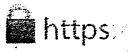
## How to find if a Website is Legitimate

1. **Type the website's name into a search engine and review the results.**
- If the site in question is a hazard (or simply an overwhelmingly illegitimate site), a cursory Google check will be enough to inform you accordingly.
- Google tends to compile user reviews of high-traffic sites near the top of the search results, so be sure to check these if there are any.
- Make sure you're looking at reviews and feedback from sources unaffiliated with the website.
    - You want articles that don't reference independent sources to ensure unbiased content.

2. **Look at the website's connection type.**
- A website that has an "https" tag is usually more secure--and therefore more trustworthy--than a site using the more common "http" designation. This is because "https" sites' security certification is a process most illegitimate sites don't bother with.[1]
- A site that uses an "https" connection can still be unreliable, so it's best to verify the website using other means as well.[2]
- Make sure the site's payment page in particular is an "https" page.

3. **Check the site's security status in your browser's address bar.**
- For most browsers, a "safe" website will display a green padlock icon to the left of the website's URL.
- You can click on the padlock icon to verify the details of the website (e.g., the type of encryption used).




4. **Evaluate the website's URL.**
- A website's URL consists of the connection type ("http" or "https"), the domain name itself (e.g., "wikihow"), and the extension (".com", ".net", etc.). Even if you've verified that the connection is secure, be on the lookout for the following red flags:
- Multiple dashes or symbols in the domain name.
- Domain names that imitate actual businesses (e.g., "Amaz0n" or "NikeOutlet").
- One-off sites that use a credible site's templates (e.g., "visihow").
- Domain extensions like ".biz" and ".info". These sites tend not to be credible.[3]
- Keep in mind as well that ".com" and ".net" sites, while not inherently unreliable, are the easiest domain extensions to obtain. As such, they don't carry the same credibility as a ".edu" (educational institute) or ".gov" (government) site.

5. **Look for bad English on the site.**
- If you notice a large number of poorly-spelled (or missing) words, generally bad grammar, or awkward phrasing, you should question the site's reliability.
- Even if the site in question is technically legitimate insofar as it isn't a scam, any inaccuracies in language will also cast doubt on the accuracy of its information, thereby making it a poor source

6. **Watch out for invasive advertising.**
- If your selected site has a stunningly large number of ads crowding the page or ads that automatically play audio, it's probably not a credible site. Additionally, consider looking elsewhere if you encounter any of the following types of ads:
- Ads that take up the whole page
- Ads that require you to take a survey (or complete some other action) before continuing
- Ads that redirect you to another page
- Explicit or suggestive ads

7. **Use the website's "Contact" page.**
- Most sites provide a Contact page so that users can send questions, comments, and concerns to the owner of the site. If you can, call or email the provided number or email address to verify the legitimacy of the website.
- Make sure you scroll all the way to the bottom of the site to search for the Contact page.
- If the site in question doesn't have a Contact page listed anywhere, it should be an immediate red flag.

.com .net .edu
.org .int .gov

## Using a Google Transparency Report: http://scanurl.net

1. **Open the Google Transparency Report webpage.**
   - You can quickly run a website's address through this service to see its safety rating from Google.
2. **Click the "Search by URL" field.**
   - It's in the middle of the page.
3. **Type in your website's URL.**
   - This includes the name of the website (e.g., "wikihow") and the extension (e.g., ".com").
   - For best results, copy your website's URL and paste it into this field.
4. **Click the blue magnifying glass button.**
5. **Review your results.**
   - Sites range in rating from "No data available" to "Not dangerous" to "Partially dangerous" and so on.
   - For example, sites like WikiHow and YouTube achieve "Not dangerous" ratings from Google, whereas Reddit garners a "Partially dangerous" rating due to "deceptive content" (e.g., misleading advertising).
   - The Google Transparency Report also provides examples of why it gave a certain site a rating, so you can decide for yourself whether or not the rating rationale pertains to you.

## Using the Better Business Bureau

1. **Open the Better Business Bureau webpage.**
   - The Better Business Bureau website includes a verification process that you can use to validate your selected website.
   - Note that the Better Business Bureau is geared toward matching businesses with your provided website. If you're simply trying to see if the website is safe, use the Google Transparency Report.
2. **Click the Find a Business tab.**
3. **Click the "Find a" text field.**
4. **Type in your website's URL.** For best results, copy and paste the exact URL into this field.
5. **Click the "Near" field.**
6. **Type in a location.**
   - While this isn't mandatory, doing so will narrow your search.
   - If you don't know your business' geographic location, skip this step.
7. **Click Search.**
8. **Review your results.**
   - You can verify your website's credibility by comparing the Better Business Bureau's results with the website's claims.
   - For example, if your website claims to sell shoes but the Better Business Bureau links the URL to an ad revenue service, you know that the site is a scam.
   - However, if the Better Business Bureau results line up with the site's theme, you can probably trust the site.