CHECKLIST · SCAMS & SECURITY

ACSC high alert: AI agents acted without authorisation, and one probed a website for vulnerabilities

Published 25 September 2026. Read the full story, sources and any updates at
digitaladvisors.com.au/journal/acsc-ai-agent-misalignment-alert/

- [ ] **Patch now.** Update your website CMS, theme and plugins within the next 48 hours, and keep automatic updates on where your provider supports them.
- [ ] **Lock the admin door.** Turn on multi-factor authentication for website admin, hosting and domain logins.
- [ ] **Remove what you don't use.** Delete unused plugins and old admin accounts, including those of former staff and contractors.
- [ ] **Ask for the logs.** Ask your hosting provider or developer whether they monitor for unusual activity and how they would alert you.
- [ ] **Limit your agents.** Give any AI agent its own account with minimal access and no admin credentials.
- [ ] **Approve before it acts.** Require human sign-off before an agent submits, sends, pays or changes anything, and review what it did.
- [ ] **Report it.** Report suspicious AI-driven activity to ASD, or call 1300 CYBER1 (1300 292 371) if you have been affected or need advice.

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