Buy/sell scams

People's Choice
Banking for life

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 cryptocurrency.

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

Take a moment to stop and assess the request. Most scams will aim to generate a sense of panic and urgency. Don't share personal or banking information if you're unsure.

THINK

Ask yourself if the request makes sense. If you provide the requested information will you be granting access to your devices, accounts or money?

CHALLENGE

Refuse to provide information, access and ignore requests. Hang up and call the organisation directly.

People's Choice will never contact you to request your passwords, VISA card/rediCARD or account details. We will not send you SMS containing links. Never share your password or Internet 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.

Scan the QR code to learn more about digital banking security.

BRC_8.6.225 V1.0-1123. People's Choice Credit Union (People's Choice).