The site has unusual payment options. A site using unusual or unprotected payment options such as wire transfers, bank transfer, gift cards, or other payment applications, such as Venmo, Cash App, Zella, Western Union, etc, could be a scam.

Poor web design can be an indicator of a scam site. Scammers often don’t put in the time or investment to make a good-looking website.

If the price is too good to be true, it probably is. If you are looking at a site and it's offering 30-90% off other sites, it is likely that it is a scam.
The site doesn't use SSL/Lock. You should look at the top left-hand corner of the address bar. If you see a lock, it is secured with https, and if it is not, it might be a sign that the site is concerning, take precautions. CAUTION: Even if it has a lock it does not mean that the site is safe, it is just one thing to look for. Look at the URL, look for any typos, or inconsistencies, such as: Amaz0n instead of amazon.

The site portrays a sense of urgency. Most scams try to create a sense of urgency such as better act now, scare tactics, limited time only, or a countdown for a sale.

The site has limited or no contact information. If the business has limited to no contact information, doesn’t provide an address, or a no return policy, it should be cause for concern.
Advanced/Investigative Tools

Domain Age Lookup
Look for a website that has been established for a long period of time. A good website is https://lookup.icann.org/lookup. Check out the image below.

It is important to look at the date it was created as many scam sites are less than a year old.

Google Street View
Go to Google maps and search the address in the search bar. Once found click and drag the orange guy in the bottom right-hand corner on road to see the surroundings. Does the business name on the website match what you see?

Online Reviews
Conduct a search of the website name and look for customer reviews, or sites such as Yelp, Angie's List, Better Business Bureau, or Consumer Affairs.