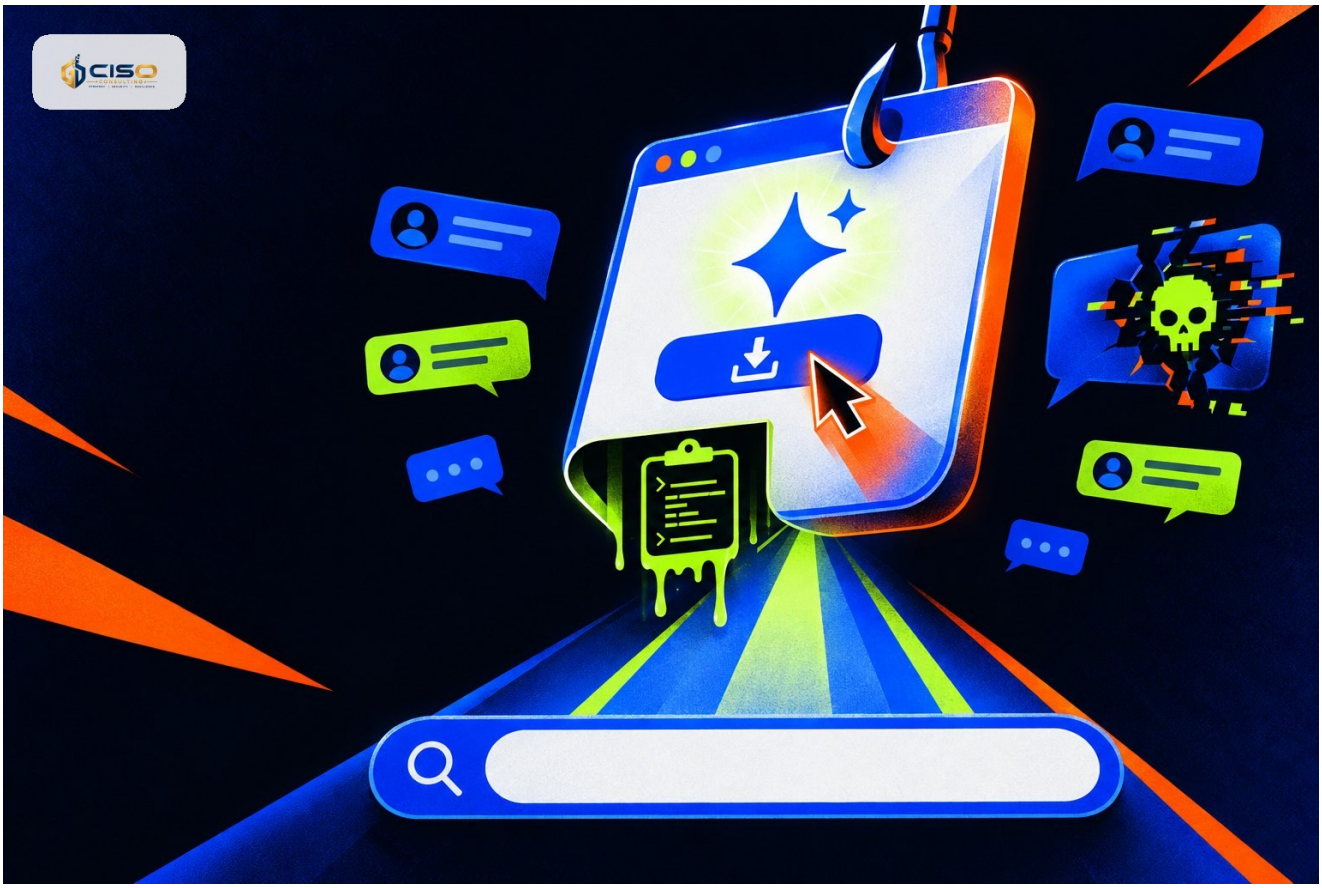
ClickFix Attacks Now Use Fake AI Tool Pages as Bait



A sponsored Push Security report says ClickFix is now the most common browser-based attack it detects, and that fake AI-tool install pages and shared chats are an increasingly effective lure. Most pages are reached through search, not email.

- Push reports ClickFix averaged 52% of its detections through Q2 2026 and reached 67% in August; 4 in 5 ClickFix pages were reached from search engines.
- InstallFix clones install pages for AI tools and swaps in a malicious command; the copy button can place a different command on the clipboard than the one displayed.
- LLMshare hosts lures in shared chats and custom GPTs on ChatGPT and Claude, so URL reputation checks tend to trust them.
- ANY.RUN linked 1,258 sandbox analyses to fake AI tool campaigns between April 15 and October 5, 2026; 81% impersonated Claude or ChatGPT and Codex.

> - Email filtering, URL reputation and endpoint tools can all miss these attacks, especially on BYOD, contractor and developer machines. The report is vendor-sponsored.

A report sponsored and written by Push Security describes ClickFix, the technique that tricks users into pasting a command themselves, as one of the most widely used methods among attackers in 2026. The report is vendor-authored, so its figures reflect Push's own detection data and should be read in that light.

What is changing

Push says ClickFix averaged 52% of its detections through Q2 2026, overtaking AiTM and device code phishing, and reached 67% in August. About 4 in 5 ClickFix pages it intercepted in 2026 were reached from search engines, through compromised sites, malvertising and SEO poisoning.

The newest lures target people looking for AI tools. In InstallFix, attackers clone an install page, for example for Claude Code, and replace the command with a malicious one. In one case, the page showed the genuine command while the copy button placed a different one on the clipboard. LLMshare places lures inside shared chats and custom GPTs on legitimate AI platforms, so reputation checks see a trusted domain.

Why controls miss it

According to the report, email security never sees a page reached through search, URL reputation sees trusted domains, and the pasted command runs in a legitimate shell and in memory. Devices without EDR, such as BYOD, contractor, Mac and developer machines, are most exposed.

The pattern is built on two workforce habits: installing tools from the terminal and searching for AI apps instead of going to them directly. Reviewing both is a sensible starting point.

What to do now

1. Brief staff and developers: never paste a command from a web page or shared AI chat without checking it, and reach approved AI tools through bookmarks or the internal portal, not search ads.
2. Publish an approved AI tools list with official install sources, and give employees a fast route to request new tools.
3. Restrict or monitor terminal and script execution launched from user sessions, and review EDR coverage on BYOD, contractor, Mac and developer devices.
4. Add browser-level visibility and controls to cover attacks that arrive via search and never touch the email gateway.
5. Add ClickFix and fake AI-tool install scenarios to phishing awareness exercises and incident response playbooks, including how to preserve evidence of pages that may disappear.