

Shining a light on web skimming:

7 security stats for eCommerce merchants

Small and medium sized eCommerce businesses are target #1 for online payments fraud

But knowledge (and awareness) is power. Here's what your eCommerce merchants are up against and how, together, you can combat cyber-attacks.

46%
of cyber breaches impact businesses with **1,000** employees or less

51%
of impacted websites are down for 8-24 hours after a breach

95%
of small business cybersecurity incidents cost an average of **\$650K**

Don't let online fraud sink your business

Cyber criminals are launching sophisticated web skimming attacks on SMBs. In fact, impacted merchants often don't know they've been compromised until someone outside of their organization has notified them of the breach.

On average, it takes **204 days** to identify a breach and **72 days** to contain it

\$165
is the average cost per record involved in a data breach

Every fraudulent transaction costs businesses **3.49x the lost** transaction value, on average



How web skimming works

Breach
Attacker compromises the website

Inject
Malicious code is added to the payments script

Collect
Card data is copied and sent to the attacker

So long, skimmers. Hello PCI DSS.

PCI DSS is the global security standard adopted by the payment card brands. Its primary goal is to increase awareness of good data security practices and reduce fraud for everyone in the payments ecosystem. Due to the rise in web skimming attacks, PCI DSS 4.0 includes more stringent controls to help SMBs and software providers protect themselves and cardholders.



Safeguard every transaction

Help ensure everyone has the necessary safeguards in place by preparing for the new PCI 4.0 requirements. We know PCI compliance can be tough to navigate, we're here to help.

Are you ready for PCI DSS 4.0?

[Learn more](#)