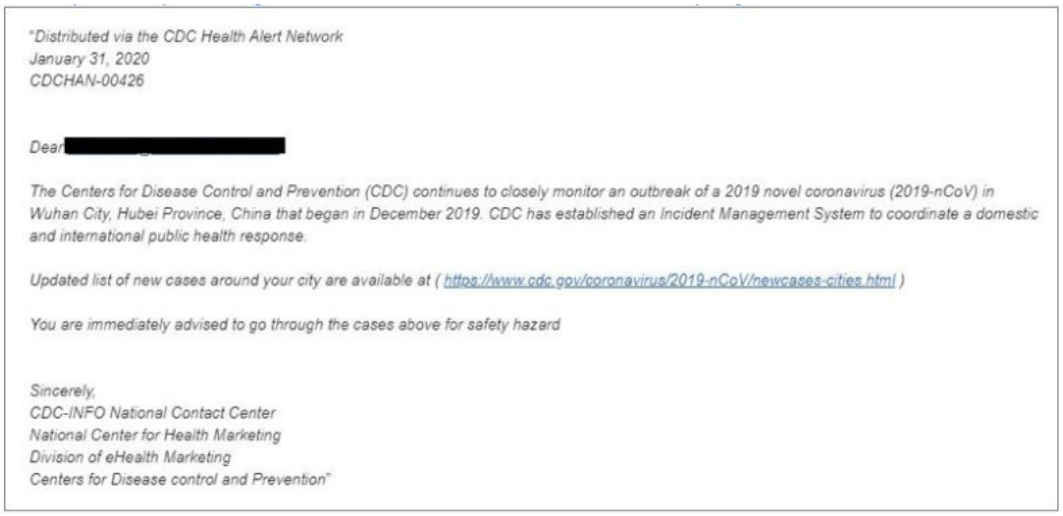
COVID-19: Beware of Phishing Scams & Fake Ads

COVID-19 news coverage has created a new danger: phishing attacks looking to exploit public fears. Scams and fake ads abound with messages claiming to be from prestigious medical organizations, announcing new medical policy, or even selling the latest "wonder drug." With so many criminals working so hard to get your information, it may feel overwhelming. Fear not, because we have examples of the latest scams and easy ways to identify fake ads to help keep you and yours safe.

How do I spot a coronavirus phishing email?

Coronavirus-themed phishing emails can take different forms, including these:

- **CDC ALERTS:** Cybercriminals have sent phishing emails designed to look like they are from the U.S. Centers for Disease Control. The email might falsely claim to link to a list of coronavirus cases in your area. "You are immediately advised to go through the cases above for safety hazard," the text of one phishing email reads.



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

Dear [redacted]

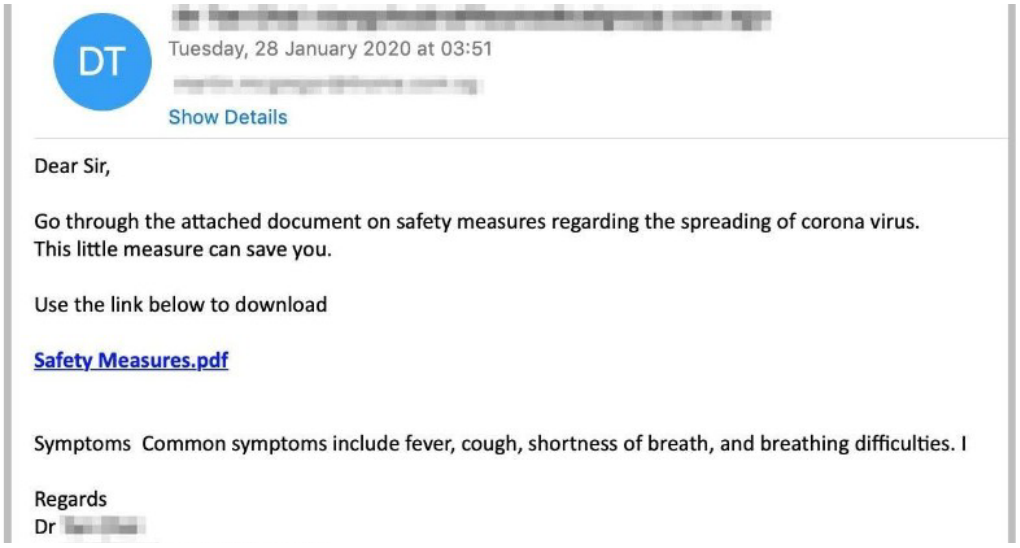
The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health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

- **HEALTH ADVICE EMAILS:** Phishers have sent emails offering "medical advice" to help protect you against the coronavirus. The emails might claim to be from medical experts near Wuhan, China, where the coronavirus outbreak began. "This little measure can save you," one phishing email says. "Use the link below to download Safety Measures."



DT

[redacted]

Tuesday, 28 January 2020 at 03:51

[redacted]

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

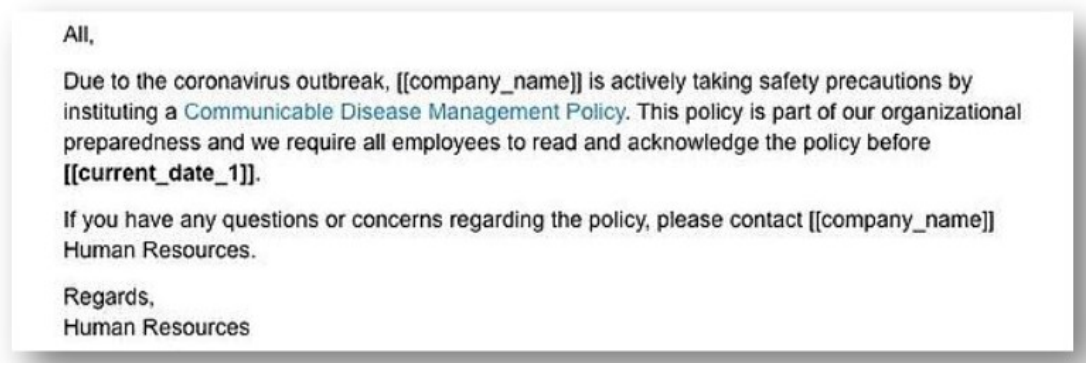
Safety Measures.pdf

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

Regards
Dr [redacted]

Source: https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html

- **WORKPLACE POLICY EMAILS:** Cybercriminals have targeted employees' workplace email accounts. One phishing email begins, "All, Due to the coronavirus outbreak, [company name] is actively taking safety precautions by instituting a Communicable Disease Management Policy." If you click on the fake company policy, you'll download malicious software.



All,

Due to the coronavirus outbreak, [[company_name]] is actively taking safety precautions by instituting a Communicable Disease Management Policy. This policy is part of our organizational preparedness and we require all employees to read and acknowledge the policy before **[[current_date_1]]**.

If you have any questions or concerns regarding the policy, please contact [[company_name]] Human Resources.

Regards,
Human Resources

How do I avoid scammers and fake ads?

Scammers have posted ads that claim to offer treatment or cures for the coronavirus. The ads often try to create a sense of urgency — for instance, "Buy now, limited supply."

At least two bad things could happen if you respond to the ads. One, you might click on an ad and download malware onto your device. Two, you might buy the product and receive something useless, or nothing at all. Meanwhile, you may have shared personal information such as your name, address, and credit card number. Bottom line? It is smart to avoid any ads seeking to capitalize on the coronavirus.

How can I recognize and avoid phishing emails?

Here are some ways to recognize and avoid coronavirus-themed phishing emails trying to lure you into clicking on a link or providing personal information to be used to commit fraud or identity theft. Here are some tips to avoid getting tricked.

- Beware of online requests for personal information. A coronavirus-themed email that seeks personal information like your Social Security number or login information is a phishing scam. Legitimate government agencies won't ask for that information. Never respond to the email with your personal data.
- Check the email address or link. You can inspect a link by hovering your mouse button over the URL to see where it leads. Sometimes, it's obvious the web address is not legitimate. But keep in mind phishers can create links that closely resemble legitimate addresses. Delete the email.
- Watch for spelling and grammatical mistakes. If an email includes spelling, punctuation, and grammar errors, it's likely a sign you've received a phishing email. Delete it.
- Look for generic greetings. Phishing emails are unlikely to use your name. Greetings like "Dear sir or madam" signal an email is not legitimate.
- Avoid emails that insist you act now. Phishing emails often try to create a sense of urgency or demand immediate action. The goal is to get you to click on a link and provide personal information — right now. Instead, delete the message.

Source: https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html