Avoiding COVID-19 Scams

Unfortunately, some people—including criminals—often look for opportunities to take advantage of others during times of national crisis. The coronavirus (COVID-19) pandemic created a perfect environment for lawbreakers who may be targeting vulnerable victims. Very often, their targets may be older adults.

Here are some effective defenses to help stop criminals in their tracks. Arm yourself with these smart strategies to protect yourself and your family against scammers.

First Step

Make sure to fact-check all the COVID-19 information you receive. Don’t share any messages about the virus on social media or email—or even in conversation with friends and family—unless you verify the information is from a trusted source.

Look to government agencies such as:

Also ask:

- Centers for Disease Control and Prevention https://www.cdc.gov/
- Food and Drug Administration https://www.fda.gov/
- Federal Trade Commission https://www.ftc.gov/
- If you’re unsure about a news item or piece of information, use a fact-checking website such as Snopes https://www.snopes.com/

Telephone Fraud

You get a call that seems to be coming from the CDC. It’s a plea for a donation to them during COVID-19. But in reality, this is “government impersonation fraud,” say CDC officials. “Federal agencies do not request donations from the general public.”

Other phone frauds include fake coronavirus treatments, vaccinations, work-at-home schemes, or opportunities to provide personal protective gear and cleaning products. Some scammers may also call claiming to be friends or relatives who need immediate financial assistance related to COVID-19.

Protect Yourself:

- Do not take calls from phone numbers you don’t recognize.
- Never give out your personal information, banking information, Social Security number, or any other information over the phone or to strangers.
- Hang up on robocalls. Don’t press any numbers. The recording might say that pressing a number will remove you from their call list or send you to a live operator, but it could lead to even more robocalls.
Email Scams

CDC officials are warning consumers about a widespread campaign of “phishing” emails that claim to be from the CDC and mention a flu pandemic. The email instructs you to open a document that supposedly tells you how to prevent the spread of the disease https://www.cdc.gov/media/releases/2019/s0322-phishing.html.

If you get an email like this, know that it comes from hackers trying to gain access to your personal computer files, as well as files on networks you’re connected to. After you open the attachment, you may get a note demanding some type of payment to remove the virus from your computer.

You should also pay careful attention to web links you click or find from search results. Never trust websites claiming to be from the government if they don’t end in .gov. Websites using .org or .edu are also among the safest to use, since those types of links are used by non-profits or educational institutions like universities. Be the most wary of .com websites, since these can be set up by almost anyone.

Beware of Fake COVID-19 Tests, Vaccines, and Treatments

The FDA is actively and aggressively monitoring for any companies that may be selling products for fraudulent coronavirus (COVID-19) testing, prevention, and treatment. As a result of these activities, the agency is beginning to see fake products being marketed to test for or treat COVID-19 in the home. See https://www.fda.gov/consumers/consumer-updates/beware-fraudulent-coronavirus-tests-vaccines-and-treatments for more information.

Protect Yourself:

- Never open unsolicited emails or attachments from people you don’t know.
- DO NOT CLICK ON ANY LINKS OR ATTACHMENTS in the email or visit websites that seem unfamiliar or have strange web addresses.
- Never share personal information, especially passwords or account numbers, with anyone via email.