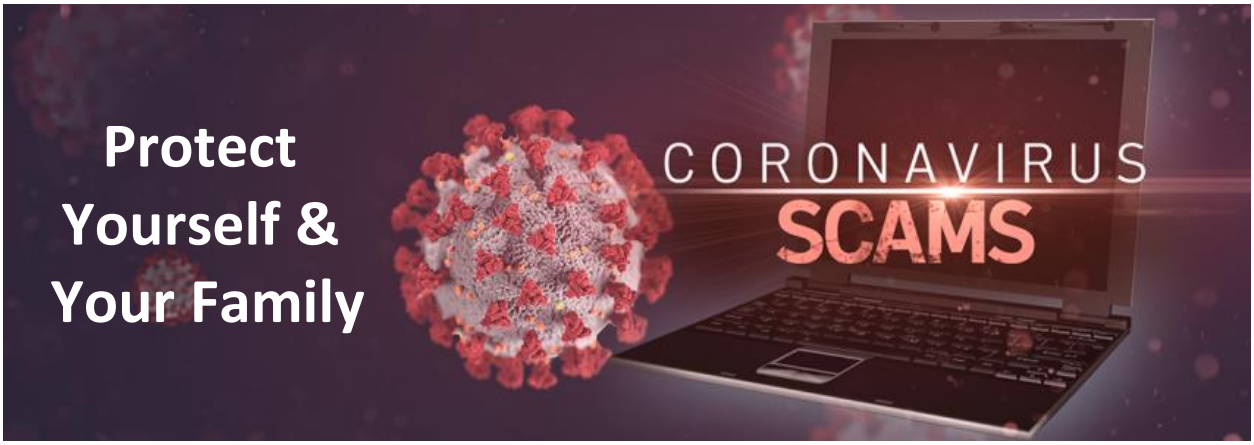

COVID-19 Fraud and Scams

Learn about the different Fraud and Scams being used to take advantage of citizens during this pandemic.

Misinformation & Rumors:

Scammers, and sometimes well-meaning people, share information that hasn't been verified. Misinformation can lead to people overreacting, making misguided purchases, or increasing general fear and panic.

What to do: Before you pass on any messages, make purchases based off of rumored information, and certainly before you pay someone or share your personal information, do some fact checking by contacting trusted sources.

Undelivered Goods & Counterfeit Supplies:

Online sellers may claim they have in-demand products, like cleaning, household, and health/medical supplies. This includes coronavirus testing kits, as well as hand sanitizers, disinfecting wipes and other supplies. Personal Protective Equipment (PPE) is also being counterfeited such as the N95 respirator masks, goggles, full face shields, protective gowns and gloves. You may place an order, but you never get your shipment, or what you received was not what you ordered. Remember anyone can set up shop online under almost any name.

What to do: Check out the seller by searching online for the person or company's name, phone number and email address, plus look up a company "review," "complaint" or "scam." If everything checks out, pay by credit card and keep a record of your transaction. Avoid suspicious sellers by only purchasing Personal Protective Equipment from well-known reputable sources.

Fake Cures & Treatments:

There are individuals and businesses online, even sometimes going door-to-door, selling fake cures or investments in cures for COVID-19. The scammer will ask for a Medicare or Medicaid number with the promise of providing a coronavirus testing kit, or ask you to pay your way into a get-rich-quick scheme.

What to do: These "cures" can be extremely dangerous to your health—even fatal. You should never accept a medical treatment or virus testing supplies from anyone other than your doctor, pharmacist, or local health department. Remember, if a vaccine or successful treatment becomes available, you won't hear about it the first time through an email, online ad, a spam call or unsolicited sales pitch. Ignore offers from anyone selling products that claim to prevent, treat, diagnose or cure COVID-19. Ignore offers or advertisements for COVID-19 testing or treatments on social media sites. Be cautious with your Medicare, Medicaid, or health plan member identification number.

Phone Fraud:

Criminals are calling victims pretending to be clinic or hospital officials. They will make up stories about one of your relatives falling sick with COVID-19. The scammers then request payment for their medical treatment, or may ask for additional personal information. Sometimes they will call pretending to be government officials, trying to convince someone that they need to provide money for COVID-19 testing, financial relief, or medical equipment. Scammers are also using robo-calls. These robo-calls use fear and lies about the coronavirus to make you buy fake health insurance. They may also ask for your personal information in order to get a free coronavirus test kit. This is all fraud to get your private information for use in other schemes.

What to do: If someone reaches out to you directly and says they're from the government/hospital helping you with virus-related issues, it's likely a scam. The

government will not ask you for personal information to give you your financial benefits. If you receive an email, text message, or phone call claiming to help you get your benefits, do not respond. Hang up. Don't press any numbers. The recording might say that pressing a number will let you speak to a live operator or remove you from their call list, but it might lead to more robo-calls instead. If you are eligible to receive the benefits, your government check will be mailed to you or will be direct deposited into your bank account.

Email Phishing:

Scammers use fake emails or texts, claiming to be from the Centers for Disease Control and Prevention (CDC) or other government agencies, to get you to share valuable personal information — like account numbers, Social Security numbers, or your login IDs and passwords. They use your information to steal your money, your identity, or both. Some fake emails offer information, products, or services related to COVID-19. The scammers want you to tap links to malicious websites that will access to your computer or network. If you click on a link, they can install ransomware or other programs that can lock your device. Then they might ask for payment to unlock your device.

What to do: Protect your computer by keeping your software up to date and by using security software. Protect your cell phone by setting software to update automatically. Secure your accounts by using multi-factor authentication, and your data by backing it up. Look carefully at the website addresses and email addresses in these emails. Scammers often use addresses that are only a little bit different from the real thing. For example, they might use "cdc.com" or "cdc.org" instead of "cdc.gov." Do not open emails asking you to verify your personal information in order to receive an economic stimulus check from the government. This is another scam.

Fake Charities:

As we try to help each other, criminals are trying to use our goodwill by asking for donations for fake charities. Some scammers use names that sound a lot like the names of real charities. The scammers may even copy logos from other real companies, or create fake ones that look very professional. Money lost to bogus charities means less donations to help those in need.

What to do: Before donating, do your own research the identity of any company, charity, or individual that contacts you regarding COVID-19. An organization may not be legit even if it uses words like "CDC" or "government" in its name. Be careful with 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. If you donate, use your credit card and keep records of all donations. For online resources on donating wisely, visit the Federal Trade Commission (FTC) website.

Report Them

Criminals will continue to use new methods to exploit COVID-19 worldwide.
If you think you are a victim of a scam or attempted fraud involving COVID-19, you can report it without leaving your home.

The U.S. Department of Justice has a National Center for Disaster Fraud Hotline.
Call 1-866-720-5721 to report any fraud related to COVID-19 and the coronavirus.

For scams related to the Internet (e.g., email, websites, social media), you can also file a complaint online at the FBI Internet Complaint Center.