



Top 5 Hidden Threats Costing SMB Retailers' Revenue — And How to Stop Them

c/side: **Campaign Strategy Concept**

Author: Christopher "Keith" N. Carlos

© 2025 Copyright. All rights reserved worldwide.

July 10, 2025

Campaign Title:

"Top 5 Hidden Threats Costing SMB Retailers' Revenue — And How to Stop Them"

Target Audience:

- SMBs/SMEs ecommerce and retail companies
- Geography: US, EU (Western), APAC, GCC + Global (with landing page localization)
- Roles: Owners, CTOs, Ecommerce Managers, Site Ops, and Security/Compliance Leads

Channel Strategy (Omnichannel):

- LinkedIn InMail (ABM-focused, warm & cold)
- LinkedIn Organic + Paid (carousel + dark posts)
- Email CRM (MQL > SQL nurturing)
- Website, Landing Page, Content Pillars, and Target Audience-specific pages
- YouTube Shorts (educational, 60s format)
- Google Ads (Display + Search)
- Twitter/X + Reddit (security and ecommerce threads)
- Quora Ads (targeting “website security”, “why is my checkout broken?”)

Lead Magnet

- PDF: “Top 5 Hidden Threats Costing SMB Retailers' Revenue — And How to Stop Them”
- CTA: Instant download
- Supports funnel via gated landing page + retargeting

LinkedIn InMail – Subject Line + Message

Subject:

“Is your checkout leaking revenue? (5 threats you didn’t know to check for)”

Message:

Hi [Prospect],

Your website may appear secure, but hidden client-side threats are silently stealing data, hijacking sessions, and compromising checkouts. For small to medium-sized business ecommerce and retail brands, one invisible breach can result in thousands of lost sales, abandoned carts, or regulatory fines.

We put together 5 must-know client-side risks every growing brand should be aware of. More importantly, we have tips on how to stop them.

Download the quick-read PDF here: [Landing Page Link]

Or feel free to DM me for a copy.

Let’s make sure your customers convert—securely.

– [Name], on behalf of c/side

Top 5 Tips in the PDF (headline bullets):

1. Stop Third-Party Script Hijacks
2. Prevent Checkout Breakage from Geo-Targeted Malware
3. Block Formjacking Before It Reaches Your Cart
4. Secure Browser Extensions Your Users Don’t Know Are Infected
5. Detect & Resolve in Real-Time with AI-Powered Indicators