Technologies de l'information
Université de Montréal

DATE : Le 15 janvier 2024

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 et particulièrement à chaque rentrée universitaire. 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.

Malgré les actions proactives de l'équipe de sécurité des TI et les contrôles de sécurité en place qui bloquent des milliers d'attaques quotidiennement, il demeure 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.

Si vous avez des questions ou désirez signaler un cas d'hameçonnage, veuillez contacter signalement-hameconnage@umontreal.ca.

Pour des renseignements supplémentaires sur les manières de prévenir les attaques d'hameçonnage, nous vous invitons à consulter les liens suivants :

- Sensibilisation et formation
- Conseils pour déjouer les tentatives d'hameçonnage
- Réflexes numériques - Hameçonnage
- La cybersécurité en milieu universitaire

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