CHECKLIST · SCAMS & SECURITY

Black Friday scams: fake shops, fake parcels and fake buyers

Published 23 November 2026. Read the full story, sources and any updates at digitaladvisors.com.au/journal/black-friday-cyber-monday-scams/

- [ ] **Go to shops directly.** Type the retailer's web address yourself instead of tapping a sale ad or a link in a message.
- [ ] **Look up the ABN.** Check the shop's ABN on the government's ABN Lookup before you buy.
- [ ] **Check when the website was registered.** Use ICANN Lookup, and auDA's WHOIS to see who registered a .com.au address.
- [ ] **Search the shop's name with "scam" or "review".** Read independent reviews, not just the ones on the shop's own site.
- [ ] **Pay by credit card or PayPal.** Don't pay by gift card or crypto, and check the payee name matches the shop before any PayID or bank transfer.
- [ ] **Check parcels in the courier's own app.** Don't tap links in delivery texts or emails; check in the AusPost app or on the courier's own website.
- [ ] **Keep marketplace sales on the platform.** Never follow a link in a message saying your item has sold, and never refund a buyer's overpayment.
- [ ] **Call your bank straight away if you've been caught.** Then change your passwords and report it to Scamwatch and ReportCyber.

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