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

"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 10 most common COVID-19 related scams we have seen so far:

I. Stimulus Check

a. The Federal Government is working on a COVID-19 relief package that would send checks to many Americans. However, at this time the bill is not yet finalized.
b. While the details are still being worked out, there are a few important things to know no matter what the relief bill ends up looking like.
    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 now, is a scammer.

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. 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.

BEST PRACTICES AND TIPS

- Have your guard up!
    - Times like these brings out opportunistic scammers.
- 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.
- If you are not sure if something is legitimate, call our office and we can help.
    - **Consumer Protection Unit Fraud Hotline: 530-225-5391**