OPTIMJACK

Response checklist



Six checks for investigating the Optimizely Web compromise. Check off the subtasks as you complete each step.

1 Audit every Optimizely Web project

- [ ] Inspect **Project JavaScript** in every project. A text search of the delivered snippet alone is insufficient.
- [ ] Audit any copy of the snippet hosted on your own domain.
- [ ] Save suspicious code for incident records before removing confirmed malware.

2 Block known domains and review logs

- [ ] Add known OPTIMJACK domains to DNS and proxy deny lists.
- [ ] Review logs from **04:00 UTC on November 16, 2026** onward for matches.

3 Lock down vendor access

- [ ] Audit every user and API token on your Optimizely account.
- [ ] Revoke access you cannot identify.
- [ ] Ask Optimizely which projects changed, when, and under which account.

4 Preserve browser evidence

- [ ] Save **Content Security Policy (CSP) reports** and browser telemetry.
- [ ] Use calls or attempted calls to attack domains to identify affected pages.

5 Assess customer exposure with your teams

- [ ] Check whether customers entered payment details or copied wallet addresses on affected pages during the incident.
- [ ] If so, involve **payments, fraud and legal** to decide next steps.

6 Inventory scripts on sensitive pages

- [ ] List every script on checkout, login and account pages, and its source.
- [ ] Record what data each script can reach.
- [ ] Record who can change each script.

FREE WEB SCANNER ASSESSMENT

See what runs on your checkout.

Inventory scripts and see which can access customer data.

Get a Free Assessment →

feroot.com/checkout-scanner