Holiday Scams

The holiday season is a time of joy and giving, but it's also a prime time for scammers to take advantage of preoccupied and unsuspecting individuals. While you're busy planning festivities and shopping for gifts, fraudsters are plotting ways to separate you from your hard-earned money. According to AARP, three-quarters of U.S. consumers have experienced or been targeted by at least one form of fraud that can be tied to the holidays. This week we'll share some details on common holiday scams and some tips to help you protect yourself.

Online Shopping Scams: Online shopping scams involve fraudulent websites or sellers that offer enticing deals on holiday gifts, but the either don't deliver the products or they sell you counterfeit items.

- Only buy from reputable online retailers.
- Check for secure website connections (https://).
- Read product and seller reviews.
- Use secure payment methods to protect your financial details.
- Be cautious of deals that seem too good to be true.

Charity Scams: Scammers exploit people's generosity during the holiday season by impersonating charitable organizations and soliciting donations for bogus causes.

- Independently research charities before donating.
- Verify the legitimacy of the charity's website and contact information.
- Be cautious of high-pressure donation requests.
- Consider donating directly through the charity's official website.

Travel and Accommodation Scams: Scammers will often set up bogus travel agencies or list fake vacation rentals to trick holiday travelers into booking non-existent trips or accommodations.

- Research travel providers and accommodations.
- Verify the legitimacy of websites and listings.
- Use secure payment methods to protect your financial details.
- Be wary of travel offers advertising unbelievable promotions.

Fraudulent Communication: Scammers may send fraudulent emails, texts, or phone calls claiming to be from legitimate companies. They might impersonate trusted organizations, friends, or family members to trick you into providing information or sending money for various reasons.

- Verify the authenticity of communication by independently contacting the organization or person using official or known contact information. Never trust contact details provided in correspondence.
- Be cautious of unexpected requests for personal details, payments, or urgent actions.
- Be wary of unsolicited messages or pop-up ads containing links as they could lead you to phony sign-in pages asking for sensitive information or even to websites infested with malware.
- Trust your instincts. If something feels off or too good to be true, it probably is.