

Shopping online to stay safe during the pandemic? Here are 10 tips for avoiding scams

October 6, 2020

The holiday season is already a booming time for [online shopping](#).

The [COVID-19 pandemic only increases](#) the likelihood that when people shop this holiday season, they will choose online shopping over brick-and-mortar stores. However, this also means there is likely to be a boom in [online scams](#).

Already, multiple companies from outside the U.S. are advertising relatively unchecked on the internet, selling – or even just pretending to sell – all manner of products. The items are typically advertised using designs stolen from legitimate businesses and artists, often ripped off from Etsy, especially if those designs have been featured on popular sites like Bored Panda.

When people buy these scam products, what arrives is typically of [low quality](#). That's if anything ever arrives. Often the company just shutsters and renames itself without sending anything. In worst-case scenarios, they also steal customers' credit card information.

So how to shop smart and spot scams? Here are some clues to watch for.

1. Is it too good to be true?

Does the product pictured match the price? Know the market. An amazing product for a low price is cause for suspicion. For example, Instagram was featuring photos of a “Halloween Advent Calendar.” The ad listed a price of US\$59.99, but available for a limited time for \$29.80. At first glance you might think you're getting a great deal, but take a moment to think it through. That price would barely cover the cost of shipping and handling for a product of that size. The original product, [sold on Etsy](#), retails for over US\$1,800, and the creator has a backlog of orders.

2. When in doubt: Google it

Perhaps you're not familiar enough with Etsy workmanship to recognize a likely ripoff. When in doubt, search the product name or download the image and run a [Google image search](#). You are likely to find the original source. If the

product really exists – unlike this [CG baby shark](#) that one company used as an ad for its alleged baby shark robot toy – you can choose to pay the original artist for their hard work or take the risk and try to get the knockoff. The search will also reveal whether there are multiple alleged businesses selling the same “unique” and “exclusive” items using the same exact pictures. Once you start seeing double or more, that’s a warning sign.

3. Check the business reputation

Searching for the business name will likely just take you to the business’s site. Instead, search the business name with the word “scam.” You will be able to tell pretty quickly if there is a worrisome history associated with the business. You can also try [Scamvoid](#), which is dedicated to identifying the trustworthiness of online links. There may be a Better Business Bureau listing for the company, but [be careful about relying on these](#). You can also find Facebook groups, like this one for [fashion-related scams](#), that track untrustworthy sites.

4. Too new to trust

In some cases the business is so new that you won’t be able to find a track record. This is a red flag. They are likely one of those companies that close up once they’ve gotten enough orders then set up a new name and new domain and do it all over again. There is a chance that it’s a legitimate new businesses trying to open shop during a pandemic. To tell the difference between a legitimate new business and a fly-by-night operation, apply some of the following steps to judge them.

5. Review the reviews

Take a close look at the reviews. If there aren’t any, back away. If there are, check for the following warning signs. The reviews are few and unanimously five stars with no comments. If there are comments, they are loaded with broken English or vague praise that could have been copied and pasted from any product. None of the reviews includes pictures of the actual received product. There aren’t any negative reviews, which is a red flag because even the best legitimate businesses can’t please everyone all the time. As a side note, if you are looking at a legitimate product offering, be careful not to [read too much into the negative reviews](#).

6. Is it a ‘good’ site?

Does the business have a website, and not just a Facebook page? If not, that's a big no. If they do, is it a complete website, or is it barely there? Check that the business has a phone number that works, and when you search the number it doesn't have 12 other "businesses" associated with it. Check that it lists a mailing address, preferably one that isn't just a post office box.

Check the site's "about us" page. Doesn't have one? That's another no. Does the "about us" include a year the business started? Does it include information about the products' creators? If the page has a photo purporting to be of the owner or artist, you can do a Google image search to see if it's a photo copied from another webpage, a stock photo or a fake created by an AI system. Do their claims about themselves hold up to scrutiny? For example, does the site claim to be an American Black-owned business but their [WHOIS domain information](#) lists a company in China?

7. Social media presence: Do they have one?

Similarly, do they have a social media presence outside of the ad that pops up in your newsfeed? If not, steer clear. If so, you can click on the poster's name to see where the person or business is located and when the page was started. You can also see how far back their posts go, as well as check the quality of those posts and chatter about the company.

8. Beware the 'going out of business' story

During the pandemic, [legitimate businesses are, in fact, closing](#). Illegitimate businesses have been latching onto this as a tool to tug at people's heartstrings to trick shoppers. It is [illegal for American businesses to do this](#), but businesses outside of the U.S. are not subject to the same laws. One way to tell the legitimate businesses from the frauds is to check the starting date on [website domain registrations](#) and social media sites. If the business popped up during the pandemic just in time to go out of business, steer clear.

9. Fad ad clickbait

Watch out for fad items. Knockoffs and ripoffs abound on any hot or trendy item. Nowadays marketers are also picking up on political trends. Businesses crop up with names like "WeLuvTrump," "FemPower" and "BlackGoodness." The same is happening with political news. For example, RBG items are all the rage in the wake of Justice Ruth Bader Ginsburg's death. Again, following the steps above will help you sort out which products are legitimate.

10. Social influence tricks

Also watch out for the common marketing techniques originally uncovered by social psychologist [Robert Cialdini](#) that are used by legitimate and illegitimate businesses alike. The most common you are likely to see in scam sites are claims of exclusive access, which appeal to your [need for uniqueness](#), claims of limited supply or time running out on a “sale,” which play on the [psychological value](#) people place on scarce items, and claims like “Karen S. from Indianola just purchased this item,” which are “[social proof](#)” that a behavior is safe or appropriate because others have done it.

Ultimately, if these 10 tips seem like too much to go through just to get that unique toy for your grandkid, buy instead from a trusted source you have counted on in the past. It’s also a good idea to use credit cards or payment services like PayPal that protect consumers from fraudulent charges.

Shop wisely. Your bank account is counting on you!

Copyright © 2010–2020, [The Conversation US, Inc.](#) - Reprinted with permission.