Hackers use COVID-19 in scam tactics

As concern around the Coronavirus grows, hackers are targeting mailboxes to try and catch businesses and individuals out with their usual tricks, using COVID-19 to lure people in. We know that these types of emails are not always easy to spot, so we have identified a few examples to share with you. This article should help increase your awareness of what to keep an eye out for, so you won't be a victim of these malicious campaigns.

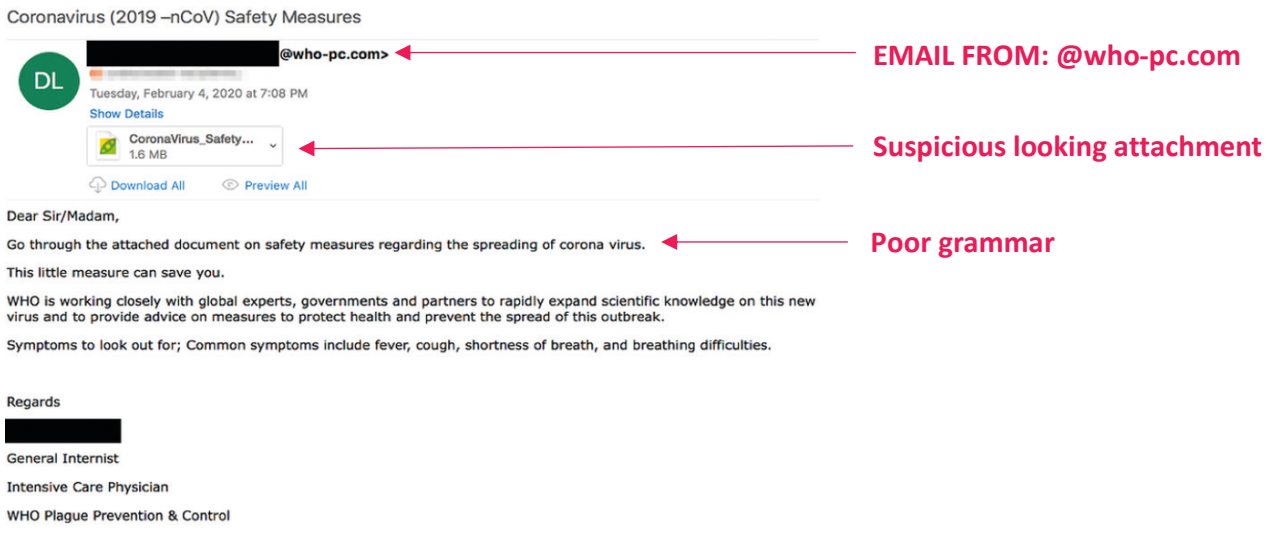
STICK TO THE FOLLOWING TIPS TO ENSURE THAT YOU DON'T GET CAUGHT OUT:

1. Look out for poor grammar or spelling mistakes.
2. Never click on the links or open any attachments from emails you are not expecting.
3. Check the sender – does it look legitimate?
4. Don't forward the emails to anyone, instead use the reporting button if you have that option on your email platform.
5. Are you being asked to verify your bank details? Be wary of this.
6. Does it use your full name? Phishing emails usually use terms like 'Dear Customer' as they don't have your personal details.
7. Does it use an attention-grabbing subject header? Look for phrases like "you've won!", "forward this to everyone you know!" or "this is NOT a hoax!"

EXAMPLES OF MALICIOUS COVID-19 EMAILS

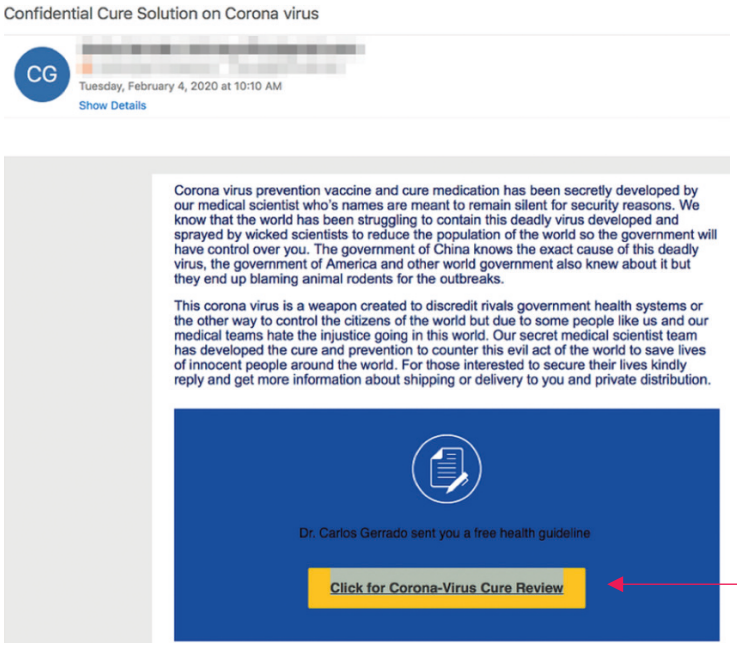
Example 1

On first glance, this email looks like it's been sent from a medical specialist, with an informative attachment providing safety tips. However, if you look closer, you can see that there several red flags such as poor grammar, the suspicious email address it's been sent from, and the attachment it's telling you to download.



Example 2

Using an enticing subject title to draw you in, at first it seems to be a free health-checker which in the current circumstances, you may be drawn to open. On closer inspection, the suspicious hyperlinks in the document and poor grammar should make you question whether the email is genuine, and in this case, it's not.



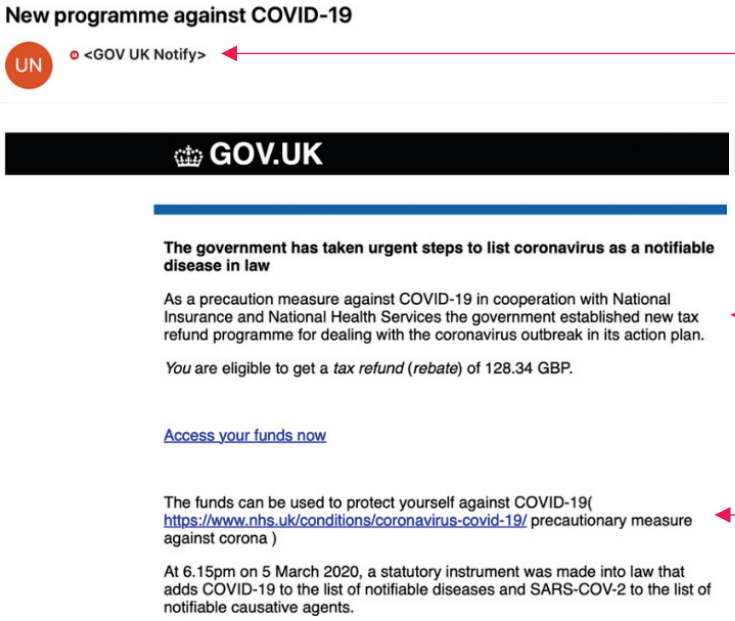
Poor grammar

Suspicious hyperlinks

Example 3

This appears to be a genuine email from the Government advising on a tax rebate. However, you can see that there are some details that don't add up; the hyperlink, poor grammar and strange content, as well as the lack of recipient address and suspect sender name.

This is a well-documented scam, you can read more about it here:
https://www.yourmoney.com/saving-banking/abhorrent-coronavirus-tax-rebate-scam-warning/



Suspicious sender name and missing recipient address

Poor grammar

Suspicious hyperlinks