Tips for Keeping Information Secure during COVID-19

How can you stay secure?

1. **Make sure to use #secure when dealing with any sensitive information in emails.** If you must send an email that includes sensitive information (PII, Payment Information, Medical Information) make sure to encrypt it by typing *#secure* anywhere within the body of the email. Even if the email was sent to you with sensitive information in it, make sure to encrypt it when you send a response.

2. **Verify the sender by checking their email address.** Make sure the email address matches the one you have on file. Attackers like to copy names, so verify the address is exactly what it is supposed to be. If you know the sender, or do business with them, reach out using the contact information you have on file for them to confirm they sent that email.

3. **Think before you click!** First, ask yourself if this is an email you should receive. Next, ask yourself if this is something you need to open. Whether it is a link or an attachment, ask yourself if it is something that you have to open for a job function. If something seems too good be true, it probably is going to be.

4. **Be careful when providing personal information.** Always consider why someone wants information and if it is appropriate. You will never need to use your email and password to access news information on the pandemic.

5. **Only use verified sources for information.** If the email is not a Company or Agency communication, go out and get the information yourself. If you are looking for news, do not open attachments or click on links that you receive. Search and visit the news sites yourself, and eliminate the risk of clicking a bad link.

6. **Do not rush or feel under pressure.** Cybercriminals use emergencies, such as COVID-19, to get people to make decisions quickly. Always take time to think about a request for your personal information, and whether the request is appropriate.

What do these emails look like?

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

CDC alerts. Cybercriminals have sent phishing emails designed to look like they are from the U.S. Center 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.

Note: The example below was submitted within Pekin Insurance. They are trying to get you to give up your email and password for information on the virus.

Office 365 ***Coronavirus Review***

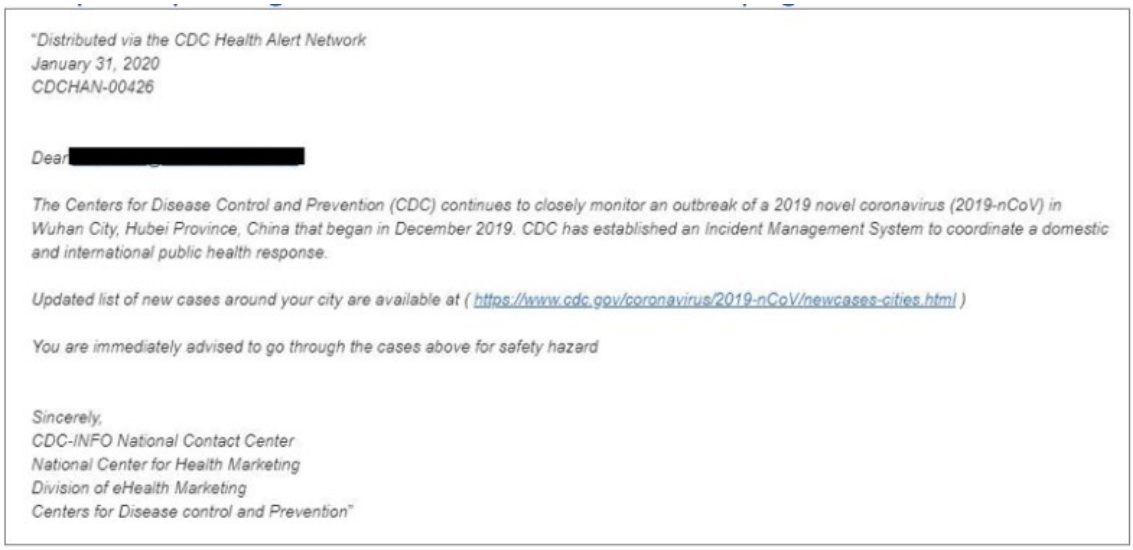
Recent Update on Coronavirus disease (COVID-19)
COVID-19 ID: #NIPH

CASE ID: Coronavirus
EMMERGENCY NO: 911 - 112
EMAIL ID: EDCARN@ who.int

REVIEW NOW;:

Review on how to recover from covid-19.

Next, here's an example of a fake CDC email. (The following examples all come from the U.S. Health and Human Services website.)



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

Dear [redacted]

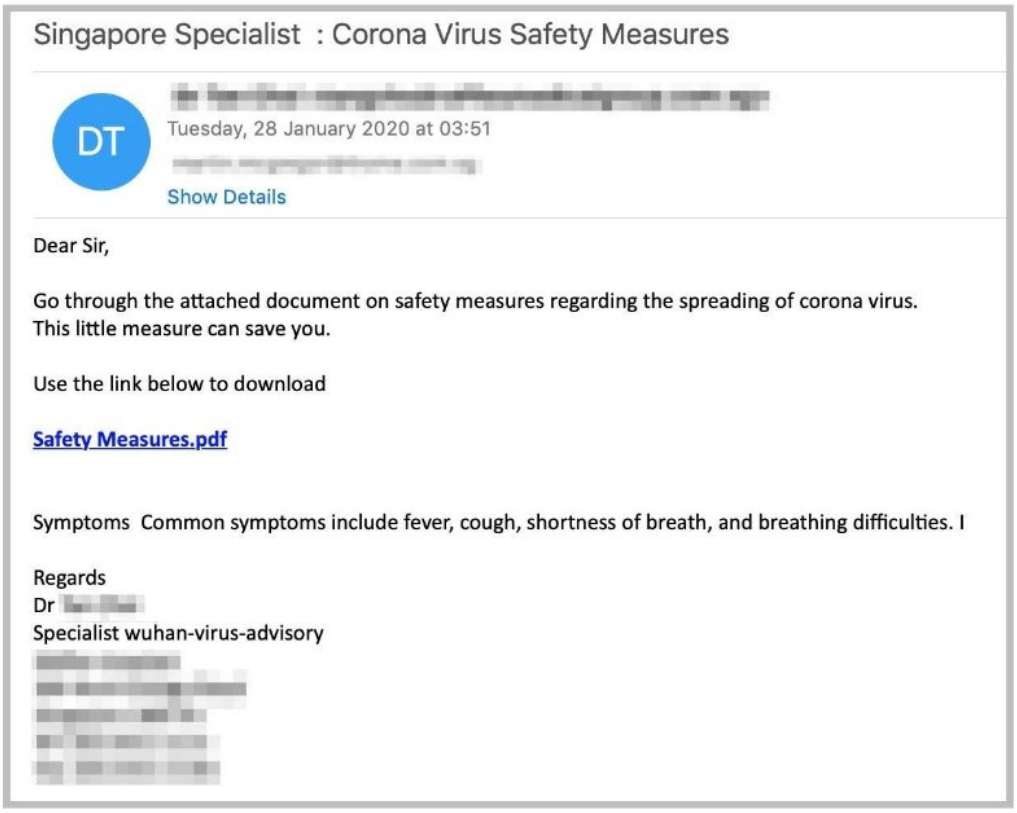
The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health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



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.

Here's an example: