

CYBERSECURITY COMMUNICATION

Please circulate

April 30, 2018

To: University Cybersecurity Communication Recipients

From: University Systems

RE: **Phishing Message: Case ID UOF43CTB0**

Several faculty and staff have received the following phishing message with the subject **RE: Case ID UOF43CTB0**.



Dear colleague/student,

This email is to verify you requested a change of name associated with your email address of the [University of Victoria](#) electronic resource.

Your request has been submitted and will be processed in 2 days.

If you never made this request, you can cancel this request [HERE](#) (as it's the sole purpose of this notification) otherwise no action is required.

Notification was sent on 04/30/2018  
Ticket ID [UOF43CTB0](#)

Kind regards,  
Information Services  
**Service Desk**  
University of Victoria  
PO Box 1700  
Victoria BC V8W 2Y2

Clicking on any of the links in the email presented a fake Outlook Web Access login page designed to capture your username and passphrase. If you inadvertently provided your credentials in response to this message, **change your passphrase at [www.uvic.ca/uvicid](http://www.uvic.ca/uvicid)**.

University Systems is removing all copies of this phishing message from UVic email accounts to reduce the chance that the university community falls for this phishing scam.

There are many additional resources to help all faculty and staff avoid falling for a phish at [www.uvic.ca/phishing](http://www.uvic.ca/phishing). Find tips to avoid phishing, sign up for an interactive course in CourseSpaces, or attend a phishing information session.

If you have any questions about this issue, please reply to this message or contact the Computer Help Desk at [helpdesk@uvic.ca](mailto:helpdesk@uvic.ca).

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](http://www.uvic.ca/systems/verify)