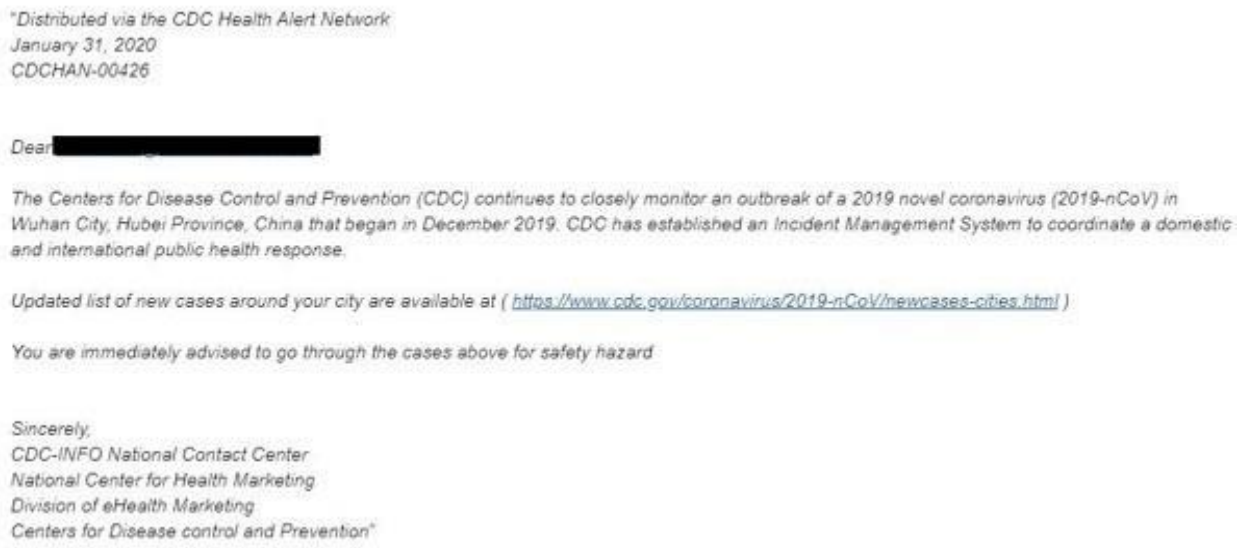
Take Cyber Precautions as Scammers Exploit COVID-19 Fears

COVID-19 continues to spread throughout the country, as does the fear and panic that is associated with the virus. Organizations in every industry are sending out communications to clients, prospects, and subscribers to inform them of their contingency plans and policies related to COVID-19.

However, this onslaught of information combined with anxiety over the unknown is also creating a prime playing field for scammers hoping to obtain your personal information for their gain.

Reports of phishing scams related to coronavirus have escalated quickly, with professionals receiving emails that seem to be from reputable organizations offering information on COVID-19, providing advice, and even attempted to sell fake products related to maintaining your health during this time of uncertainty. When individuals click on the link, either on their phone or desktop computer, they open up their network and sensitive information to bad actors.

CreditUnionTimes shared an example of one such email:



"Distributed via the CDC Health Alert Network
January 31, 2020
CDCHAN-00426

Dear [redacted]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above for safety hazard

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention"

Professionals would be well-served to revisit cyber liability best practices. Maintaining a level head and adhering to cyber security guidelines may prevent a potential breach of data for you and the organization you work for.

Best practices to avoid a cyber breach due to phishing scams

- Keep your guard up when you receive an unexpected email, even if it's from a source that you believe you recognize and trust.

- Navigate directly to official websites of the CDC, WHO, and more instead of clicking a link through an email.
- Working remotely can present even higher risks for cyber breaches. Ensure that you are following company guidelines for accessing servers securely.

Business leaders should be aware of their cyber liability protection, as a breach caused by a COVID-19 related phishing scam can result in a claim for your organization.