PROTECT YOURSELF

1. DON’T GIVE OUT YOUR BANK ACCOUNT INFORMATION: Never give out your bank account information or social security number over the phone. The IRS will NEVER ask for this type of information.

2. FACT CHECK INFORMATION: Contact trusted sources to verify information before you pass it on. For the latest information from the Centers for Disease Control visit www.CDC.gov.

3. HANG UP ON ROBOCALLS: Scammers are using illegal robocalls to pitch everything from scam coronavirus treatments to home test kits.

4. AVOID CLICKING ON UNKNOWN LINKS: Don’t respond to text messages or emails about checks from anyone.

5. RESEARCH CHARITABLE DONATIONS: Do your homework when it comes to donations, whether through charities or crowdfunding sites.

U.S. Attorneys’ Offices for the Eastern, Northern, and Western Districts of Oklahoma and the Oklahoma Attorney General’s Office urge the public to remain vigilant for coronavirus fraud.

- Unsolicited calls, social media platforms, apps, emails, texts, and door-to-door visits are often used to target victims
- Anyone selling fake testing kits, treatments, or cures for COVID-19
- Websites seeking donations for illegitimate or nonexistent COVID-19 charities
- Fraudulent phone calls from individuals posing as health insurers seeking personal information
- Robocalls offering medical supplies with no intent to deliver
- Websites claiming to provide stimulus funds when consumers input their bank information
- Fake mobile apps claiming to “track the spread of COVID-19” but instead insert malware to compromise users’ devices and personal information
- Fraudulent medical billing for procedures related to COVID-19
- Threats to public officials advocating quarantines
- Hoarding or price-gouging of necessary supplies
- Threats to intentionally infect individuals with COVID-19
- Offers to help individuals file claims for unemployment benefits and ask for personal information like SSN, DOB, credit card number
- Phishing emails from scammers posing as national and global health authorities, including the CDC and WHO, sent to trick recipients into downloading malware or providing personal identifying and financial information
- Phone calls/emails claiming to be health care providers that have treated a friend or relative for COVID-19 and demand payment

For more information go to:

https://www.justice.gov/coronavirus
http://www.oag.ok.gov/coronavirus-fraud-resources

Report suspected coronavirus fraud:

Department of Justice
1-866-720-5721
disaster@leo.gov

Oklahoma Attorney General’s Consumer Protection Unit
Call: 405-521-2029
consumerprotection@oag.ok.gov