What evidence should you collect before tackling spam links?

Before you attempt any spam link recovery, you need solid evidence that the links are actually harmful and that they did not come from your own past efforts. Without that evidence, you risk wasting time on links that are benign or even valuable, and you might submit a disavow file that does more harm than good.

Spam link recovery is the process of identifying, documenting, and neutralizing low-quality or manipulative backlinks that point to your site. The goal is to stop those links from dragging down your rankings or triggering a manual penalty. But jumping straight to a disavow or a reconsideration request without first gathering proof is like calling the fire department before you know where the smoke is coming from. You need to know what you are dealing with, where the links live, and how they got there.

Start with the raw data: your backlink profile

The first piece of evidence is a complete, unfiltered list of your backlinks. Use a reputable backlink analysis tool to export every link that points to your domain. Look for patterns that indicate spam: links from sites in unrelated languages, links from domains with no real content, links embedded in auto-generated comments, or links from sites that exist only to host paid links. Pay special attention to anchor text that is overly commercial or that uses exact-match keywords for terms you do not usually target.

Once you have the raw list, sort the links by date. Spam attacks often arrive in a sudden spike. If you see a large batch of links appearing over a few days or weeks, that is a strong signal of a negative SEO attack. Compare the timing of that spike against your site's traffic and ranking history. A sudden drop in organic traffic that coincides with a link spike is compelling evidence that the links are harmful.

Check for manual actions and algorithmic signals

Log into your Google Search Console account and check the Manual Actions report. If Google has issued a manual penalty for unnatural links, that report will tell you. A manual action is clear, direct evidence that spam links are hurting your site. But even if no manual action is present, algorithmic filters like Penguin can still devalue your links. Look at your Search Console data for a sudden drop in indexed pages or a sharp decline in impressions for your key landing pages. Those drops, when paired with a link spike, point to algorithmic devaluation.

You should also review your Google Analytics data for changes in referral traffic. Spam links often generate no real referral traffic because they are placed on pages that no human visits. If a link from a suspicious domain shows zero referral sessions, that is further evidence it is spam. However, a small amount of referral traffic does not automatically make a link safe; some spam networks send bot traffic to make links look legitimate.

Audit the linking domains individually

Do not rely solely on aggregate metrics like Domain Authority or Trust Flow. Those scores can be misleading for individual domains. Instead, look at each linking domain manually. Check whether the domain has a clear topic or purpose. Does it publish original content, or is it a collection of scraped articles? Does it have a real about page, contact information, or a privacy policy? Spam domains often lack these basics. Also check the domain's age. A brand-new domain that suddenly links to your site is more suspicious than an older, established domain.

Look at the specific page where the link appears. Is the link surrounded by gibberish text, or is it in a section of unrelated links? Is the page itself indexed in Google? If you search for the page URL and it does not appear in the index, that is a sign the page is low quality or hidden from search engines. Also check whether the page uses nofollow or sponsored attributes. If the link is already nofollowed, it may not be passing link equity, but it could still be a sign of an ongoing attack that includes other, followed links.

Document the evidence before you act

Keep a detailed log of every suspicious link you find. For each link, record the source URL, the target URL on your site, the anchor text used, the date you discovered it, and the date the link first appeared (if available). Note why you believe the link is spam: is it from a link network, a hacked site, a comment spam campaign, or a paid link scheme? This documentation is essential if you later need to submit a reconsideration request or explain the situation to a client or a colleague.

If you are working with a forensic SEO recovery service, this documentation becomes the foundation of their analysis. Professionals at a firm like SEO Fire Fighter rely on this kind of evidence to distinguish between a genuine negative SEO attack and a site's own past link-building efforts. They can then recommend the right response, whether that is a targeted disavow, a reconsideration request, or simply waiting for the algorithmic filters to refresh.



Distinguish between spam and low-quality links

Not every low-quality link is spam. A link from an old blog post that has since been abandoned may be low quality but not malicious. Spam links are those that violate Google's Webmaster Guidelines: links from link networks, links with automated anchor text, links from hacked or compromised sites, and links from sites that exist solely to pass link equity. Low-quality links from legitimate but thin sites are a different problem and require a different approach.

To make this distinction, look at the context of the link. A link from a forum post that someone wrote years ago is likely not spam, even if the forum has since been overrun with ads. A link from a site that was hacked and filled with pharmaceutical spam is definitely spam, and you need to act quickly. If you cannot tell the difference, err on the side of caution and document the link, but do not disavow it until you have more evidence.

Gather evidence from multiple sources

Do not rely on a single tool or data source. Cross-reference your backlink export with Google Search Console's link data. Compare the lists and look for discrepancies. If a link appears in your backlink tool but not in Search Console, it may be a sign that Google has already discounted it. That does not mean it is safe, but it does mean the link may not be your top priority.

Also check your server logs for requests from the linking domain. If the domain's IP address is making frequent requests to your site, that could indicate a bot is checking whether the link is

still active. That behavior is common in link spam networks. If you see such activity, record the IP addresses and timestamps as additional evidence.

Finally, review your site's historical link-building efforts. If you or a previous SEO provider engaged in aggressive link building, some of the links you now consider spam may be remnants of those campaigns. Honest self-audit is crucial. A forensic recovery specialist at seofirefighter.com often finds that what looks like an attack is actually a site's own past work coming back to haunt it. Knowing the difference saves time and prevents unnecessary disavowals.

When to involve a professional

If the evidence points to a large-scale negative SEO attack, or if you are unsure whether the links are spam, consider bringing in a specialist. A professional forensic SEO analyst has the tools and experience to trace link patterns, identify the source of an attack, and build a case for a reconsideration request. They can also help you avoid common mistakes, such as disavowing links that are actually helping your site or failing to disavow links that are causing a penalty.

Spam link recovery is not a one-size-fits-all process. The evidence you collect determines the next steps. Without proper evidence, you risk making the situation worse. With careful documentation and analysis, you can clean up your backlink profile and restore your site's rankings.