Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Threat Update COVID-19 Malicious Cyber Activity

25 March 2020

Overview

This update is designed to raise awareness of increasing COVID-19 themed malicious cyber activity, and provide practical cyber security advice that organisations and individuals can follow to reduce the risk of being impacted.

Malicious cyber actors are actively targeting individuals and Australian organisations with COVID-19 related scams and phishing emails. These incidents are likely to increase in frequency and severity over the coming weeks and months. This is due, in part, to the ease in which existing scam emails and texts can be modified with a COVID-19 theme.

Opportunistic malicious actors are exploiting people's concerns and desire for information about COVID-19 pandemic by directing them towards websites designed to either install malicious software or steal personal information. In the last few weeks, the Australian Cyber Security Centre (ACSC) has observed thousands of COVID-19-related websites being registered. While the majority of these websites are legitimate, many are being registered by malicious cyber actors seeking to exploit Australians during this difficult time.

The malicious COVID-19 websites are designed to look legitimate or impersonate well-known organisations, making it difficult for individuals to detect. Cybercriminals are using these malicious websites to install computer viruses onto people's devices, such as banking Trojans or different variants of ransomware, in order to generate profit. In other cases, they seek to harvest user credentials, such as personal identification, passwords and bank details, which are then used to gain access to the user's networks, devices or online financial accounts. The ACSC, with assistance from our law enforcement and industry partners, is engaged in efforts to disrupt or prevent these malicious COVID-19 themed cyber activities.

An ongoing analysis of COVID-19 scams and phishing emails indicates that the majority of them are quite sophisticated, often impersonating trusted entities such as the Australian government. The methods used are constantly evolving, with the malicious actors behind this activity regularly adapting their tradecraft to circumvent attempts to stop them.

Cybercriminals are not constrained by geographic borders and their actions can have far-reaching consequences. The ACSC is aware of reports that malicious actors based in both Eastern and Western Europe, as well as Asia and Africa, have been responsible for launching COVID-19 themed malicious cyber activity, including against Australians.

The ACSC strongly encourages organisations and individuals to remain vigilant against the threat of COVID-19 themed scams, phishing emails and malicious websites.

Volume of COVID-19 themed malicious cyber activity

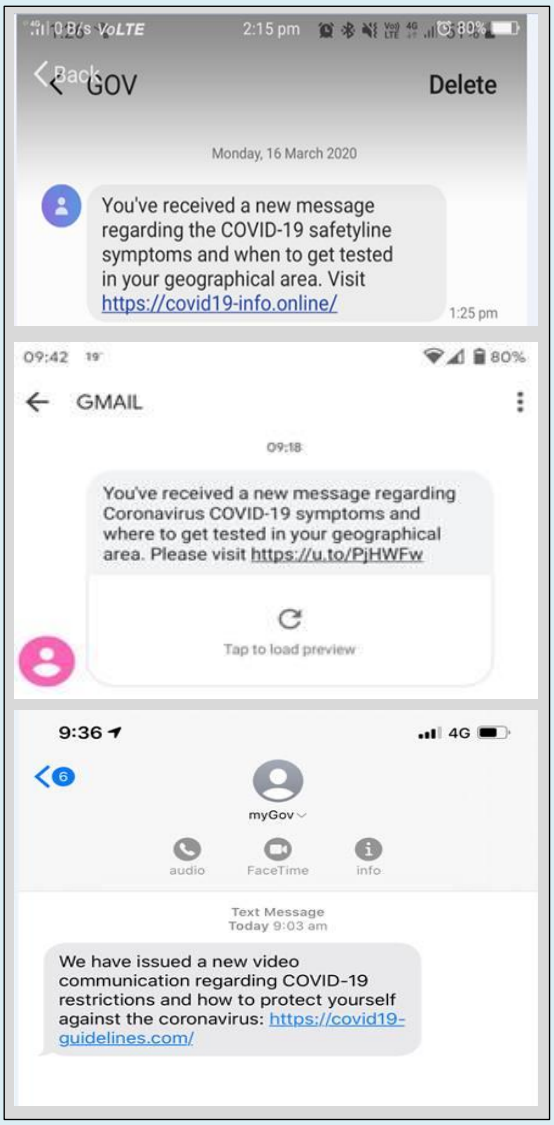
Since early March 2020, there has been a significant increase in COVID-19 themed malicious cyber activity across Australia. The Australian Competition and Consumer Commission's Scamwatch has received more than 100 reports of scams about COVID-19 in the last three months, and the volumes continue to rise. Between 10 and 22 March, the ACSC has 13 cybercrime reports from individuals and businesses, and a further 14 cyber security incidents, all related to COVID-19 themed scam and phishing activity. The true extent of this malicious activity is likely to be much higher, as these numbers only represent those incidents reported to the ACSC and ACCC.

COVID-19 Themed Phishing and Spear-Phishing

Malicious cyber actors are spreading phishing emails that pretend to be reputable organisations, seeking to deceive recipients into visiting websites that host computer viruses or to steal their personal information. To increase the appearance of legitimacy, these phishing emails are sent from addresses that closely resemble the official organisations or entities, adopting the official message format and include well-known branding and logos.

Case Study 1: SMS Phishing Campaign

On Monday 16 March 2020, a malicious cyber actor registered a COVID-19 themed website in the United States. Shortly afterwards members of the public in Australia began reporting receiving text messages that re-directed them to a malicious website (see opposite). The text message appeared as though it came from the Government. This technique is designed to increase the legitimacy of the message and the likelihood that the recipient will click the link.



Assessment by the ACSC identified that the website was hosting a well-known banking Trojan (Cerberus) that targets Android devices and is designed to steal people's financial information. This form of malware is easily available for purchase online through cybercrime forums.

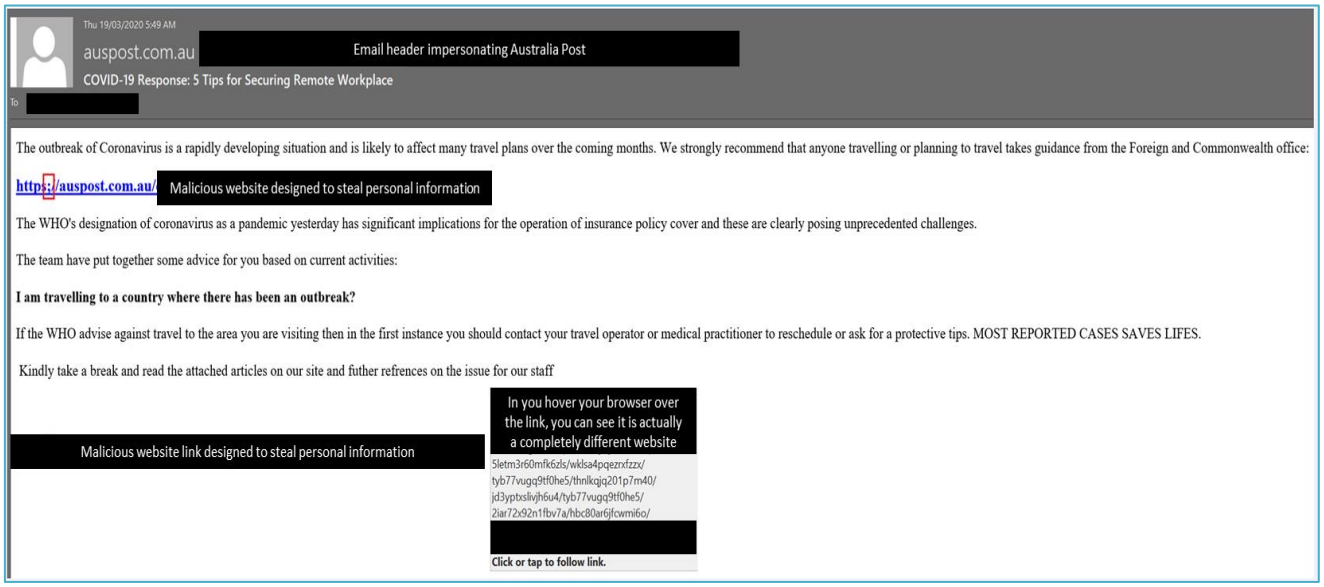
The ACSC formally lodged a take-down request with the domain registrar in the United States. In the meantime, the ACSC reached out to Australia's six major telecommunications providers as well as Google and Microsoft, to block this malicious website from being accessed and flagged at the browser-level as being malicious.

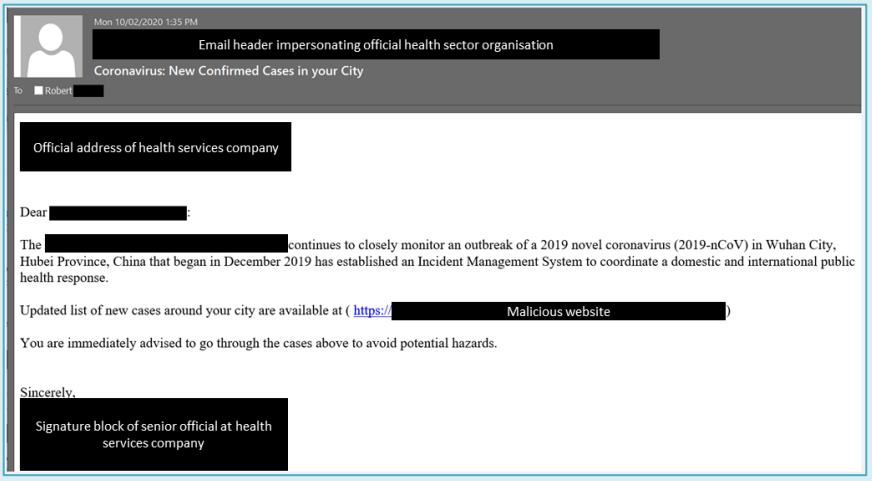
On 19 March 2020, the ACSC received a report from a telecommunications partner that this COVID-19 themed SMS phishing campaign had recommenced. After their website had been shut-down, the malicious actor had registered a new one and was using a different phone number and sender name ('GMAIL'). Anyone who receives these types of COVID-19 themed SMS phishing attempts should simply delete the message.

On 20 March 2020, the ACCC alerted the ACSC to a new variant of this SMS phishing campaign. In this instance, the malicious actor had utilised an alpha tag of "myGov", meaning the text messages appeared on recipients' phones below previous official messages from myGov. This adaptation shows how quickly cyber criminals react to disruption and education campaigns by government and business.

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

On Thursday 19 March, the ACSC received a report from Australian Post about a COVID-19 phishing email that was impersonating their organisation. Under the guise of providing advice about travelling to countries with confirmed cases of COVID-19, the email tries to deceive the recipient into visiting a website that will harvest their personal identifying information (PII). Once the cybercriminals have obtained the PII, historically they often open bank accounts or credit cards in the person's name, using the illicit funds to purchase luxury items or transfer the money into untraceable crypto-currencies such as bitcoin.





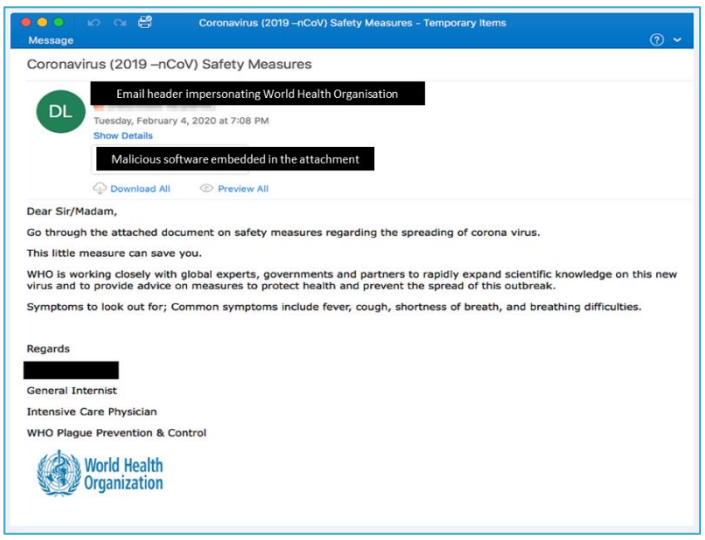
Case Study 3: Phishing campaign pretending to be international health sector organisation

This is an example of one COVID-19 themed phishing email where the sender is pretending to be a well-known international health organisation, inviting recipients to click on the weblink to access information about new cases of the COVID-19 virus in their local area.

Case Study 4: COVID-19 phishing emails containing malicious attachments

The ACSC has also received reports of COVID-19 phishing emails that have malicious word documents or other attachments that contain embedded computer viruses.

In this example, the phishing email is pretending to originate from the World Health Organisation and invites the recipient to open the 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 the recipients device, providing the malicious actor with ongoing access which is



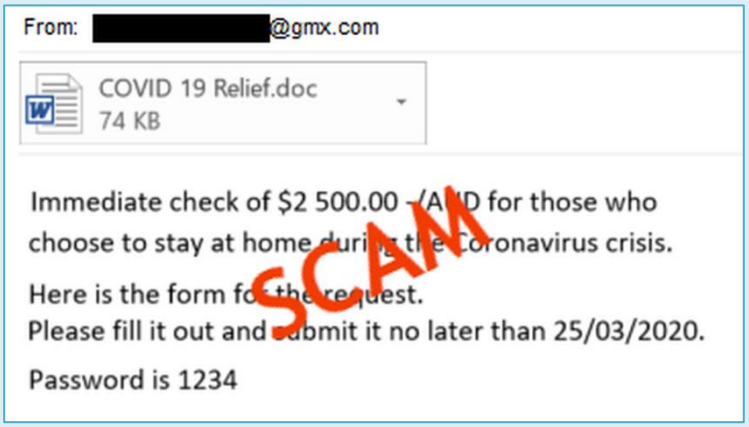
commonly used to install other types of malware, such as spyware (used to track everything the user does) or obtain the individuals' contact details (in order to target the friends and family with further scams).

'Working from home' scams

Cybercriminals are also developing a range scams targeting an increasing number of Australians that are working from home at this time. The ACSC has been made aware of an overseas scam that invites people to support a 'Coronavirus Relief Fund' as a casual employee or volunteer. Applicants are told they will be assisting with processing 'donations' intended for COVID-19 support services. In reality, individuals who are caught up in this scam are unwittingly becoming money-mules for the cybercrime syndicates, transferring proceeds of crime into untraceable crypto-currency. Australians have been targeted in similar ways.

Case Study 5: COVID-19 relief payment scam

On 20 March 2020, the ACCC warned Australians about a phishing email that offers recipients $2,500 in COVID-19 assistance payments if they complete an attached application form. The attachment contains an embedded macro that downloads malicious software onto the recipients' device. If you receive these types of phishing emails, do not open the attachments and simply delete the message.



Other variants of work from home scams include people receiving an invitation to make some quick money by transferring a payment from a reputable company to another party. The cybercriminals will ask to use your bank account to receive a payment from a foreign company and then forward the funds to another account. The cybercriminals will offer you a flat fee, or a percentage commission, in order to facilitate the transfer. Undertaking such activities is known as 'money laundering', which is a criminal offence.

Those who are actively looking for work are also being targeted with fake employment advertisements that are designed to steal personal information for malicious purposes. Often these scams will request applicants to provide a form of identification, such as a driver license or passport, in order to validate the application. Once you provide your personal information, it is then often used in identity theft cases. A range of COVID-19 themed job scams are currently active in Australia and around the world.

Mitigation strategies for combatting COVID-19 scams

How to spot if an email or text message is phishing?

There are some key things to look for to determine if the text message or email is phishing:

- Read the message carefully, look for anything that isn't quite right, such as tracking numbers, names, attachment names, sender, message subject and URLs.
- On a PC or laptop, hover your mouse over links to see if the imbedded URL is legitimate, but don't click.
- Google information such as sender address or subject line to see if others have reported it as malicious.
- Call the organisation on their official number as it appears on their website (separate to any contact details in the received message) 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.

Protecting yourself against phishing emails

As the examples above illustrate, cybercriminals and scammers can produce phishing emails that look very legitimate. By following these simple steps, you can assist in protecting yourself against phishing emails:

- Before opening an email, consider who is sending it to you and what they are asking you to do. If you are unsure, call the organisation you suspect the suspicious message is from using contact details from a verified website or other trusted source.
- Do not open attachments or click on links in unsolicited emails or messages.
- Do not provide personal information to unverified sources and never provide remote access to your computer.
- Remember that reputable organisations locally and overseas - including banks, government departments, Amazon, PayPal, Google, Apple, and Facebook - will not call or email to verify or update your personal information.
- Use email, SMS or social media providers that offer spam and message scanning.
- Use two-factor authentication (2FA) on all essential services such as email, bank and social media accounts, as this way of 'double checking' identity is stronger than a simple password. 2FA requires you to provide two things, your password and something else such as a code sent to your mobile device or your fingerprint, before you - or anyone pretending to be you - can access your account.

ACSC advice for individuals and IT providers about secure remote working

In light of the COVID-19 pandemic, organisations are developing strategies to protect staff and vulnerable members of our community. The Australian Signals Directorate (ASD) would like to remind you to incorporate cyber security into your contingency planning. As more staff may work from home, and the use of remote access technology increases, adversaries may attempt to take advantage. ASD's Australian Cyber Security Centre (ACSC) encourages Australians to remain vigilant and ensure sound cyber security practices.

- Review your business continuity plans and procedures.
- Ensure that your systems, including Virtual Private Networks and firewalls, are up to date with the most recent security patches (see guidance for Windows and Apple products).
- Increase and test your cyber security in anticipation of higher demand on remote access technologies.
- If you use a remote desktop client, make sure you are aware of the security risks and have implemented appropriate mitigations.
- Ensure there are risk management processes in place for work devices, laptops and mobile phones.
- Implement multi-factor authentication for remote access systems and resources (including cloud services). Multi-factor authentication can make it significantly more difficult for an adversary to steal legitimate credentials to facilitate further malicious activities on a network
- Ensure that you are protected against Denial of Service (DoS) threats.
- Ensure that you, your staff and stakeholders are all informed and educated about good cyber security practices, particularly in relation to common threats such as detecting socially-engineered messages.
- Ensure that staff working from home have physical security measures in place. This minimises the risk that information may be accessed, used, modified or removed from the premises without authorisation.

To report a cyber-security incident, email asd.assist@defence.gov.au or call 1300 CYBER1 (1300 292 371).

Individuals and small businesses can report cybercrime activity to the ACSC and law enforcement agencies via www.cyber.gov.au/report.

Together we can ensure Australia is the safest place to work online.