

SÉCURITÉ DE L'INFORMATION

VICTIME D'UNE FRAUDE OU D'UNE ARNAQUE INFORMATIQUE ?
QUOI FAIRE ?



Vous avez reçu un courriel d'hameçonnage

1. Si vous avez un doute concernant un courriel reçu, communiquer par téléphone ou demander à l'expéditeur en personne de confirmer que le courriel provient bel et bien de lui.
2. Si vous soupçonnez que votre mot de passe a été compromis, modifiez-le immédiatement par le lien suivant : <https://identification.umontreal.ca/cas/ChangerMDP.aspx>
3. Si vous avez ouvert une pièce jointe contenue dans un courriel d'hameçonnage, communiquez immédiatement avec les Technologies de l'information par le [formulaire d'aide](#) ou par téléphone au 514-343-7288.
4. Si vous avez fourni vos données financières ou votre numéro d'assurance sociale (NAS), veuillez vous référer à la page suivante : <https://www.mantifraudcentre-centreantifraude.ca/scams-fraudes/victim-victime-fra.htm>
5. Si vous recevez des courriels d'hameçonnage, veuillez signaler les messages à l'adresse : signalement.hameconnage@umontreal.ca

Quelques liens utiles pour en savoir plus sur l'hameçonnage

- [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.
- [Blog de sécurité](#) des TI.