Université de Montréal | Technologies de l'information

**DATE :** Le 16 septembre 2019

**DESTINATAIRES :** Communauté de l'UdeM

**OBJET :** Vague d'hameçonnage à l'UdeM
Informations et précautions à prendre

Chers membres de la communauté UdeM,

Au cours des dernières années, l'hameçonnage par courriel est devenu le vecteur d'attaque privilégié des fraudeurs pour orchestrer des cyberattaques dont les conséquences peuvent parfois être désastreuses. À ce sujet, nous désirons sensibiliser l'ensemble de la communauté de l'UdeM aux risques liés à ce type d'attaque et indiquer les mesures à prendre pour assurer la sécurité de chacun.

En ce moment, il y a une vague d'hameçonnage qui cible quelques universités du Québec, dont l'Université de Montréal. Des mesures de sécurité pour diminuer l'impact de cette attaque ont été prises par les Technologies de l'information, mais il en demeure que la vigilance de chacun est nécessaire.

➢ ***Reconnaitre la fraude par courriel***

Ce type de fraude peut prendre diverses formes. Toutefois, il s'agit, la plupart du temps, d'un courriel appelant à l'action (exemples : ouvrir une pièce jointe, cliquer sur un lien URL, transférer des fonds, etc.) et provenant d'une personne de confiance ou possédant un statut hiérarchique vous incitant à agir sans vous poser de questions (exemples : un proche, un patron, un membre du personnel d'une institution financière ou d'une instance gouvernementale, etc.).

La situation décrite comporte souvent un élément d'urgence afin de pousser le destinataire à agir sans vérification (exemples : l'université vous demande de prendre connaissance du message pour une adhésion rapide, un responsable exigeant un transfert de fonds immédiat, un proche voyageant à l'étranger demandant de l'aide pour payer une facture d'hôpital, un représentant bancaire vous annonçant que votre compte est en suspend et prétextant une vérification de vos renseignements personnels, etc.).

➢ ***Quelques mesures de précaution***

Généralement, l'objectif de ce stratagème est de collecter des fonds ou des renseignements personnels pouvant être utilisés à des fins d'usurpation d'identité, de vol et de fraude. Il est donc primordial de faire preuve de vigilance avant de poser quelque geste que ce soit. Voici quelques mesures de précaution à adopter :

- Faire des vérifications appropriées auprès des personnes concernées avant de poser une quelconque action.

- Ne jamais cliquer sur un lien URL ni ouvrir des fichiers présents dans un courriel suspect, car celui-ci pourrait télécharger un virus sur votre ordinateur.

- Ne pas utiliser la fonction «Répondre» (ou *Reply*) pour répondre à un courriel qui semble suspect. L'adresse de courriel de destination pourrait être substituée de façon invisible et vous laisser croire que vous communiquez avec une personne de confiance. Si vous désirez communiquer par courriel avec la personne concernée, il est préférable d'utiliser un nouveau courriel et de saisir vous-même l'adresse de destination.

- Ne pas prendre pour acquise la véracité d'un courriel simplement parce que :
  - un numéro de téléphone est fourni. Certains fraudeurs vont jusqu'à fournir un numéro de téléphone permettant de communiquer avec un faux représentant. Si vous désirez communiquer par téléphone avec la personne concernée, il est préférable de la contacter directement en utilisant un numéro de téléphone connu.
  - Un lien web affichant la page d'accueil d'une compagnie avec le bon logo y apparait. Certains fraudeurs créent des copies de pages d'accueil similaires à celles d'entreprises existantes telles que des d'institutions financières. Vérifiez toujours l'URL de la page en question pour vous assurer de son authenticité.

➢ ***Faire preuve de vigilance***

En tout temps, lorsque vous communiquez par courriel, limitez les informations personnelles que vous partagez. Ne jamais inscrire un numéro d'assurance sociale, des données de comptes bancaires ou toute autre information susceptible d'être utilisée malicieusement contre vous. N'oubliez pas que l'information contenue dans un courriel circulant sur l'internet est entièrement publique.

Voici quelques articles illustrant des cas de fraudes par courriel :

- https://www.sans.org/sites/default/files/2018-09/201809-OUCH-September-French.pdf
- https://www.sans.org/sites/default/files/2019-02/201902-OUCH-February-French.pdf
- http://www.lapresse.ca/actualites/justice-et-affaires-criminelles/affaires-criminelles/201603/16/01-4961617-des-arnaques-qui-font-des-ravages.php
- http://plus.lapresse.ca/screens/399b31be-ca01-40d1-b156-1935db8a2faf%7CCo1qibaeh_wd.html
- https://www.sq.gouv.qc.ca/communiques/comprendre-fraude-president/

Vous pouvez à tout moment consulter les articles concernant l'hameçonnage ainsi que des conseils pour le prévenir

➢ ***En cas de doute***

Si vous doutez de la légitimité d'un courriel, communiquez immédiatement avec les Technologies de l'information par le formulaire d'aide en ligne ou par téléphone au 514-343-7288.

Les Technologies vous remercient de votre collaboration.