CYBERSECURITY COMMUNICATION

April 11, 2017
To: University community
From: University Systems
RE: Cybersecurity communications from University Systems

The University of Victoria is targeted by fraudulent emails, phishing message, virus-infected attachments, and other cybersecurity threats each day. Many of these attacks or emails are blocked or filtered before reaching their intended recipients; however, some do reach UVic users. University Systems has created a cybersecurity communications plan that aims to warn key contacts in departments across campus of information security risks like these.

You are receiving this message because you have been identified as a contact to receive these messages on behalf of your department. You will receive messages such as:

- Notices of sophisticated phishing and spear phishing campaigns
- Warnings of malicious software circulated to UVic users
- Other cybersecurity events we feel pose a credible threat to UVic users

Note that not all cybersecurity events will be communicated via this list; only those that University Systems believes to be a credible threat to UVic.

You can verify the authenticity of messages sent to this distribution group by visiting www.uvic.ca/systems/verify. A PDF copy of each message will be posted with the date stamp when it was sent.

When you receive a message to this list, we ask that you communicate the information that you feel is relevant to your staff or department.

If there are additional individuals from your department that you feel should be subscribed to receive cybersecurity communications, please email David Street at dstreet@uvic.ca or Marcus Greenshields at mgreens@uvic.ca.

Having introduced the purpose of this communication medium, we would like to communicate a new threat targeting UVic users:

> A vulnerability has been identified in Microsoft Word where an attacker can gain full control of a Windows computer when a malicious Word document is opened. Microsoft has issued a security update that patches this vulnerability and has made it available through the Windows Update service. Computers that are supported by University Systems Desktop Support Services, will automatically install this update provided the computer is powered on tonight. If you are not supported by University Systems, we recommend you update your Windows computer.
>
> University Systems strongly recommends that you do not open any email attachments that you are not expecting.

Please distribute the indented paragraphs above to staff and faculty in your departments as appropriate.

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

Thank you.

Marcus Greenshields & David Street
mgreens@uvic.ca dstreet@uvic.ca
University Systems | University of Victoria

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