



FBI Warning: Watch Out for These Coronavirus Scams


Scammers, despicable as ever, are rushing to take advantage of the global COVID-19 pandemic. Indeed, customs agents have already seized packages filled with vials claiming to be home-use test kits—and that’s just the beginning.

Among the most common scams that the FBI wants you to be aware of, in addition to phony test kits:



 **Emails from “official” sources.** Phishing scammers often leverage news events. The FBI says many messages claim to be from the U.S. Centers for Disease Control or other organizations offering information on COVID-19. “Fraudsters can use links in emails to deliver malware to your computer to steal personal information or to lock your computer and demand payment,” the FBI notes. Be wary of websites and apps claiming to track COVID-19 cases worldwide; crooks are using malicious websites to infect and lock devices until payment is received.

 **Phone calls asking for personal information.** Some scammers are using phone calls (made with both live operators and robocalls), to gain personal information such as bank account and Social Security numbers. And in some areas, con men are spoofing local health-department phone numbers and texting potential victims for their Medicare or Medicaid information.

 **Criminals knocking on doors claiming to be health officials.** Some brazen criminals have been knocking on doors, claiming to be from the Red Cross, and seeking “donations.” Elsewhere, imposters in white lab coats, masks, and gloves are going house to house and saying they’re from the CDC.

As you can see, criminals have lots of nerve and no shame when it comes to leveraging a tragedy for money. That’s why it’s up to you to be vigilant.