HOW TO DETECT FRAUDULENT SITES SELLING FAKES

Public awareness and prevention

LOOK FOR THESE RED FLAGS:

If the price seems too good to be true, it probably is.

Be suspicious of websites offering highly discounted prices. Scam websites use low prices to lure shoppers to quickly sell fake or non-existent items.

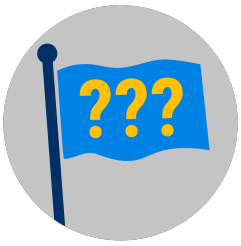
Check if the “About us” and “Contact us” pages contain full details: name of the company, address, phone number or an official email address.

If the site does have a 'Contact us' page but only offers a form to fill out, this can also be an indicator of a fraudulent website.

.

Check if there are grammar and/and spelling mistakes or the site looks unfinished.

This should be an instant red flag.



Check if the domain name contains the words “genuine”, “replica” or “original”, or the name of a brand or product, but adding words like “offer” or “discount”.

Be also cautious of domains which end in .net or .org, as they are rarely used for online shopping.

Check if the domain is registered in a different country than yours.

Even if the site uses your country’s domain, do not assume that it is registered in your country. Be suspicious of websites that are written in your language but use a domain from another country.

Check how long the domain has existed. If it has been active for less than a year, it could be a scam website.

You can check who owns the domain by using a WHOIS database, which can be found easily on any popular search engine by searching this tag.

Check if the photos are of bad quality, are resized or difficult to see, or the opposite, are copied from original websites or are stock photos.

Illicit websites might use images from a brand's most recent advertising campaign or from the original website to boost their credibility. Websites selling counterfeit clothes often use stock photos from the runway shows.

Read reviews from different pages, online forums and search engines.

Check the company's social media pages for information. Be aware that reviews can also be fake. For example, if there is a similarity in the reviews across several websites, or the same users are commenting, be suspicious.

Search for information about replicas and fakes of the product you intend to buy, so you know what to look for.

Check that the site is secure and its URL begins with “https” instead of “http”.

This means that the site is secured using an SSL Certificate (the s stands for secure). Even if a website shows secured pictures from most known payment institutions it could be fake.

Check if the site offers a return policy, terms and conditions and a privacy policy.

A real company should tell you how and where to return a faulty item, as well as what they do with your data.

AVOID...

- Don’t trust websites just because they show the logo or original photos of a reputable brand. This doesn't necessarily mean they are genuine.
- Avoid buying goods from websites that are selling all categories of branded products in a single page.
- Don’t buy pharmaceutical products from unofficial sites.
- If you are asked to pay for product online via a bank transfer, don’t. If you buy a product with a credit or debit card that turns out to be fake or non-existent, you do have some rights to get your money back. But if you pay by bank transfer there’s very little you can do to get your cash back.

WHEN IN DOUBT...

- Ask the seller questions about the products, for extra, non-generic pictures, and if they offer an after-sales service, or a guarantee. By contacting the seller you can also find out if the phone and email address provided are non-existent or fake.
- Contact an authorised re-seller or official representative of the brand to check if they know the seller or the suspicious website. Be aware that some luxurious brands cannot be sold on the Internet, only in physical shops through an official retail network.

WHAT SHOULD I DO IF I SPOT A FRAUDULENT WEBSITE?

- Exit the site to avoid a cyber-attack.
- Report the website to your local or national police
- Report it to the genuine brand holder.
- Warn the people around.

I AM A VICTIM OF COUNTERFEIT GOODS FRAUD. WHAT SHOULD I DO?

If you have bought an item online and later discovered that it is not original…

- Report it to your local or national police.
- Report it to the genuine brand holder.
- Report it to your bank, if you paid the product with a credit or debit card. You may have some rights to get your money back.

CRIME AREAS: Intellectual property crime • Counterfeiting and Product Piracy
TARGET GROUPS: General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
ENTITIES: Intellectual Property Crime Coordinated Coalition (IPC3)

Source URL: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/how-to-detect-fraudulent-sites-selling-fakes