



# WHITE PAPER | Coronavirus Themed E-mail Phishing

Date February 3, 2020

TLP: WHITE

Health Sector Cybersecurity Coordination Center (HC3) | HC3@HHS.GOV

## Executive Summary

Recently, malicious cyber threat actors have been leveraging the current news cycle to launch Coronavirus themed cyberattacks at their targets. Prominent news reporting and the resulting elevated concern for the Coronavirus issue is being used as context for a malicious email phishing campaign. The phishing emails contain links to malware that is frequently used to target healthcare organizations and their IT systems.

Attempting to exploit human greed, fear, and curiosity are common tactics among phishing campaigns – malicious e-mails deliberately crafted to entice the recipient to click a link or open an attachment in the e-mail which, while appearing helpful, compelling, or interesting, actually contains malicious code. Victims who interact with malicious links or attachments may expose their systems, networks, and valuable information. These exposures allow an attacker to use infected systems as a platform to launch additional attacks. The new Coronavirus themed phishing campaign is attempting to capitalize on concerns about the Coronavirus, a respiratory illness currently in the news and frequently making headlines. Researchers are reporting that these Coronavirus themed phishing emails contain links and downloads for the Emotet malware. At least one campaign has been identified as attempting to impersonate the Centers for Disease Control and target Americans and other English-speaking victims.

## Countermeasures and Mitigations

Recommended actions to protect against such an attack are to implement:

- User awareness and training to help identify and avoid phishing scams
- Operationalization of Indicators of Compromise
- Automatic banners for any e-mails that originate outside the organization
- Use of blacklisting of malicious sites and whitelisting for known trusted sites
- Integrate anti-spoofing technologies Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC)
- Update operating systems and applications with the latest security updates, including 3rd party software
- Implement and update endpoint security systems

## Endnotes

### Industry Best Practices Resource

- <https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx>

### Open source news resources

- <https://www.govtech.com/blogs/lohrmann-on-cybersecurity/coronavirus-scams-prepare-for-a-deluge-of-phishing-emails-fake-alerts-and-cyberthreats.html>
- <https://www.proofpoint.com/us/corporate-blog/post/emotet-leverages-coronavirus-and-greta-thunberg-again-while-coronavirus-threats>
- <https://www.independent.co.uk/life-style/gadgets-and-tech/news/coronavirus-china-computer-virus-face-mask-malware-emotet-a9314761.html>
- <https://www.straitstimes.com/tech/wuhan-virus-hackers-exploiting-fear-of-bug-to-target-computers-gadgets>
- <https://www.techrepublic.com/article/hackers-using-coronavirus-scare-to-spread-emotet-malware-in-japan/>

- <https://www.helpnetsecurity.com/2020/02/03/wuhan-coronavirus-exploited-to-deliver-malware-phishing-hoaxes/>
- <https://exchange.xforce.ibmcloud.com/collection/18f373debc38779065a26f1958dc260b>
- <https://www.straitstimes.com/tech/wuhan-virus-hackers-exploiting-fear-of-bug-to-target-computers-gadgets>
- <https://threatpost.com/coronavirus-propagate-emotet/152404/>
- <https://www.wired.com/story/coronavirus-phishing-scams/>
- <https://www.csa.gov.sg/singcert/alerts/malicious-cyber-activities-leveraging-wuhan-coronavirus-situation>
- <https://www.kaspersky.co.za/blog/coronavirus-used-to-spread-malware-online/25570/>
- <https://www.bleepingcomputer.com/news/security/coronavirus-phishing-attacks-are-actively-targeting-the-us/>
- <https://blog.knowbe4.com/heads-up-scam-of-the-week-coronavirus-phishing-attacks-in-the-wild?nCOV-2019-bc-index>
- <https://www.bleepingcomputer.com/news/security/coronavirus-phishing-attacks-are-actively-targeting-the-us/>
- <https://www.itwire.com/security/criminals-use-coronavirus-fears-to-launch-%E2%80%98theft-malware%E2%80%99-says-analyst.html>
- <https://securitybrief.eu/story/cyber-criminals-exploiting-coronavirus-fears>

## Contextual Information

- <https://www.cdc.gov/coronavirus/index.html>

## Examples of phishing e-mails from the Coronavirus campaign

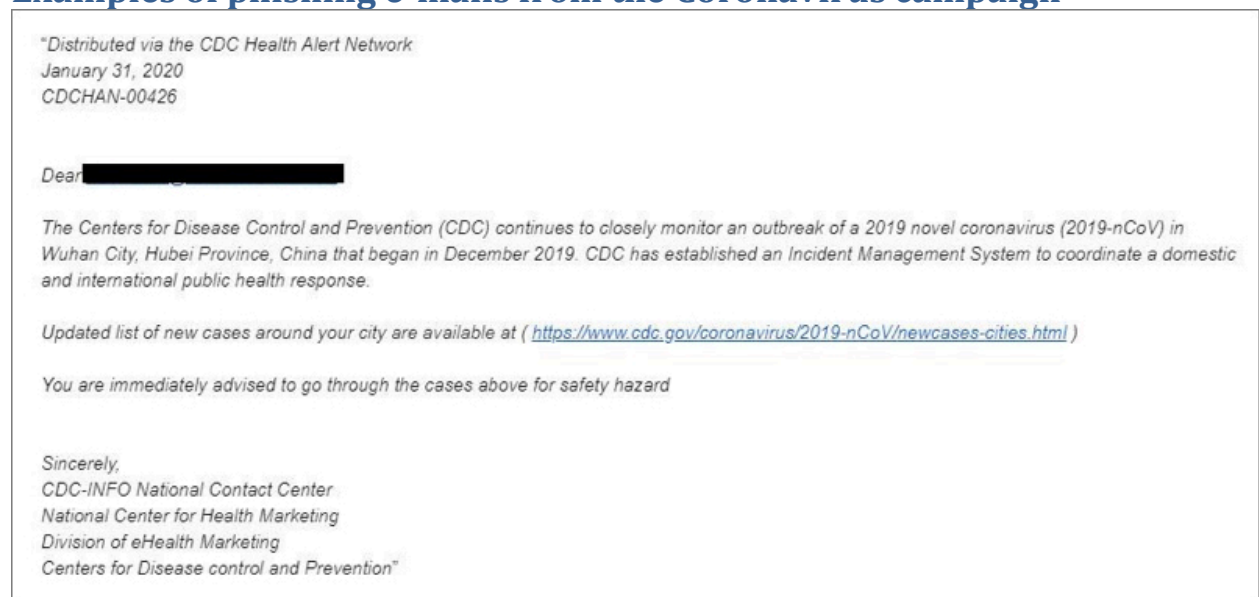


IMAGE SOURCE: <https://www.helpnetsecurity.com/2020/02/03/wuhan-coronavirus-exploited-to-deliver-malware-phishing-hoaxes/>

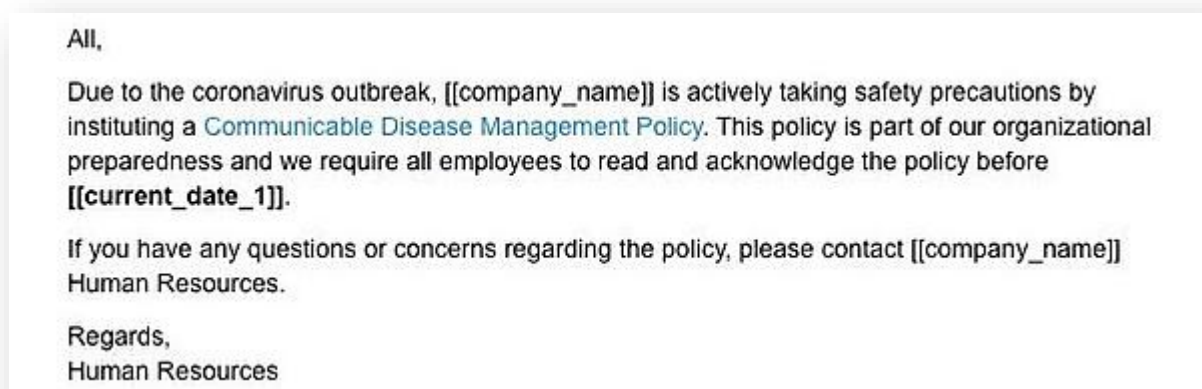


IMAGE SOURCE: <https://blog.knowbe4.com/heads-up-scam-of-the-week-coronavirus-phishing-attacks-in-the-wild?nCOV-2019-bc-index>

## Singapore Specialist : Corona Virus Safety Measures



Tuesday, 28 January 2020 at 03:51

[Show Details](#)

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus. This little measure can save you.

Use the link below to download

[Safety Measures.pdf](#)

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

Regards

Dr

Specialist wuhan-virus-advisory

IMAGE SOURCE: <https://www.wired.com/story/coronavirus-phishing-scams/>