



COVID-19

Scam Alert: Things a COVID Contact Tracer Wouldn't Say

By Julie Appleby • AUGUST 20, 2020



(KHN illustration; Getty Images)

State officials and federal agencies warn there's a new phone scam circulating: Some callers posing as COVID-19 contact tracers try to pry credit card or bank account information from unsuspecting victims.

The grifters apparently are taking advantage of a genuine public health intervention that's crucial to stopping the spread of the novel coronavirus: contact tracing.

In one such scheme, detailed in [a warning from the Montana attorney general](#), scammers tell their victims, “I’m calling from your local health department to let you know that you have been in contact with someone who has COVID-19.” Then they move in for the kill, asking for payment information “before we continue.”

Don’t fall for that, say public health advocates and officials. Legitimate contact tracers don’t ask for payment or seek other financial information.

“That is absolutely not part of the process,” said Crystal Watson, a senior scholar at the Johns Hopkins Center for Health Security. “No one should give bank information or credit card information.”

Real contact tracers generally work for health departments. They contact COVID-positive patients to track symptoms; they help the people they call figure out how to isolate themselves from others until they clear the virus, and determine which friends, neighbors, colleagues or acquaintances they might have been near in the days just before or after they tested positive for the coronavirus. Those contacts, in turn, are sought out by the tracers, who are in a race against the clock, hoping to get those folks to quarantine as well.

This tried-and-true public health tool (along with hand-washing, wearing a mask in public and maintaining 6 feet of physical distance from people outside your household) is one of the few strategies available to slow the spread of the virus while scientists work on treatments and vaccines.

Legitimate contact tracing is being employed widely in some [areas](#), such as the District of Columbia and Hawaii, and has been credited with helping [countries](#) such as New Zealand and Taiwan contain the virus.

But with this success also comes bad actors. [The Federal Trade Commission](#), Department of Justice, and Department of Health and Human Services, as well as [the Better Business Bureau](#) and state law enforcement and health officials from [across the nation](#), have issued [consumer alerts](#) about unscrupulous people not affiliated with health departments using phone calls, texts or emails to get personal information from those they scam.

What differentiates a real call from a fake one? For one thing, legitimate tracing calls might be preceded by a text message, notifying patients of an upcoming call from the health department. Then, in that initial call, the legitimate tracer seeks to confirm an address and birthdate, especially if you are the COVID-positive patient, Watson said.

“They ask about your identity to make sure you are the person they are trying to reach so they don’t disclose potentially private information to the wrong person,” Watson said.

The tracers can also help people who must isolate or quarantine by connecting them with resources, such as food or medicine delivery.

“Some can even provide you with a separate place to quarantine safely” if, for example, you live in a multigenerational house with no separate bathroom or bedroom in which to isolate, said Watson.

At the end of the call, the tracer may ask if they can call or text you in the coming days to check on how any symptoms may be progressing.

What should you watch for?

Be concerned if you get an initial text asking you to click on a link, which might be spam and could download software onto your phone, the FTC warned in May.

“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,” the agency said.

Another clear red alert: being asked for your Social Security number. Contact tracers in most regions do not ask your immigration or financial status, either.

Also, watch out if any names of COVID patients are provided.

“An authorized contact tracer will not disclose the identity of the person who tested positive and is the starting place for that tracing effort,” the Wisconsin attorney general’s office said in a release warning consumers about scams. Another piece of advice: Do a little research before you respond.

“Anytime someone calls you for information, you should be concerned about who is calling,” said Dr. Georges Benjamin, executive director of the American Public Health Association. “If they are legitimate, you can say ‘Give me your name and phone number’ and you can always call them back” after doing some checking.

Did the caller ID indicate the call was from a health department? Some states are including that information. For example, Virginia’s calls are from the “VDH COVID Team.” Call the health department if you have any questions.

“Scammers prefer to prey on individuals who may be more trusting, are alone, or may respond out of confusion or fear,” Pennsylvania Secretary of Aging Robert Torres said in an Aug. 12 press release. “It’s important that they stay alert about any contact from anyone identifying themselves as a contact tracer and do not provide personal information until they are sure the individual and information are legitimate.”

And, finally, if you think you’ve been contacted — by phone, email or text — by a scammer, report it to agencies, such as your state attorney general’s office.

“If you see something, say something,” California Attorney General Xavier Becerra said in a recent consumer alert his office issued. “We are working to track these impostors.”

Julie Appleby: jappleby@kff.org, [@Julie_Appleby](https://twitter.com/Julie_Appleby)