








CALIFORNIA STATE THREAT ASSESSMENT CENTER

EMERGING SITUATION BULLETIN | 9 JULY 2020

(U) Scammers Exploit California's COVID-19 Contact Tracing Program

(U) In ongoing efforts to mitigate the spread of COVID-19, Governor Gavin Newsom launched "California Connected," the state's comprehensive contact tracing program and public awareness campaign. Malicious actors are utilizing previously seen scam tactics, techniques, and procedures (TTPs) in order to exploit California's contact tracing program and the public.

- (U) California Connected, California's contact tracing program, is a confidential process used by public health departments to slow the spread of COVID-19. Under this program, public health representatives will telephonically interact with those who have tested positive, alert anyone that may have exposed, keeping personally identifiable information (PII) confidential. Representatives will also inquire about symptoms, offer testing guidance, and discuss next steps like self-isolation and medical care.
- (U) Scammers are impersonating contact tracers so that they can profit from the current public health emergency. Along with calls, scammers are sending out links in text messages about fictitious COVID-19 cases. Scammers may ask for information such as, your social security number, financial information, and other sensitive information **not** required for authentic contact tracing.

A contact tracer from your state or local health department might call if you've been exposed to COVID-19. But scammers are pretending to be contact tracers too. Here's how you can spot the scam.	
	Real contact tracers won't ask you for money. Only scammers insist on payment by gift card, money transfer, or cryptocurrency.
	Contact tracing doesn't require your bank account or credit card number. Never share account information with anybody who contacts you asking for it.
	Legitimate contact tracers will never ask for your Social Security number. Never give any part of your Social Security number to anyone who contacts you.
	Your immigration status doesn't matter for contact tracing, so real tracers won't ask. If they do, you can bet it's a scam.
	Do not click on a link in a text or email. Doing so can download malware onto your device.

(U) 5 things to know about a Contact Tracing Call

(U) Source: Federal Trade Commission

- (U) Legitimate contact tracers may call, email, text, or visit your home to collect information. They will only send you texts or emails indicating when they will contact you and will not ask you to click or download anything. The information a legitimate contact tracer may ask you for include: your name and address, health information, and the names of places and people you have visited.
- (U) **Tips on Identifying COVID-19 Themed Scams and Reporting Resources**
 - Be wary of suspicious emails, phone calls, and text messages. Contact your local health department to verify that the call or messages are valid, think before clicking on any links, and be aware of suspicious attachments.
 - For additional information regarding California Connected or COVID-19 visit [CDPH Contact Tracing](#), [CDPH COVID-19](#)