

How to Protect Yourself from Holiday Shopping Scams

National nonprofit credit counseling agency Take Charge America arms consumers with knowledge to keep scammers from playing the Grinch this year

PHOENIX – (**Nov. 10, 2022**) – Online scams cost Americans nearly \$7 billion throughout 2021, according to the FBI, and with the holiday shopping season ramping up, it's vital that people understand how to avoid falling victim to scams.

"Scams often increase with consumer spending, making the holidays ripe for scammers trying to take advantage of the season's sense of urgency and scarcity," said Amy Maliga, a financial educator with Take Charge America, a <u>nonprofit credit counseling and debt management agency</u>. "It's not enough to be aware of scams, though. You have to learn how to watch for and avoid them so your happy holidays don't turn into a nightmare."

Maliga shares several things to do and watch out for to avoid falling prey to holiday shopping scams:

- Use secure payment methods: Be wary of websites or sellers that request unusual payment methods like wire transfers, cashier's checks or apps. Stick to secure payment options such as major credit cards or PayPal.
- Check for site security: Look for 'https' at the front of the site's URL and the small lock icon in the browser window. These indicate that the website is secure, ensuring any data you share (such as credit card numbers or shipping details) will be encrypted when you submit it.
- Watch for spelling and grammatical errors: If you notice a plethora of spelling and grammar mistakes on a website, social media posts or other promotional materials, you likely want to shop elsewhere.
- Pay attention to reviews: Reviews can reveal much about online retailers and sellers. Are there lots of poor reviews from buyers who didn't receive what they purchased? Or are there numerous glowing reviews that all read alike? Either may indicate the site isn't what it claims to be.
- Watch for 'phishy' confirmation emails: If you receive a confirmation email for an order you didn't place, ignore and delete it. Knowing people are likely making several orders, scammers will send a phishing email disguised to resemble a confirmation notice from legitimate retailers. If it appears legit, try manually searching the order number on the retailer's website instead of clicking on any included links.

Don't let scammers steal your money or your holiday cheer. If a deal or website appears too good to be true, it likely is.

For additional resources to combat financial scams and ensure holiday shopping success, explore Take Charge America's Budget Tools.

About Take Charge America, Inc.

Founded in 1987, Take Charge America, Inc. is a nonprofit agency offering financial education and counseling services including credit counseling, debt management, housing counseling and bankruptcy counseling. It has helped more than 2 million consumers nationwide manage their personal finances and debts. To learn more, visit takechargeamerica.org or call (888) 822-9193.



###

Contact:

Tim Gallen Aker Ink (480) 335-6619 tim.gallen@akerink.com