SECURITY INSIGHTS:

Your 'Privacy' VPN Might Be Selling Your AI Conversations

Genady Vishnevetsky, Chief Info Security Officer, Stewart Title Guaranty Company

Have you ever shared something deeply personal with ChatGPT or Claude? A health question you were too embarrassed to ask your doctor? Financial details while sorting out your budget? Work frustrations you wouldn't share with colleagues? You're not alone. Millions of people treat AI assistants with a level of candor they don't have with most humans.

Now imagine all of that-every prompt, every response, every private thought-being captured and sold to advertisers. That's exactly what's happening to over 8 million users of popular browser extensions like **Urban VPN Proxy**.

Urban VPN Proxy has over 6 million users, a 4.7-star rating, and Google's "Featured" badge-meaning it passed manual review and supposedly meets "a high standard of user experience and design." It's exactly the kind of tool someone installs when they want to protect their privacy online.

Security researchers recently discovered this privacy tool has been secretly harvesting complete conversations from ten AI platforms: ChatGPT, Claude, Gemini, Microsoft Copilot, Perplexity, DeepSeek, Grok, and Meta AI. Every prompt you send. Every response you receive. Timestamps, session data, which AI model you used-all of it packaged and transmitted to Urban VPN's servers.

When you visit any of these AI platforms with the extension installed, it injects monitoring code directly into the page. This code intercepts every communication between you and the AI-before your browser even displays the response. The data gets compressed and sent to their servers, regardless of whether the VPN is actually connected.

Here's the twist. The extension advertises an "AI Protection" feature that supposedly checks your prompts for personal data and warns you about suspicious links. But this "protection" operates completely independently from the data collection. Harvesting runs in the background, regardless of the settings you choose. The only way to stop it is to uninstall the extension entirely.

The AI conversation harvesting wasn't always there. It appeared in version 5.5.0, released in July 2025. Browser extensions auto-update by default. Users who installed Urban VPN years ago for legitimate VPN functionality woke up one day with new code silently capturing their AI conversations. No notification. No consent request for the new capability.

This trend is becoming commonplace: vendors introduce browser extensions that undergo rigorous security review and validation by the browser vendor, only to completely change their model or what the extension does later.

Seven other extensions from the same publisher contain identical code: **1ClickVPN Proxy**, **Urban Browser Guard**, and **Urban Ad Blocker**-across both Chrome and Edge. Users installing an ad blocker have no reason to expect that their Claude conversations are being harvested.

Urban VPN is affiliated with BiScience, a data broker company. Their privacy policy states they share data with BiScience, which "creates insights which are commercially used and shared with Business Partners." It also confirms they "disclose the AI prompts for marketing analytics purposes."

The Chrome Web Store listing, however, says data is "Not being sold to third parties." The contradiction is significant, and the place where users actually decide to install says nothing about AI conversation harvesting.

TAKEAWAYS

- Check your browser extensions now. Look for Urban VPN Proxy, 1ClickVPN Proxy, Urban Browser Guard, and Urban Ad Blocker in both Chrome and Edge. If you have any of them, remove them immediately
- Audit your extension list regularly. Extensions run in the background with broad access to your browsing activity. Review what you have installed and remove anything you don't actively use
- Be skeptical of free privacy tools. If a VPN or security tool is free, ask yourself how they make money. You might be the product
- Don't trust badges blindly. Google's "Featured" badge means the extension passed review-but as this case shows, review processes miss things. A badge is not a guarantee of safety
- Be mindful of what you share with AI. Treat AI conversations like you would a public conversation. Avoid sharing sensitive personal or work information unless absolutely necessary

Confidence in software vendors is rapidly diminishing, with some tools becoming personal liabilities rather than enhancing productivity or security.