Watch Out for These Coronavirus Scams

As the situation surrounding the coronavirus continues to develop, your health and financial security continues to be our priority. Beware of the many circulating scams which exploit the fear and the uncertainty surrounding the virus.

Here are some of the most prevalent ones:

The fake funding scam. In this scam, victims receive bogus emails, text messages or social media posts, asking them to donate money to a research team which is on the verge of developing a drug to treat COVID-19, and/or a vaccine to immunize the population against the virus. There have also been ads circulating on the internet with similar requests. Unfortunately, nearly all of these are fakes, and any money donated to these "funds" will go directly into the scammers' pockets.

The bogus health agency. There is so much conflicting information on the coronavirus that it's really a no-brainer that scammers are exploiting this confusion. Scammers are sending out alerts that appear to be from the Centers for Disease Control and Prevention (CDC) or the WHO, when in fact they're created by the scammers themselves. These emails sport the logo of the agencies that allegedly sent them, and the URL is similar to those of the agencies as well. Some scammers will even invent their own "health agency," such as "The Health Department," taking care to evoke authenticity with (bogus) contact information and logos.

Victims who don't know better believe these missives are sent by legitimate agencies. While some of these emails and posts may actually provide useful information, they often also spread misinformation to promote fear-mongering, such as non-existing local diagnoses of the virus. Even worse, they infect the victims' computers with malware which is then used to scrape personal information off the infected devices.

The phony purchase order. Scammers are hacking the computer systems at medical treatment centers and obtaining information about outstanding orders for face masks and other supplies. The scammers then send the buyer a phony purchase order listing the requested supplies and asking for payment. The employee at the medical treatment center wires payment directly into the scammer's account. Unfortunately, they'll have to pay the bill again when contacted by the legitimate supplier.

Basic preventative measures can keep the scammers from making you their next target.

As always, it's important to keep the anti-malware and antivirus software on your computer up-to-date and to strengthen the security settings on all of your devices.

Practice responsible browsing when online. Never download an attachment from an unknown source or click on links embedded in an email or social media post from an unknown sender. Don't share sensitive information online either. If you're unsure about a website's authenticity, check the URL and look for the lock icon and the "s" after the "http" which indicate that the site is secure.

Finally, it's a good idea to stay updated on the latest news about the coronavirus to avoid falling prey to misinformation. Check the actual CDC website for the latest updates.