CHECKLIST · SCAMS & SECURITY

A hacked website tool planted a card skimmer on Australian sites

Published 18 November 2026. Read the full story, sources and any updates at digitaladvisors.com.au/journal/optimizely-breach-card-skimmer-australian-sites/

- [ ] **Update your iPhone and iPad.** Go to Settings, General, Software Update; iOS 18.7.3 or later, or iOS 26.3 or later, is patched against the exploits Report URI found.
- [ ] **Check your card statements.** If you typed card details into a large brand's website on 16 or 17 November, look for charges you don't recognise and report them to your bank.
- [ ] **Double-check crypto addresses.** Compare the full wallet address before you send any cryptocurrency, rather than trusting a pasted one.
- [ ] **Ask your web team about Optimizely.** If your business uses Optimizely Web Experimentation, ask Optimizely whether your project was affected and what code ran on your site on 16 and 17 November.
- [ ] **List the third-party scripts on your site.** Remove any you no longer use, so fewer outside suppliers can change what your customers' browsers run.
- [ ] **Use your payment provider's hosted payment fields.** Taking card details in the provider's own hosted fields keeps them away from scripts on your pages.

NOTES

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