

1. Click here for a cure

The screenshot shows an email interface with a blue header bar containing the text "Confidential Cure Solution on Corona virus - Temporary Items" and "Message". Below the header, the email title "Confidential Cure Solution on Corona virus" is displayed. The sender is identified as "CG" with a circular profile picture, and the timestamp is "Tuesday, February 4, 2020 at 10:10 AM". A "Show Details" link is visible below the sender information.

The main body of the email contains the following text:

Corona virus prevention vaccine and cure medication has been secretly developed by our medical scientist who's names are meant to remain silent for security reasons. We know that the world has been struggling to contain this deadly virus developed and sprayed by wicked scientists to reduce the population of the world so the government will have control over you. The government of China knows the exact cause of this deadly virus, the government of America and other world government also knew about it but they end up blaming animal rodents for the outbreaks.

This corona virus is a weapon created to discredit rivals government health systems or the other way to control the citizens of the world but due to some people like us and our medical teams hate the injustice going in this world. Our secret medical scientist team has developed the cure and prevention to counter this evil act of the world to save lives of innocent people around the world. For those interested to secure their lives kindly reply and get more information about shipping or delivery to you and private distribution.

Below the text is a blue rectangular box with a white icon of a document and a pencil. The text inside the box reads: "Dr. Carlos Gerrado sent you a free health guideline". At the bottom of the box is a yellow button with the text "Click for Corona-Virus Cure Review".

Below the blue box, there is a blurred signature area and the text "Thank You,". In the bottom right corner of the email content area, the word "PROOFPOINT" is visible in a grey box.

A black banner at the bottom of the screenshot contains the text: "Victims looking for a cure face having personal details stolen".

Researchers at the cyber-security firm Proofpoint first noticed a strange email being sent to customers in February. The message purported to be from a mysterious doctor claiming to have details about a vaccine being covered up by the Chinese and UK governments.

The firm says people who click on the attached document are taken to a spoof webpage designed to harvest login details. It says up to 200,000 of the emails are being sent at a time.

"We have seen 35-plus consecutive days of malicious coronavirus email campaigns, with many using fear to convince victims to click," says Sherrod DeGrippe from the company's threat research and detection team.


Proofpoint says three to four variations are launched each day.


"It's obvious these campaigns are returning dividends for cyber-criminals," says Ms DeGrippe.

The best way to see where a link will take you is to hover your mouse cursor over it to reveal the true web address. If it looks dodgy, don't click.

2. Covid-19 tax refund

New programme against COVID-19

 <GOV UK Notify>



The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a *tax refund (rebate)* of 128.34 GBP.

[Access your funds now](#)

The funds can be used to protect yourself against COVID-19(<https://www.nhs.uk/conditions/coronavirus-covid-19/> precautionary measure against corona)

At 6.15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

MIMECAST

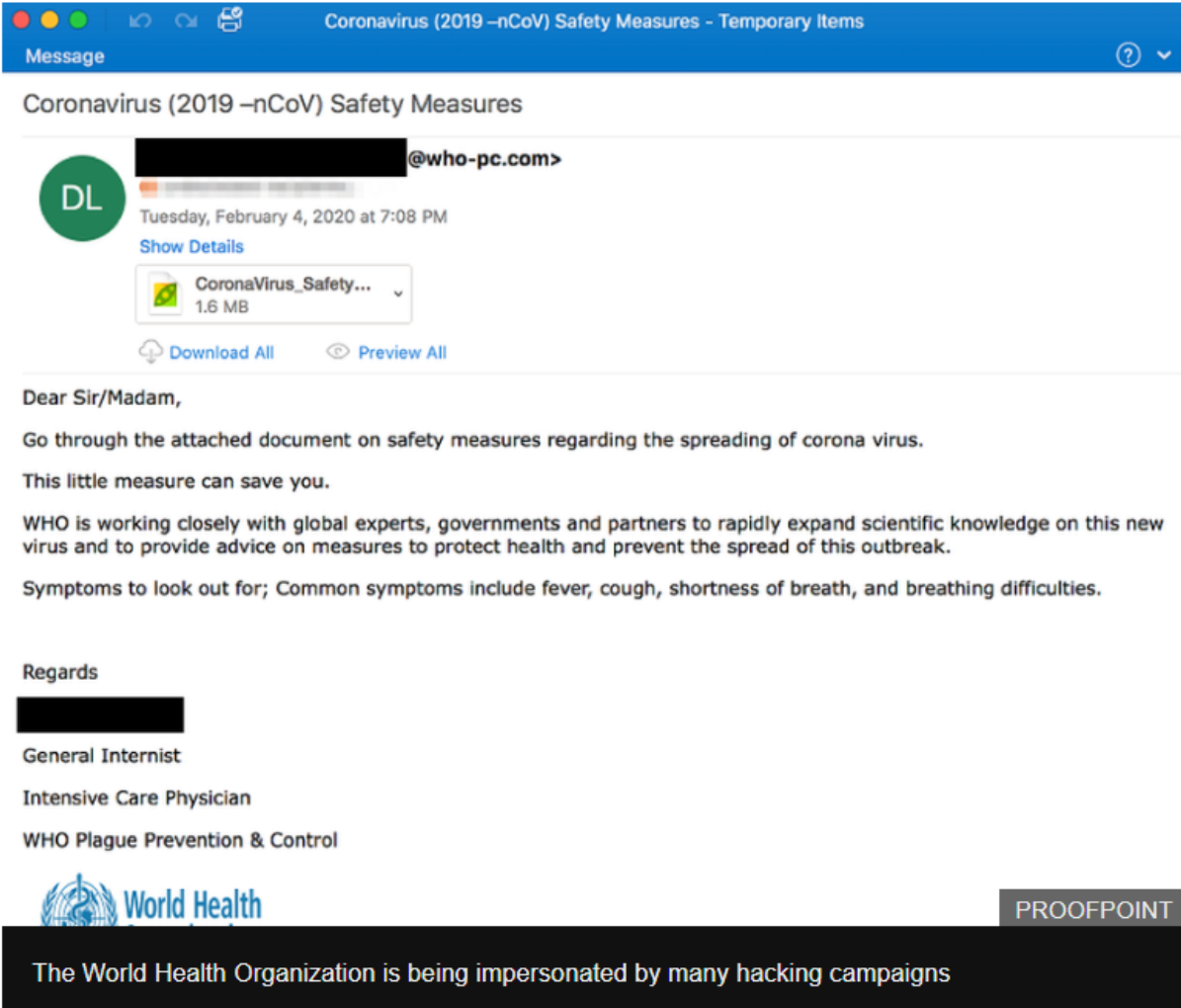
HM Revenue and Customs is not trying to give you a Covid-19 tax rebate

Researchers at cyber-security firm Mimecast flagged this scam a few weeks ago. On the morning they detected it, they saw more than 200 examples in just a few hours.

If a member of the public clicked on "access your funds now", it would take them to a fake government webpage, encouraging them to input all their financial and tax information.

"Do not respond to any electronic communication in relation to monies via email," says Carl Wearn, head of e-crime at Mimecast. "And certainly do not click on any links in any related message. This is not how HMRC would advise you of a potential tax refund."

3. Little measure that saves



The screenshot shows an email interface with a blue header bar. The subject line is "Coronavirus (2019 -nCoV) Safety Measures - Temporary Items". The sender is a contact with a green circular profile picture containing the letters "DL" and an email address starting with "@who-pc.com". The email is dated "Tuesday, February 4, 2020 at 7:08 PM" and includes a "Show Details" link. An attachment is visible: "CoronaVirus_Safety..." (1.6 MB). Below the attachment are "Download All" and "Preview All" options. The email body contains the following text:

Dear Sir/Madam,

Go through the attached document on safety measures regarding the spreading of corona virus.

This little measure can save you.


WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

[Redacted Name]

General Internist
Intensive Care Physician
WHO Plague Prevention & Control

 **World Health**

PROOFPOINT

The World Health Organization is being impersonated by many hacking campaigns

Hackers pretending to represent the World Health Organization (WHO) claim that an attached document details how recipients can prevent the disease's spread.

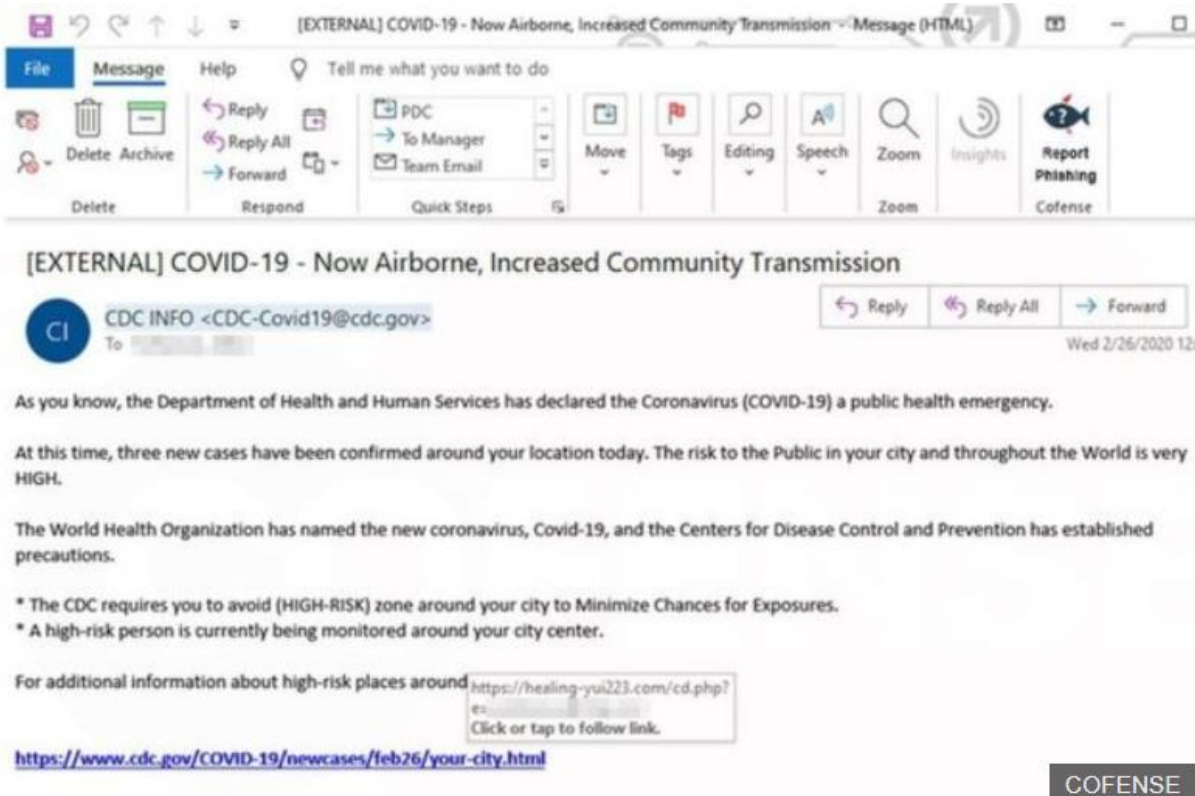
"This little measure can save you," they claim.

But Proofpoint says the attachment doesn't contain any useful advice, and instead infects computers with malicious software called AgentTesla Keylogger.

This records every keystroke and sends it to the attackers, a tactic that allows them to monitor their victims' every move online.

To avoid this scam, be wary of emails claiming to be from WHO, as they are probably fake. Instead visit its official website or social media channels for the latest advice.

4. The virus is now airborne



Hackers are using fear-mongering tactics to encourage clicks and downloads

The subject line reads: Covid-19 - now airborne, increased community transmission.

It is designed to look like it's from the Centres for Disease Control and Prevention (CDC). It uses one of the organisation's legitimate email addresses, but has in fact been sent via a spoofing tool.

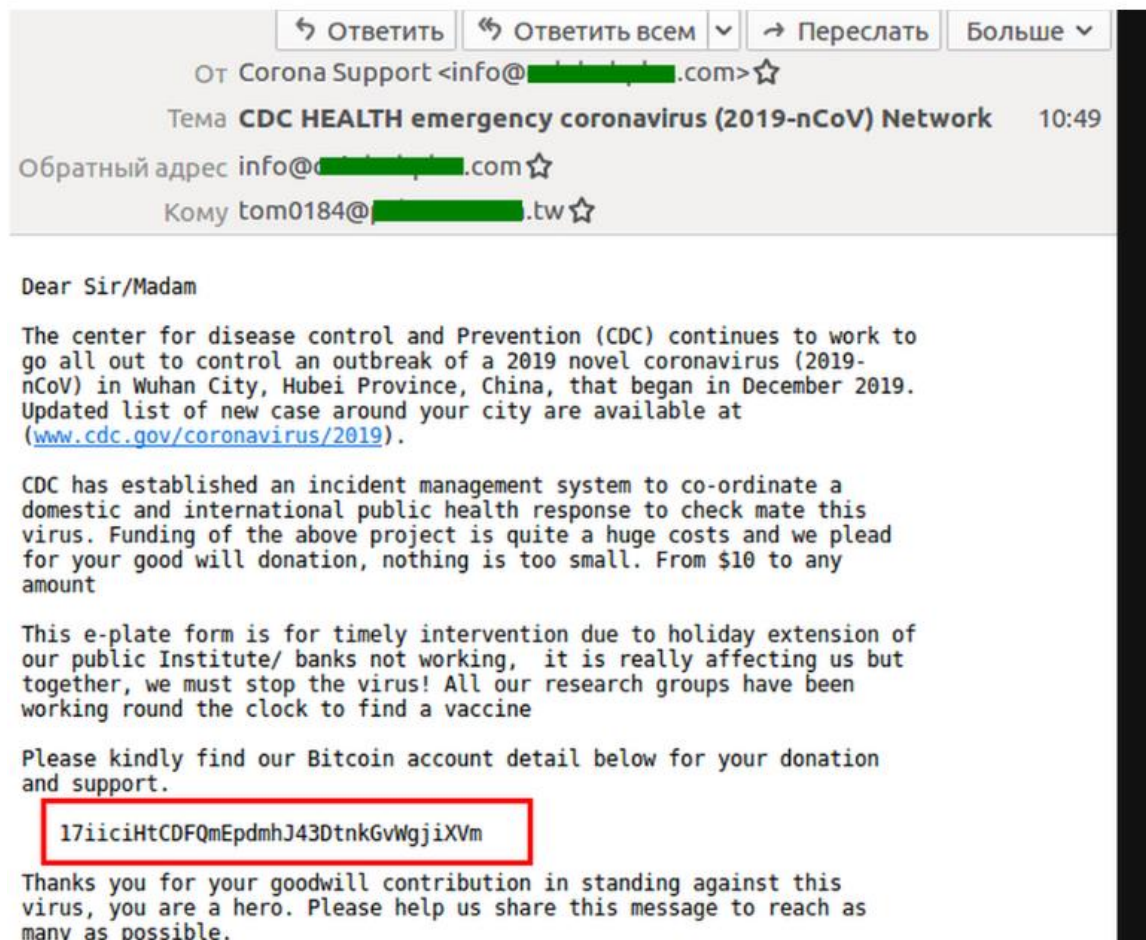
Cofense, the cyber-defence provider, first detected the scam and describes it as an example of hackers "weaponising fear and panic".

It says the link directs victims to a fake Microsoft login page, where people are encouraged to enter their email and password. Then victims are redirected to the real CDC advice page, making it seem even more authentic. Of course, the hackers now have control of the email account.

Cofense says the combination of a "rather good forgery" and a "high stress situation" make for a potent trap.

One way to protect yourself is to enable two-factor authentication, so that you have to enter a code texted or otherwise provided to you, to access your email account.

5. Donate here to help the fight



От Corona Support <info@[redacted].com> ☆

Тема **CDC HEALTH emergency coronavirus (2019-nCoV) Network** 10:49

Обратный адрес info@[redacted].com ☆

Кому tom0184@[redacted].tw ☆

Dear Sir/Madam

The center for disease control and Prevention (CDC) continues to work to go all out to control an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China, that began in December 2019. Updated list of new case around your city are available at (www.cdc.gov/coronavirus/2019).

CDC has established an incident management system to co-ordinate a domestic and international public health response to check mate this virus. Funding of the above project is quite a huge costs and we plead for your good will donation, nothing is too small. From \$10 to any amount

This e-plate form is for timely intervention due to holiday extension of our public Institute/ banks not working, it is really affecting us but together, we must stop the virus! All our research groups have been working round the clock to find a vaccine

Please kindly find our Bitcoin account detail below for your donation and support.

17iiciHtCDFQmEpdmhJ43DtnkGvWgjiXVm

Thanks you for your goodwill contribution in standing against this virus, you are a hero. Please help us share this message to reach as many as possible.

This example was reported to malware experts Kaspersky. The fake CDC email asks for donations to develop a vaccine, and requests payments be made in the cryptocurrency Bitcoin.

The premise is of course ridiculous, but the email address and signature look convincing.

Overall, Kaspersky says it has detected more 513 different files with coronavirus in their title, which contain malware.

"We expect the numbers to grow, of course, as the real virus continues to spread," says David Emm, principal security researcher at the firm.