Consumer Alert: Avoiding COVID-19 Scams

During this time of social distancing, people spend more time on their phones and computers for work, shopping and entertainment. Cyber criminals take advantage of widespread fear, panic and worry. They may use your extra screen time and time at home as an opportunity.

Protect yourself by being aware of different types of scams

According to the U.S. Department of Justice, the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC), there are several ways scammers will use COVID-19 to target people.

Vaccine and treatment scams. Scammers may advertise fake cures, vaccines and advice on unproven treatments for COVID-19.

Shopping Scams. Scammers may create fake stores, e-commerce websites, social media accounts, and email addresses claiming to sell medical supplies currently in high demand. Supplies might include things like hand sanitizer, toilet paper and surgical masks. Scammers will keep your money but never provide you with the merchandise.

Medical scams. Scammers may call and email people pretending to be doctors and hospitals that have treated a friend or relative for COVID-19 and demand payment for treatment.

Charity scams. Scammers sometimes ask for donations for people and groups affected by COVID-19.

Phishing and Malware scams. During the COVID-19 crisis, phishing and malware scams may be used to gain access to your computer or to steal your credentials.

Malware is malicious software such as spyware, ransomware, or viruses that can gain access to your computer system without you knowing. Malware can be activated when you *click* on email attachments or install risky software.

When Phishing is used, bad actors send false communications from what appears to be a trustworthy source to try to convince you to share sensitive data such as passwords or credit card information.

For example, scammers may pose as national and global health authorities, including the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC) and send phishing emails designed to trick you into downloading malware or providing your personal and financial information.

App scams. Scammers may create mobile apps designed to track the spread of COVID-19 and insert malware into that app, which will compromise users' devices and personal information.

Investment scams. Scammers may offer online promotions on things like social media, claiming that products or services of publicly traded companies can prevent, detect, or cure COVID-19, causing the stock of these companies to dramatically increase in value as a result.

Louisiana Department of Insurance
Jim Donelon, Commissioner

1-800-259-5300
www.ldi.la.gov