Université de Montréal | Technologies de l'information

DATE : Le 10 septembre 2021

DESTINATAIRES Membres de la communauté de l'UdeM
(Employés et étudiants)

OBJET : Courriels d'hameçonnage : Faites preuve de vigilance

Chers membres,

Les membres de la communauté l'UdeM sont ciblés par des campagnes d'hameçonnage de manières fréquentes. Des personnes malveillantes conçoivent des courriels et des sites Web qui ressemblent à ceux d'organisations légitimes et connues, dans le but d'inciter les utilisateurs à divulguer leurs renseignements personnels, comme les noms d'utilisateur et les mots de passe.

Certains de ces messages peuvent contenir un lien ou une pièce jointe malicieuse. Une action de la part de l'utilisateur est nécessaire afin de déclencher le comportement désiré par l'expéditeur. La consultation du lien ou de la pièce jointe pourrait altérer l'intégrité, la confidentialité et la disponibilité de l'appareil de l'utilisateur ainsi que les données de celui-ci.

Il est donc primordial de faire preuve de vigilance avant de répondre à un courriel, d'ouvrir une pièce jointe ou de consulter un lien provenant d'un courriel suspect.

En cas de doute, voici quelques mesures de précaution à adopter.

Apprenez à repérer un courriel suspect

- Méfiez-vous toujours des demandes de nom d'utilisateur et de mot de passe. **L'Université de Montréal ne vous demandera JAMAIS de communiquer votre mot de passe par courriel ni par téléphone**.
- Avant de cliquer sur un lien, prenez l'habitude de passer votre souris sur celui-ci afin de vous assurer qu'il pointe bien vers une URL légitime.
- Méfiez-vous des courriels dont l'adresse d'envoi ne correspond pas au nom de l'expéditeur. En cas de doute, ne répondez pas au courriel reçu.

Méfiez-vous des liens et des pièces jointes

Ne cliquez pas sur des liens ni sur des fichiers joints qui sont contenus dans un courriel suspect. Les liens pourraient vous diriger vers un site Web malveillant et les fichiers joints pourraient contenir des macros intégrées visant à compromettre votre appareil et vos données.

Pour plus d'information et pour demeurer à l'affût de ce type d'attaque, veuillez consulter les liens suivants :

- Réflexes numériques : une nouvelle section ajoutée au site Cybersécurité pour des conseils sur les manières de prévenir la fraude informatique.
- Conseils pour déjouer les tentatives d'hameçonnage : information publiée par les Technologies de l'information.

Si vous avez cliqué sur un lien ou ouvert un fichier joint provenant d'un courriel suspect, **communiquez immédiatement** avec les Technologies de l'information par le formulaire d'aide ou par téléphone au 514-343-7288.

Les Technologies de l'information vous remercient de votre attention.