

HOW TO SPOT

**A FAKE ONLINE
STORE**





VERIFY THE 'ABOUT US' PAGE

Copy text from their description and Google it. If the same description appears on multiple sites, avoid that store.



2

DO THE SAME FOR THE CONTACT DETAILS

**Just like you did with the About Us text,
run a quick online search for the listed
email, phone number, and physical
address.**

**Is the same info used for multiple sites?
If so, that's a big red flag.**



3

CROWDSOURCE INSIGHTS

Use platforms like Reddit and Quora to get more insights about user experiences. Search for mentions of 'scam' or 'fraud' and get a feel for the site's reputation.



4

HOW NEW IS THE SITE?

This is a little technical, but you can see how established a website is based on its launch date. Copy the domain name or IP address and perform a 'WhoIS Lookup'. If you see the site is only a couple of months old, be especially cautious.



BONUS TIPS!

DON'T REUSE PASSWORDS

Ecommerce sites frequently experience hacks, and if your password is used for more than one account criminals can use that password to try to access other online accounts, too.



STICK TO CREDIT OR GIFT CARDS

You may be paid back if you quickly report fraudulent transactions. Avoid using debit cards, bank account details, or other payment that have less fraud protection. Better yet - pay with a gift card, as they are not tied to your personal information.

The image features a large, stylized, light green letter 'W' in the background. The 'W' is composed of several overlapping, rounded shapes. In the center of the 'W', the word 'wizer' is written in a white, lowercase, sans-serif font. The letter 'i' has a small white triangle above it, resembling a play button. The entire graphic is set against a solid green background and is enclosed in a black rounded square border.

wizer

wizer-training.com