Université de Montréal

TECHNOLOGIES DE L'INFORMATION

SÉCURITÉ DE L'INFORMATION - RESPONSABILITÉ DE TOUS

FRAUDE AU PRÉSIDENT : NE SOYEZ PAS UNE VICTIME

Qu'est-ce que la « fraude au Président / courriels d'imposteurs » ?

La « fraude au Président » ou « courriels d'imposteurs » consiste en une attaque ciblée par courrier électronique qui vise à duper les victimes en les poussant à prendre des mesures ou des actions qu'elles ne devraient pas. Dans la majorité des cas, le but principal de ce type d'attaques est de soutirer de l'argent aux victimes.

Modus operandi

Le cyber attaquant utilise Internet afin d'effectuer des recherches sur la victime et collecter des informations au sujet des personnes avec lesquelles cette dernière interagit. Ces personnes peuvent être des gestionnaires, des collègues ou des fournisseurs. Par la suite, le cyber attaquant usurpe l'identité de l'une de ces personnes en créant une adresse courriel avec le nom de celle-ci et envoie un courriel à la victime en demandant d'agir dans l'immédiat, tel que de faire un paiement ou un transfert d'argent.

Dans d'autres scénarios, le cyber attaquant utilise des moyens différents pour entrer en communication avec les personnes ciblées, tels que les appels téléphoniques ou les messages textes.

Comment se protéger : reconnaitre les signes de ce type d'attaque

Le courriel électronique est :

1. très court et urgent pour vous pousser à contourner les procédures standards.
2. lié au travail, mais utilise une adresse électronique suspecte.
3. en provenance d'un dirigeant, d'un collègue ou d'un fournisseur.
4. utilisé pour fournir les instructions de paiement, telles qu'une demande de paiement immédiat sur un compte bancaire.

En cas de doute, quoi faire ?

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

Quelques liens utiles

- Pratiques exemplaires en cybersécurité pour la COVID-19, publiées par le Centre canadien pour la cybersécurité.
- 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, publiés par les Technologies de l'information.
- Le blog de sécurité des Technologies de l'information.