Money Talks by Dave Helscher

March 2020

With the advent of sheltering in place and staying at home, many are turning to their email, social media, and web sites to obtain information or to stay in contact with family, friends, and acquaintances. The majority of information on our favorite news sites relate to Covid-19. Unfortunately, some of the very worst of human behavior rears its ugly head during a health crisis such as this one, preying upon fear, misinformation, ignorance, and even malicious disinformation. I am referring to all sorts of scams related to the virus outbreak. These can run the gamut from ordinary spam attempting to use the crisis for a quick financial gain to downright dangerous emails designed to compromise victims' online accounts and install malware.

You should be on the lookout for emails that appear to be from organizations such as the CDC (Centers for Disease Control) or WHO (World Health Organization). Scammers have crafted emails that appear to come from these sources but may contain malicious phishing links or dangerous attachments. Watch for emails asking for donations for studies, doctors, or victims that have been affected by the virus. Fake charity emails are often created after global phenomena occur, like natural disasters or heath scares. Watch for emails that claim new information or updated lists of cases in our area. These could contain dangerous links and information designed to scare you into clicking on the link.

Both the Federal Trade Commission (FTC) and the Secret Service have alerted businesses and the public of the prevalence of these scams. Some will hawk health products, dangle the hint of a vaccine or cure, or appeal to your more charitable instincts, exploiting fear and ignorance to peddle malware or gain access to your accounts. These are only a few examples these scam artists use and they are constantly coming up with new ways to fool you and have you part with your information or money. Some appear quite crude but others have become very sophisticated in targeting a particular audience or appealing to our darkest instincts.

The recent passage of the federal stimulus legislation is going to provide scammers another opportunity. The FTC has issued some warnings. The government will not be asking you to pay anything to get this money: no fees, no charges. The government will not be calling you to ask for your social security number, bank account, or credit card numbers. Anyone that does is a scammer. These payments are in process and anyone that tell you they get you're the money early is a scammer.

You should remain especially cautious during this time. There are some steps you can take to help protect yourself from these scams. Never click on links or download attachments from an email that you were not expecting. If you receive a suspicious email that appears to come from an official organization such as the WHO or CDC, report the email to the official organization through their website. If you want to make a charitable donation, go to the charity's website to submit your payment. Type in your charity's web address in your browser instead of clicking on any links in emails, or other messages.

These precautions can be especially necessary with the closure of schools and many students trying to fill up their time at interactive web sites, social media, and other electronic means. It is important to be able to spot and handle these correctly and to teach others as well. For bad actors, Covid-19 provides endless opportunities to steal from anxious and concerned people their passwords, logins, and their money. You are already dealing with several new challenges posed by the virus, there is no reason to increase this threat by allowing these bad actors to cash in by any means necessary.