Protect Yourself from COVID-19 Scams

Scammers are using the COVID-19 pandemic crisis to take your money or steal your identity. Here is what you need to know to avoid getting scammed.

**Stimulus Check Scams:** Do not respond to texts, emails, calls, or visits about government checks. Do not give out your bank account or Social Security numbers to anyone reaching out to you and requesting this information. The IRS will not call you and request this information. You do not need to do anything to get your stimulus check!

**Claiming to be from FDIC Scams:** Scammers will claim to be from the FDIC and will try to persuade you to pay them in order to receive a benefit authorized by the recently enacted Coronavirus Aid, Relief, and Economic Security Act (CARES Act). They might use a fraudulent FDIC logo, fake FDIC email addresses, names of individuals purportedly from the FDIC, and bogus images of FDIC identification credentials, with FDIC officials depicted. If you receive such correspondence, refer it to the FDIC OIG Hotline: https://www.fdicoig.gov/oig-hotline.

**Online Shopping Scams:** Anyone can set up shop online under almost any name — including fraudsters! Beware of unfamiliar sites claiming that they have those hard-to-find items: toilet paper, cleaning supplies, health and medical supplies. Before you click to make a purchase, research the seller online: look for reviews or complaints before making purchases.

**Coronavirus Treatment Scams:** Ignore online offers for vaccinations, home test kits and other products like teas, essential oils, and colloidal silver, claiming to treat or prevent Coronavirus. According to the FDA, currently, there are no products to treat or prevent COVID-19.

**Email Scams:** Delete emails claiming to be from the CDC or the WHO. Do not click on links or attachments from sources you don't know. Beware of “investment opportunities” claiming they are related to prevention, cure and treatment of Coronavirus. For the most updated information, go to coronavirus.gov and usa.gov/coronavirus and mass.gov.

**Charity Scams:** Scammers are online and making robocalls; they are taking advantage of these difficult times and trying to take your money. Before you open your wallet, do your research. Look for reviews and complaints. Make sure you can find the nonprofit's EIN on their website or donation page. Most nonprofits have a .org website rather than a .com. Never pay by gift card or wire transfer.

**Coronavirus Test Scams:** There are no home test kits for Coronavirus and the CDC does not go door-to-door conducting tests. Scammers target Medicare beneficiaries and offer free COVID-19 tests kits in exchange for healthcare information. They then use this information to fraudulently bill healthcare programs. This information can also be used to commit medical identity theft. Do not provide personal and/or medical information to anyone reaching out to you claiming to be from Medicare. Beware of phony house visits from alleged employees of the CDC. The impersonators are dressed in medical gear and present fake credentials. They claim that they will test members of the household and scan the house for signs of Coronavirus.

**Grandparent/Family Emergency Scams:** You answer the phone and hear the following: "Grandma/Grandpa/Auntie, I'm in the hospital and I'm sick! Please send money!" or “I’m stuck overseas and can’t get home.” Resist the urge to act immediately. Hang up and call a family member, a friend or your police department to help you verify the story even if you are told to keep the call a secret.

**ADDITIONAL RESOURCES**

MASS.gov  
Consumer.FTC.gov  
CDC.gov  
FDIC.gov  

Visit www.dedhamsavings.com/coronavirus to learn more.