Information Technology Services
http://www.lander.edu/its
help@lander.edu
864.388.8234

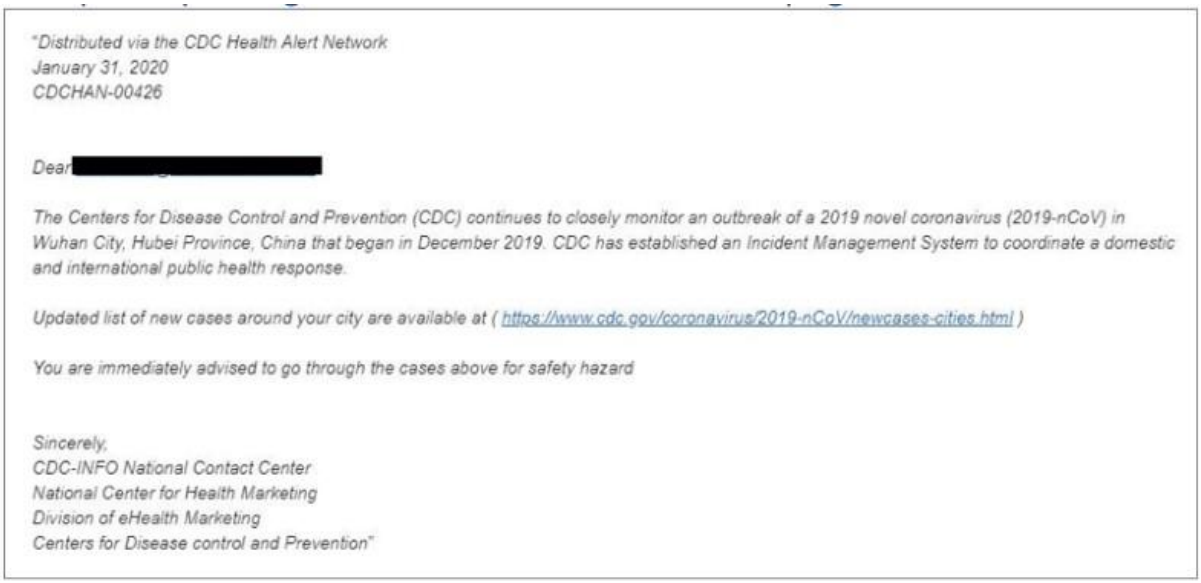
COVID-19 (Coronavirus) Phishing Emails

Due to the massive amount of news coverage surrounding COVID-19, a new danger has emerged: phishing attacks attempting to exploit public fears about the virus. Cybercriminals are sending emails that claim to be from legitimate organizations with critical information on COVID-19. The email may ask you to open an attachment to see statistics on how the virus is spreading. Clicking on the link, however, may download some form of malware on your computer. The malware could then allow cybercriminals to take control of your system, log your keystrokes, or access personal and financial information.

How to spot a COVID-19 phishing email

COVID-19 phishing emails can take on many different forms, including (but not limited to) these:

- CDC Alerts
  - Cybercriminals send phishing emails impersonating officials from the US Center for Disease Control (CDC)
  - The email may falsely claim to link to a list of coronavirus cases in your area



"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"

Figure 1: Example of a fake CDC email

- Health advice emails
  - Cybercriminals send emails that offer supposed medical advice to help protect against COVID-19
  - The email may claim to be from medical experts near Wuhan, China, where the outbreak began
  - The email may have an attachment that claims to be a PDF or text document containing health advice, but will more likely be a form of malware

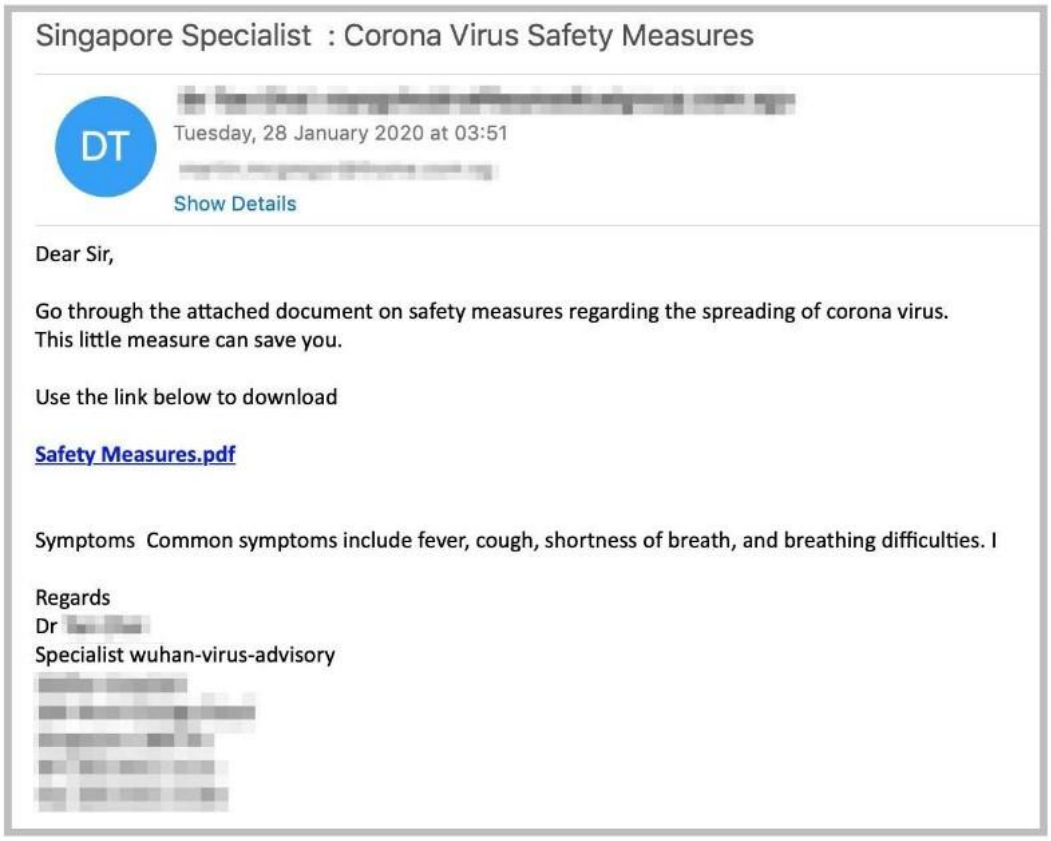


Figure 2: Example of fake health advice email

- Workplace policy emails
  - Cybercriminals target workplace email accounts urging users to click on a link to fake company policy information regarding COVID-19
  - Like the fake health advice email, the email may urge an individual to review an attached file, which may be malware

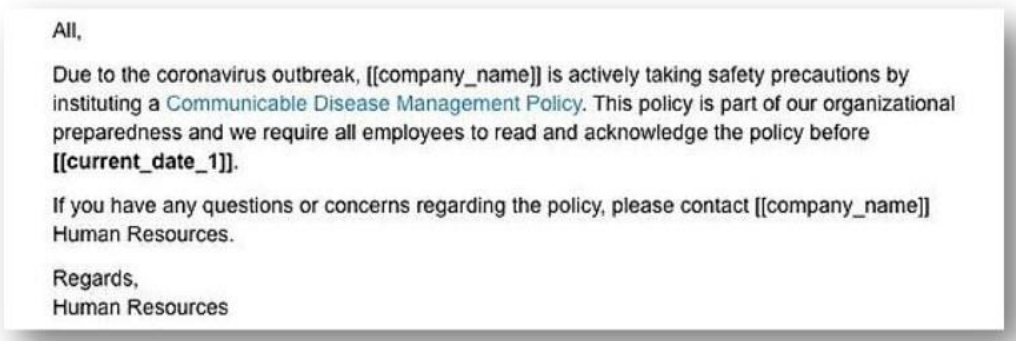


Figure 3: Example of fake workplace policy email

Recognizing and avoiding phishing emails

Here are some ways to recognize and avoid COVID-19 themed phishing emails. Like other phishing attacks, the messages usually try to get an individual to click on a link or provide personal information that can be used to commit fraud or identity theft. Here are some tips to avoid getting scammed.

- Be wary of requests for personal information
    - This information can be used by cybercriminals to steal your identity or commit fraud. Legitimate organizations will never ask for that information.
- Check that the email address of the sender is correct
    - Phishing emails often come from cybercriminals impersonating someone else. Check that their name and email address are correct
- Check that hyperlinks lead to the correct website
    - This can be done by hovering over the link and verifying the address that pops up
- Watch for spelling and grammatical mistakes
    - If an email contains several spelling or grammar mistakes, it's likely that it is a phishing email
- Look for generic greetings
    - Phishing emails are not likely to use your name. Look for greetings like "Dear sir or madam" or "Greetings, valued customer"
- Avoid emails that urge immediate action
    - Phishing emails attempt to manufacture a sense of urgency in hopes that you aren't watching carefully