MULTILOGIN

Scrape Websites Without Blocks — Proven Methods & Tools (2025 Guide)

Scrape websites without blocks — proven methods & tools (2025 guide)

Built for people who scrape at scale

Data engineers, growth marketers, and research teams who need stable scraping workflows and can’t afford constant blocks.

Why most scrapers get blocked

Websites track IPs, browser fingerprints, and cookies. One wrong setup leads to bans, CAPTCHAs, throttling, and lost accounts — costing time, data, and money.

What you’ll learn here

A practical framework for running long-lasting scrapers: how to rotate IPs, manage fingerprints, separate sessions, and use Multilogin to keep profiles undetectable.

Contents

Scrape websites Without Blocks: Proven Methods and Tools (2025 Guide)

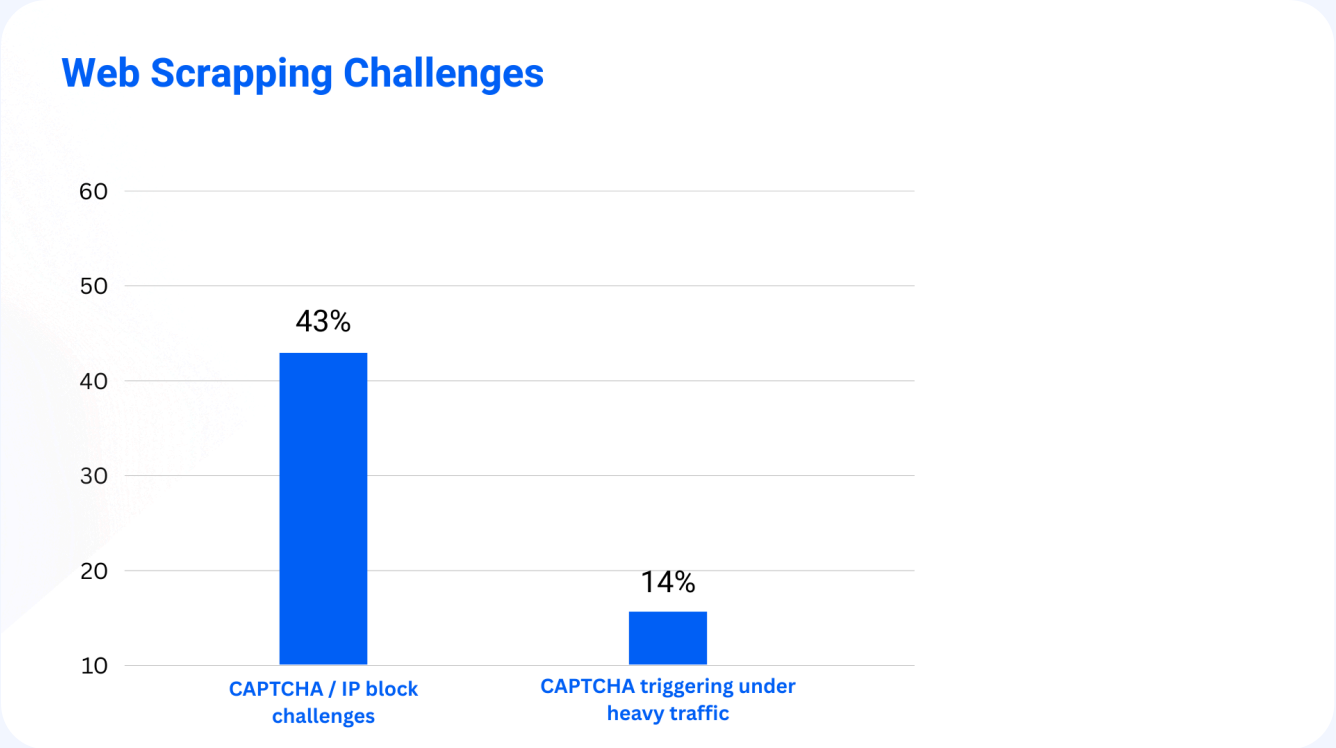
In 2025 Websites don't just sit back and let anyone pull their data. They track every click, request, and login. The moment your activity looks different from a normal visitor, their system reacts. Too many requests from the same IP? Blocked. A browser fingerprint that looks fake? Flagged.

When that happens, you lose time, data, and money. Accounts can even get restricted. If you rely on web scraping for work, a block can set you back fast.
The key isn't scraping more — it's scraping in a way that looks natural. And the demand is only growing: the web scraping market is valued at USD 1.03 billion in 2025!

Main reasons websites block data scraping

Scraping tools often get stopped because their traffic looks different from a normal user. Here are the most common triggers:

- **Same IP too often** – scraping from one IP gets flagged fast; normal users don't send that many requests from one place.
- **Too many requests too quickly –** rapid hits look automated; real people click at uneven speeds.
- **Fake-looking fingerprints** – every browser has a fingerprint; if yours repeats or looks odd, it gets flagged.
- **Shared cookies across sessions** – running scrapers in one browser mixes cookies and links your traffic.
- **Low-quality or datacenter proxies** – free, public, or reused datacenter IPs are often blacklisted and easy to detect.
- **Outdated bots** – old or cheap tools leave detectable patterns that platforms recognize instantly.



What happens if websites detect you

- **IP bans** – your IP gets blocked and requests stop working.
- **CAPTCHAs** – constant challenges pop up to slow you down.
- **Login checks** – extra verifications or 2FA requests appear.
- **Rate limits** – sites throttle requests, making scraping crawl.
- **Account bans** – linked accounts can be suspended or removed.

Types of websites that block scrapers the most

Not every site reacts the same way to scraping. Some barely notice, while others guard their data like a fortress. If you scrape the wrong way, these are the sites most likely to block you fast:

- **Social media platforms:** Facebook, Instagram, X, LinkedIn. They track fingerprints, IPs, and cookies. Even a minor mistake can trigger login challenges or account bans.
- **E-commerce websites:** Amazon, eBay, Walmart. They block repeated price or product scraping because it cuts into their market data advantage.
- **Ticketing sites:** Ticketmaster, Eventbrite. They fight bots aggressively to stop scalping. Too many requests = instant blocks.
- **Search engines:** Google, Bing. They flag automated queries quickly, often throwing CAPTCHAs or temporary IP bans.

Results of scraping errors here

- **Social media platforms** – Account bans, shadowbans, or endless login checkpoints.
- **E-commerce websites** – IP bans, throttled requests, or permanent loss of access.
- **Ticketing sites** – Instant blocks, blacklisted proxies, and flagged payment details.
- **Search engines** – Flood of CAPTCHAs, temporary IP bans, and reduced query limits.

How to avoid detection while scraping

If you scrape like a bot, you'll get blocked. The fix is to make your scraping setup move like a real person. Here's what to do:

Rotate IPs

Change fingerprints

Rotate IPs: Don't hammer a site with the same IP. Use mobile or residential proxies and assign different IPs to different sessions. Change them regularly so each request looks like it's coming from a new visitor.

Change fingerprints: Every browser reveals details like screen size, fonts, timezone, and OS. If these stay the same across sessions, sites spot you. Use an **antidetect browser** to randomize these settings so each profile looks like a unique user.

Keep sessions separate: Never run multiple accounts in the same browser. Cookies and local storage will overlap and link them. Instead, use isolated **browser profiles** so each account has its own cookies, cache, and device setup.

Slow down requests: Humans click unevenly — sometimes fast, sometimes slow. Add delays between actions, vary request timing, and avoid sending bursts of traffic. Scrape in patterns that look like normal browsing.

Adjust automation tools: Tools like Puppeteer, Postman, Selenium, and Playwright are powerful, but their default behavior looks robotic. Add random mouse movements, scrolling, and time gaps to your scripts. Script your bot to "act" human.

Use an antidetect browser: This is the backbone of scraping safely. An antidetect browser like Multilogin gives each profile a unique fingerprint, isolated storage, and its own proxy. That makes your scraping sessions look like dozens of different real users instead of one bot.

The outcome: stable, long-lasting scraping

- **Fewer IP bans and restrictions** – rotating clean proxies and unique fingerprints keep your access open instead of blocked.
- **Longer sessions without interruptions** – isolated profiles and natural request timing let you run accounts for hours or days.
- **Data collection that runs smoothly** – fewer CAPTCHAs and errors mean your scripts finish without constant retries.
- **Accounts that stay active and usable** – separating cookies and identities prevents bans that wipe out multiple accounts at once.
- **Less time wasted fixing blocked setups** – a stable configuration saves you from rebuilding scrapers or replacing accounts every week.

How Multilogin helps you scrape websites without getting blocked

Standard browsers tie all your activity to one identity. That makes it easy for websites to connect your sessions and block you.

Multilogin solves this by letting you create separate profiles, each with its own fingerprint, cookies, and browsing environment. Nothing leaks between them, so every profile looks like it belongs to a different real user.

You can also plug in proxies, giving each profile its own IP. That way your scraping traffic spreads out naturally across different locations and networks.

Multilogin offers full integration with **Selenium**, **Puppeteer**, **Playwright**, and **Postman**, along with its own **CLI**. Build automation flows using your preferred frameworks or command-line tools, all powered by Multilogin's robust API to keep profiles isolated and harder to trace.


Postman

Selenium


Playwright

Puppeteer

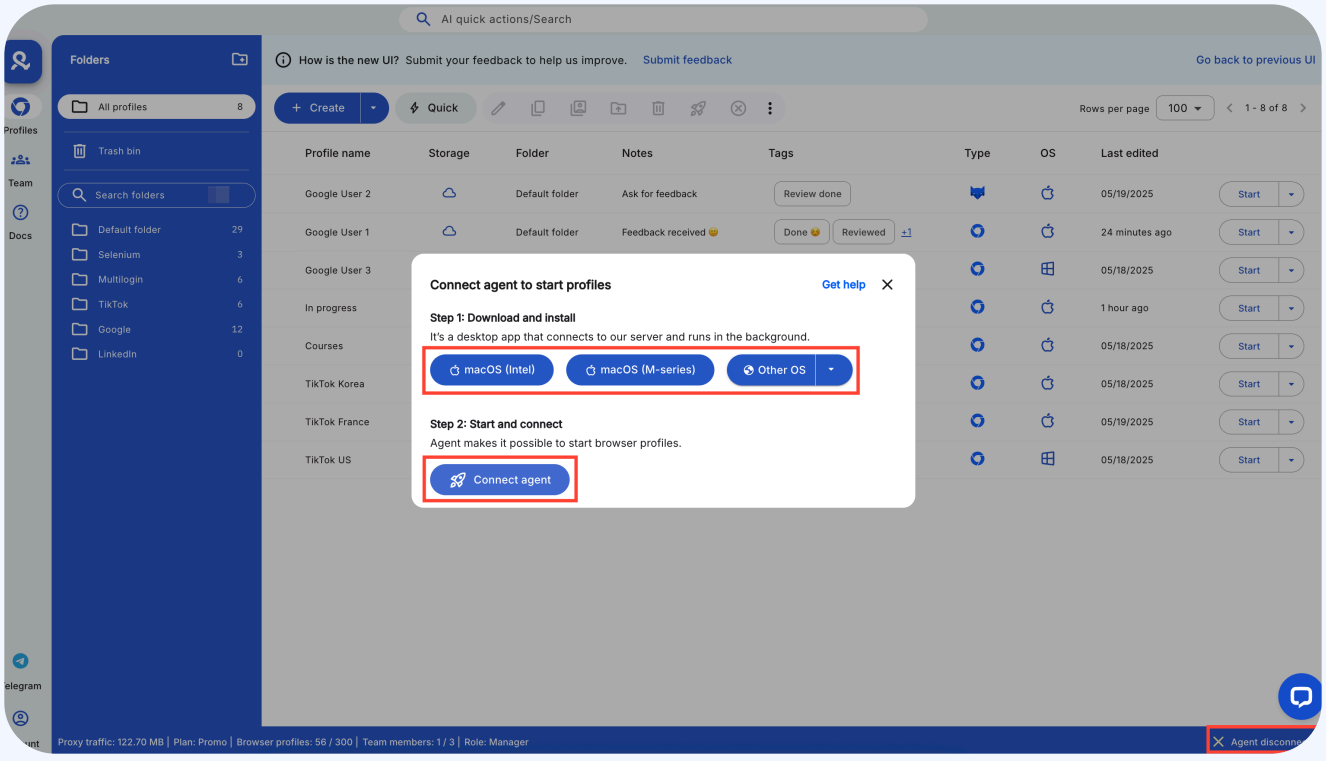
Key features that make Multilogin effective for scraping:

- **Unique fingerprints** – Every profile mimics a real user device with over 25 fingerprinting parameters randomized.
- **Profile isolation** – Cookies, storage, and cache never overlap, keeping accounts and sessions fully separate.
- **Proxy control** – Assign residential, mobile, or datacenter proxies per profile, with easy switching and rollover options.
- **Stability** – Profiles stay consistent for weeks or months, supporting long-term scraping projects without constant resets.
- **Chrome flexibility** – Based on Chromium, Multilogin supports Chrome extensions, developer tools, and real-world browsing behavior for natural sessions.
- **Team sharing** – Share or transfer profiles securely with teammates without exposing raw logins or sensitive data.
- **Automation support** – Full compatibility with Puppeteer, Selenium, Playwright, Postman, and CLI for safe, large-scale automation.

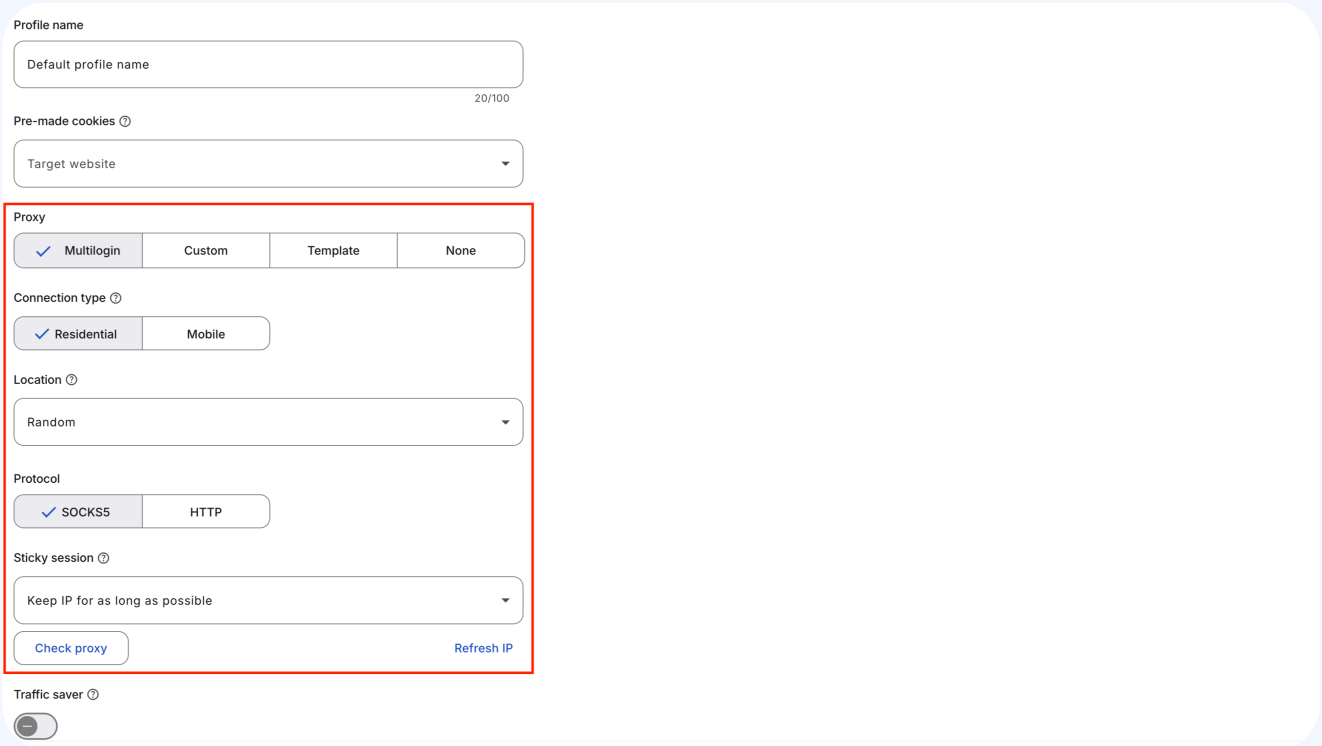
Run Multilogin for scraping in easy 3 steps

Step 1: Subscription: Go to the Multilogin pricing page, choose the plan that fits you best, or start with the trial for just €1.99!

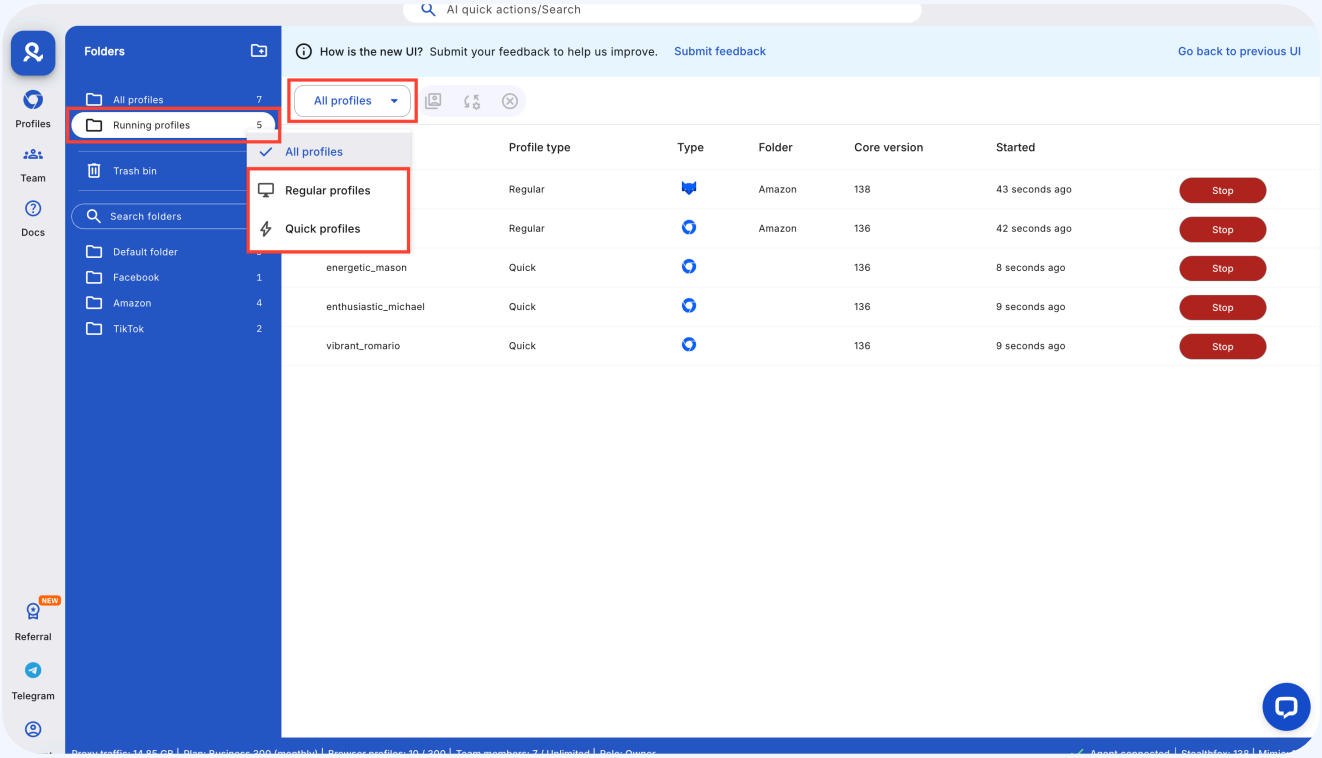
Step 2: Create profiles: Open Multilogin and create a new browser profile. Each profile gets its own screen size, fonts, OS, timezone, and other settings so sessions look like different users.



Step 3: Connect proxies: assign a residential or mobile proxy to each profile so each one runs on its own IP.



Step 4: Launch and automate: run profiles by hand or link them to tools like Puppeteer, Selenium, CLI, Playwright, or Postman. Each session stays isolated, with no cookie or login leaks.



Benefits of using Multilogin for scraping :

- **Stealthfox and Mimic engines** – Advanced fingerprint cloaking for Firefox - and Chromium-based sessions.
- **Chromium-based browsing** –Full Chrome flexibility with extension support, developer tools, and natural browsing behavior.
- **Full automation compatibility** – Works with Puppeteer, Selenium, Playwright, Postman, and CLI for safe, scalable automation.
- **Built-in residential proxy support** – Every plan includes premium proxy traffic, with options for mobile and datacenter IPs.
- **Scalable to hundreds of profiles** – Run small tests or manage thousands of accounts with consistent performance.
- **Android and mobile simulation** – Emulate real mobile devices to scrape mobile-first platforms without detection.

Start with Multilogin for just €1.99 and run separate, undetectable browser profiles with unique fingerprints and proxies to scrape without blocks.

Typical errors when scraping websites

Mistake	What happens
Sending too many requests too fast	Triggers CAPTCHAs, rate limits, or IP bans
Using free or public proxies	Most are blacklisted and get blocked immediately
Reusing the same fingerprint	Repeated browser details make traffic look automated
Mixing cookies across sessions	Links accounts together and leads to bans
Relying on outdated bots	Old tools leave detectable patterns and fail checks

Best practices for scraping without getting blocked

Scraping only works long-term if you treat it like real browsing. Here are the habits that keep you safe:

- **Start small and scale slowly:** Don't blast a site with thousands of requests on day one. Build up traffic over time.
- **Mix your activity:** Add delays, random clicks, or different browsing patterns. The less robotic your traffic looks, the longer it lasts.
- **Test your setup often:** Check if IPs, fingerprints, and sessions still pass as natural before running big jobs.
- **Keep backups:** Have spare profiles and accounts ready in case one gets flagged.
- **Stay updated:** Websites change their defenses. Update your tools and methods to stay ahead.
- **Use trusted tools:** A stable setup with an anti-detect browser and clean proxies will always outlast cheap bots and public proxies.

The goal isn't speed at any cost—it's scraping that looks real enough to avoid detection for the long run.

Final Verdict

Scraping isn't about blasting sites for quick data. If you move like a bot, you get blocked. If you move like a person, you last. That means rotating IPs, managing fingerprints, keeping sessions separate, and running automation with care. Tools like **Multilogin** antidetect browser make this possible by giving each profile its own unique identity, pre farmed cookies, and proxy setup. With the right workflow, you can scrape steady, safe, and without constant setbacks.

MULTILOGIN

Thank You!

www.multilogin.com