

CHECKLIST · SCAMS & SECURITY

Hijacked Shopify app settings sent shoppers to fake checkouts: what to check on your store

Published 16 October 2026. Read the full story, sources and any updates at digitaladvisors.com.au/journal/shopify-apps-hijacked-fake-checkout/

-
- ☐ **Run the private-window checkout test.** Open a fresh incognito window, add an item to the cart, click checkout and confirm the address is your real checkout.
 - ☐ **Check your installed apps.** Look for Selleasy, Hulk Product Options and Swym Wishlist Plus, and ask each developer whether your store was among those affected.
 - ☐ **Check custom JavaScript fields in app settings.** Report any script you or your developer didn't add to the app developer and Shopify.
 - ☐ **Change passwords and turn on two-factor authentication.** Do it for your Shopify account and every app developer account linked to the store.
 - ☐ **Contact the app developer and Shopify straight away if checkout redirects.** Tell them which app is installed and what the test showed.
 - ☐ **Assess whether customers entered card details.** If the Privacy Act covers your business, use the OAIC's guidance to decide whether you have a notifiable data breach.
 - ☐ **Report the incident.** Use "Report a cyber security incident" at cyber.gov.au/report if your store was affected.
-

NOTES

More free checklists, plus the Friday briefing: digitaladvisors.com.au/newsletter

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

Page 1 of 1