

WORKDAY THEMED SELF-PHISHING CAMPAIGN

TREVOR CARPENTER – CONTENT STRATEGIST | CYBERSECURITY



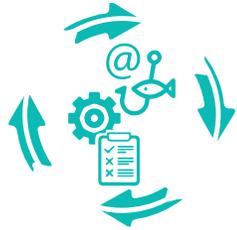
BE VIGILANT: Know the warning signs

UBC-wide Self-phishing is coming!

As go-live for Workday is imminent, cyber criminals will inevitably attempt to take advantage of the high volume of communication associated with this change by launching a Workday themed phishing campaign against UBC faculty and staff.



Train for the inevitable



To help employees better understand how they can quickly spot some of the most common types of phishing and avoid falling victim to their attacks, the UBC Cybersecurity team has established a *Self-Phishing* training exercise.



This means that the University sends our own phishing messages (crafted to look just like the criminals) to UBC employees. When users correctly spot the attempt, they are congratulated, and when they succumb to the attempt, they are notified and presented with corrective materials.

The service is meant to be educational not punitive. Campaign results are kept confidential and the collected results for individuals will not be shared with anyone.



Phishing email samples

BR BURCKEL Regine 10:13 AM
To: BURCKEL Regine >

RE:Admin, Staff Self-service 2020

[CAUTION: Non-UBC Email]

Welcome to the new Outlook Web App

The new Outlook Web App for new home and online self-service and information.

Click on [Login here](#) and login to:

- Access the new staff directory
- Access your pay slips and P60s
- Update your ID photo
- E-mail and Calendar Flexibility
- Connect mobile number to e-mail for Voicemail

.....

Afin d'éviter toute propagation de virus informatique, et en complément des dispositifs en place, ce message (et ses pièces jointes s'il y en a) a été automatiquement analysé par un antivirus de messagerie.

.....

From: Victoria.smith@skype <roland@sportworks.nl>
Sent: Thursday, October 1, 2020 9:13 AM
To: Smith, Victoria <victoria.smith@ubc.ca>
Subject: Skype notificaton for victoria.smith@ubc.ca on 1st October 2020

[CAUTION: Non-UBC Email]

Skype

 Recording

[Listen 01:41 sec](#)

You have a new message, find the details below:

Caller ID: 13258
Date: 1st October 2020
User: victoria.smith@ubc.ca
Organization: ubc

Watch out for suspicious emails, similar to these samples.



You can expect to see Workday related self-phishing message in your UBC FASmail inbox very soon

How can you identify whether a Workday message is fraudulent or not? Some common characteristics to watch out for include a sense of urgency and time constraint conveyed within the body of the message, poor grammar and spelling, and links that don't quite look right: (e.g. @workday.svc.u-bc.ca instead of @workday.svc.ubc.ca).



So what should you do if you have any concerns about a Workday message that you receive?

Don't open the message or click on any links, instead forward the message as an attachment to security@ubc.ca



More information

<https://privacymatters.ubc.ca/self-phishing>

<https://privacymatters.ubc.ca/workday-notifications>



**PRIVACY
MATTERS**
@ UBC