CHECKLIST · SCAMS & SECURITY

Buying and selling scams are six in 10 scam-loss reports to Scamwatch

Published 7 November 2026. Read the full story, sources and any updates at digitaladvisors.com.au/journal/scamwatch-shopping-scams-2026-figures/

- [ ] **Go to the shop yourself.** Type the retailer's web address rather than following an ad, social post or message.
- [ ] **Pause when a site rushes you.** Big discounts, countdown timers and pressure to pay immediately are reasons to check the seller first.
- [ ] **Read the web address letter by letter.** Look for extra dashes or symbols, or a name that imitates a real business, such as Ap9le.
- [ ] **Look up the ABN.** Check it on the ABN Lookup service at business.gov.au, and remember a real ABN can be copied by a fake shop.
- [ ] **Match the payee name.** When paying by PayID or bank transfer, make sure the account name matches the business or person you think you're paying.
- [ ] **See big-ticket items first.** Don't pay for a car, caravan or boat before inspecting it in person.
- [ ] **Keep sales on the platform.** If you're selling, keep messages and payment inside the marketplace, and don't follow a link to "verify" your account to get paid.
- [ ] **If you've paid or shared bank details, call your bank now.** Change any passwords you gave away, turn on multi-factor authentication, report it at scamwatch.gov.au or reportcyber.gov.au, and contact IDCARE if you need help with your identity.

General information only, not legal, tax or financial advice. Check the full story and its sources before acting.