COVID-19 contact tracing text message scams

May 19, 2020
by
Colleen Tressler
Consumer Education Specialist, FTC

You've probably been hearing a lot about contact tracing. It's the process of identifying people who have come in contact with someone who has tested positive for COVID-19, instructing them to quarantine and monitoring their symptoms daily.

Contact tracers are usually hired by a state's department of public health. They work with an infected person to get the names and phone numbers for everyone that infected person came in close contact with while the possibly infectious. Those names and phone numbers are often kept in an online system. People who had contact with someone infected with COVID-19 may first get a text message from the health department, telling them they'll get a call from a specific number. The tracer who calls will not ask for personal information, like a Social Security number. At the end of the call, some states ask if the contact would like to enroll in a text message program, which sends daily health and safety reminders until the 14-day quarantine ends. But tracers won't ask you for money or information like your Social Security, bank account, or credit card number. Anyone who does is a scammer.

There's no question, contact tracing plays a vital role in helping to stop the spread of COVID-19. But scammers, pretending to be contact tracers and taking advantage of how the process works, are also sending text messages. But theirs are spam text messages that ask you to click a link. Check out the image below. Unlike a legitimate text message from a health department, which only wants to let you know they'll be calling, this message includes a link to click.

Don't take the bait. Clicking on the link will download software onto your device, giving scammers access to your personal and financial information. Ignore and delete these scam messages.

There are several ways you can filter unwanted text messages or stop them before they reach you.

- Your phone may have an option to filter and block messages from unknown senders or spam.
- Your wireless provider may have a tool or service that lets you block texts messages.
- Some call-blocking apps also let you block unwanted text messages.

Here are several other steps you can take to protect yourself from text scammers.

- Protect your online accounts by using multi-factor authentication. It requires two or more credentials to log in to your account, which makes it harder for scammers to log in to your accounts if they do get your username and password.
- Enable auto updates for the operating systems on your electronic devices. Make sure your apps also auto-update so you get the latest security patches that can protect from malware.
- Back up the data on your devices regularly, so you won't lose valuable information if a device gets malware or ransomware.

For more information, see How to Recognize and Report Spam Text Messages.