As the COVID-19 situation evolves, cyber criminals continue to use the heightened public interest to lure individuals to open and interact with phishing emails posing as payroll information requests, government economic relief offers, 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, collect usernames and passwords, or commit other crimes.

The following messages are examples of this type of scam seen recently at UVic:

```
Attention: Coronavirus (COVID-19) # 75628

Public Health Agency of Canada <support@voyeurfactor.com>
Mon 4/13/2020 12:30 PM

To: [redacted]

0: 1 attachment

April 13, 2020

Dear Parents and Guardians,

We are writing to provide you with another update from Public Health Agency of Canada with regards to the novel coronavirus (COVID-19).

Letter from Medical Officer of Health:

http://angelamaria.com/circ3

Thank you.
```
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,

David

David Street
Cybersecurity Working Group
University Systems
University of Victoria

To verify the authenticity of this message, visit:
www.uvic.ca/systems/verify