SOUTHWEST HERITAGE BANK



Stay One Step Ahead of Holiday Scams

Holiday shopping, travel, and unexpected messages can create opportunities for scammers to catch you off guard. Southwest Heritage Bank is committed to helping you recognize the warning signs. Explore this season's fraud reminders and practical tips to protect your money, your personal information, and your peace of mind.

Holiday Scams to Avoid

Unexpected Packages & QR Code Traps

A surprise package may seem like a holiday gift, but an enclosed QR code could lead to a scam. Fraudsters send inexpensive items with instructions to scan a code to identify the sender or arrange a return. The linked website may ask for passwords, card numbers, or other personal information. Don't scan codes in packages you weren't expecting. Instead, check your shopping accounts directly, contact the marketplace through its official app or



AI Voice Cloning

A frantic call that sounds like a loved one can be difficult to question, especially when family members are traveling for the holidays. Scammers can use artificial intelligence to imitate a familiar voice and claim someone needs urgent money after an accident, arrest, or other emergency. Don't rely on the voice alone. Hang up and call your loved one at a number you already know, or contact another trusted relative. Requests for secrecy or immediate payment are warning signs.

website, and report unfamiliar orders.

Fake Bank Alerts & "Safe Account" Scams

An unexpected call or text about suspicious holiday purchases may actually come from someone impersonating your bank. Scammers create urgency, ask for online banking passwords or security codes, or tell you to move money into a “safe” account. Caller ID can be faked, so a familiar number doesn’t prove the contact is legitimate. Hang up and call the number on your card or statement. Never share login codes with an unexpected caller or transfer money because someone says it needs protection.

Holiday Vacation Rental Scams

Planning a holiday getaway? Scammers copy real vacation rental listings or advertise properties they don’t control, then pressure travelers to pay before someone else books the dates. Some ask you to leave a booking platform and send money directly, putting your payment and personal information at risk. Research the property address and rental company, review cancellation terms, and keep communication and payment within a trusted booking platform. Be cautious of unusually low prices and demands for wire transfers, cryptocurrency, or gift cards.

Other Holiday Scams to Note

- Fake online stores and lookalike retailer websites
- “Free” gift card offers and prize giveaways
- Fake charities and urgent donation appeals
- Seasonal job offers that require upfront payments
- Fake delivery texts requesting fees or address updates

Click Here to Learn About Other Holiday Scams

Fraud in the News



Tucson Woman Scammed by AI on Neighborhood App

Pima County investigators warn that AI is making familiar scams more convincing and harder to spot. A Tucson woman encountered several schemes, including a fake dog-sitting job on Nextdoor that sent her a fraudulent check to cover pet food, toys, and supplies.



Deed Fraud–or Title Theft–Puts Homeowners at Risk

Criminals use stolen identities and forged documents to fraudulently transfer property deeds, then attempt to sell homes or borrow against their value. Homeowners should be aware of warning signs such as unfamiliar loans or unexpected changes to property records.



Travel Scams Are Getting Harder to Spot

Travel scams can happen before you even step foot on a plane. Scammers are using AI to create convincing travel websites and posing as hotels or airlines to request payments and personal information. Learn more about recognizing suspicious messages.

Watch Video | Read Article | Read Article

Helpful Resources



AARP: Six Holiday Scams to Watch for in 2026

Explore recent holiday scams and learn practical tips to protect your money and personal information.

Learn More



Federal Trade Commission: Helping Veteran-Owned Businesses Avoid Scams

Learn about scam prevention for veteran-owned businesses during National Veterans Small Business Week.

Learn More



Federal Trade Commission: Smart Shopping and Safe Giving

Find tips for shopping safely, recognizing fake charities, and avoiding scams when making purchases or donations.

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 also now on Facebook– click the icon above for our official Facebook channel!

Southwest Heritage Bank is Member FDIC.

Southwest Heritage Bank | 8777 East Hartford, Suite 100 | Scottsdale, AZ 85255 US

Unsubscribe | Update Profile | Constant Contact Data Notice

Constant Contact

Try email & social marketing for free!