



YOUR HOLIDAY EDITION OF OUR

Fraud Awareness Newsletter

Helping you stay protected against the newest holiday scams.



Holiday Scams Are on the Rise This Season

According to the FTC, consumers lose tens of millions of dollars each year to holiday-related fraud. Southwest Heritage Bank is committed to helping you stay one step ahead. Read below for practical tips to safeguard your money and your peace of mind.

Holiday Scams to Avoid

Fake Online Stores & Lookalike Sites

Scammers build polished, fake storefronts that mimic real retailers—complete with logos, product photos, and bogus reviews. They lure shoppers with hard-to-find items or deep discounts, take your payment, and you never receive the goods. Beyond the lost purchase, your card or personal data can be harvested and used for further fraud. Always check the URL for typos, avoid unfamiliar sellers with no contact info or return policy, and pay with a credit card when possible.

Fake Charities & Donation Appeals



"Free" Gift Card Offers

"Free gift card" messages—whether email, pop-up, or text—are a common phishing tactic during the holidays. Scammers promise free rewards to get you to click links or share personal and financial information. Once you share data or enter card numbers, money or identity details can be stolen. Treat unsolicited gift card offers as suspicious: don't click links, mark the message as spam, and verify any promotion directly with the company.

Seasonal Job Scams

Fraudsters exploit holiday generosity by creating fake charities or impersonating legitimate organizations to solicit donations. These appeals often use urgent, emotional stories or social media fundraisers to pressure you into giving immediately. If you donate via links in texts or emails, your payment & personal details can be stolen, and your gift won't go where you intended. Always research organizations before you give, donate directly through a charity's verified website, and avoid paying by wire transfer or gift card.

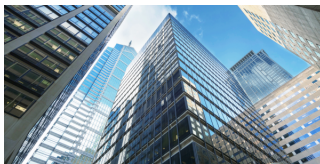
During the holidays, scammers take advantage of job seekers looking for extra income. They post fake listings for easy, high-paying remote or retail positions, often asking for personal details or upfront payments before "hiring." Once you share your information, your identity or money can be stolen. Be cautious of jobs that require fees, promise quick hiring without interviews, or sound too good to be true.

Misleading Social Media Ads

Holiday feeds are full of tempting ads, but some promote products that are counterfeit, never delivered, or enroll you in recurring charges after a "free trial." Scammers can build fake profiles and paid ads that look legitimate, then disappear after collecting payments or data. Before you click "buy," verify the seller and read reviews outside the ad. Visit the merchant's official site, check BBB or other review sites, and be wary of deals that seem too good to be true.

[Click Here to Learn About Other Holiday Scams](#)

Fraud in the News



Holiday Scam That Cost One Company \$60 Million

Cybercriminals posed as a trusted vendor and tricked a company into wiring \$60 million through a fake invoice. The scam exploited the rush of year-end business, underscoring the need for strict verification and internal payment controls during the holidays.

[Read Article](#)



Fake Toll Texts Target Drivers in Arizona & Other States

Drivers in Arizona and other states are being targeted with texts about "unpaid tolls," even in areas where no toll roads exist. These messages are designed to steal personal and financial information, so never click links and always verify any suspicious notifications.

[Read Article](#)



16 Holiday Scams to Look Out for in 2025 & How to Avoid Them

From fake online stores and phony delivery texts to misleading travel deals and gift card tricks, scammers are active across shopping, giving, and holiday travel. Learn how to spot common scams and protect your money & personal information this season.

[Read Article](#)

Helpful Resources



FBI: Holiday Scams and How to Protect Yourself

Learn more about common holiday scams like non-delivery, non-payment, and auction fraud.

[Learn More](#)

Neural Technologies: How to Safeguard Your Business and Customers

Explore how businesses can prevent holiday fraud and protect customers from common scams.

[Learn More](#)

Truist: How to Spot These 6 Common Holiday Scams

Learn more about six common holiday scams and simple steps to stay safe while shopping and giving this season.

[Learn More](#)

Southwest Heritage Bank: Fraud Prevention

Visit our website for tips on spotting scams, reporting suspicious activity, and protecting your accounts.

[Learn More](#)

*If you suspect that you have been targeted for a scamming scheme, please **contact** Southwest Heritage Bank immediately.*



For more fraud awareness tips, follow along with us on social media!

Southwest Heritage Bank is Member FDIC.



Try email & social marketing for free!