

Stay Vigilant This February

The month of February brings love, celebrations, and, unfortunately, opportunities for fraudsters to take advantage of trusting people and busy lives. Scammers use a mix of romantic bait, impersonation, and business schemes to target both individuals and business owners. We are committed to helping you stay one step ahead. Read below for practical tips to safeguard your money and your peace of mind.

Scams to Avoid

Romance & Sweetheart Scams

Romance scams occur when someone builds an online connection—often through dating apps, social media, or email—and then slowly gains your trust before asking for money, gifts, or help with a supposed emergency. Scammers often use fake photos and elaborate stories to appear genuine, and their requests can escalate over time. These scams can affect all ages, but are most commonly targeted at older adults. Be extra vigilant around Valentine's Day.



Business Email Compromise

Especially common for business owners, Business Email Compromise (BEC) scams involve cybercriminals spoofing a trusted vendor or supplier's email address to request changes in payment information or send fake invoices. If payments are made without verification, businesses can lose significant sums before noticing the fraud. Always double-check payment details and confirm via a trusted phone number or in-person contact.

Bank Impersonation Scams

Scammers may contact you by phone, text, or email pretending to be a bank employee and claim there's suspicious activity on your account. They often create a sense of urgency, asking you to "verify" account details, provide one-time passcodes, or move funds to a "secure" account. Remember, Southwest Heritage Bank will **never** ask for your full password, PIN, or one-time security codes. If something feels off, hang up and call your local branch directly using a trusted phone number.

Online Marketplace Scams

Fraudsters post fake listings on online marketplaces (OfferUp, Facebook Marketplace, Craigslist, eBay, etc.) for high-demand products or services at extremely low prices. When a customer pays, the item never arrives or is counterfeit. Always check seller ratings, use secure platforms with buyer protection, and avoid deals that look unrealistically cheap.

Smishing Scams

Smishing is text-message phishing: scammers send messages that appear to be from banks, delivery services, or government agencies with links that steal login credentials or install malware if clicked. These can be tied into Valentine's Day themes ("Your gift is waiting, click here!") or everyday banking alerts. **Never** click unsolicited links and confirm with the institution directly through official channels.

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

Fraud in the News



Romance Scams Put Millions of Adults Aged 50+ at Risk

About 1 in 6 adults age 50 or older say they or someone they know has had money stolen through a romance scam. While 90% of adults *believe* they would report a loss, over half of those who lost money did not report it anywhere. Learn more about ways to protect yourself below.

[Read Article](#)



AZ Attorney General Issues Crypto ATM Scam Alert

Arizona Attorney General Kris Mayes is warning residents about a sharp rise in cryptocurrency ATM scams, which cost Arizonans more than \$177 million in 2024 alone. A new [fraud complaint form](#) for Arizonans has also been launched.

[Read Article](#)



Mesa Woman Loses Home in Online Romance Scam

A Mesa woman lost her home and life savings to an online romance scammer posing as a Naval officer. The scammer convinced her to sell her house to fund their fake relationship. The incident highlights the prevalence of these scams in our local communities.

[Watch Video](#)

Helpful Resources



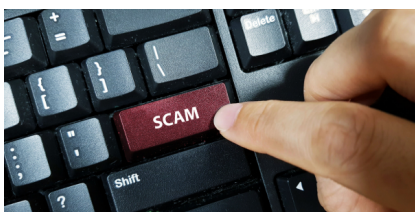
Federal Trade Commission: What to Know About Romance Scams

Learn about romance scams, common tactics scammers use, and how to report it.

[Learn More](#)

AARP: Top Tax Season Scams to Be Aware Of

Avoid tax prep schemes, fake rebate promises, and IRS impersonators when filing in 2026.

[Learn More](#)

Better Business Bureau: Scam Tracker and Reports

Read real reports from consumers, understand trending scams, and access prevention tips.

[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!