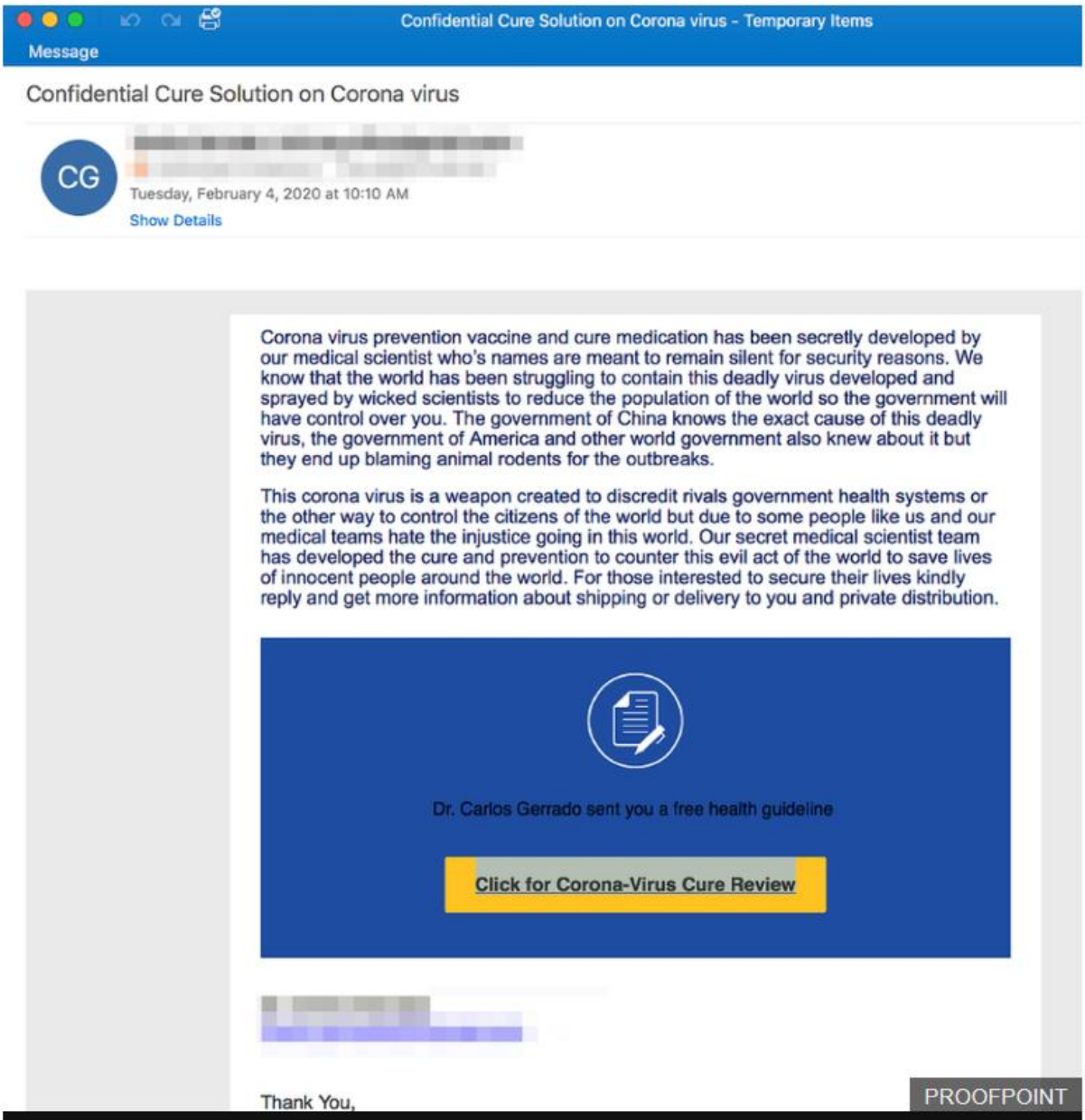
1. Click here for a cure



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.

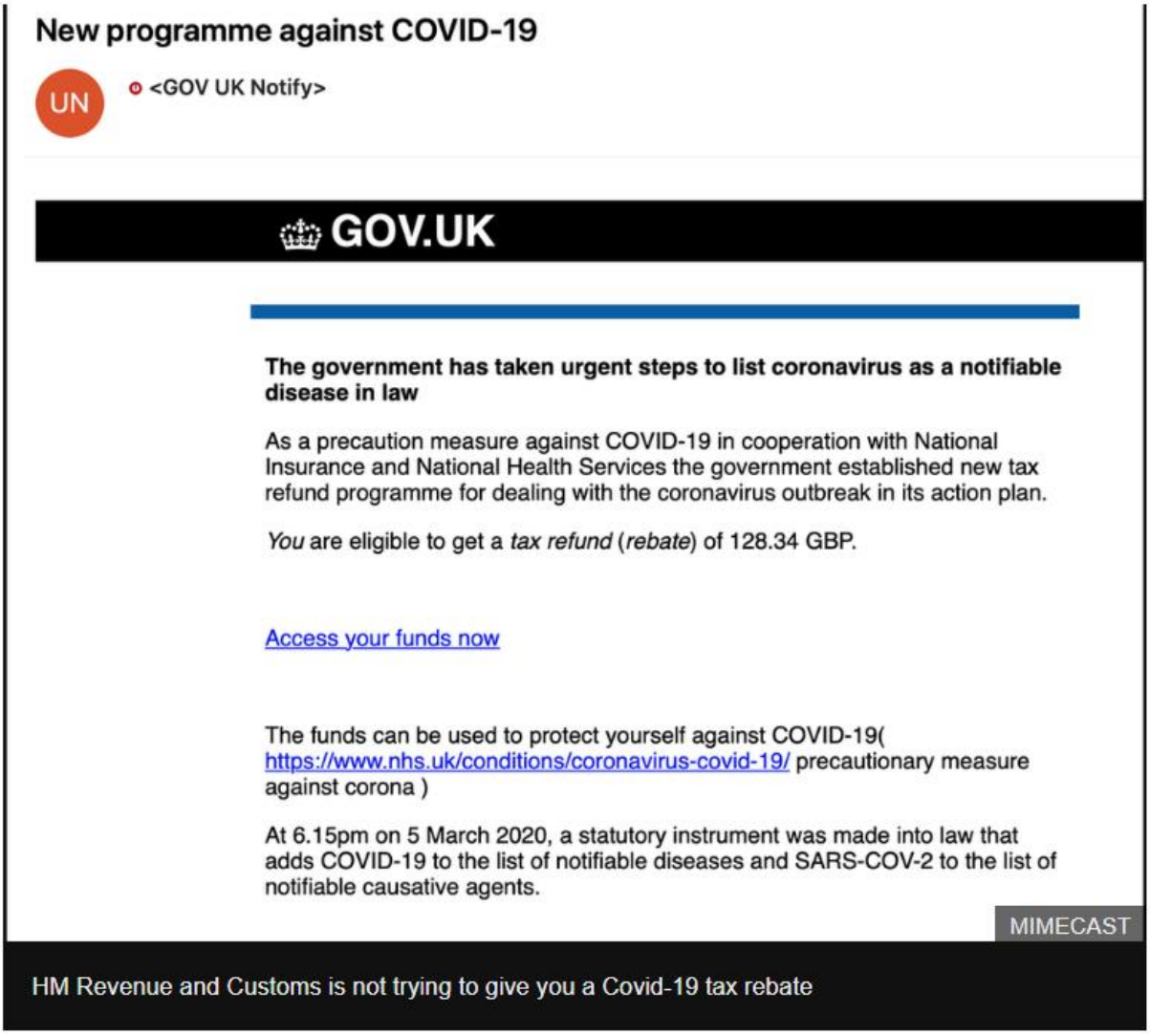
"We have seen 35-plus consecutive days of malicious coronavirus email campaigns, with many using fear to convince victims to click," says Sherrod DeGrippo from the company's threat research and detection team.

Proofpoint says three to four variations are launched each day.

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

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



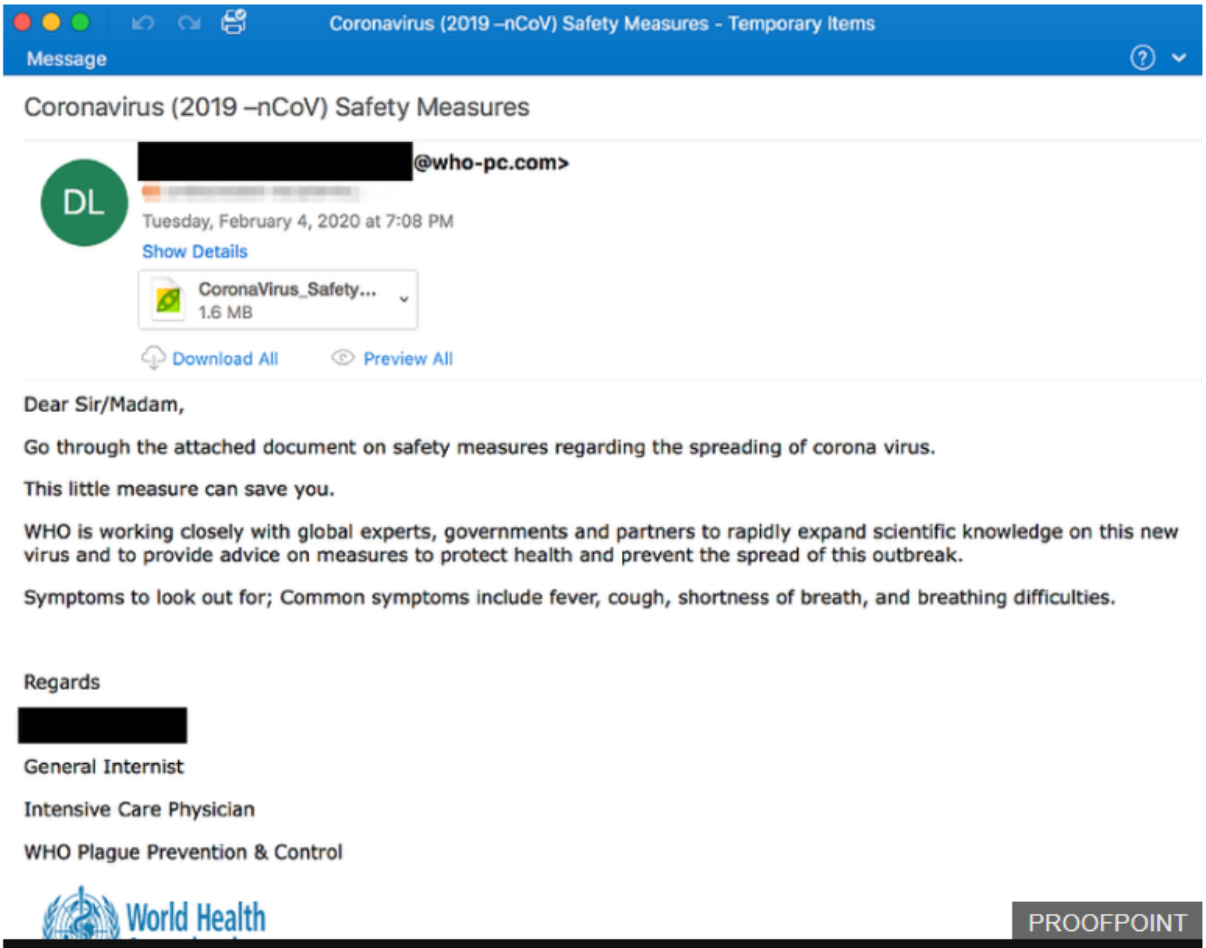
HM Revenue and Customs is not trying to give you a Covid-19 tax rebate

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 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.

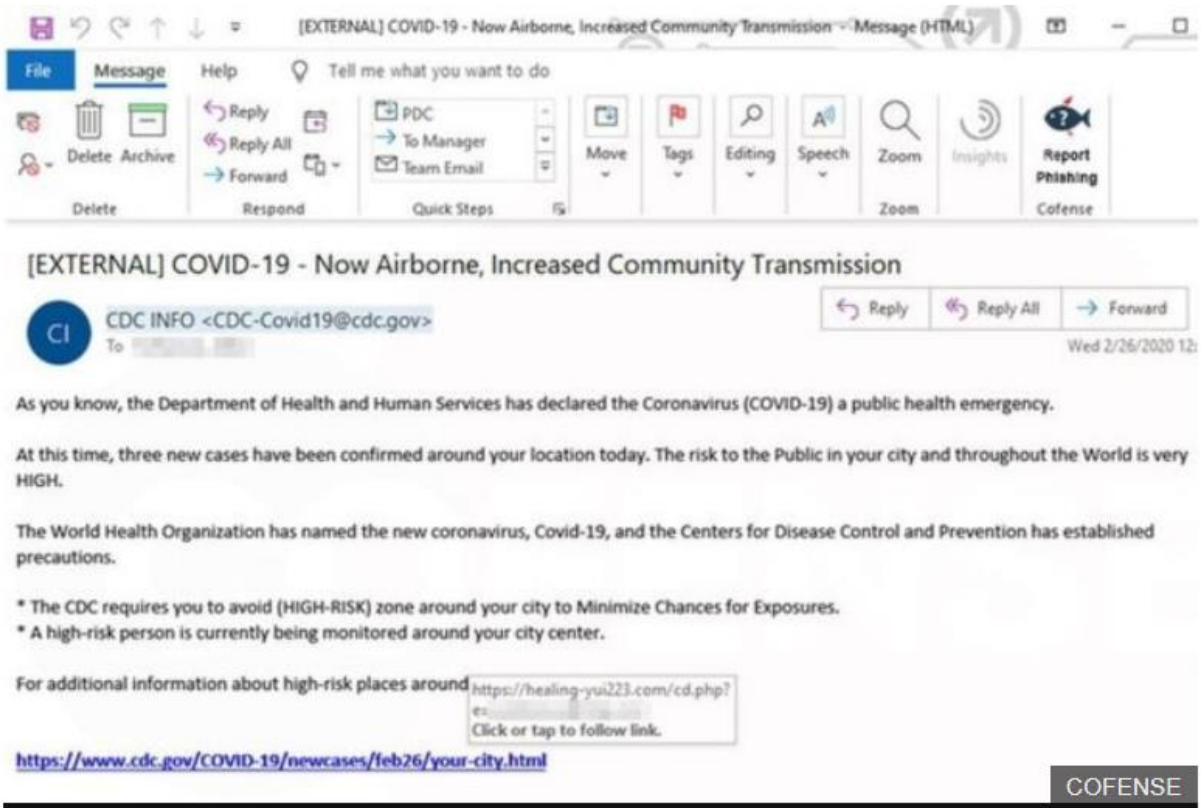
"This little measure can save you," they claim.

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 encourge 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.

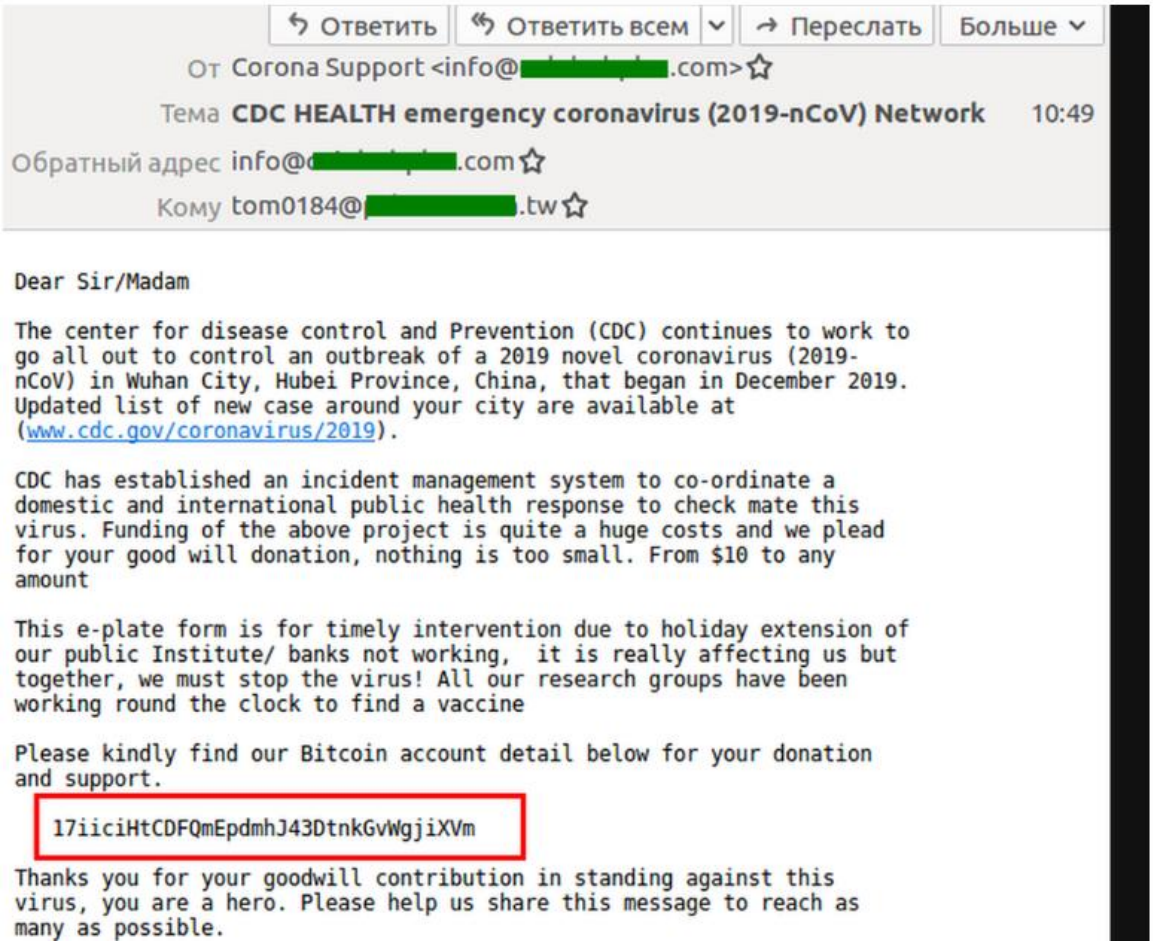
Cofense, the cyber-defence provider, first detected the scam and describes it as an example of hackers "weaponising fear and panic".

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



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.