COVID-19 SCAMS

FRAUDULENT WEBSITES, EMAILS AND DONATION REQUESTS

Residents are reminded of several fraud schemes designed to prey on the vulnerable in the midst of the COVID-19 public health crisis. Reports of malicious websites, email schemes, and suspicious links have come to the attention of law enforcement and public officials.

"Malicious actors can prey upon those that are distracted by the COVID-19 pandemic, and use it to their advantage," stated Los Angeles County Chief Information Officer William Kehoe. "The public needs to be mindful and careful, and avoid websites, phishing emails, and scams that engage people through false information about the health crisis, and steal personal user information and data. By clicking on fraudulent weblinks, hackers can deliver malware and then gain access to passwords, browsing information, credit card numbers, and other personal information. We all need to stay vigilant."

Currently, there are several Coronavirus tracking and mapping sites that are actually malware websites. Instead of clicking on these links, cybersecurity experts advise that website users should instead hover over the link to verify the uniform resource locator (URL) before moving forward. Online hackers may also send users emails from fraudulent accounts impersonating official websites and doctors, or offering medical supplies and services.

A trusted COVID-19 mapping resource is the Johns Hopkins Coronavirus Global Map, which can be found at coronavirus.jhu.edu. Additionally, there are several websites the County of Los Angeles recommends for accurate, up-to-date information on COVID-19.

The following is a list of trusted sites:

- **County of Los Angeles:** covid19.lacounty.gov

- **County of Los Angeles Public Health:** publichealth.lacounty.gov

- **California Department of Public Health:** cdph.ca.gov

- **Centers for Disease Control and Prevention:** cdc.gov

The following is a list of safety tips the public can follow:

- Avoid online advertising offers related to COVID-19

- Decline door-to-door solicitations claiming COVID-19 fundraising

- Do not click on emails and attachments that you do not recognize

- Visit trusted websites for COVID-19 related information

Everyone should remain vigilant and take these steps to avoid being victimized by malicious scammers trying to profit from the COVID-19 crisis. If you believe you have been scammed, contact your bank immediately and report the information to local law enforcement.