



Coronavirus or COVID-19 Scams

Coronavirus or COVID-19 is affecting millions of people worldwide. Identity thieves are taking full advantage individuals fears of the Coronavirus outbreak. Fraudsters are exploiting the opportunity to steal the Personally Identifiable Information (PII), financial and medical information, of those looking for knowledge, protection and treatment for the viral infection.

Spoofed Government and Health Organization Communications

Scammers disguising themselves as government and health organizations such as the World Health Organization (WHO) or Federal Trade Commission (FTC) are contacting individuals by email, asking them to visit a "protected" site requiring personal information to set up a user account to view safety tips or make (fake) donations.

Medicare -Scammers are offering COVID-19 tests or checks to Medicare beneficiaries in exchange for personal details, including Medicare information. Fraudsters are targeting beneficiaries by telemarketing calls, social media platforms, and door-to-door visits. The personal information collected can be used to fraudulently bill Federal health care programs and commit medical identity theft. If Medicare/Medicaid denies the claim for an unapproved test, the beneficiary could be responsible for the cost.

U.S. Department of Health and Human Services (HHS) - Cybercriminals hacked into HHS and posed as the nation's system and sent out text messages warning individuals of a national quarantine and lockdown. The National Security Council confirmed the rumors were false.

U.S. Centers for Disease Control (CDC) - Cybercriminals have sent phishing emails designed to look like they are from the CDC. The email falsely claims to link to a list of coronavirus cases in your area. Here's an example of a fake CDC email. (*The example is from the U.S. Health and Human Services website.*)

**Distributed via the CDC Health Alert Network
January 31, 2020
CDCHAN-00426*

Dear [REDACTED]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (<https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html>)

You are immediately advised to go through the cases above for safety hazard

*Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention**

Miracle Cures or Vaccines

The Federal Trade Commission (FTC) and U.S. Food and Drug Administration (FDA) warns that there are "no vaccines, pills, potions, lotions, lozenges, or other prescription or over-the-counter products available to treat or cure Coronavirus." False miracle health claims are used to collect your personal financial and medical details that can be used to commit medical identity theft.

Cure - One post falsely claims that "it's actually widely acknowledged in both science and the medical industry that ionic silver kills coronaviruses," while another suggests a sufficient dose of basil or bergamot may provide effective treatment of the disease. This site also sells the silver, basil and bergamot.

Fake Tests – Another site claimed to sell "vaccine kits" from the WHO and used a photograph of Anthony Fauci, head of the National Institute of Allergy and Infectious Diseases at the National Institutes of Health, to give the illusion of an official governmental aligning with this site.

Phishing

Cyberthieves are creating websites that collect your personal information under the pretense of sharing important Coronavirus updates, taking donations for victim care or emergency response plans, which seem legit, but your money is sent to criminals. Other fraudulent websites create e-commerce vendors promoting the sale of protective face masks, sanitizers, test kits, and other high demand items, often collecting payment and credit card information never shipping the item.

As employees frequently check for updates on work conditions, conference and event status, they may be tricked into clicking links that capture sensitive business and customer information.

Fake Job Postings

Fake job postings designed to recruit individuals who are unemployed or forced to take time off from work during the COVID-19 outbreak. After applying for the job, the fake "non-profit" organization will ask the job seeker to process donations made to the charity into their own account and then to transfer the money into another account all before the bank can alert the individual of the fraudulent check and deposit. Fake job postings collect PII such as name, address, Social Security number and personal financial account information.

Protect Yourself

- Beneficiaries use caution of unsolicited requests for their Medicare/Medicaid numbers
- Be suspicious of any unexpected calls or visitors offering COVID-19 tests or supplies
- Ignore offers or advertisements for COVID-19 testing or treatments on social media sites
- A physician or other trusted healthcare provider should assess your condition and approve any requests for COVID-19 testing

National Center for Disaster Fraud Hotline (866) 720-5721 or disaster@leo.gov

Centers for Disease Control and Prevention (CDC) – <https://www.cdc.gov/>

World Health Organization (WHO) – <https://www.who.int/>

USA.gov – <https://www.usa.gov/coronavirus/>

U.S. Food and Drug Administration (FDA) – <https://www.fda.gov/home>

Federal Trade Commission (FTC) – <https://www.consumer.ftc.gov>

U.S. Securities and Exchange Commission (SEC) – <https://www.sec.gov/investor/alerts>