COVID-19 (Coronavirus) phishing scams

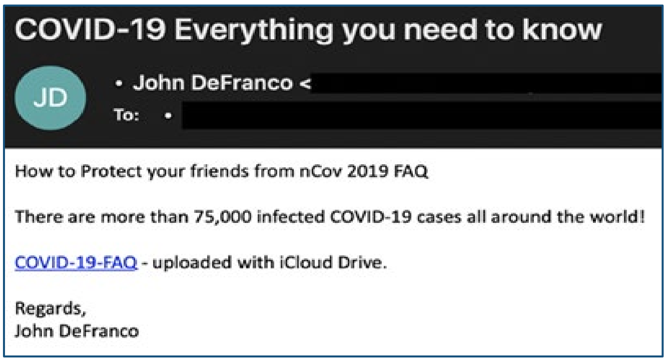
Cybercriminals are sending email and SMS phishing attacks to profit from the COVID-19 outbreak.

These attacks are designed to make you divulge personal information, visit malicious websites or download malicious files.

Below are some tips for recognising and avoiding COVID-19 related scams to protect your privacy and the department's information.

Deceptive / Impersonation Phishing via email

An email from a scammer impersonating a legitimate company, with advice about the COVID-19 outbreak, in an attempt to steal your personal data or login credentials.



COVID-19 Everything you need to know

• John DeFranco < [redacted]

To: • [redacted]

How to Protect your friends from nCov 2019 FAQ

There are more than 75,000 infected COVID-19 cases all around the world!

COVID-19-FAQ - uploaded with iCloud Drive.

Regards,
John DeFranco

Do

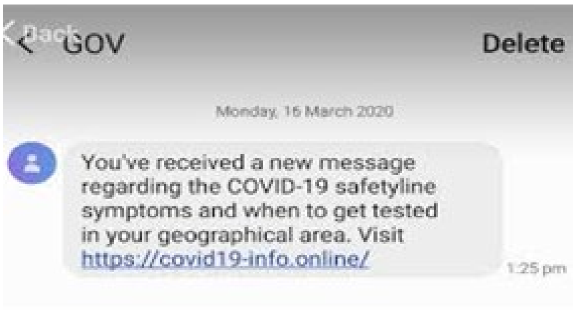
- Inspect the URLs which may look unfamiliar or just plain silly. For example, the ATO ATO@TheRealAto.com.au.
- Look out for generic salutation, grammar or spelling mistakes. For example, 'Dear Customer'.
- Look out for threats and a sense of urgency to scare you into action. For example, 'You have 24 hours to claim a refund'.
- Ignore any unsolicited emails.
- Contact the IDS Service Desk if you are unsure.

Don't

- Do not click on links or download any attachments.

Deceptive / Impersonation Phishing via text message (SMS)

The scammer may send you a fake text message regarding information about COVID-19 testing facilities around your area.



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/

Do

- Contact the IDS Service Desk if you receive an email or SMS message you're unsure about.
- Delete the message.

Don't

- Do not click the link. The link in these text messages is not legitimate and if clicked on, it may install malicious software on your device, designed to steal your banking details.

Fraudulent emails / SMS / calls that claim to be from authorities with information about COVID-19

If the sender/caller claims to be from the Australian Medical Association (AMA) or global bodies like World Health Organization (WHO) promising information on COVID-19, watch out for:

- requests to login to pages or download from a website
- requests to open attachments (they may be malicious)
- requests to follow links designed to steal login details.

AMA AUSTRALIAN MEDICAL ASSOCIATION

World Health Organization

Do

- Be vigilant.

Don't

- Do not respond to unexpected messages over any communications platform, especially those which ask to click a link or open an attachment.

Other COVID-19 related phishing scams

- Scammers are falsely selling COVID-19 related products online which they claim to be a vaccine or cure for the virus.
- Investment scams claiming COVID-19 has created opportunities for you to make money.
- Flight / cruise cancellation scams where the scammer might call you and ask for your details to refund you.

Do

- Be vigilant.

  Be aware of new copycat websites that are likely to surface, potentially containing the same scam content.

Don't

- Do not reveal personal or financial information in email communications, over the phone or text messages, and do not respond to email solicitations for this information.

Report phishing scams

FACS system users:

- Call 9765 3999
- Email infosec@facs.nsw.gov.au

Justice system users:

- Call 8688 1111
- Email security.incident@justice.nsw.gov.au
- Log a ServiceNow ticket

For the latest information on COVID-19 phishing scams

- Australian Cyber Security Centre
- Scamwatch

For information about COVID-19

- NSW Health – information about Coronavirus
- NSW Health – FAQ on Coronavirus