

Red flags for affiliate scams – Hostinger Learning lab

CONTENTS

What's inside

01	Affiliate marketing scam red flags	p.03
02	If you're an affiliate marketer	p.03
03	Unrealistic income promises	p.03
04	Suspicious program structure	p.04
05	Tracking and payment red flags	p.05
06	If you run an affiliate program	p.06
07	Fake traffic and conversion fraud	p.06
08	Brand and SEO abuse	p.07
09	How to protect yourself — quick rules	p.08
10	Ready to build a legitimate affiliate business?	p.09

Affiliate marketing scam red flags

Know what to watch for before you join a program or accept an affiliate partner. These are the warning signs that separate legitimate opportunities from schemes designed to waste your time and money.

How to use this guide: This card covers red flags from two angles — scams targeting affiliate marketers, and fraud targeting merchants running affiliate programs. Read both sections regardless of which side you're on. Knowing how fraud works on the other side makes you a better affiliate partner.

If you're an affiliate marketer

Affiliate marketers are targeted by fraudulent programs that promise high earnings, charge upfront fees, or manipulate tracking to steal your commissions. Before joining any program, check it against the red flags below.

Unrealistic income promises



Legitimate programs let results speak — they don't need to oversell.



Guaranteed income claims

No affiliate program can guarantee earnings. Income depends entirely on your traffic, niche, and effort. Any program promising fixed monthly income regardless of performance is a scam.



Extraordinary commission rates with no credible explanation

Commission rates above 50% on physical products or 80%+ on digital products without a clear business model behind them are a warning sign. Ask how the merchant makes money if affiliates take most of the margin.



"Get rich quick" language

Phrases like "earn \$500 a day from your phone" or "passive income with zero effort" signal a scheme, not a business. Real affiliate income takes months of consistent work to build.

Suspicious program structure



Legitimate affiliate programs are free to join and pay on real results.



Upfront fees to join

Reputable affiliate networks — Amazon Associates, ShareASale, CJ Affiliate, Awin — charge nothing to affiliates. Any program asking for a joining fee, "training fee", or "starter pack" purchase is not a legitimate affiliate program.



Recruiting-based earnings

If a program pays you primarily for recruiting other affiliates rather than for actual product sales, it's structured as a multi-level marketing scheme — not affiliate marketing. Avoid it.



No verifiable merchant or product

Before joining any program, verify that the merchant actually exists, has a real product, and has an established online presence. Search for reviews from other affiliates. No company history or address is a serious red flag.



Vague or missing payment terms

A legitimate program clearly states commission rates, payment schedules, payment methods, and minimum thresholds. If this information is buried, absent, or changes after you join, treat it as a warning.

Tracking and payment red flags



If you can't verify your commissions, you can't trust the program.



No access to a real-time dashboard

Legitimate programs give affiliates access to a dashboard showing clicks, conversions, and earnings in real or near-real time. If there's no dashboard — or it's impossible to audit — you have no way to verify you're being paid correctly.



Consistently low or declining conversion rates with no explanation

Cookie manipulation — where a fraudster overrides your tracking cookie with theirs — can cause legitimate referrals to be attributed elsewhere. If your conversion rate drops significantly without a change in your traffic quality, investigate.



Late payments, changed terms, or disappeared commissions

A program that consistently delays payment, quietly changes commission rates after you've already sent traffic, or removes previously approved commissions without explanation should be abandoned immediately.

If you run an affiliate program

Merchants face a different set of threats – affiliates who generate fake traffic, abuse your brand name in paid search, or exploit your program to collect commissions on sales they had no real part in driving. These are the patterns to monitor for.

Fake traffic and conversion fraud



High numbers that produce no real customers are a sign of fraud.



Unusually high click volume with near-zero conversion rate

Bots generate fake clicks and impressions that drain your budget without producing real customers. If an affiliate sends thousands of clicks but converts far below the program average, investigate the traffic source.



Suspicious conversion spikes from a single affiliate

A sudden surge in conversions from one affiliate — especially one with no track record — can indicate fabricated sign-ups using stolen or fake data. Validate lead quality before paying out.



High chargeback rates tied to affiliate traffic

Criminals sometimes use stolen payment details to make purchases through affiliate links, collecting commissions while leaving you liable for chargebacks. A spike in chargebacks from a particular affiliate's traffic is a serious red flag.

Brand and SEO abuse



Affiliates should drive new traffic — not steal yours



Branded keyword bidding

Some affiliates bid on your brand name in paid search, intercepting customers who were already searching for you directly and claiming commission for "referring" them. Check your affiliate agreement and monitor search ads for your brand terms.



Domain name exploitation

Fraudsters register domains similar to yours — slight misspellings, added hyphens, different extensions — to redirect your organic traffic through affiliate links. Monitor for lookalike domains regularly.



Counterfeit product promotions

Affiliates sometimes create fake listings or ads using your brand name to promote non-existent or counterfeit versions of your products, damaging your reputation while collecting data or payments from deceived customers.

How to protect yourself — quick rules

Apply these regardless of which side of the affiliate relationship you're on

- 01** Only join affiliate networks that are free to sign up – never pay to become an affiliate
- 02** Verify any merchant or program through independent reviews before promoting
- 03** Read the full terms before joining – pay close attention to payment terms and cookie policy
- 04** Monitor your tracking dashboard regularly and question unexplained drops in conversions
- 05** Never rely on a single affiliate program — diversify across multiple programs and networks
- 06** If you run a program, validate lead quality before paying out and monitor for brand abuse

Ready to build a legitimate affiliate business?

A credible affiliate business starts with a proper website. Hostinger gives you fast hosting, a free domain, an AI-powered website builder — everything you need to build an affiliate site that earns trust as well as commissions.

Protect your affiliate program with Hostinger

Build and manage a secure affiliate marketing program with Hostinger's trusted hosting infrastructure. Learn best practices to identify and prevent scams before they impact your business.

[Get started →](#)