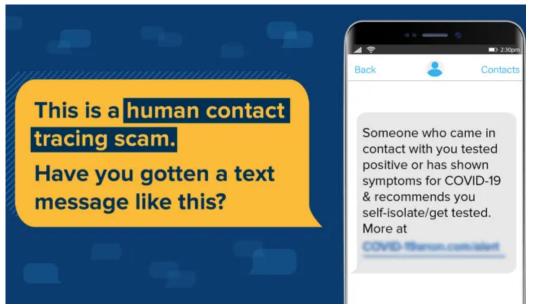
dailyvoice.com /new-jersey/wyckoff/news/covid-19-scam-alert-contact-tracer-or-con-artist-heres-how-to-tell/788433/

## COVID-19 SCAM ALERT: Contact Tracer Or Con Artist? Here's How To Tell

4-4 minutes

05/23/2020 5:53 p.m.



Example of a bogus contact tracing text. Photo Credit: Federal Trade Commission

In case you haven't already heard, identity thieves have been texting people pretending to be coronavirus contact tracers in order to steal their money.

Contact tracers are hired by public health departments to get hold of people who've had close contact with those who've tested positive for COVID-19.

The goal is to warn those people to self-quarantine, and monitor their systems daily, in case they may have been infected themselves.

Contract tracing has helped curb the spread of COVID-19. But, as with any public emergency, it's also become a popular tool for scammers looking to take your money, the Federal Trade Commission says .

How can you tell the difference between the true contact tracers and the cons?

Simple:

- You won't get a cold call out of the blue. To guard against fraud, health departments text people first with the specific number that they'll get a call from.
- The text won't ever include a link of any kind the sole purpose is to give you the proper phone number;
- When you do get that call, the contract tracer won't ask for a Social Security number or any other
  personal information (credit or debit card number, for instance) that could be used to steal your
  identity.

Anyone who texts you a link or calls and at some point asks for personal identifying information is a crook, the Federal Trade Commission warned.

"Don't take the bait," the FTC warning urges . "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 guard against text scammers:

- 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.
- 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.

Click here to sign up for Daily Voice's free daily emails and news alerts.