Fake Shopping Sites

Scammers and fraudsters know everyone is looking for a bargain during the holidays. With technology and social media, it's just too easy to shop from the convenience of your phone or computer. Scammers create convincingly fake websites that mirror bank login pages, password reset pages for services like Amazon and Netflix, or package delivery requests. But any information you enter goes straight to the scammers — who then use it for identity theft or financial fraud.

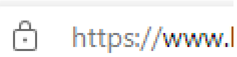
Don't fall prey to a super low price! When it sounds too good to be true it usually is.

Examples of possible scam websites designed to deceive users into fraud or malicious attacks:

1. Fake online stores with too-good-to-be-true deals.
2. Fake password login pages.
3. Malicious pop-ups that download malware.
4. Fake customer support websites.
5. Fraudulent Medicare or health insurance websites.
6. Fake package delivery websites.
7. Bogus flight-booking websites.

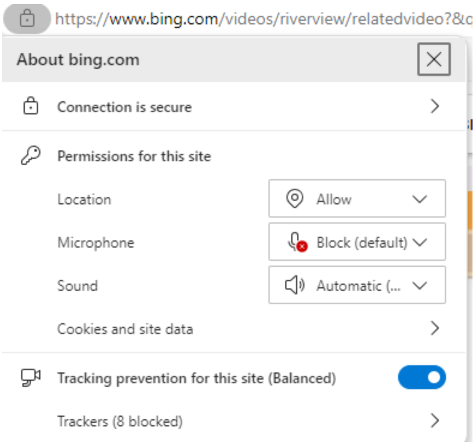
How to identify fraudulent website:

1. Check the domain name carefully**.** Look for misspellings and transposed letters. A scam website will be VERY similar to a legitimate site.
2. Look for the padlock symbol to show the website is secure, using the HTTPS designation.



https://www.l

. You can click on the lock to check if the connection is secure as well.



https://www.bing.com/videos/riverview/relatedvideo?&c

About bing.com

Connection is secure

Permissions for this site

Location: Allow

Microphone: Block (default)

Sound: Automatic (...

Cookies and site data

Tracking prevention for this site (Balanced)

Trackers (8 blocked)

3. Once on the site, look for poor spelling, language inaccuracies, design issues, logos that look distorted and other red flags
4. Check the age of the domain.
5. Use a website scanner to look for malware.
6. Do not be conned by typical “Trust Signals” images embedded on a webpage.
7. Remember deals that are too good are the most common way fraudsters get you to their fake sites. These will be in your social media pages and as adds on websites.
8. Read the shipping and return policy closely. Official retailers have a dedicated webpage detailing their shipping and return policy. If the website you’re on doesn’t explain how to return an item, it’s a scam. The website should also include basic legal information, such as its terms and conditions, privacy policy, and data collection policy. If you can’t find this information, it’s likely not a legitimate company.
9. Beware of non- traditional payment methods. You should never be forced to pay for a purchase with a gift card, cryptocurrency, or Zelle or cash payment apps. Use traditional, safer methods that are protected for consumers like VISA or MC debit and credit cards, PayPal, or Buy now Pay later solutions such as Klarna or Afterpay.

Check out the articles linked below from the Federal Trade Commission and Better Business Bureau for more details on ways to avoid fraudulent websites:

- **Don’t let scammers get in the way of your holiday shopping | Consumer Advice**
- **BBB Tip: How to identify a fake website**