Unfortunately, the spammers and scammers of the world are using the COVID-19 pandemic to take advantage of people, many of whom may be more vulnerable to their nefarious efforts than usual during these uncertain times. A handful of government agencies and other groups are stepping in to fight off the scammers, but there are still some steps you can take to avoid being a victim.

Here's what to know about the COVID-19 scams out there, as well as some precautionary measures you can take to avoid being scammed during the coronavirus outbreak.

Many of the COVID-19 scams going around involve attempts by companies and individuals to sell products they claim can prevent or cure the novel coronavirus, which has already killed thousands of people in the United States and tens of thousands worldwide. They are using this fear to create urgency, this urgency allows the scammers to illicit information or convince a victim to purchase untested and unverified "remedies." Scammers are peddling fake remedies ranging from colloidal silver to cow manure. But the novel coronavirus is exactly that — new — and there is no known cure yet. Vaccine trials are underway, but any verifiable treatment is likely months away at best.

Watch for scam emails and texts

Phishing schemes, when a scammer sends an email or text meant to trick you into handing over your personal info, have become very sophisticated in recent years, and can even include elements like official imagery or email addresses that look similar to email addresses used by official businesses.

Likewise, phone calls and texts from scammers will often attempt to pretend to be official businesses and may include information like your name or phone number to try to convince you that they're real. A real business will NEVER ask for information such as bank information or your social security number over an unsolicited phone call or email, especially from Bank of Commerce.

To spot COVID-19 email and text scams, look for generic greetings (like "Hello, Sir/Madame"), requests for confirmation of personal information, or emails related to updating your billing details. If a message's language seems urgent, as though it's attempting to pressure you into giving up your information to avert some sort of disaster, it could very well be fake. If you receive a suspicious email from a particular company or even a friend or your employer, contact them separately via phone to verify the message before replying or otherwise acting on it.

For more information visit the sites below:

Coronavirus Scams: What the FTC is doing

FCC COVID-19 Consumer Warnings and Safety Tips

Department of Justice Coronavirus (COVID-19)

If you have been a victim of a scammer file a complaint with the FBI at:

Federal Bureau of Investigation Internet Crime Complaint Center (IC3)