Abstract: The novel coronavirus (COVID-19) crisis this year has created ample opportunities for dishonest individuals and criminal organizations. This article suggests various protective actions to take to avoid becoming a victim.

Protecting yourself from opportunistic fraud

The novel coronavirus (COVID-19) crisis has spurred much confusion and unprecedented economic challenges. It has also created ample opportunities for dishonest individuals and criminal organizations to prey on the anxieties of many Americans.

As the year rolls along, fraud schemes related to the crisis will continue as well, potentially becoming even more sophisticated. Here are some protective actions you can take.

Watch out for phony charities

When a catastrophe like COVID-19 strikes, the charitably minded want to donate cash and other assets to help relieve the suffering. Before donating anything, beware that opportunistic scammers may set up fake charitable organizations to exploit your generosity.

Fake charities often use names that are similar to legitimate organizations. So, before contributing, do your homework and verify the validity of any recipient. Remember, if you're scammed, not only will you lose your money or assets, but those who would benefit from your charitable action will also lose out.

Don't get hooked by phishers

In a "phishing" scheme, victims are enticed to respond to a deceptive email or other online communication. In COVID-19-related phishing scams, the perpetrator may impersonate a representative from a health agency, such as the World Health Organization (WHO) or the Centers for Disease Control and Prevention (CDC). They may ask for personal information, such as your Social Security or bank account number, or instruct you to click on a link to a survey or website.

If you receive a suspicious email, don't respond or click on any links. The scammer might use ill-gotten data to gain access to your financial accounts or open new accounts in your name. In some cases, clicking a link might download malware to your computer. For updates on the COVID-19 crisis, go directly to the official websites of the WHO or CDC.

The IRS reports that its Criminal Investigation Division has seen a wave of new and evolving phishing schemes against taxpayers — and among the primary targets are retirees.

Shop carefully

In many parts of the United States, and indeed around the world, certain consumer goods have become scarce. Examples have included hand sanitizer, antibacterial wipes, masks and toilet paper. Scammers are exploiting these shortages by posing as retailers or direct-to-consumer suppliers to obtain buyers' personal information.

Con artists may, for instance, claim to have the goods that you need and ask for your credit card number to complete a transaction. Then they use the card number to run up charges while you never receive anything in return.

Buy from only known legitimate businesses. If a supplier offers a deal out of the blue that seems too good to be true, it probably is. Also watch out for price gouging on limited items. If an item is selling online for many times more than the usual price, you probably want to avoid buying it.

Hang up on robocalls

You may have noticed an increase in "robocalls" — automated phone calls offering phony services or demanding sensitive information — since the COVID-19 crisis began. For instance, callers may offer COVID-19-related items at reduced rates. Then they'll ask for your credit card number to "secure" your purchase.

Reputable companies, charities and government agencies (such as the IRS) won't try to contact you this way. If you receive an unsolicited call from a phone number that's blocked or that you don't recognize, hang up or ignore it.

In addition, don't buy into special offers for items such as COVID-19 treatments, vaccinations or home test kits. You'll likely end up paying for something that at best doesn't exist and at worst could harm you.

Tarnish their gold

For fraudsters, this year's worldwide crisis is a golden opportunity. Don't let them take advantage of you or your loved ones.