Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Threat Update COVID-19 Malicious Cyber Activity

20 April 2020

Overview

The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) continues to receive reports from individuals, businesses and government departments about a range of COVID-19 themed scams, online fraud and phishing campaigns. This threat update seeks to raise awareness of the evolving nature of COVID-19 related malicious cyber activity impacting Australians. The Australian Competition and Consumer Commission's (ACCC) Scamwatch page also has helpful information about the different types of COVID-19 scams and how to prevent yourself becoming a victim[1].

Cybercrime actors are pivoting their online criminal methods to take advantage of the COVID-19 pandemic. On average each month, the ACSC receives about 4,400 cybercrime reports through ReportCyber, and responds to 168 cyber security incidents. Since 10 March 2020, the ACSC has:

- Received more than 95 cybercrime reports (approx. two per day) about Australians losing money or personal information to COVID-19 themed scams and online frauds;
- Responded to 20 cyber security incidents affecting COVID-19 response services and/or major national suppliers in the current climate; and
- Disrupted over 150 malicious COVID-19 themed websites, with assistance from Australia's major telecommunications providers, Google and Microsoft.

Cybercrime actors are registering COVID-19 themed websites to conduct widespread phishing campaigns that distribute malicious software (malware) or harvest personal information from unsuspecting Australians. The Australian Signals Directorate is committed to protecting Australians from malicious cyber activity during this difficult time, including by striking back at these cyber criminals operating offshore.

Malicious cyber adversaries will continue to use COVID-19 themed phishing campaigns to obtain user credentials, allowing them to bypass security controls in order to gain access to accounts and networks belonging to individuals and businesses. This could include targeting employees working from home and the remote systems they are relying upon. Sophisticated adversaries will also be focused on covertly obtaining COVID-19 information such as details of Australia's pandemic responses and research on vaccines and treatments, broadening the types of information they typically target.

Those engaged in cybercrime activities continue to rapidly adapt their techniques in response to changes in the current environment. The ACSC is observing new phishing campaigns that align with breaking developments, such as government relief payments or public health guidance, within days, even hours, of these announcements occurring. Cyber criminals are also amending previously used methodologies or widespread scam campaigns with a COVID-19 theme. The ACSC strongly encourages all organisations and individuals to remain vigilant against the threat of COVID-19 themed cybercrime activity, including sophisticated scams, phishing emails and malicious websites.

[1] ACCC's Scamwatch: Current COVID-19 (coronavirus) scams - https://www.scamwatch.gov.au/types-of-scams/current-covid-19-coronavirus-scams

Volume of COVID-19 themed malicious cyber activity

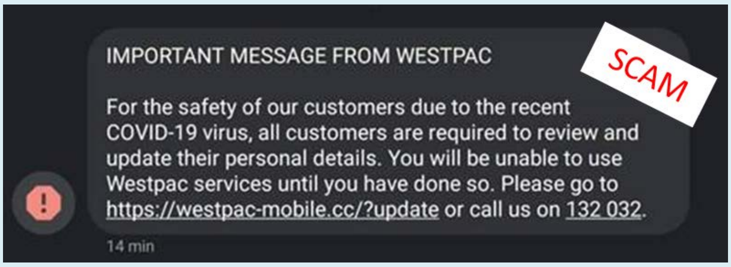
Since March 2020, cybercriminals and other malicious actors are distributing widespread COVID-19 themed SMS and email campaigns, together with a variety of scams. The ACCC's Scamwatch has received over 1,100 reports about COVID-19 scams, with almost $130,000 in reported losses reported. The ACSC has received over 115 cybercrime and cyber security incident reports from individuals and businesses. The true extent of this malicious activity is likely to be much higher, as these numbers only represent cases reported to the ACSC and the ACCC. The ACSC is working closely together with our industry, government and law enforcement partners, including the ACCC, Services Australia, Australian Federal Police and Australian Criminal Intelligence Commission to share information and disrupt this COVID-19 themed scam and other malicious cyber activity.

COVID-19 themed SMS phishing campaigns

The ACSC is tracking a number of different SMS phishing campaigns that seek to trick recipients into clicking on a malicious web link contained in the message. While the links appear to come from legitimate organisations, such as the Australian government or a financial institutions, they actually direct the recipient to a malicious website that is hosting malware. For example, in one campaign, the malicious actor is directing people to a website hosting the Cerberus banking Trojan, a form of malware that has been carefully crafted to steal your financial information.

Case Study 1: Banking themed SMS phishing campaign

On Monday 30 March 2020, the ACCC received sixteen reports of a Westpac themed phishing text. The link in the SMS directed recipients to a website that attempts to harvest personal information.



IMPORTANT MESSAGE FROM WESTPAC

For the safety of our customers due to the recent COVID-19 virus, all customers are required to review and update their personal details. You will be unable to use Westpac services until you have done so. Please go to https://westpac-mobile.cc/?update or call us on 132 032.

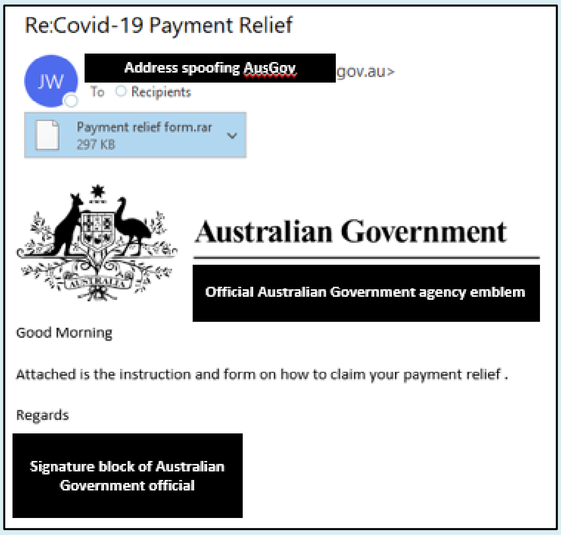
14 min

The ACSC formally lodged a take-down request with the domain registrar. The ACSC also reached out to Australia's major telecommunications providers, as well as Google and Microsoft, to block this website from being accessed and flag it as malicious at the browser-level.

COVID-19 payment phishing campaigns using Australian Government branding

The ACSC is aware of a range of payment themed scams targeting Australians that use official Australian Government branding. The fraudulent emails come from addresses that very closely resemble or spoof official Australian Government email accounts. The emails aim to trick the recipient into installing malware onto their device and/or to harvest their personally identifiable information (PII).

Case Study 2: Australian Government official spoofed in email phishing campaign



Re:Covid-19 Payment Relief

JW Address spoofing AusGov gov.au>

To ○ Recipients

Payment relief form.rar
297 KB

Australian Government

Official Australian Government agency emblem

Good Morning

Attached is the instruction and form on how to claim your payment relief .

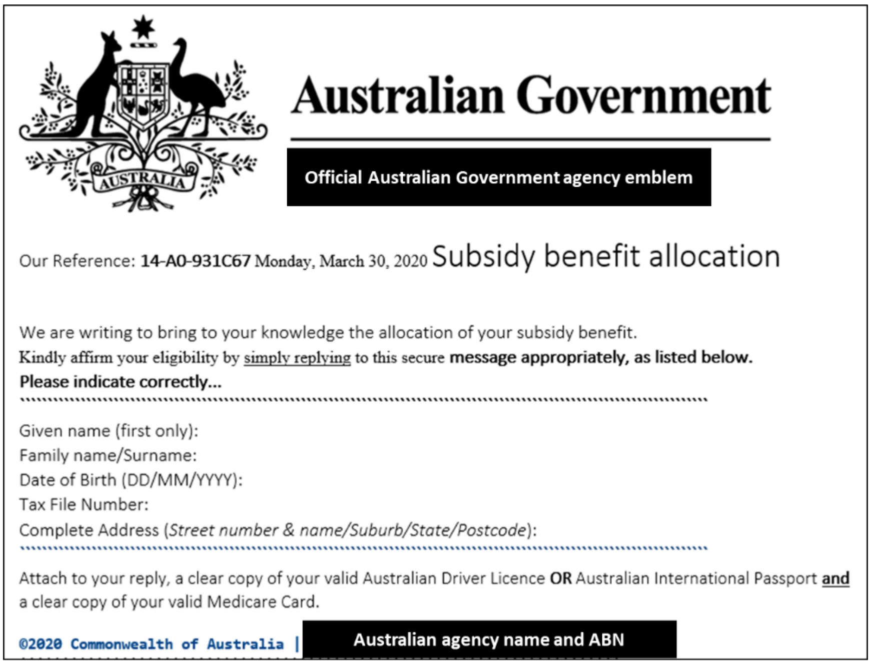
Regards

Signature block of Australian Government official

On 7 April 2020, the ACSC received a report from an Australian Government department that a senior staff member's email was being spoofed as part of a COVID-19 themed phishing campaign. The email contained an attachment with embedded malware that was designed to steal sensitive information such as banking usernames and passwords.

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

Case Study 3: Phishing campaign pretending to come from Australian Government



Australian Government

Official Australian Government agency emblem

Our Reference: 14-A0-931C67 Monday, March 30, 2020 Subsidy benefit allocation

We are writing to bring to your knowledge the allocation of your subsidy benefit.
Kindly affirm your eligibility by simply replying to this secure **message appropriately, as listed below.**
Please indicate correctly...

Given name (first only):
Family name/Surname:
Date of Birth (DD/MM/YYYY):
Tax File Number:
Complete Address (*Street number & name/Suburb/State/Postcode*):

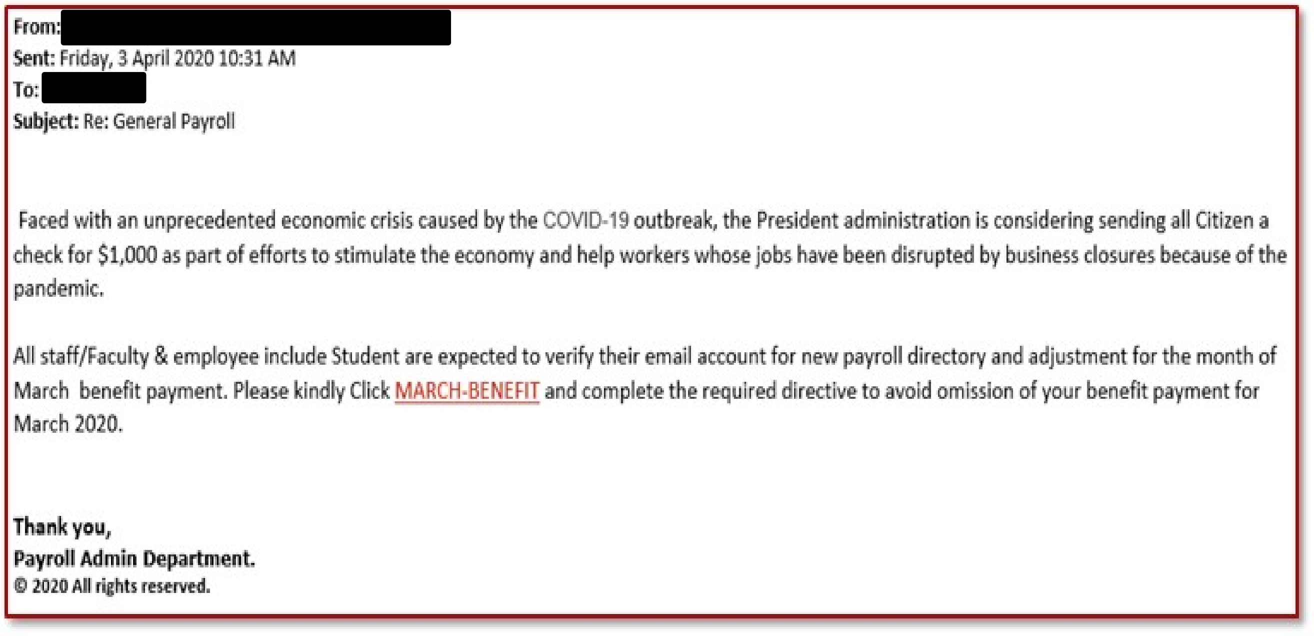
Attach to your reply, a clear copy of your valid Australian Driver Licence **OR** Australian International Passport **and** a clear copy of your valid Medicare Card.

©2020 Commonwealth of Australia | **Australian agency name and ABN**

Cybercriminals are impersonating official Australian Government correspondence about COVID-19 assistance payments in order to steal PII. In this example, the phishing email invites the recipient to provide all of their PII, including tax file number and copies of their identity documents (driver licence or passport and Medicare card) in order to access a benefit payment. Individuals who provide their personal information are at significant risk of identity theft. With this information, criminals could open bank accounts or take out loans in your name.

Case Study 4: Economic stimulus payment phishing email

Cyber criminals are preying on people who are out of work and seeking to access financial assistance from the government or their employer. On 3 April 2020, this phishing email was sent to hundreds of employees within a large Australian company. Recipients were asked to click on the link in order to receive a $1,000 benefit payment to be delivered in the March payroll. The link re-directs users to a website designed to install malicious software onto the company's corporate network.



From: [redacted]
Sent: Friday, 3 April 2020 10:31 AM
To: [redacted]
Subject: Re: General Payroll

Faced with an unprecedented economic crisis caused by the COVID-19 outbreak, the President administration is considering sending all Citizen a check for $1,000 as part of efforts to stimulate the economy and help workers whose jobs have been disrupted by business closures because of the pandemic.

All staff/Faculty & employee include Student are expected to verify their email account for new payroll directory and adjustment for the month of March benefit payment. Please kindly Click MARCH-BENEFIT and complete the required directive to avoid omission of your benefit payment for March 2020.

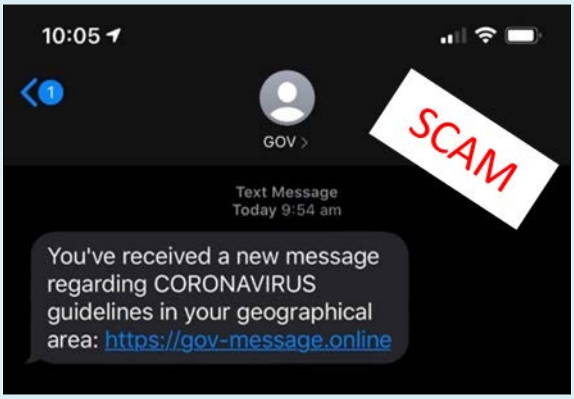
Thank you,
Payroll Admin Department.
© 2020 All rights reserved.

SMS phishing scams about COVID-19 testing and restrictions

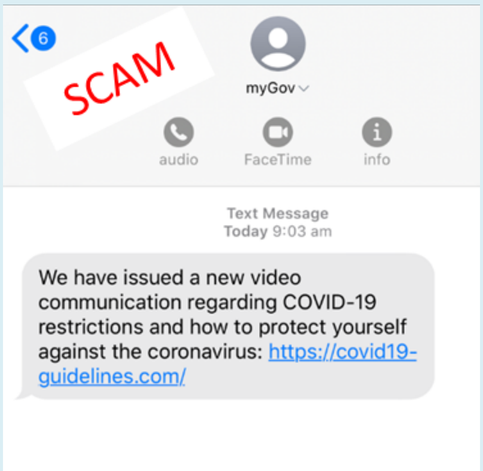
The ACSC has received reports about a number of malicious emails and text messages from cyber criminals that claim to provide information on how to get tested for, or stay protected from, COVID-19. These malicious messages claim to be from Australian Government agencies or other trusted sources such as the World Health Organisation (WHO). They try to convince the recipient to click on a link or open an attachment that will then install malware and steal sensitive information such as bank account details.

Case Study 5: COVID-19 testing themed SMS phishing campaign

On 31 March 2020, the ACSC received a report from an Australian Government agency about an SMS phishing campaign. The message was designed to appear as though it came from 'Gov' and requested that recipients click on a malicious web link that spoofed an official government domain. This website was hosting malware. After the domain used in this initial campaign was taken down, the cybercriminals quickly switched tactics. A new domain was created to host the malware and messages were redesigned to spoof 'MyGov'. By replacing the alpha tags in the SMS header with 'MyGov', the malicious actor was able to deliver these messages within the existing legitimate SMS chain between individuals and Services Australia.



You've received a new message regarding CORONAVIRUS guidelines in your geographical area: https://gov-message.online



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

Remote access scams targeting people working from home

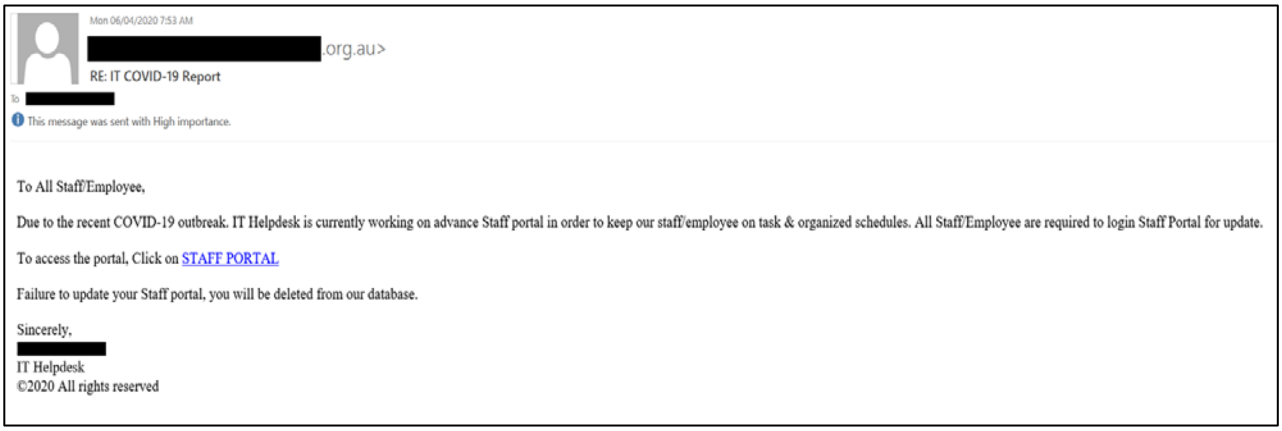
The ACSC is receiving an increasing number of reports from businesses and members of the public about remote access scams. Most of these reports indicate that the scammers are pretending to be from IT companies, telecommunications companies, banks, and even from the ACSC. Cybercriminals often attempt to persuade you to give them remote access to 'fix an issue', and will provide a range of scenarios to convince you that they need immediate access to your device. Allowing anyone access to your devices can, and usually does, result in devastating consequences, including financial loss or the compromise of your personal accounts. The ACSC will never ask you for remote access to your computer. If you are unsure about the identity of a caller, just hang up and check their official website for the legitimate contact details and then call them back.

Case study 6: Microsoft themed remote access scam

Scammers are impersonating a legitimate United States Microsoft support number - (1) (800) 642 7676. However when dialing a 1800 number in Australia, only the next six numbers after 1800 will be accepted. When Australians dial the legitimate United States support number, they dial 1800 642 767 which has been registered by cybercriminals. On calling the number registered by cybercriminals, victims are asked to provide their name and date of birth for verification and are informed someone will call back shortly. The cybercriminal calls back and directs people to download a remote access program that gives the criminals access to their computer. Once access has been gained, the cybercriminal convinces the victim that their computer is compromised and that they need to pay a large sum of money for it to be fixed. The scammers are insistent that due to the COVID-19 conditions in Australia they are required to pay in untraceable crypto-currency. The scammers will also try to extract banking details while they have remote access and drain people's bank accounts and access any other sensitive information.

Case study 7: IT Helpdesk scam

Cybercriminals are aware that increased numbers of Australians are working from home at the moment, and are crafting their scams accordingly. This phishing email below pretends to come from your employer's IT Helpdesk, requesting that staff log into a new portal in order to access the latest information about tasks. Recipients who click on the link are directed to a malicious website that seeks to collect their username and password, which the cybercriminals then use to gain unauthorised access to the company's corporate networks.



Mon 06/04/2020 7:53 AM
[redacted].org.au>
RE: IT COVID-19 Report
To [redacted]
This message was sent with High importance.

To All Staff/Employee,

Due to the recent COVID-19 outbreak. IT Helpdesk is currently working on advance Staff portal in order to keep our staff/employee on task & organized schedules. All Staff/Employee are required to login Staff Portal for update.

To access the portal, Click on STAFF PORTAL

Failure to update your Staff portal, you will be deleted from our database.

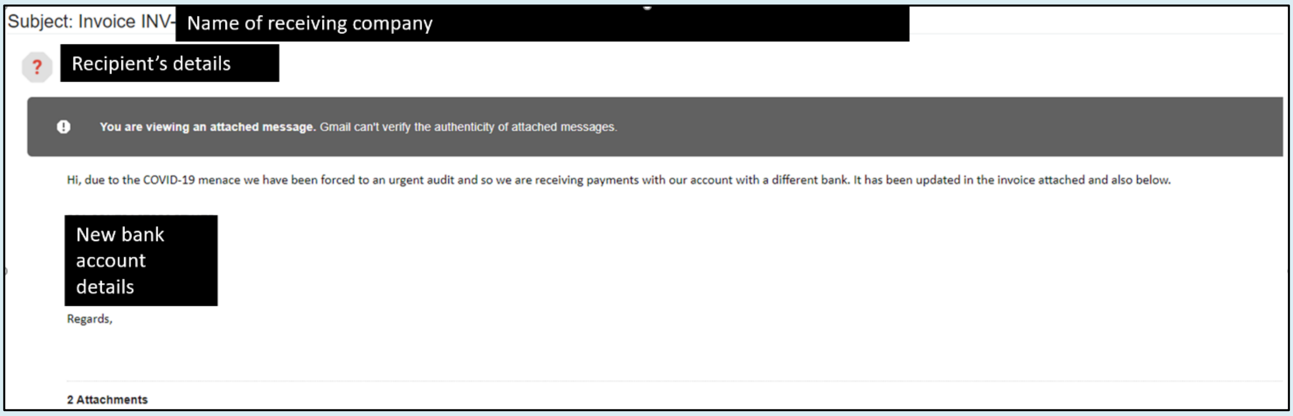
Sincerely,
[redacted]
IT Helpdesk
©2020 All rights reserved

Fraudulent payments over the internet and business email compromise

Cybercriminals continue to adapt previously successful methodologies to leverage the COVID-19 pandemic, and one such approach is known as business email compromise, or fraudulent payments over the internet. This method attempts to convince businesses and/or clients to redirect payments, such as payroll or supplier and invoice payments, to a bank account run by the criminals. Cybercriminals attempting to obtain fraudulent payments over the internet will often use a compromised email account, or a spoofed/fake email address of the business, supplier, or client. Scams like this commonly target businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments.

Case study 8: COVID-19 themed wire-fraud email

On 26 March 2020, a business notified the ACSC that one of their clients had received a COVID-19 themed fraud email. The business email account of their manager was compromised, which was then used to send the invoice-themed email. The email was identified as suspicious by the person who received the email.



Subject: Invoice INV- Name of receiving company

Recipient's details

You are viewing an attached message. Gmail can't verify the authenticity of attached messages.

Hi, due to the COVID-19 menace we have been forced to an urgent audit and so we are receiving payments with our account with a different bank. It has been updated in the invoice attached and also below.

New bank account details

Regards,

2 Attachments

Mitigation strategies for combatting COVID-19 scams and phishing emails

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

There are some key details to look out for to help determine if a text message or email is phishing:

- Read the message very carefully, look for anything that isn't quite right, such as spelling, tracking numbers, names, attachment names, sender, message subject and URLs.

- On a PC or laptop, hover your mouse over links to see if the embedded 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 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.

Protect yourself against phishing emails

As shown in the examples above, cybercriminals and scammers produce phishing emails that look 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're 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 (e.g. a code sent to your mobile device or your fingerprint) before you, or anyone pretending to be you, can access your account.

The ACSC has published a range of information about COVID-19 related malicious activity, as well as guidance on securing remote working and video conferencing. For more information, please visit:

- ***Cyber security is essential when preparing for COVID-19***
  https://www.cyber.gov.au/news/cyber-security-essential-when-preparing-covid-19
- ***Threat update: COVID-19 malicious cyber activity***
  https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity
- ***COVID-19 scam messages targeting Australians***
  https://www.staysmartonline.gov.au/alert-service/covid-19-scam-messages-targeting-australians
- ***Web Conferencing Security***
  https://www.cyber.gov.au/publications/web-conferencing-security
- ***Protecting small business against cyber attacks during COVID-19***
  https://www.cyber.gov.au/news/protecting-small-business-against-cyber-attacks-during-covid-19
- ***COVID-19: Cyber Security Tips When Working From Home***
  https://www.cyber.gov.au/advice/covid-19-cyber-security-tips-when-working-home

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 connect online.