

# How to Avoid Online Purchase Scams

## What Is an Online Purchase Scam?

Online purchase scams typically involve the purchase of products and/or services where the transaction occurs via a website or other online means. Scammers utilize online technology to offer attractive deals, but once the payment is made no product or service is delivered. In another version, fraudsters pretend to purchase an item only to send a fake check and ask for a refund of the “accidental” overpayment; by the time the victim realizes the check is bad they’ve already sent the funds from their account.

## 9 Online Purchase Scam Prevention Tips

1

### If the deal looks too good to be true, it probably is.

The top motivating factor for people who made a purchase and then lost money was price. Don’t shop on price alone.

2

### Before you buy, do your research.

Out of the 57 percent who did not research the website or business via an independent source before making a purchase, 81 percent lost money.

3

### Beware of fake websites.

Check the URL for errors/inconsistencies. Watch for bad grammar. Beware of new domain names. Search for accessible contact information. Read online reviews about the company and/or website.

## Online Purchase Scam FINDINGS

Online purchase scams were **among the top three riskiest scams** in 2017, 2018, and 2019.

**Low price was the top reason** victims purchased a product online and lost money.

**73%** of online purchase scam victims **paid but never received a product.**

**63%** were actively **searching for a product** when they lost money to an online purchase scam.

4

**Beware of making quick purchases while scrolling social media.**

Did you see an ad for those red shoes you've been searching for, and they're a steal? Like marketers for real companies, scammers have access to the tools they need to learn about your buying behaviors, offering up exactly what you want at enticing prices.

5

**That shipment tracking information you received might be fake.**

Look closely to make sure you are dealing with a legitimate business. Don't just click on the tracking link; go to the shipper's website and type in the code yourself to see if it's real.

6

**Use secure and traceable transactions.**

Avoid paying by wire transfer, prepaid money card, gift card, or other non-traditional payment methods.

7

**Don't believe everything you see.**

Scammers are great at mimicking official seals, fonts, and other details. Just because a website or email looks official does not mean it is. If a business displays a BBB Accreditation Seal, you can verify its legitimacy via the [BBB.org](http://BBB.org) website.

8

**Make sure the website is secure.**

Look for the "https" in the URL (the extra s is for "secure") and a small lock icon on the address bar. Never enter payment or personal information into a website with only "http" (it is not secure).

9

**Be careful purchasing sought-after products, especially during the holiday season.**

The risk of online purchase scams rises during the holidays because more people are making online purchases, but also because scammers are offering the most popular products for the season at great prices.

**81% of those who did not research the website via an independent source lost money.**

Of the 59% who received shipping information, **54% said it was fake.**

Those who did NOT lose money were 22% more likely than those who did to say **the BBB Accreditation seal helps them decide who to trust online.**

**▶ LEARN MORE AT:  
[BBB.org/OnlinePurchaseScams](http://BBB.org/OnlinePurchaseScams)**