# Ne vous faites pas pirater !

*Protégez-vous contre la fraude*

Chaque jour, le CSAP bloque des milliers de messages avant même qu'ils n'atteignent votre boîte de réception. Malheureusement, il est impossible de tous les attraper. C'est pourquoi il est important de toujours être vigilant lorsque vous utilisez le courrier électronique du CSAP. Voici quelques-uns des types de fraude par courriel les plus courants :

## 1. Spam

Également connu sous le nom de courrier indésirable, le spam est conçu pour vous faire croire que leur message vaut la peine d'être lu. Exemple : Un magasine médical de grande valeur !

## 2. Fraude

Les escroqueries sont des tromperies intentionnelles faites dans un but lucratif. Exemple : Vous avez gagné un million de dollars ! Cliquez pour réclamer votre récompense.

## 3. Canular

Il s'agit d'avertissements sur une menace inexistante. Exemple : Votre compte CSAP sera désactivé dans les 24 heures, à moins que vous ne confirmiez votre adresse électronique et votre mot de passe

## 4. Hameçonnage

Les courriels d'hameçonnage tentent de vous inciter à divulguer des informations personnelles, telles que votre nom d'utilisateur, votre mot de passe et/ou vos informations bancaires. Exemple : Votre compte est compromis, veuillez vous connecter ici et changer votre mot de passe pour recevoir votre dépôt.

## 5. Harponnage

Il s'agit de courriels destinés à des personnes qui connaissent généralement le nom de la personne imitée. Exemple : un membre du personnel reçoit un courrier électronique d'un expéditeur se faisant passer pour un collègue et lui demandant d'acheter des cartes-cadeaux ou autre chose de valeur.

## 6. Parodie

Dans ces courriels, l'adresse de l'expéditeur a été modifiée pour masquer sa véritable origine, une technique utilisée par les auteurs de virus et de spam pour donner à leurs courriels une apparence légitime. L'e-mail semble provenir d'une adresse, mais le survol de celle-ci révèle une autre adresse.

## 7. Scareware

Ces messages sont destinés à vous extorquer de l'argent afin d'empêcher l'expéditeur de diffuser des images de vous ou de distribuer vos informations bancaires. L'expéditeur vous demande de cliquer pour installer un logiciel car votre ordinateur est infecté par un virus.

## *Comment pouvez-vous vous protéger contre la fraude par courrier électronique ?*

Ne répondez pas aux courriels qui vous demandent des informations personnelles telles que des identifiants ou des mots de passe.

Veuillez noter que le CSAP ne vous demandera JAMAIS votre mot de passe.
Ne partagez pas d'informations personnelles, ne téléchargez pas/ouvrez pas de pièces jointes, et ne cliquez pas sur les liens contenus dans les courriels si vous n'êtes pas certain de leur authenticité.

Passez votre souris sur les liens ou les adresses électroniques pour voir si l'adresse semble légitime. Au lieu de cliquer sur les liens, ouvrez un nouveau navigateur et saisissez manuellement l'adresse.

**En cas de doute, contactez votre technicien par courriel ou par téléphone.**

CSAP Conseil scolaire acadien provincial