Office Of The
DISTRICT ATTORNEY
County of Shasta

Stephanie A. Bridgett
District Attorney

FOR IMMEDIATE RELEASE
March 25, 2020
www.da.co.shasta.ca.us

CONTACT: Consumer Protection Unit
PHONE: 245-6300
FAX: (530)245-6334
1355 West Street
Redding, CA. 96001

UPDATED APRIL 10, 2020

"Shasta DA Issues COVID-19 Fraud Alert"

Scammers are taking advantage of fears surrounding COVID-19. In an effort to keep you well informed, here are the most common COVID-19 related scams we have seen so far:

I. Stimulus Check

a. The Federal Government has created a COVID-19 relief package that will send checks to many Americans.
b. Most people who qualify for a check will automatically get it direct deposited by the IRS within weeks. But as details emerge about how and when payments will arrive, some scammers may start using official-looking fake checks to steal money and confuse people into turning over personal information. Here's some information to help avoid fake check scams that might be arriving soon.
    i. The government will not ask you to pay anything up front to get this money.
    ii. The government will not call to ask for your Social Security number, bank account, or credit card number. Anyone who does is a scammer.
    iii. Anyone who tells you they can get you money right away, or is telling you to sign up through anything other than an official government website, is a scammer.
    iv. The check's not in the mail – yet. Reports say that paper checks – for people without direct deposit – will start arriving in May at the earliest. So, if you get an economic impact payment, stimulus, or relief check before then, or you get a check when you're expecting a direct deposit, it's a scam
    v. The IRS will not send you an overpayment and make you send the "extra" money back in cash, gift cards, or through a money transfer.
    vi. The IRS is not calling, texting, or emailing. Scammers are sending official-looking messages – including postcards with a password to be used online to "access" or "verify" your payment or direct deposit information. The IRS will not contact you to collect your personal information or bank account.

II. Bogus and Counterfeit Medical Products/Medications

a. There currently are no vaccines, pills, lotions, teas, lozenges, or other prescription/over-the-counter products available to treat COVID-19. Do not make any purchases for any such products.
b. At this time, there are no authorized Test Kits available for testing yourself at home for COVID-19. Any website claiming otherwise is trying to scam you!
c. Masks and other products are in short supply, so scammers are selling counterfeit products online. Only buy medical supplies from legitimate sources to ensure your protection needs are met.
d. The FDA is aware of people trying to prevent COVID-19 by taking a product called "chloroquine phosphate". Do not take any form of chloroquine unless it has been prescribed for you by your health care provider and obtained from legitimate sources.
    i. Products for veterinary use or for "research use only" may have adverse effects, including serious illness and death, when taken by people.

III. Price Gouging

a. Under Penal Code section 396, it is illegal to charge a price for goods or services that is more than 10% higher than the price charged immediately before the emergency declaration.
    i. Please note, due to exceptions under the law, there may be circumstances that permit an increase in price. All facts will be investigated before our office makes a determination of whether price gouging has occurred.
b. Governor Gavin Newsom, through Executive Order N-44-20, further ordered that:
    i. the price gouging prohibitions in PC 396(b) are extended until at least September 4, 2020; and
    ii. the new price gouging prohibitions, in general terms, (1) prohibit the sale of certain goods for a price greater than the seller charged for those goods on February 4, 2020, and (2) for sellers who were not selling a product on February 4, 2020, prohibit sales for more than 50% more than the seller's cost of buying or producing the goods.
c. Violation of the statute is a misdemeanor with up to one year in county jail and/or a fine of up to $10,000. A violation may also be subject to a civil prosecution with penalties of up to $2,500 per violation, injunctive relief, and mandatory restitution.

IV. Charity Fraud

a. Fake charities, and individuals falsely claiming to be from legitimate charities, are requesting donations for COVID-19 support. If someone requests a donation in cash, gift card, or money-wire, do not do it. Contribute by way of check/credit card only.
b. When it comes to donations, whether through charities or crowdfunding sites, do not let anyone rush you into making a donation. Always research the charity and only donate to organizations that you have properly vetted.
    i. The IRS's Tax Exempt Organization Search tells you if your donation would be tax deductible. You can also find your state charity regulator at www.nasconet.org.

V. Scam E-mails/Text Messages/Social Media Posts

a. Scammers are sending messages posing as the CDC, WHO, or other "experts" and are claiming to have special information about the virus. Their claims include

insider information about COVID-19 statistics in your neighborhood, access to medical supplies, or secret ways to avoid getting sick.

i. These messages contain malware and could threaten your privacy and financial information. DO NOT open such messages, view any attachments, or click on any links.

VI. Look-A-Like Government Websites

a. There has been an increase in website addresses being registered with names that could lead a person to believe the website is an official government website. Such websites are trying to steal your personal information for identity theft purposes.

i. Take steps to ensure you are visiting an official website. Specifically, check if the website is a ".gov" website and look for "https://" before the web address. In general, "http://" websites are vulnerable to attack.

VII. Investment Schemes

a. Scammers are targeting individuals to invest in companies that can prevent, detect, or cure COVID-19. At this time, no company has such capabilities and claims that a company "will dramatically increase in value", should be treated as suspect.

VIII. I.T. Scams

a. Scammers are posing as technology staff asking for passwords or directing the recipient to download software. These scams pose a particular problem now, due to the fact that so many people are working from home.

b. Your employees already may be distracted by changes to their routine and your tech support team is overwhelmed. Taking advantage of this temporary "upside down-ness," con artists may do a quick online search to glean information about your company to really sell their story – for example, "I spoke with Fred, who said you were having a computer problem" or "The meeting has been shifted to our new teleconferencing platform. Here's the link."

c. Your best defense is a workforce warned against this form of fraud. An in-house source for accurate information can help protect your company as well.

IX. Data Scams

a. With more people telecommuting, hackers are hoping companies will drop their online defenses, making it easier to infiltrate data-rich networks

b. The FTC has excellent tips to help your staff maintain security when working from home. Also, the National Institute of Standards and Technology (NIST) has resources on making a safer transition to a remote workplace. A good place to start: NIST's updated Telework Cybersecurity page.

X. Small Business Wire Fraud

a. The economic upheaval caused by COVID-19 has led to a flurry of unusual financial transactions: expedited orders, cancelled deals, refunds, etc. Before an "emergency request" would have raised suspension, however, with many businesses not operating as usual, individuals may not have their typical guard up.

i. Compounding the problem is that teleworking employees can't walk down the hall to investigate a questionable directive.

b. Companies, especially small business should warn their staff about such scams and give them a central in-house contact where they can verify requests they may receive.

XI. SBA Relief Scams

a. If you own a small business, you've seen the headlines about financial relief that may be available to some companies through the Small Business Administration (SBA). To ensure you get accurate information for your small business, please go "straight to the source" and visit the SBA's dedicated website, sba.gov/coronavirus
    i. The SBA's Coronavirus Small Business Guidance & Loan Resources page offers the latest information about the Paycheck Protection Program, Economic Injury Disaster Loans and Loan Advances, SBA Debt Relief, and SBA Express Bridge Loans.
    ii. There are legitimate business groups and financial institutions sharing information. However, there also are fraudsters with bogus websites and phony email, so your safest bet is to go straight to the SBA by carefully typing the URL sba.gov/coronavirus into the address bar at the top of your browser.
b. Here are some more tips to help you avoid scams targeting small businesses:
    i. Watch out for application scams.
        1. Some small businesses report they've received unsolicited calls or email from people claiming to have an inside track to expedite financial relief.
        2. Applying for a loan was a step-by-step process before the COVID-19 crisis and it's a step-by-step process now. That's why the SBA's sba.gov/coronavirus site is the safest place for you to start.
    ii. Be suspicious of unsolicited phone calls.
        1. Some scammers may try the personal approach by calling you and impersonating someone from a financial institution or government agency. Don't engage in conversation. If you think you may need to respond, call using a number you know is legit.
    iii. Scammers often mimic the look and feel of legitimate email.
        1. You've heard warnings for years about email phishing attempts. Fraudsters have upped their game in response. They've been known to copy logos of financial institutions and government agencies, including the SBA, and use wording that sounds familiar. They also manipulate email addresses so that a message looks to be from a legitimate source – but isn't. That's why it's dangerous to respond to those emails. Instead go directly to the SBA site.

XII. Quarantine assistance scam

a. If you're an older adult or a caregiver for one, you may need help picking up groceries, prescriptions, and other necessary supplies. If someone you don't know offers to help, be wary.
b. Some scammers offer to buy supplies but never come back with the goods or your money. It's usually safer to find a trusted friend or neighbor or arrange a delivery with a well-known company.
c. Use an established delivery service, or order directly from the store. Many grocery stores and pharmacies are offering contactless delivery.

i. If you need additional help for yourself or a loved one, the Eldercare Locator, a public service of the U.S. Administration on Aging, can connect you to services for older adults and their families. You can also call 1-800-677-1116.

BEST PRACTICES AND TIPS

- Have your guard up!
  - Times like these brings out opportunistic scammers.
- Share information
  - People who know about scams are much less likely to fall for them. So by discussing them you are helping protect people you care for and people in your community.
- Do not open emails or any attachments claiming to provide COVID-19 relief.
- Do not be tempted to buy or use questionable products that claim to help diagnose, treat, cure, and even prevent COVID-19.
  - If you have symptoms of COVID-19, follow the Centers for Disease Control and Prevention's guidelines, and speak to your medical provider. Your health care provider will advise you about whether you should get tested and the process for being tested in your area.
- Do not trust Caller ID
  - Scam calls may show up on caller ID as a government agency and look like the agency's real number
- If you are not sure if something is legitimate, call our office and we can help.
  - **Consumer Protection Unit Fraud Hotline: 530-225-5391**