CYBERSECURITY COMMUNICATION
Please circulate

August 24, 2017

To: University Cybersecurity Communication Recipients
From: University Systems
**RE: Phishing Messages Posing as Voicemail Messages**

A number of universities are being targeted by phishing messages posing as voicemail notifications. These messages contain attachments that appear to be the voicemail, but are really a .zip file with malicious software. Some messages contain links that direct users to websites that attempt to install malicious software.

Please remember to examine all email for signs of phishing:

- Does the file extension of the attachment match what you expect? Avoid attachments ending in .wav.zip; these are attempting to hide the true file type.
- Hover your mouse over links included in the message. You can see the URL before clicking on the link. Is the URL a website you trust?
- Did you miss a call? Is the message light on your phone lit? Be suspicious of any message indicating you have a voicemail if there is no evidence to support that you missed a call.

There are many additional resources to help all faculty and staff avoid falling for a phish at www.uvic.ca/phishing. Find more tips, sign up for an interactive course in CourseSpaces, or attend a phishing information session. Those departments who are participating in the phishing awareness training program recently received a simulated phishing message masquerading as a voicemail notification to help raise awareness are prepare participants for this type of phish.

If you have any questions about these issues or recommendations, please reply to this message.

Regards,

Marcus

**Marcus Greenshields**
Cybersecurity Working Group
University Systems
University of Victoria

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