CYBERSECURITY COMMUNICATION

Please circulate

March 11, 2020

To: University Cybersecurity Communication Recipients
From: University Systems
RE: Cyber exploitation of COVID-19

Cyber criminals are using the heightened public interest in the COVID-19 outbreak as a means to lure individuals to open and interact with phishing emails posing as disease centre alerts, information on the spread of the virus, expert protection advice, or offers of "cures". Links and attachments often lead to malicious software that tries to steal data or commit other crimes.

The following message is an example of this type of scam:

Credit: SOPHOS *Coronavirus "safety measures" email is a phishing scam*

Please take this opportunity to remind everyone of the importance of taking time to analyze the message, look for indications of a phishing email, and avoid opening any unexpected, untrusted attachments. To learn more about how to identify malicious email messages, please visit www.uvic.ca/phishing.

If you have any questions about this notice, please reply to this message.

Regards,

Marcus

Marcus Greenshields
Cybersecurity Working Group
University Systems
University of Victoria