How To Protect Yourself From Pandemic Scammers

The current coronavirus pandemic has been hard on most folks, but scammers and criminals have come out in force to make things even harder.

It seems pandemics bring out the best and
worst in people.

On the one hand, you have the front liners and regular folks coming together to fight the virus. In contrast, you have the criminals and scammers that want to take advantage of the already chaotic situation to steal from other people. The COVID-19 crisis the country faces is an unprecedented nightmare as the government is struggling to flatten the curve and reduce the number of infections and fatalities. This pandemic is a real SHTF emergency, and people are afraid, hurting, and looking for help anywhere they can get it.

Scammers know about the fear and panic
everyone feels and swoops in to offer a helping hand, but little do these
people know they’re dealing with criminals who want to take everything from
them. It is plain old despicable that someone would want to take advantage of
another person in a time like this, but this is the world we live in now. While
there are still a lot of decent people out there, sometimes the universe coughs

up a bad seed. With all the COVID-19 scams happening during this trying time,
your best defense is arming yourself with information about these criminal
activities to avoid becoming a victim.

The Rise of Coronavirus-Related Domains.

Cybercriminals have been working hard to
register as many COVID-19-related domains as they can using cheap hosting
services that offer automated registration. The good news is that domain
registrars are fighting back and are working with authorities to prevent new
registrations while taking down known fraudulent domains. However, with the
sheer number of registrars and domains already registered, it’s an uphill
battle to weed them all out.

The Facts:

- According to Check Point Software Technologies, more than 16,000 coronavirus-related domains have been registered during the start of the outbreak in January 2020.
- About 0.8% of these websites (93) were found to be malicious, and another 19% (2,200 sites) were labeled suspicious. The researchers also warned that coronavirus-related domains were 50% likely to be more dangerous than other domains listed during the same period.
- US and UK agencies are currently tracking 2,500 coronavirus-themed threats and have already issued a

joint alert.

Scammers have been using the media's relentless coverage on COVID-19 to enable their schemes and spread their malicious activities. Much like "Black Friday" or "Cyber Monday" deals, cybercriminals have been using "coronavirus specials" to peddle their illegal tools and hacking services on the Dark Web using "coronavirus" or "COVID19" discount codes. These criminals also dupe regular people by offering premium products at unbelievably low prices labeled as "coronavirus specials." Of course, these products don't exist, and folks lose not only their money but quite possibly their credit card details and personal information.

Common Types of COVID-19 Scams During the Pandemic.

To better protect yourself from coronavirus scams running rampant during this pandemic, it pays to know what these are so you can identify them and stay away.

Phishing Attempts.

Criminals have been using various types of phishing methods during the COVID-19 pandemic, including unsolicited text, phone calls, emails, and fake websites. Phishing attacks are designed to collect as much data on their victims as possible, either via tricking people into providing their details or by including malware that infects computers and steals credentials to be used for identity theft. Malicious software or "malware" consist of viruses, trojans, spyware, or ransomware that can be activated when you install untested software or download and click on an email attachment.

A phishing email impersonates a trustworthy source, usually a government agency like the Centers for Disease Control and Prevention (CDC) or the World Health Organization (WHO). It can also come from fake private companies offering masks, medical equipment, or assistance in exchange for sensitive data such as passwords or banking details. Be wary of emails from unknown senders or ones with "COVID-19" or "Coronavirus" on the title. A quick email lookup can provide additional information on the sender and help protect from identity theft.

Government Scams.

One of the most effective schemes
doing the rounds this pandemic are scammers impersonating the government.

Criminals are using email, phone calls, and social media to reach out to people
and pretend they’re representatives of so and so agency. There have even been
reported cases of scammers going door-to-door, trying to trick people into
giving them money for medical equipment, COVID testing, or financial aid.

It’s important to note that the government will NEVER reach out to you via email, phone call, chat, or text. It would be a monumental task to reach all 328 million Americans, so if someone contacts you and claims to be from the government offering you COVID-19 assistance, it’s a scam or most likely a phishing attempt to get your sensitive data or money.

Fake Vaccines and Medical Treatment Scams.

Criminals peddle fake vaccines and unproven treatments for COVID-19 that can be extremely dangerous or even fatal to your health. Scammers call or email people pretending to be from treatment centers or doctors that have treated a friend or relative for coronavirus and demand payment for services that never happened. The FTC is already tracking criminals attempting to sell fraudulent products that claim to diagnose, treat, or prevent COVID-19.

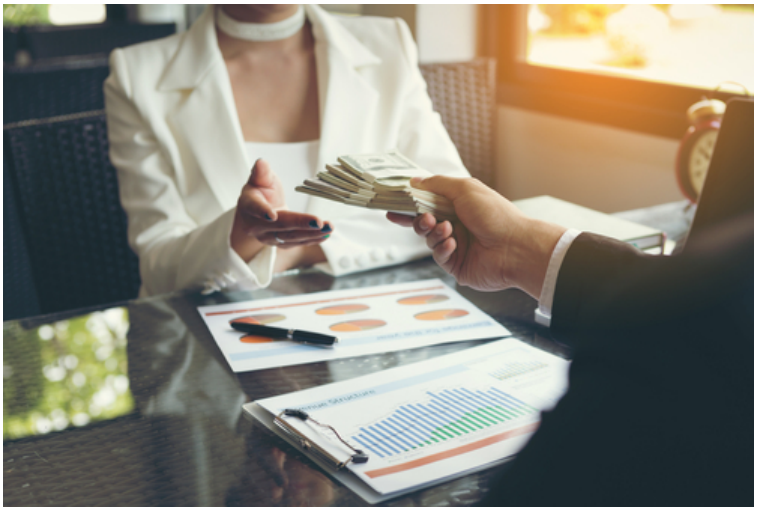
So far, the FDA hasn't approved any products or drugs to treat COVID-19, except for Remdesivir, an experimental broad-spectrum antiviral currently undergoing clinical trials. The FDA also issued an Emergency Use Authorization that allows the use of hydroxychloroquine and chloroquine products (used to treat lupus) for adolescents and adult patients hospitalized with COVID-19 who aren't part of any clinical trials, but that's about it.

There are also scammers selling fake and unauthorized home testing kits. There's only one FDA-approved coronavirus home testing kit available to people in most states, but you'll need a doctor's order to get one. Never accept medical treatment or a virus test from anyone other than your doctor, local health department representative, or trusted pharmacist.

Work From Home Scams.

Plenty of people are either out of work or working from home during this pandemic, making them a prime target for scammers. If you receive an unsolicited email about a job from a person or company that you never knew existed and are asked to pay a "fee," you're dealing with a con artist. Legitimate companies will never ask you to pay them. Run a reverse email lookup if you get an email from a person you don't know to be sure of the source. Be wary of "money mule" jobs that offer to pay you handsomely to move money. This act is illegal and a federal crime if you get caught.

CARES Fraud.

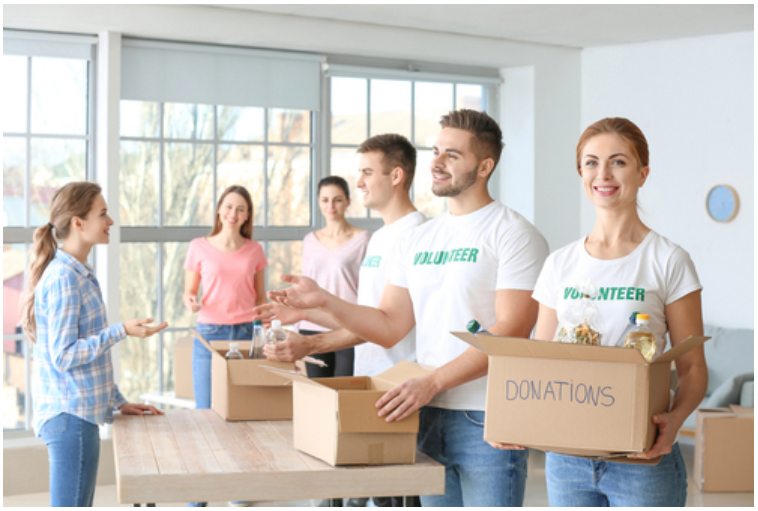


The IRS warns about schemes related to “Economic Impact Payments” being sent to taxpayers under the CARES (Coronavirus Aid, Relief, and Economic Security) Act. Be wary of scammers who use the words “stimulus payment” and ask you to sign up to get your check or contact you by email, text, phone, or social media to “verify” your personal and banking information to move things along. The official term is “economic impact payment,” and the IRS will never call or email you about it. The economic impact payment is deposited directly into an account that you provided on your tax return, or a check is mailed to the address the IRS has on file. If you haven’t submitted your direct-deposit information to the IRS yet, you can do it online at irs.gov/coronavirus.

Investment Scams.

Investment fraud is one of the most
lucrative schemes during the coronavirus pandemic because it plays on FOMO and
get-rich-quick tendencies that affect many people. Scammers offer would-be
investors the chance to “invest” stocks in a publicly-traded company
focused on COVID-19 treatment, which dramatically increases its value (pump and
dump) and dumps it, leaving the investors with a stock that has no value.

Charity Fraud.



Scammers impersonate legitimate charitable institutions and play on the heartstrings of people, asking them to donate money for those affected by the pandemic. Be wary of charities with names similar to more well-known organizations. If an organization is blatantly asking for money and wants you to send it via wire transfer or gift cards, you're most likely dealing with a scammer. Before taking action and donating, make sure the charity is legitimate by checking their status at irs.gov/charities-and-nonprofits.

Fake Shopping Websites and Apps.

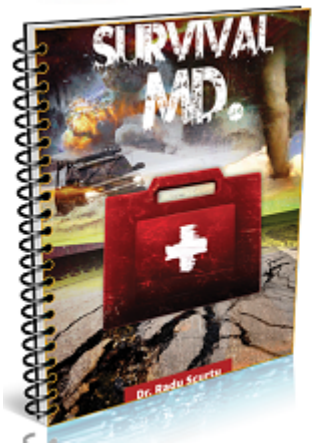
Cybercriminals create bogus e-commerce
websites, online stores, email addresses, and social media accounts that sell
surgical masks, hand sanitizer, toilet paper, or other medical supplies that
are currently in demand. If you get duped into paying for cheap items in bulk,
don't expect to get any merchandise.

It's a shame that folks have to deal with
these pathetic scammers and criminals on top of all the problems brought about
by the coronavirus pandemic. Trust is a valuable commodity,

and these people
are attacking it daily.

Please report COVID-19 scams to the
National Center for Disaster Fraud hotline at 1-866-720-5721.

Stay safe, everyone.



CLICK HERE

to find out more on the first aid techniques that will save your life when surviving in the wilderness!