STAYSMARTONLINE

ALERT SERVICE

Delivered by ACSC Australian Cyber Security Centre

27 March 2020

What’s happened?

The Australian Cyber Security Centre (ACSC) is aware of a significant increase in Australians being targeted with COVID-19 related scams and phishing emails.

In the last three months, the ACSC and the Australian Competition and the Consumer Commission’s (ACCC) Scamwatch has received over 140 reports from individuals and businesses across Australia.

These phishing emails are often sophisticated, preying on people’s desire for information and imitating trusted and well-known organisations or government agencies.

Clicking on these malicious links or visiting fake websites may automatically install computer viruses or malware and ransomware onto your device, giving cyber criminals the ability to steal your financial and personal information.

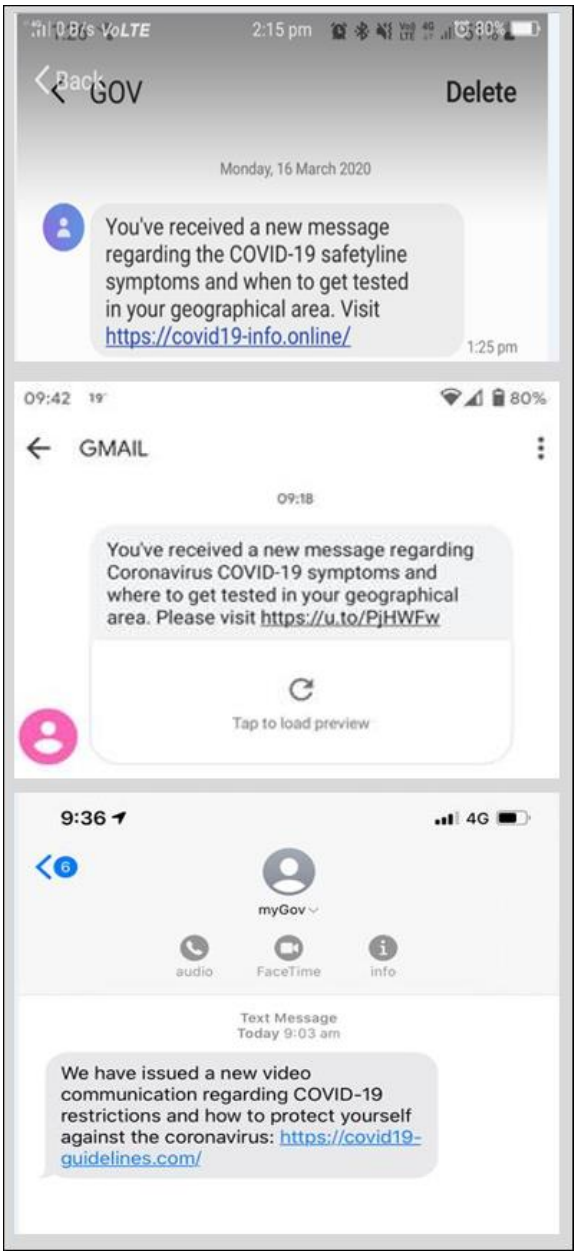
These scams are likely to increase over the coming weeks and months and the ACSC strongly encourages organisations and individuals to remain alert.

Here are some examples of what to look out for now:

Example 1: SMS phishing scam messages offering where to get tested for COVID-19 or how to protect yourself.

In these examples, the SMS appears to come from ‘GOV’ or ‘GMAIL’, with a malicious link to find out where to get tested in your local area.

Scamwatch and the ACSC is also aware of a SMS scam using the sender identification of ‘myGov.’ These scam messages are appearing in the same conversation threads as previous official SMS messages you may have received from myGov.



Monday, 16 March 2020

You've received a new message regarding the COVID-19 safetyline symptoms and when to get tested in your geographical area. Visit https://covid19-info.online/

1:25 pm

09:18

You've received a new message regarding Coronavirus COVID-19 symptoms and where to get tested in your geographical area. Please visit https://u.to/PjHWFw

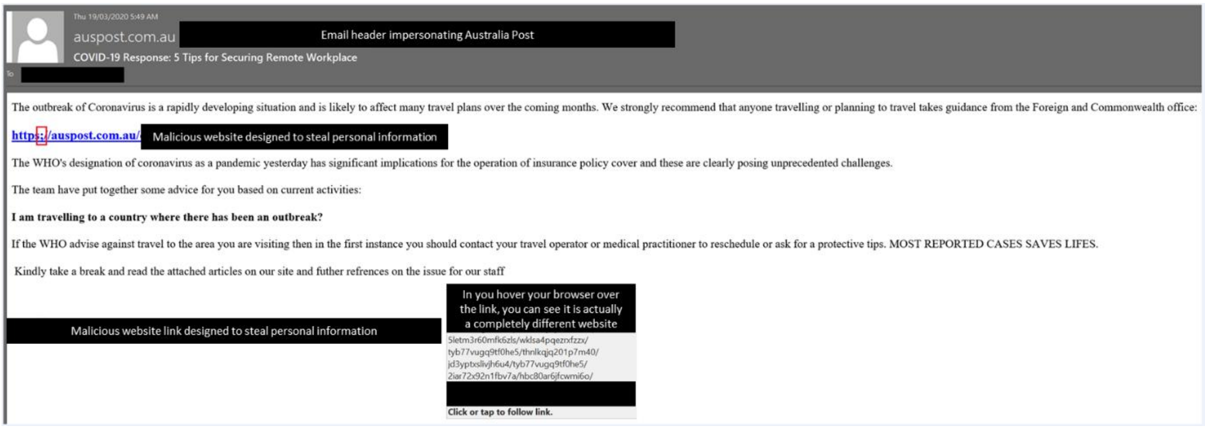
Text Message
Today 9:03 am

We have issued a new video communication regarding COVID-19 restrictions and how to protect yourself against the coronavirus: https://covid19-guidelines.com/

Example 2: COVID-19 phishing email impersonating Australia Post to steal personal information

Under the pretence of providing advice about travelling to countries with confirmed cases of COVID-19, this phishing email aims to trick you into visiting a website that will steal your personal and financial information.

Once they have your personal information, the scammers can open bank accounts or credit cards in your name, often using these stolen funds to purchase luxury items or transfer the money into untraceable crypto-currencies such as bitcoin.



Thu 19/03/2020 5:49 AM

auspost.com.au Email header impersonating Australia Post

COVID-19 Response: 5 Tips for Securing Remote Workplace

To [redacted]

The outbreak of Coronavirus is a rapidly developing situation and is likely to affect many travel plans over the coming months. We strongly recommend that anyone travelling or planning to travel takes guidance from the Foreign and Commonwealth office:

https://auspost.com.au/ Malicious website designed to steal personal information

The WHO's designation of coronavirus as a pandemic yesterday has significant implications for the operation of insurance policy cover and these are clearly posing unprecedented challenges.

The team have put together some advice for you based on current activities:

I am travelling to a country where there has been an outbreak?

If the WHO advise against travel to the area you are visiting then in the first instance you should contact your travel operator or medical practitioner to reschedule or ask for a protective tips. MOST REPORTED CASES SAVES LIFES.

Kindly take a break and read the attached articles on our site and futher refrences on the issue for our staff

Malicious website link designed to steal personal information

In you hover your browser over the link, you can see it is actually a completely different website

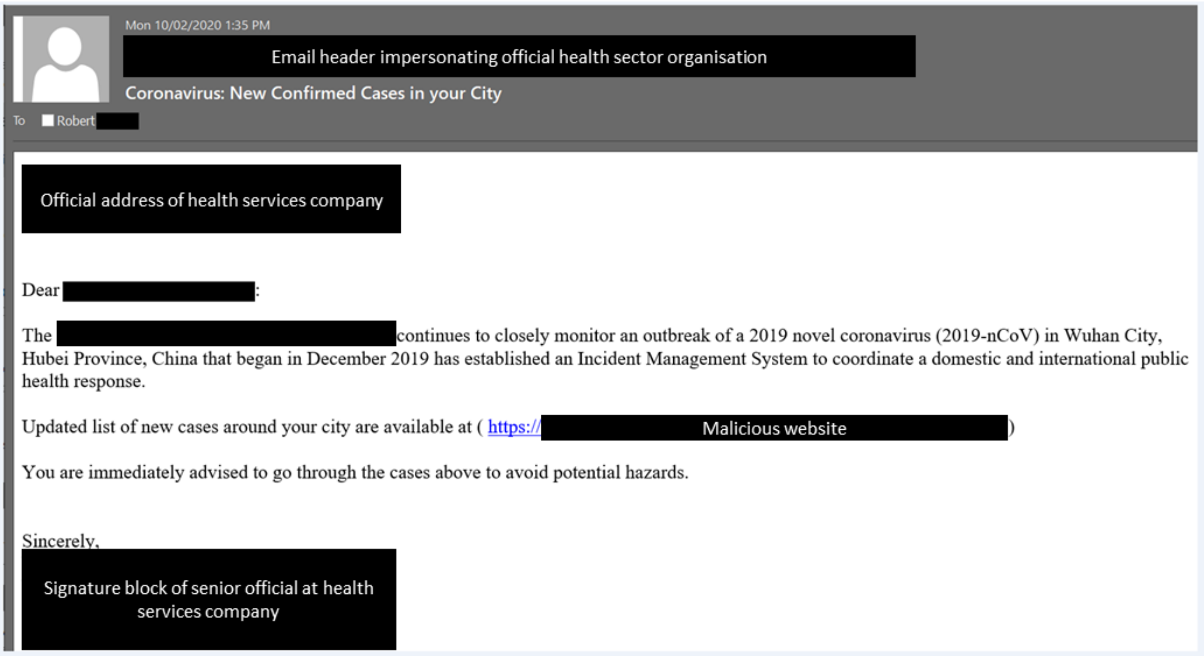
5letm3r60mfk6zls/wklsa4pqezrxfzzx/
tyb77vugq9tf0he5/thnlkqjq201p7m40/
jd3yptxslivjh6u4/tyb77vugq9tf0he5/
2iar72x92n1fbv7a/hbc80ar6jfcwmi6o/

[redacted]

Click or tap to follow link.

Example 3: Phishing emails pretending to be an international health sector organisation

This is an example of one COVID-19 themed phishing email where the sender is pretending to be a well-known international health organisation. The email prompts you to click on the web link to access information about new cases of the virus in your local area, or to open an attachment for advice on safety measures to prevent the spread.



Mon 10/02/2020 1:35 PM

Email header impersonating official health sector organisation

Coronavirus: New Confirmed Cases in your City

To Robert [redacted]

Official address of health services company

Dear [redacted]:

The [redacted] continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019 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:// Malicious website)

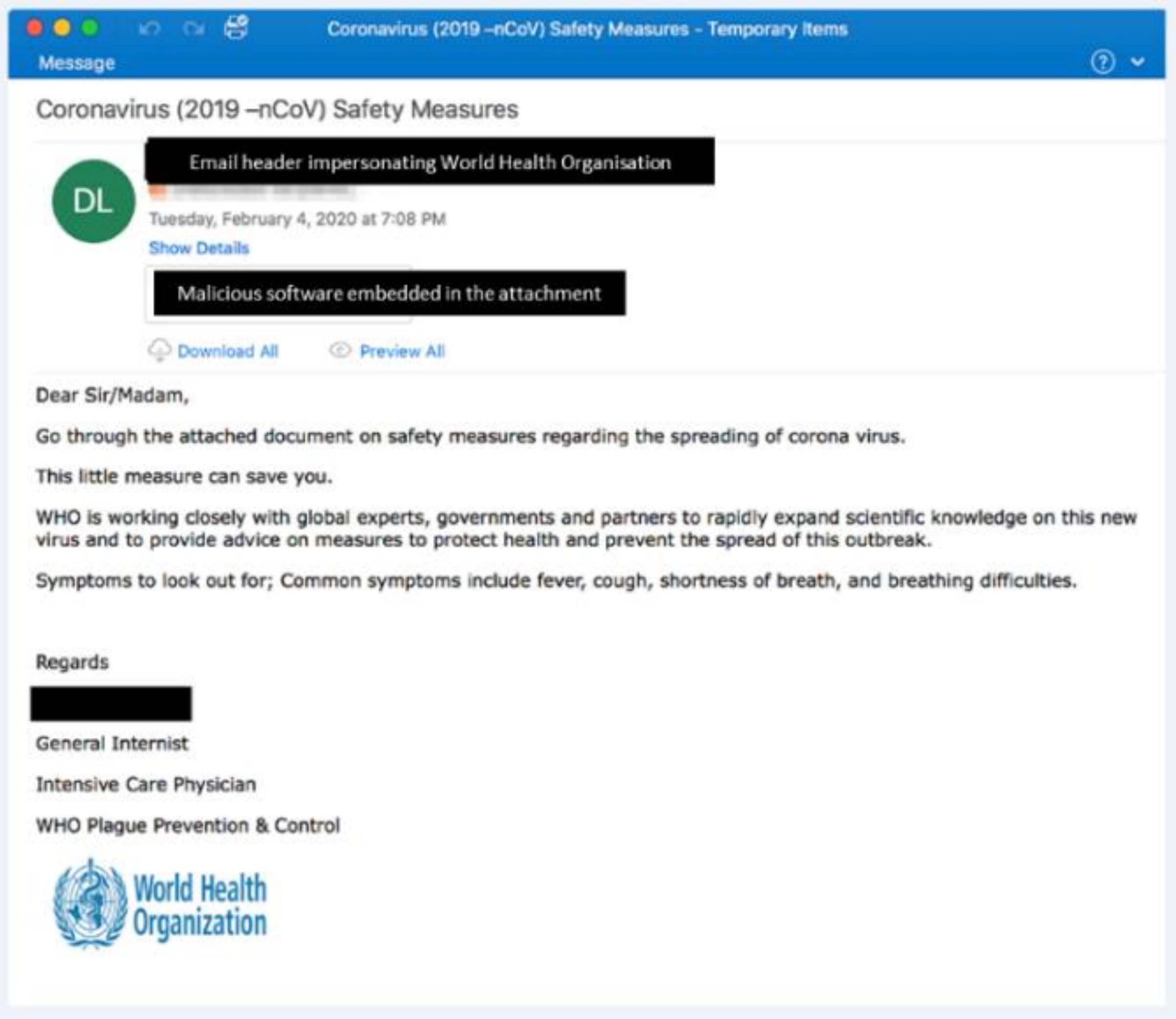
You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,

Signature block of senior official at health services company

Example 4: Phishing emails containing malicious attachments

In this example, the phishing email is pretending to be from the World Health Organization and prompts you to open an attachment for advice on safety measures to prevent the spread of COVID-19. When opened, the attached file contains malicious software that automatically downloads onto your device, providing the scammer with ongoing access to your device.



Coronavirus (2019 –nCoV) Safety Measures

Email header impersonating World Health Organisation

DL

[redacted]

Tuesday, February 4, 2020 at 7:08 PM

Malicious software embedded in the attachment

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]

General Internist

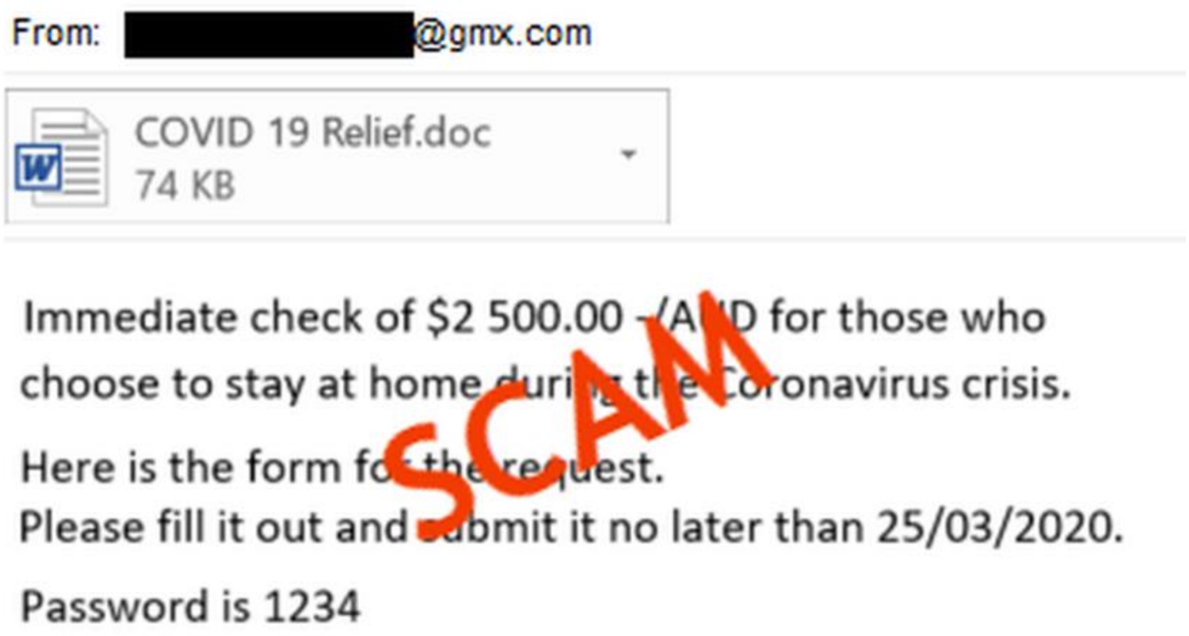
Intensive Care Physician

WHO Plague Prevention & Control

World Health Organization

Example 5: COVID-19 relief payment scam

Scammers are also sending phishing emails targeting an increasing number of Australians that are seeking to work from home, wanting to help with relief efforts or requiring financial assistance if they find themselves out of work. In this example, the email offers recipients $2,500 in 'COVID-19 assistance' payments if they complete an attached application form. Opening the attachment may download malicious software onto your device.



From: [redacted]@gmx.com

COVID 19 Relief.doc
74 KB

Immediate check of $2 500.00 - (AUD for those who choose to stay at home during the Coronavirus crisis.

Here is the form for the request.
Please fill it out and submit it no later than 25/03/2020.

Password is 1234

How do I stay safe?

The ACSC has produced a detailed report, including practical cyber security advice that organisations and individuals can follow to reduce the risk of harm.

You can read the report and protect yourself by following these simple steps:

- Read the message carefully, and look for anything that isn't quite right, such as tracking numbers, names, attachment names, sender, message subject and hyperlinks.
- If unsure, call the organisation on their official number, as it appears on their website and double check the details or confirm that the request is legitimate. Do not contact the phone number or email address contained in the message, as this most likely belongs to the scammer.
- Use sources such as the organisation's mobile phone app, web site or social media page to verify the message. Often large organisations, like Australia Post, will have scam alert pages on their websites, with details of current known scams using their branding, to watch out for.

If you've received one of these messages and you've clicked on the link, or you're concerned your personal details have been compromised, contact your financial institution immediately.

More information

If you’ve suffered financial loss from cybercrime, report it to ReportCyber at www.cyber.gov.au/report.

Visit cyber.gov.au for advice to help businesses stay secure from cyber threats, whilst managing a remote workforce.

To stay up to date on the latest online threats and how to respond, sign up to the Stay Smart Online Alert Service, www.staysmartonline.gov.au/alert-service.

More advice and support is available on our Get help page.

For information on the COVID-19 pandemic, visit https://www.health.gov.au.

The information provided here is of a general nature. Everyone's circumstances are different. If you require specific advice you should contact your local technical support provider.

Feedback

Thank you to those subscribers who have provided feedback to our Alerts and Newsletters. We are very interested in your feedback and where possible take on board your suggestions or requests.

Disclaimer

This information has been prepared by the ACSC. It was accurate and up to date at the time of publishing.

This information is general information only and is intended for use by private individuals and small to medium sized businesses. If you are concerned about a specific cyber security issue you should seek professional advice.

The Commonwealth and all other persons associated with this advisory accept no liability for any damage, loss or expense incurred as a result of the provision of this information, whether by way of negligence or otherwise.

Nothing in this information (including the listing of a person or organisation or links to other web sites) should be taken as an endorsement of a particular product or service.

Please note that third party views or recommendations included in this information do not reflect the views of the Commonwealth, or indicate its commitment to a particular course of action. The Commonwealth also cannot verify the accuracy of any third party material included in this information.

CONTACT US
Facebook: www.facebook.com/staysmartonline
Email: staysmart.online@defence.gov.au
Web: www.staysmartonline.gov.au

You are receiving this message at the address fiona.homan@ato.gov.au. If you no longer wish to receive this information, you can unsubscribe.

STAYSMARTONLINE.GOV.AU