CYBERSECURITY COMMUNICATION

Please circulate

December 13, 2019

To: University Cybersecurity Communication Recipients
From: University Systems
RE: Ransomware Cyberattack at NVIT

Last week, Nicola Valley Institute of Technology (NVIT) was significantly impacted by a ransomware cyberattack. The ransomware-based cyberattack caused service disruptions to workstations, phones, email, and other systems were taken offline as a precautionary measure. NVIT continues to work to restore services and recover from this cyberattack.

This incident reminds us of the high risk of attacks targeting our university community. Please take time to examine email messages for signs of phishing and avoid clicking on suspicious links or opening questionable email attachments. Tips on how to identify and avoid phishing messages can be found at our phishing awareness training website:

https://www.uvic.ca/phishing

If you believe you have inadvertently opened a suspicious attachment, or clicked a dubious link, please **report it as soon as possible** to the Computer Help Desk, your Desktop Support Analyst, or your supervisor. The malicious attackers are committing a crime; you will not be penalized as a victim of this crime. The sooner we are able to respond to an incident, the greater the chance we can minimize the impact.

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

University of Victoria

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