What to Check Before Linking to a Website from Your Website

A Practical Safety Checklist for Linking to Other Websites

At some point, every site owner runs into this: someone asks for a backlink, or you find a resource you want to reference… and a little voice in your head goes, “Wait. What if this site is shady?”

Good instinct. You don’t need to panic, but you also don’t want to casually send your readers into a trap. Here’s a simple, repeatable way to vet outbound links before you publish them.

Takeaways:

- Linking to a bad site usually won’t “infect” *your* website, but it can hurt your readers and your reputation.
- Before you link, do a 2-minute check: **Google Safe Browsing** + **VirusTotal** + a quick “does this feel legit?” scan.
- If the link is paid, label it properly with **rel=”sponsored”** (and add a disclosure).
- If the link opens in a new tab, use **noopener**/**noreferrer** to reduce tabnabbing risk.
- Keep a simple “outbound links log” so you can re-check sponsor links later.

First… How to Link to Another Website

Linking out is simple, but doing it *well* matters. A good outbound link helps your reader, supports your point, and doesn’t accidentally create a security or SEO mess.

The easy way (Gutenberg)

- Highlight the text you want to turn into a link.
- Click the link icon (or press **?K** on Mac / **Ctrl+K** on Windows).
- Paste the URL.
- If it’s an external site, it’s usually fine to enable **“Open in new tab”**.

Tip: When you open a link in a new tab, WordPress typically adds the safety attributes for you (so the new site can’t mess with your original tab). Still, it’s worth knowing what they are, just in case you’re editing HTML manually.

The “I’m editing HTML” version

This is a clean, safe default for most external links:

Copy

```
<a href="https://example.com" target="_blank" rel="noopener noreferrer">Example site</a>
```

If you don’t need a new tab, just remove `target="_blank"` and you can also remove `noopener noreferrer`.

If the link is paid (sponsored), do this

If someone paid for the link (or it’s part of an agreement), label it correctly:

Copy

```
<a href="https://example.com" target="_blank" rel="sponsored noopener noreferrer">Brand name</a>
```

And add a simple disclosure near it, like: **“This is a sponsored link.”** (No legal novel required.)

You can do this in the Gutenberg editor:

- Click the block that contains the link
- Use the block menu (three dots) ? Edit as HTML
- Add your rel values manually

Here’s what each relationship means:

- rel=”sponsored”
  Tells search engines the link is an advertisement, sponsorship, or paid placement (a “paid link”). Google specifically recommends using sponsored to identify paid links.
- rel=”noopener”
  A security setting for links that open in a new tab/window (target=”_blank”). It prevents the new page from getting access to the page that opened it (via window.opener), which helps protect against “reverse tabnabbing” style attacks.
- rel=”noreferrer”
  A privacy + security setting. It tells the browser not to send referrer information (the Referer header) to the site you’re linking to — and it also behaves as if noopener was set too.

Anchor text (what your link should say)

- **Be specific:** “Amazon advertising guide” is better than “click here.”
- **Match expectations:** If the link goes to a checklist, say it’s a checklist.
- **Don’t overdo keywords:** Natural is best. Your reader is the priority.

Quick “should I link to this?” check

- Does the site look legit (real company info, real content, no weird popups)?
- Does it force downloads or spammy “allow notifications” prompts?
- If it’s a sponsor link, did you label it as `rel="sponsored"` and add a disclosure?
- If it opens in a new tab, did it get `noopener` added?

The Real Risk of Linking Out

Linking to a sketchy site doesn’t usually compromise your own server the way an infected plugin or hacked password can. A normal hyperlink is just a doorway.

But doorways matter. If you send readers to a phishing page, a “download this” trap, or a scammy checkout flow, you take a hit on trust. And trust is hard to rebuild.

Malware vs. Phishing vs. “Just Sketchy”

- **Malware**: the site (or something it downloads) tries to install unwanted software.
- **Phishing / social engineering**: the site tries to trick people into entering passwords, payment info, or personal data.
- **Sketchy**: not necessarily malicious, but deceptive — aggressive popups, forced redirects, fake “system alerts,” junk content, etc.

Google Safe Browsing specifically tracks threats like phishing and malware, and exposes checks through the Transparency Report and Safe Browsing tools.

The 2-Minute Link Safety Check (my default process)

If I’m about to publish a new outbound link — especially a sponsor link — I run this quick checklist:

1. Check Google Safe Browsing (site status)

Google provides a Site Status tool in the Transparency Report that can show whether a site is currently flagged as dangerous.

Run the URL through VirusTotal

VirusTotal checks URLs/domains using many security engines and blocklisting services, and returns a report so you can see if anything looks suspicious.

Important: treat these scans as “signals,” not absolute truth. Both false positives and false negatives happen. The goal is to reduce risk, not pretend you can get to 0% risk.

3. Do a fast human sniff test

- Does the site have real contact info, a real brand presence, and coherent content?
- Does it immediately push downloads, browser notifications, or “urgent” popups?
- Does it look like a thin site created only to funnel traffic somewhere else?

4. Watch for weird redirects

If a link silently bounces through multiple domains before landing, that’s not automatically malicious — but it’s a yellow flag, especially if you’re linking in exchange for money.

What to do if a Site Gets Flagged

If Google Safe Browsing or VirusTotal shows warnings, don’t auto-assume “guilty”… but don’t ignore it either. Here’s the practical decision tree I use:

- **Hard no**: multiple strong warnings + you can’t independently verify legitimacy ? don’t link.
- **Soft no**: one weak/uncertain warning + the site feels low-quality ? don’t link (not worth the risk).
- **Proceed carefully**: you trust the company, can verify their real presence, and warnings look like possible false positives ? you might link, but treat it as a sponsor link if it’s paid (and consider using a redirect page or disclosure).

If You’re Getting Paid for the Link, Do it the Right Way

Paid placements are a separate issue from malware — but they overlap because sponsors sometimes come from outside your normal orbit.

Google recommends qualifying paid links using `rel="sponsored"` (and notes that `nofollow` is still acceptable).

At minimum, do these two things:

- Use **rel=”sponsored”** on the link (optionally combined with `nofollow` if you prefer).
- Add a simple disclosure near the link (example: “This is a sponsored link”).

WordPress Linking Hygiene: Small Things That Matter

Open in new tab safely

There's a security issue called *reverse tabnabbing*, where a site opened in a new tab can try to manipulate the original page via `window.opener`. OWASP documents this risk and the typical mitigation (`rel="noopener"`).

In modern WordPress/Gutenberg, `rel="noopener noreferrer"` is often added automatically when you set a link to open in a new tab.

Don't confuse "noopener" with "nofollow"

`noopener`/`noreferrer` are about browser security and referrer behavior. `nofollow`/`sponsored`/`ugc` are about how search engines interpret the relationship. Different tools, different jobs.

Ongoing Safety: Don't Publish and Forget

Sites change hands. Domains expire. "Normal" businesses get hacked. So if you do sponsored links (or lots of outbound links), keep it simple:

- Keep a basic spreadsheet: URL, anchor text, page it's on, date added, whether it's sponsored.
- Re-check sponsor links periodically with the same 2-minute scan.
- If something gets flagged later, remove the link first and investigate second.

FAQs About Safely Linking to Other Websites

Can linking to a bad site hurt my website?

Usually it won't compromise your server directly, but it can absolutely hurt your readers and your reputation. And if it's a paid link that isn't qualified, that can create SEO compliance issues too.

Is VirusTotal always right?

No. It's a powerful signal because it aggregates multiple engines and services, but it can miss things or flag false positives. Use it as one input.

What's the simplest safe approach for sponsor links?

Vet the site, qualify the link with `rel="sponsored"`, add a disclosure, and keep a log so you can revisit it later.

Sources

- Google Safe Browsing / site status tool (Transparency Report): https://safebrowsing.google.com/
- Transparency Report page: https://transparencyreport.google.com/safe-browsing?hl=en)
- VirusTotal: how URL scanning works: https://docs.virustotal.com/docs/how-it-works and URL reference: https://docs.virustotal.com/reference/url
- Google Search Central: qualify outbound links (sponsored/nofollow/ugc): https://developers.google.com/search/docs/crawling-indexing/qualify-outbound-links
- Google Search Central blog: evolving nofollow + sponsored/ugc: https://developers.google.com/search/blog/2019/09/evolving-nofollow-new-ways-to-identify
- OWASP: Reverse Tabnabbing: https://owasp.org/www-community/attacks/Reverse_Tabnabbing

Original article: https://tonyherman.com/how-to-link-to-a-website/
PDF version: https://tonyherman.com/how-to-link-to-a-website/?apa_pdf=1

Special Offer for Readers

1,000+ Channels • On-Demand Movies • **5 Devices**

$69.99/mo (~$2.33/day)

Try it for a month and see if you like it, then switch.

Start Your Trial

Click to learn more about CUE Broadcast

Tip: Get 3 friends of family to sign up and you it for free.