to spot a buy/sell scam

Scammers set up accounts or use hacked accounts to pose as sellers (or buyers) on popular online marketplaces such as Facebook, Gumtree or eBay. They may even create fake adverts or post fake reviews.

## If you're a seller

- The buyer is willing to buy a valuable or highly priced product without viewing it in person, or states that a friend or family member will be collecting the product.
- The buyer asks to pay via PayID, direct bank transfer or crypto currency.
- The buyer will overpay and then ask you to pay the difference back to them.

## If you're a buyer

- The seller offers unrealistic pricing, if it feels too good to be true, it probably is.
- The seller requests payment via PayID, money order, pre-loaded card or to pay to several PayID's or accounts.
- An online store does not have any terms and conditions, ABN or privacy policy on their website.
- You receive an invoice for a product or service you haven't purchased, or new payment details which do not match the identity of the account holder or are different to historical payments you've made.

## How to protect yourself

- Check the website for information about privacy, terms and conditions of use, dispute resolution and contact details as well as secure payment services such as PayPal or credit card.
- Be wary of social media stores or adverts for new products at low prices. Always verify the organisation before making a payment.
- Check for minor differences in website URLs that may act to imitate legitimate business such as additional or missing characters.
- Research the seller by checking independent reviews of online stores or the seller history on classified websites.

### Stop

Say no, hang up or delete suspicious messages. Take your time, trust your instincts and avoid giving out any personal information or money if you're unsure.

### Check

Ensure the person you're dealing with is real. Contact organisations directly using contact details you find yourself. Verify investment offers through ASIC and confirm with family, friends or a professional before acting.

### Protect

Act quickly if you're concerned you've been in contact with a scammer. Contact us immediately and help others by reporting scams to Scamwatch ([www.scamwatch.gov.au](http://www.scamwatch.gov.au)) or the police ([www.cyber.gov.au](http://www.cyber.gov.au)).

**People First Bank will never contact you to request your passwords, VISA card or account details.**

We will not send you SMS containing links. Never share your password or Online Banking login credentials.

If you have been contacted or are concerned about your privacy, please call us directly on **13 11 82** or visit a branch.