State of Shopify Security

Passive measurement of 1676 live stores · 2026-11-01

Method

Latest passive scan of each benchmark store (stratified sample of Shopify stores across countries and sizes; 1676 reachable with a Trust Score). Only public GET requests, public DNS/TLS and robots.txt were used: no forms, logins or payments, and look-alike domains were only resolved in DNS. Figures are unweighted shares of the stores where each check could be measured. Segments are shown only with N ≥ 30. No store is named.

Key findings

Finding	Stores %	Measured (N)
Domain can be spoofed in email (no DMARC, or DMARC p=none)	83.8	1676
No SPF record	35.6	1676
DMARC without aggregate reports (nobody sees abuse)	64.6	1059
MX pointing to a host that doesn't resolve	1.9	1282
Look-alike domains with mail, owned by third parties	8.7	1676
Third-party scripts without integrity (SRI) on static CDNs	10.3	1675
Code with skimmer-like signatures (strong: fail; weak: review)	0.8	1667
...of which strong signatures (card-field reads, keyloggers with exfiltration)	0.0	1667
Scripts from domains imitating a CDN or brand	1.0	1675
Script from an unregistered/expired domain (anyone can buy it and serve code)	0.1	1675
Broken script tags (host doesn't resolve, domain still registered)	3.0	1675
JavaScript libraries with known CVEs	6.1	1675
Legacy ScriptTags from apps (not removed on uninstall)	44.6	1645
Subdomain takeover risk (dangling CNAME/NS)	0.3	1676
Trackers firing before consent (EU/UK/BR markets)	0.7	1675
No reachable privacy policy	5.7	1622
Basic accessibility gaps on the home page	9.9	1675
Zone not DNSSEC-signed	94.6	1676

Finding	Stores %	Measured (N)
No CAA record (any CA can issue certificates)	99.3	1676

Store Trust Score

Median 80 (p10 73, p25 77, p75 83, p90 86), 0–100, higher is better (trust-1.1).

Band	%
Good	79.8
Strong	17.1
Fair	2.9
Critical	0.2

By segment

Country

Segment	N	Median Trust	Spoofable %	No SRI %	Legacy ScriptTags %
US	456	79	84.0	12.7	54.2
MX	110	81	75.5	7.3	34.5
GB	107	79	88.8	15.0	56.1
CL	106	81	88.7	9.4	31.1
AU	80	80	81.3	10.0	47.5
CA	74	80	91.9	9.5	52.7
CO	74	81	75.7	6.8	29.7
IN	70	79	71.4	7.1	41.4
ES	65	81	73.8	6.2	36.9
BR	57	81	73.7	10.5	21.1

Monthly sales (USD, estimate)

Segment	N	Median Trust	Spoofable %	No SRI %	Legacy ScriptTags %
<10k	926	81	83.7	7.2	29.3
10k–100k	518	79	88.4	13.3	56.9
100k–1M	215	79	75.3	15.8	72.6

Plan

Segment	N	Median Trust	Spoofable %	No SRI %	Legacy ScriptTags %
Shopify	1546	81	84.8	10.0	42.2
Shopify Plus	108	78	73.1	16.7	75.0

Observation: one imitation CDN, many stores

17 stores load scripts from `shopify.jsdeliver.cloud`, a domain whose name imitates jsdelivr. Whoever controls the domain can change the code served to all of these stores at once. Stores are not named here; affected merchants see it in their own report.

What a store should do first

1. Publish DMARC with p=quarantine or p=reject and a rua address (after SPF and DKIM are aligned).
2. Inventory every third-party script on storefront and checkout (PCI DSS 6.4.3); remove what nobody owns.
3. Remove ScriptTags and theme snippets left by uninstalled apps.
4. Remove tags pointing at hosts that no longer resolve; buy or block expired script domains you depended on.
5. Add a CAA record and, where your DNS host supports it, DNSSEC.

Limits

Passive checks see what a visitor's browser sees: checkout internals, admin settings and server-side controls are not observable. Skimmer signatures are heuristics and a 'review' is not an incident. Shares are not weighted to the full Shopify population.