



## Department of Administration

Mark Breunig, Chief Information Security Officer  
State Security Office

333 Willoughby Ave. 5<sup>th</sup> Floor  
Juneau, AK 99811  
Main: 907.269.5000  
[www.doa.alaska.gov](http://www.doa.alaska.gov)

# Memorandum

TO: All State of Alaska Employees

FROM: Mark Breunig, CISO, State Security Office

DATE: March 12, 2020

SUBJECT: Phishing and Scams related to COVID-19

The State Security Office has been notified of an increase in the number of email phishing scams related to the COVID-19 virus. Cybercriminals are seeking to use the current crisis to their advantage. State employees need to be extra vigilant and aware of attachments, files, and links in emails that are not from official sources. In one phishing campaign, cybercriminals sent emails that looked like they came from the World Health Organization, asking people to click on a malicious link to view coronavirus safety measures.

If you receive a suspicious email, please follow the steps below. If you receive an unusual email from someone please call the sender to verify before opening the email and ask your supervisor for guidance. If you receive fraudulent emails or reports of staff receiving these emails, please report them to the State Security Office by following these steps:

1. Select the Phishing email in your inbox to highlight it, then click on the more menu button (in the Home tab) and select Forward as an Attachment.
2. Address the message to *SOA Spam Reporting* <[reportspam@alaska.gov](mailto:reportspam@alaska.gov)> and click the Send button.
3. Once your message has been sent, delete the Phishing email.

If you suspect a hacked computer or account, please report details to [infosec@alaska.gov](mailto:infosec@alaska.gov) or 907-269-5000.

Thank you,

State Security Office  
[infosec@alaska.gov](mailto:infosec@alaska.gov)  
907-269-5000