U.S. Department of Justice

Timothy J. Shea
United States Attorney for the District of Columbia
Judiciary Center
555 Fourth Street, N.W.
Washington, D.C. 20530

PRESS RELEASE

FOR IMMEDIATE RELEASE
Monday, March 30, 2020

For Information Contact:
Public Affairs
(202) 252-6933
http://www.justice.gov/usao/dc/index.html

United States Attorney for the District of Columbia Timothy J. Shea's Statement Providing Examples of COVID-19 Scams to Avoid

The United States Attorney's Office for the District of Columbia is committed to investigating, prosecuting, and deterring those who would take advantage of the COVID-19 pandemic to prey on vulnerable citizens. Again, we urge you to **be vigilant and report** any suspected instances of fraud to the **COVID-19 Pandemic Fraud Hotline, 202-252-7022 and USADC.COVID19@usdoj.gov.**

Some examples of the scams or other fraudulent activity related to COVID-19 to be on the lookout for include the following:

- **Treatment Scams:** Scammers are offering to sell fake cures, vaccines, and advice on unproven treatments for COVID-19. All of these claims are a lie, as there is no cure or vaccine yet for COVID-19. Similarly, we have also learned that scammers are impersonating governmental organizations, such as the Centers for Disease Control and Prevention (CDC), and urging people to reserve a vaccine for COVID-19 with their credit card, and to also provide personal information such as their Social Security Number.

- **Testing Scams:** Scammers are impersonating organizations, such as The Red Cross, and saying that they are offering COVID-19 home tests door-to-door. The scammers then fraudulently charge their victims for tests that are never administered.

- **Supply Scams:** Scammers are creating fake shops, websites, social media accounts, and email addresses claiming to sell medical supplies currently in high demand, such as surgical masks. When consumers attempt to purchase supplies through these channels, fraudsters pocket the money and never provide the promised supplies.

- **Provider Scams:** Scammers are also contacting people by phone and email, pretending to be doctors and hospitals that have treated a friend or relative for COVID-19, and demanding payment for that treatment.

- **Charity Scams:** Scammers are soliciting donations for individuals, groups, and areas affected by COVID-19.

- **Phishing Scams and Cyber Intrusions:** Scammers posing as national and global health authorities, including the World Health Organization (WHO) and the CDC, are sending phishing emails designed to trick recipients into clicking on a link or opening an attachment that downloads malware, or providing personal identifying financial information. One form of malware being spread contains an interactive online map of Coronavirus-infected areas purportedly produced by Johns Hopkins University. Once someone downloads this interactive map, the malware steals the user's credentials, such as usernames, credit card numbers, passwords, and other sensitive information usually stored in internet browsers.

- **App Scams:** Scammers are also creating and manipulating mobile apps designed to track the spread of COVID-19 to insert malware that will compromise users' devices and personal information.

- **Investment Scams:** Scammers are offering online promotions on various platforms, including social media, claiming that the products or services of publicly traded companies can prevent, detect, or cure COVID-19, and that the stock of these companies will dramatically increase in value as a result. These promotions are often styled as "research reports,' make predictions of specific "target price," and relate to microcap stocks, or low-priced stocks issued by the smallest of companies with limited publicly available information.

- **Doctor's Prescription Abuse**: Other reported activity concerns doctors writing prescriptions for various medications that are believed to cure COVID-19. As of now, there is no known cure or therapeutic treatment for COVID-19, and taking any medication believed to cure or relieve the symptoms of COVID-19 can be deadly. We are already hearing reports of individuals that have died after taking medications believed to cure COVID-19. Moreover, taking unapproved medication can also deprive others who need those medicines for legitimate purposes.

- **$1,000 Check Scams:** Scammers are contacting people over email and are telling them that their $1,000 check, as part of the stimulus package responding to COVID-19, is already waiting for them and that all they need to do is to provide personal information, such as bank account numbers and Social Security Numbers, which are the key pieces of information needed to perpetrate identity theft.

If you encounter any activity that indicates one of these scams, please **report** it to the **COVID-19 Pandemic Fraud Hotline, 202-252-7022 and USADC.COVID19@usdoj.gov.**

# #

20-053

U.S. Department of Justice

Timothy J. Shea
United States Attorney for the District of Columbia
Judiciary Center
555 Fourth Street, N.W.
Washington, D.C. 20530

PRESS RELEASE

FOR IMMEDIATE RELEASE
Tuesday, March 31, 2020

For Information Contact:
Public Affairs
(202) 252-6933
http://www.justice.gov/usao/dc/index.html

United States Attorney for the District of Columbia Timothy J. Shea's Statement Providing Tips for Protection against COVID-19 Scams

The United States Attorney's Office for the District of Columbia is committed not only to deterring and to prosecuting scammers and fraudsters who would seek to benefit from the fears raised by the COVID-19 pandemic, but to assisting individuals in the District in protecting themselves from such scams. Again, we urge you to **be vigilant and report** any suspected instances of fraud to the **COVID-19 Pandemic Fraud Hotline, 202-252-7022 and USADC.COVID19@usdoj.gov.**

To protect yourself from these types of scams, the United States Attorney's Office urges everyone to take the following steps:

- Independently verify the identity of any company, charity, or individual that contacts you regarding COVID-19.

- Check the websites and email addresses offering information, products, or services related to COVID-19. Be aware that scammers often employ addresses that differ only slightly from those belonging to the entities they are impersonating. For example, they might use "cdc.com" or "cdc.org" instead of "cdc.gov."

- Be wary of unsolicited emails offering information, supplies, or treatment for COVID-19 or requesting your personal information for medical purposes. Legitimate health authorities will not contact the general public this way.

- Do not click on links or open email attachments from unknown or unverified sources. Doing so could download a virus onto your computer or device. Also, do not forward these emails to anyone.

- Make sure the anti-malware and anti-virus software on your computer is operating and up to date.

- Ignore offers for a COVID-19 vaccine, cure, or treatment. Remember, if there is a medical breakthrough, you won't hear about it for the first time through an email, online ad, or unsolicited sales pitch.

- Check online reviews of any company offering COVID-19 products or supplies. Avoid companies whose customers have complained about not receiving items.

- Research any charities or crowdfunding sites soliciting donations in connection with COVID-19 before giving. Remember, an organization may not be legitimate even if it uses words like "CDC" or "government" in its name or has reputable looking seals or logos on its materials. For online resources on donating wisely, visit the Federal Trade Commission (FTC) website.

- Be wary of any business, charity, or individual requesting payments or donations in cash, by wire transfer, gift card, or through the mail. Don't send money through any of these channels.

- Be cautious of "investment opportunities" tied to COVID-19, especially those based on claims that a small company's products or services can help stop the virus. If you decide to invest, carefully research the investment beforehand. For information on how to avoid investment fraud, visit the U.S. Securities and Exchange Commission (SEC) website.

- For the most up-to-date information on COVID-19, visit the Centers for Disease Control and Prevention (CDC) and World Health Organization (WHO) websites.

Take these measures to help protect yourself, but if you encounter any activity that indicates one of these scams, please report it to the COVID-19 Pandemic Fraud Hotline, 202-252-7022 and USADC.COVID19@usdoj.gov.

# #

20-054