

FBI talks COVID-19 scams, cons

In a Twitter chat May 15, the FBI focused attention on ways scammers operate in the era of COVID-19 and how members of the public can avoid being deceived.

Here are some things to watch out for to keep from being victimized by fraud.

- Ignore offers or advertisements for COVID-19 related vaccines, home test kits, protection, or treatments.

Unfortunately, there is currently no cure, approved treatment, or vaccine for COVID-19. While medical professionals and scientists throughout the U.S. are working hard to change that, scammers are working hard to sell bogus products that claim to prevent, treat, cure, and diagnose the disease. Some are selling fake at-home test kits and are even going door-to-door and performing fake tests for money.

- Anyone with symptoms of COVID-19 should rely on a physician or other trusted health care

provider to assess your condition and approve requests for testing.

When an approved treatment or cure becomes available, the first time you hear about it probably will not be through an email, telephone call, online advertisement, or unsolicited sales pitch from a stranger.

- Be skeptical of ads offering certified personal protective equipment (PPE).

The FBI urges everyone to be alert to counterfeit products like sanitizing products and personal protective equipment (PPE), including N95 respirator masks, goggles, full-face shields, protective gowns, and gloves.

PPE must be tested, vetted, and certified by the appropriate authorities. If anyone purports to have a significant supply of medical-grade PPE for sale on the internet, over the phone, or by mail, it could be a scam.

- Be suspicious of any unsolicited offers requiring or requesting your medical insurance, personal, or financial information.

Personal, financial, and health insurance information is valuable. Do not respond to unsolicited emails, phone calls, or visitors requesting or demanding personal information including financial information, Medicare or Medicaid numbers, or private health insurance information.

- If you do receive treatment for COVID-19, double-check the medical bills and Explanation of Benefits (EOB) for accuracy. If you find charges for services you did not receive, contact your medical provider and your insurance company.

- Beware of government impersonation scams.

Some scammers are pretending to be officials claiming the government requires you to take a COVID-19 test and asking for your health insurance information or claiming to be medical professionals demanding payment for treating a friend or relative for COVID-19.

Don’t take these claims at face value. Government officials will never contact you and demand payments in the form of cash, wire transfer, or gift card. Do not provide personal, financial, or health insurance information for unverified services.

- Resist pressure to act quickly.

Urgency is one of the most recognizable red flags of any scam. Be immediately suspicious of anyone who initiates contact and demands immediate action or sets a very short deadline, 24 to 48 hours.

- Exercise caution when making charitable contributions.

Sadly, charity scams are very common during crises as criminals exploit the good will of people wanting to help others. Be alert to charities that seem to have sprung up overnight in connection with current events.

Research the charity before donating. It is always best to donate directly to charities you know and trust. If someone insists on donations by cash, gift card, or by wire transfer, don’t do it.

- Watch out for unsolicited investment “opportunities.”

The implementation of the $2 trillion Coronavirus Aid, Relief, and Economic Security Act will provide even more opportunities for would-be criminals. Fraudsters around the world are already developing methods to steal the critical financial support intended for communities, companies, and individuals.

For example, fraudsters are offering unrealistic returns on investments in bogus businesses alleging to receive stimulus money.

- Be careful online.

Be wary before clicking on links purporting to provide information on the virus; donating to a charity online or through social media; contributing to a crowdfunding campaign; purchasing products online; or giving up your personal information in order to receive money or other benefits.

- Watch out for emails claiming to be from the Centers for Disease Control and Prevention or other organizations claiming to offer information on the virus.

- Do not click links or open attachments you do not recognize. Fraudsters can use links in emails to deliver malware to your computer to steal personal information or to lock your computer and demand payment.

- Be wary of websites and apps claiming to track COVID-19 cases worldwide. Criminals are using malicious websites to infect and lock devices until payment is received.

- Look out for phishing emails asking you to verify your personal information in order to receive an economic stimulus check from the government. While talk of economic stimulus checks has been in the news cycle, government agencies are not sending unsolicited emails seeking your private information in order to send you money.

The best advice is for the public to use the same judgment and skepticism they would normally use when an unsolicited email, caller, or visitor offers an unrealistic deal or opportunity.

For more information: https://www.ic3.gov/media/2020/200320.aspx ; Additional information on coronavirus-related scams and fraud can be found at fbi.gov/coronavirus.

For accurate and up-to-date information about COVID-19, visit: coronavirus.gov; cdc.gov/coronavirus; usa.gov/coronavirus; fbi.gov/coronavirus; justice.gov/coronavirus