Alert

March 12, 2020

COZEN O'CONNOR

Avoiding Online Scams in the Time of Coronavirus

What do tornadoes, hurricanes, earthquakes, wildfires, and the coronavirus have in common? Scams. Disasters seem to beget scammers well versed in both price gouging and knockoff peddling, as well as phishing schemes and malware distribution.

The coronavirus is no different. There has been an onslaught of phishing emails including scams promoting awareness and prevention tips ("Go through the attached document on safety measures regarding the spreading of corona virus," reads one such message that purports to come from a virologist). Other scams offer fake information about exposures or quarantines in local communities and neighborhoods that target anxious and vulnerable people ("The CDC continues to monitor the outbreak of the Coronavirus — and updated list of new cases around your city is available by clicking HERE" reads another email). The links will often launch malicious malware, steal your data, or both.

The FTC is most concerned with an uptick in scams selling fake cures, preventative measures, or charitable organizations. According to the FTC, "They're setting up websites to sell bogus products, and using fake emails, texts, and social media posts as a ruse to take your money and get your personal information." Scammers may deploy fake social media posts and register official-sounding websites to trap the unwary: Checkpoint found that more than 4,000 new domains referencing either "corona" or "COVID" had been registered in 2020, and that domains containing these words were 50 percent more likely to be associated with phishing or malware distribution.

To address this surge of scams and potential attacks, the FTC has posted guidelines that include:

- Do not click on links from emails you don't recognize. Always confirm that an email address with a link is valid and spelled correctly or use another method of communication to confirm that the sender is legitimate — call the sender, send a text message, or try a different email address to confirm.
- Consult the Centers for Disease Control and Prevention or World Health Organization website directly for information. Do not trust random emails claiming to be from those organizations.
- Ignore ads for prevention, treatment, or cures and do not invest in companies based on online information that claim they sell any of these products.
- If you donate to coronavirus relief or research, make sure the organization or online campaign you're donating to is legitimate. A good place to start is the IRS online search tool where you can confirm it is a tax-exempt organization.

Misinformation and scams are spreading faster than the virus, so stay safe and maintain your good cyber-hygiene practices.

Trevor McGuinness is director of COSEC, a wholly owned subsidiary of Cozen O'Connor that leverages the knowledge, processes, and technology of the firm to provide cybersecurity consulting to small businesses, family offices, and private clients. He is not an attorney.

Trevor McGuinness

Director,
COSEC

tmcguinness@cozen.com
Phone: (215) 665-7269
Fax: (215) 665-2013

Related Practice Areas

- Coronavirus Task Force
- State Attorneys General
- Technology, Privacy & Data Security