BankOnITUSA®

INFORMATION SECURITY BRIEF

NOVEMBER 2024

Don't let scammers get in the way of your holiday shopping.

As the holiday season approaches, there are more fake shopping sites. The ads on social media show expensive products like electric scooters, designer bags, and other popular toys and gifts at unbelievably low prices. Many of these bogus sites use photos and logos the scammers steal from legitimate businesses, but they won't send you authentic products. If you're wondering how to avoid these phony offers, there are a few ways to help you detect them.

Unusually low prices are a sign of a scam. Don't click on ads that advertise a product at a very low price when you know it's usually a costly item. Clicking the link in the ad could take you to a scamming site that takes your money and sends you something that looks different from what was advertised… or sends you nothing at all.

To protect yourself while shopping online:

- **Do some research.** Especially before you buy from an unfamiliar seller, search online for the name of the seller plus words like "review," "complaint," or "scam." See what others say about their experience with the seller.
- **Check the terms of the sale.** Look at the price, other charges, their refund policy, who pays for return shipping, and if there's a restocking fee.
- **Never buy from online sellers who demand** you pay with gift cards, wire transfers, payment apps, or cryptocurrency. Only scammers tell you to pay that way.

Did you have a problem while shopping online? First, contact the seller and try to work it out. If that doesn't work, contact the company you used to make the payment to dispute the charges. If they can't help, tell the FTC at ReportFraud.ftc.gov.