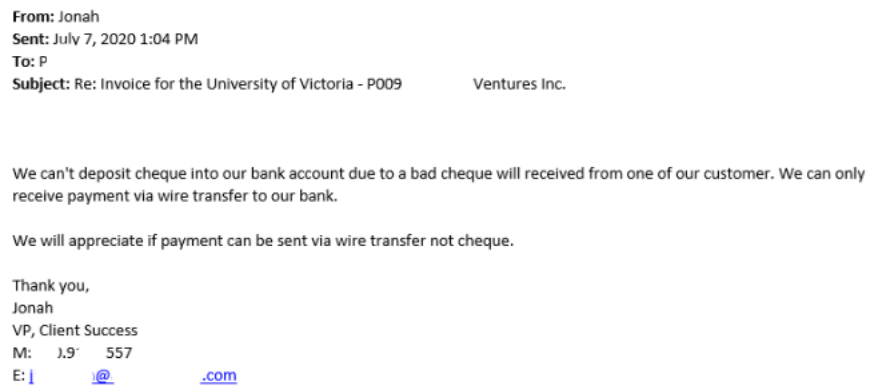
CYBERSECURITY COMMUNICATION
Please circulate

July 13, 2020
To: University Cybersecurity Communication Recipients
From: University Systems
RE: UVic Supplier Email Account Compromise

Last week, an email account at one of UVic's suppliers was compromised, and was in turn used in an attempt to have UVic staff send a payment to an account owned by the attacker. The following screenshot shows the redacted initial communication from the supplier:



From: Jonah
Sent: July 7, 2020 1:04 PM
To: P
Subject: Re: Invoice for the University of Victoria - P009 Ventures Inc.

We can't deposit cheque into our bank account due to a bad cheque will received from one of our customer. We can only receive payment via wire transfer to our bank.

We will appreciate if payment can be sent via wire transfer not cheque.

Thank you,
Jonah
VP, Client Success
M:).9 557
E: j @ .com

More details on this specific phishing attempt including subsequent communications are available on the Phish Bowl OAC blog: https://onlineacademiccommunity.uvic.ca/phishbowl/2020/07/09/invoice-payment-redirection/

If you receive suspicious emails from a supplier, please remember to always follow-up via a phone number you already have on file or reach out to UVic Accounting.

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

Thank you,

Scott

Scott Thompson
Manager, Project Management Office,
Administrative Operations, and Communications
University Systems
University of Victoria

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