

Online Scams in the Age of Coronavirus



Online scammers are not known for their decorum.

Even in the face of a global pandemic the likes of which few if anyone living has seen, hackers are using fear and worry to take advantage of all of us.

Now more than ever, critical thinking skills must be brought to bear and cooler heads must be kept.

We've put together some tips and advice for staying secure and watching out for scammers in the age of coronavirus (COVID-19).

We can't sugarcoat it. The spread of COVID-19, the respiratory disease caused by a novel strain of coronavirus making its way around the globe, is serious.

Few have escaped its impact. Businesses like ours are working from home or temporarily shuttered.

Unfortunately, challenging times for people like us mean fertile ground for scammers looking to make a quick buck through fear and misinformation.

For us, the coronavirus situation is an opportunity to exercise our critical thinking skills and work together to ensure these scammers don't even get the time of day. Here are some examples of scams to look out for and advice on how to spot them.

WHO TO TRUST

Coronavirus misinformation abounds, but here are some sources you can trust:

- City and state health officials
- The World Health Organization (WHO)
- The Centers for Disease Control (CDC) in the U.S.
- National Institutes of Health (NIH) in the U.S.
- The Federal Trade Commission (FTC) in the U.S.

Phishy Medical Alerts

Numerous kinds of phishing emails claiming to be official medical alerts about the virus have been seen in the wild. These have ranged from sketchy links to maps showing the spread of the virus to advice from health officials contained in malware-loaded PDF files.

Fortunately for us, the signs of a coronavirus phishing email are similar to any other.

Keep an eye on the "from" address for clues on the true sender. Be wary of any links in an unsolicited email. Pay attention to the tone of the email. Is the sender using scare tactics imploring you to act now? If so, that's a red flag.

Scam Robo-calls and Text Messages

The U.S. Federal Trade Commission (FTC) has received numerous complaints of robocalls and text messages asking for donations, selling scam treatments, and offering payment checks from the government. None of these are legitimate.

If you get a robocall of this type, the FTC advises simply hanging up—even if the voice says you can press a button to speak to an operator. Unsolicited text messages with links to do anything are also usually

suspect and should be considered skeptically.

The 20-second Rule

Treat any dubious email, call, text message, or other online communication like washing your hands.

Take 20 seconds to search this claim on Google or visit the legitimate site of the organization claiming to have sent the message.

If you can't find any supporting evidence, consider the claim a scam and move on.

Just like government advice to maintain social distance and avoid gathering in groups to stop the spread of COVID-19, keeping malware and misinformation from spreading is up to individual action.

Use these tips to keep both our important company information and yours secure.

We're all in this together.