











Spot the red flags of buying and selling scams

Beat the scammers by knowing the scam

Purchasing scams have recently been on the rise, with fraudsters active on both sides of a transaction. These scams take place on common ecommerce platforms used by genuine people, such as eBay, Gumtree, Facebook Marketplace and Carsales. Staying alert to the red flags below can help you spot a scammer and avoid falling victim to online fraud.

These simple steps can help prevent loss of money or personal information to scams:

Spot the red flags

-  **Identification documents.** You are asked to provide identification documents such as driver's license, passport or Medicare card number.
-  **Messaging apps.** You are asked to switch the conversation to a different platform such as WhatsApp or Messenger.
-  **Payment method.** Be cautious if asked to use payment methods such as gift cards, cryptocurrencies, money wiring services or PayPal's 'Family and Friends' method.
-  **Overpayment of funds.** A buyer falsely claims that they have overpaid you and requests that you return some of the funds to them.
-  **Upfront shipping cost.** The buyer asks you to pay upfront for transportation or shipping costs, promising to reimburse you.
-  **Communication stops.** After you send the item or pay for an item the communication stops so you can't be reimbursed for postage, or you never receive the item you paid for.
-  **Prices below usual.** If an item is advertised at a price that is well below the usual selling price - it seems too good to be true, it usually is.
-  **Communication only via email.** The buyer/seller claims they are on deployment in the armed forces, overseas, travelling, or unwell and so can only speak over email rather than on the phone, on a video call or in person.



more
than
money



Stop, Check, Protect

to minimise your chance of being scammed



Stop before you act

Where possible do some research on the buyer or seller and look for reviews and meet in person to exchange the item and cash if possible.

Conduct a reverse image search on Google for the photos of the item you are buying – you may find the picture of the item already exists on a legitimate ad, or in other fake ones, so **stop** to consider, could this be a scam?



Check before you share

Use secure payment options that come with protections, such as PayPal (not PayPal family and Friends) or a credit card.

Check your bank account to ensure the funds have cleared before proceeding with the sale. Be cautious of buyers asking to charge them extra to cover transportation costs.



Protect if you suspect

Acting quickly if something doesn't feel right goes a long way in helping to **protect** your money and information, so if you think you've been scammed or your banking details have been compromised, call us on **13 22 65** and ask for our Fraud team.

Find out more

Visit nab.com.au/security

For more tips on protecting yourself, visit nab.com.au/buyingsellingscams

