FIGHT FRAUD
IDENTIFY THIS TYPE OF SCAM

The "Your Device is Infected" Trap
Tech Scams

The "Click, Connect, Scam" Trick
Social Media Scams

The "Too-Good-to-be-True Job" Scheme
Employment Scams

HOW IT WORKS

- You receive an unexpected invoice via email saying you'll be charged automatically unless you call a provided number.
- When you call, scammers pretending to be tech support convince you to grant remote access to your device or online banking, leading to unauthorized transactions.

- Scammers create fake social media profiles or use hacked accounts to message you pretending to be friends, romantic interests, or investment gurus.
- They coax you into sharing private information, photos, or sending money through fraudulent contests, giveaways, or fake checks.

- You see a job posting promising easy, high pay or you're contacted directly through social media or text messaging.
- You complete an application or interview via messaging apps like WhatsApp or Telegram.
- Scammers send you a check upfront, instruct you to deposit it, then ask for some funds back, leaving your account overdrawn when the check inevitably bounces.

RED FLAGS

- Sudden pop-ups claiming your device is compromised.
- Unsolicited calls from supposed tech companies (Microsoft, Geek Squad).
- Emails warning of automatic billing unless you contact them immediately.
- Urgent demands for repayment via gift cards, cryptocurrency, or money transfer apps.
- Requests for remote access to your device.

- Messages from unknown profiles with minimal or no content.
- Poor grammar, spelling, or overly enthusiastic investment offers.
- Requests for personal or banking information, compromising photos, or payments.
- Links promising free giveaways, quizzes, or contests from unknown senders.

- Unsolicited job offers or contact via social media or messaging apps.
- Job descriptions that are vague, easy, and offer unusually high pay.
- Communication via generic email addresses (Gmail, Yahoo, Hotmail).
- Requests involving upfront payments, gift cards, cryptocurrency, or wiring funds.

YOUR NEXT MOVE

- Verify invoices directly with official company contacts.
- Never grant remote access unless you've initiated contact through a verified number.
- If suspicious, contact Sun Community immediately at 760-337-4200.

- Limit personal information shared on social media.
- Verify unusual requests directly with the real account holder offline.
- Report suspicious activity immediately to your bank, social media platforms, and law enforcement.
- Parents: Talk to your teens about spotting and reporting suspicious messages.

- Research employers directly on their official websites before applying.
- Never provide personal information or banking details upfront.
- Trust your instincts: High pay with minimal effort usually spells trouble.
- Report suspicious job offers immediately and freeze your accounts if you've shared sensitive information.

BRIGHT, UNIVERSAL TIPS

- Trust your gut: urgency + secrecy = scam.
- Never share your Online Banking credentials, Social Security number, or one-time passcodes.
- Confirm phone numbers and websites directly from official sources.
- Regularly monitor your accounts via our mobile app.

Need help or think you've been targeted? **CALL US: 760-337-4200.** We're here to help keep you safe.

SUN COMMUNITY *Shine On!*