CHECKLIST · SCAMS & SECURITY

ASOS says names and contact details may have been accessed after a rogue app alert

Published 9 October 2026. Read the full story, sources and any updates at digitaladvisors.com.au/journal/asos-app-hacked-notification-october-2026/

- [ ] **Ignore the ASOS HACKED notification.** Don't tap its link or reply to the senders; ASOS has asked customers not to click or engage with it.
- [ ] **Open ASOS yourself.** If a message about your ASOS account or order arrives, close it and check by opening the app or typing the website address.
- [ ] **Change reused passwords.** If your ASOS password is also used on another account, especially your email, change that account's password today.
- [ ] **Turn on multi-factor authentication for your email.** Your email account is the key to resetting every other password, so protect it first.
- [ ] **Hang up and call back on unexpected calls.** If a caller says they're from ASOS or your bank about this incident, call back on a number you've looked up yourself.
- [ ] **Watch your bank and card statements.** ASOS doesn't believe card details were affected, but keep checking for unfamiliar transactions, because scams can follow a breach some time later.
- [ ] **Warn the shared inbox.** If your business orders from ASOS on a work account, tell whoever reads that inbox to expect fake ASOS emails.

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