

EIGHT TIPS TO PROTECT YOURSELF FROM

Holiday Fraud

Holiday shopping is exciting, and it's fun finding the perfect gift for someone you love. Many businesses offer incredible deals online and in-store during this season and you may be delighted to find an excellent price for the gifts on your list.

At the same time, you need to stay vigilant against fraud while shopping. There is no shortage of horror stories involving scam artists getting the best of holiday shoppers, so let's take a look at a few ways to avoid becoming another victim.

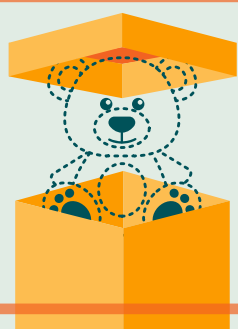


1. Only visit familiar websites.

A 2021 AARP survey found that 38% of respondents were scammed by clicking on a bogus social media ad.¹

2. Use a third-party digital wallet to pay.

Apple Pay, Google Pay and Samsung Wallet are encrypted payment services that add another layer of credit card protection.²

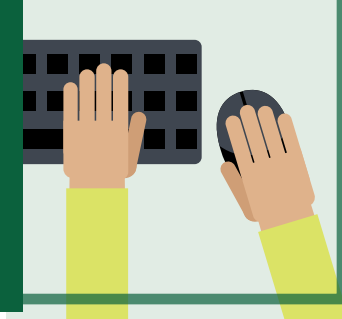


3. Purchase directly from the seller.

Buying from the original seller can help you avoid scams. Third-party e-commerce websites like Amazon and Etsy allow you to dispute charges if the item never arrives.

4. Research the business before purchasing.

If you want to purchase from somewhere new, search the charity or company online with the words "scam" or "complaints" at the end to check for legitimacy.



5. Take a look at the URL before clicking.

Hover over the link to see where it will actually take you. Watch for misspellings, atypical domain names and other irregularities.

6. Avoid deals that seem too good to be true.

If an expensive item is being sold for far less than from the trusted merchant, it may be a scam.



7. Check out the item in person.

Online marketplaces can have great prices on used items. If you're able to, check out the item in person before giving the seller money upfront.

8. Beware of emails or texts from senders you don't know.

Messages about order updates or issues could be a scammer attempting to steal your information. Don't click links. Instead, contact the seller directly.



Have fun shopping this holiday season, but be careful! The last thing you want to worry about while spending time with family is a scam. Keep a close eye on your bank account and watch out for suspicious activity. If it seems too good to be true, or the website has strange spelling errors, these could be signs that the seller may not be who they say they are.

Sign up for suspicious activity alerts and read our [2022 guide to cybersecurity](#).