

## COVID-19 (CORONA VIRUS) SCAMS

Cyber criminals will stop at nothing to acquire your personal and confidential information, even using the latest news or current events as a way to mislead you. Recently, the threat posed by coronavirus has ignited an international health emergency. That's when scammers will attempt to make your fear and concern work to their benefit with coronavirus scams.

### **How Does the Scam Work?**

Like any phishing scam, the intent is to persuade, intimidate, or even scare you into giving up personal information, opening malicious emails and/or attachments, or even donating money for a seemingly legitimate cause. In regard to coronavirus, criminals now have another tool—fear. By preying on people's fear of contracting the virus, they are hoping that you make a hasty decision to divulge your confidential information.

For example, a cybersecurity firm named Proofpoint recently reported on the existence of coronavirus-themed emails, stating that cyber criminals are sending emails with fraudulent Microsoft Word attachments that seem to promote virus awareness or safety measures. If the attachment is opened, malware or ransomware is installed on a user's computer. In another scenario, cyber criminals are going so far as to disguise themselves as the World Health Organization (WHO) or Centers for Disease Control and Prevention (CDC). At first look, it may be tempting to open an email and click on a link or open an attachment that appears to come from one of these health entities claiming to have legitimate health and safety information. That's what the scammers hope you do.

Sadly, it's not limited to cyber criminals. According to the U.S. Securities and Exchange Commission (SEC), fraudsters often use the latest news developments to lure investors into scams. In fact, the SEC's Office of Investor Education and Advocacy recently issued an Investor Alert to warn people about investment frauds involving claims that a company's products or services will be used to help stop the coronavirus outbreak.

### **How to Protect Yourself from Coronavirus Scams**

Fortunately, there are ways to counteract these attempts to steal your information or defraud you out of money:

1. Don't click on links or open attachments from sources you don't know. As mentioned in the scenario above, doing so could download a virus onto your computer or device. You should also make sure the anti-malware and anti-virus software on your computer is up to date.
2. Be alert to "investment opportunities." The SEC is warning people about online promotions, including on social media, claiming that the products or services of publicly-traded companies can prevent, detect, or cure coronavirus and that the stock of these companies will dramatically increase in value as a result.

3. Watch for emails claiming to be from the CDC, WHO or experts offering important information about the virus. For the most up-to-date information about the coronavirus, visit these entities' websites directly.

The WHO has taken specific measures to warn people about coronavirus scams. For instance, the WHO will:

- Never ask you to log in to view safety information
- Never email attachments you didn't ask for
- Never ask you to visit a link outside of [www.who.int](http://www.who.int)
- Never ask you to donate directly to emergency response plans or funding appeals

#### Keeping Your Money Safe

There is literally no end to cyber criminals and scammers trying to acquire your personal information or infiltrate your computer and/or network. The key to protecting yourself is education and awareness.