Centre Internet
Haute-Côte-Nord

Courriels indésirables et hameçonnage

Table des matières

LES COURRIELS INDÉSIRABLES ET DE HAMEÇONNAGE

Il est important de savoir reconnaitre des courriels indésirables ou des tentatives de hameçonnage dans votre boite de messagerie.

Des tentatives de hameçonnage sont de faux courriels d'organisations que vous connaissez bien et que vous utilisez probablement. Ils vous demandent généralement de cliquer sur un lien pour mettre à jour vos informations pour une raison banale. Quand vous cliquez sur le lien, il y a deux possibilités : la première est qu'un virus est lié à ce lien et vous devenez infecté instantanément; la deuxième est que vous êtes redirigé vers un site qui semble être vrai et quand vous entrez vos informations, elles sont automatiquement volées et votre compte est piraté.

Comment les reconnaitre

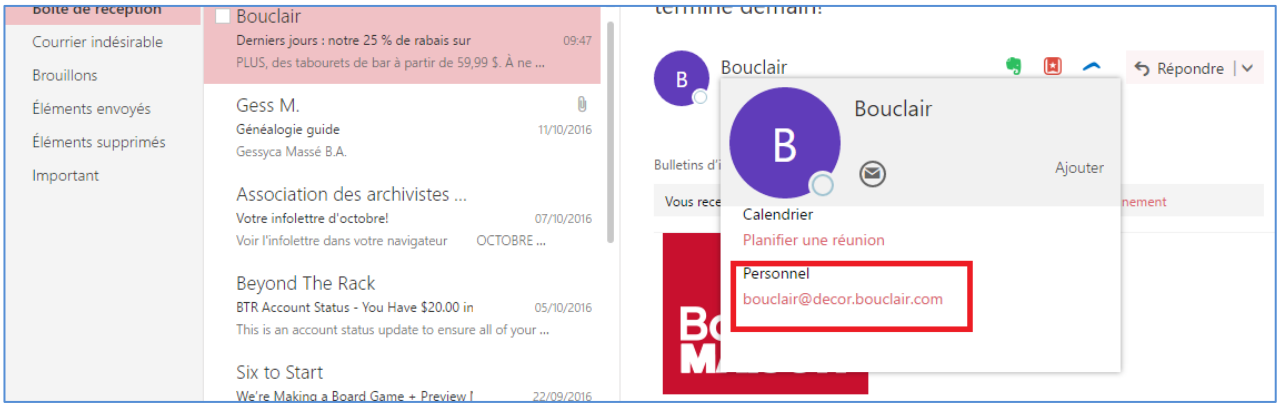
Plusieurs choses sont à vérifier quand vous recevez un courriel d'une organisation vous demandant de vérifier vos informations personnelles :

Êtes-vous un client de cette organisation?

Si non, il est simple de deviner que ce courriel est une tentative de hameçonnage.
Si oui, vérifier ce que dit le message et allez vérifier dans votre compte par le biais du vrai site de l'organisation l'état véridique de votre compte. Il ne faut en aucun cas cliquer sur le lien dans le courriel. Allez chercher le site par Google, par la suite recherchez le site de l'organisation en vous assurant que le site est sécuritaire (voir Conseil de base) et connectez-vous à votre compte.

Vérifier l'adresse courriel du message

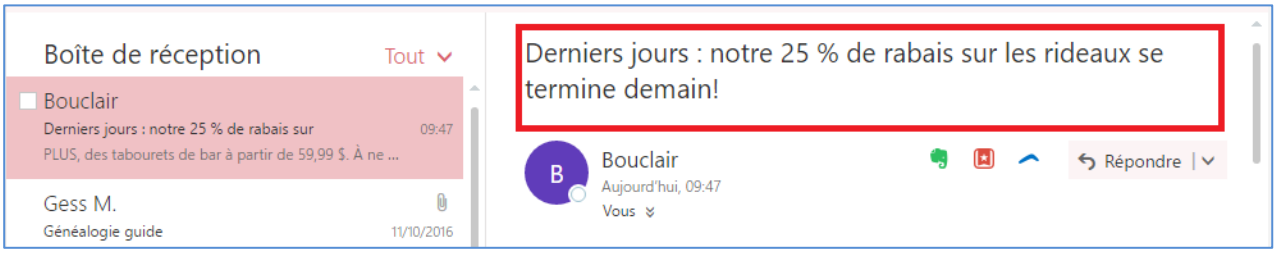
Si l'adresse courriel du message contient plein de chiffres et de lettres aléatoires, c'est un courriel généré par un ordinateur et non pas un courriel d'entreprise. Les courriels d'entreprise vont habituellement ressembler à : service@appel.com.



La plupart des grandes organisations ont leur propre adresse courriel avec le nom de leur organisation et non des courriels Sympatico ou autre, comme dans l'encadré rouge :

L'objet

Ce qui est inscrit dans l'objet est aussi très important. Si l'information dans l'objet est un numéro de facture, une information qui peut être confidentielle ou qu'il n'y a rien du tout, ce n'est pas normal. Toute organisation réelle va mettre un objet court et clair, mais jamais un numéro de facture. Voir l'encadré rouge :

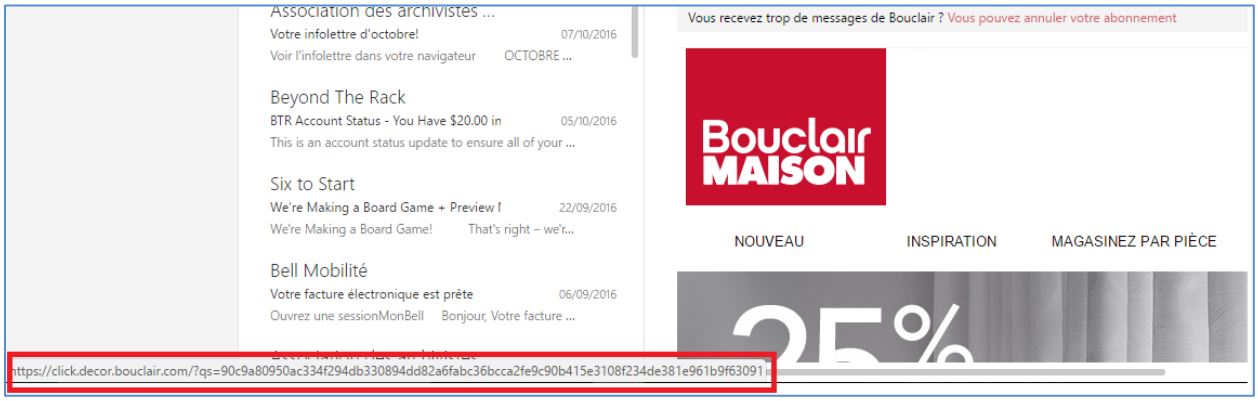


L'apparence

L'apparence du courriel est aussi importante. Il est très rare qu'une organisation envoie des courriels sans publicité pour leur organisation. Si le courriel est trop vide, cela peut être un faux. Ceci est un exemple de vrai courriel de Bouclair qui fait promotion de rabais, c'est ce qui rend un courriel plus authentique :

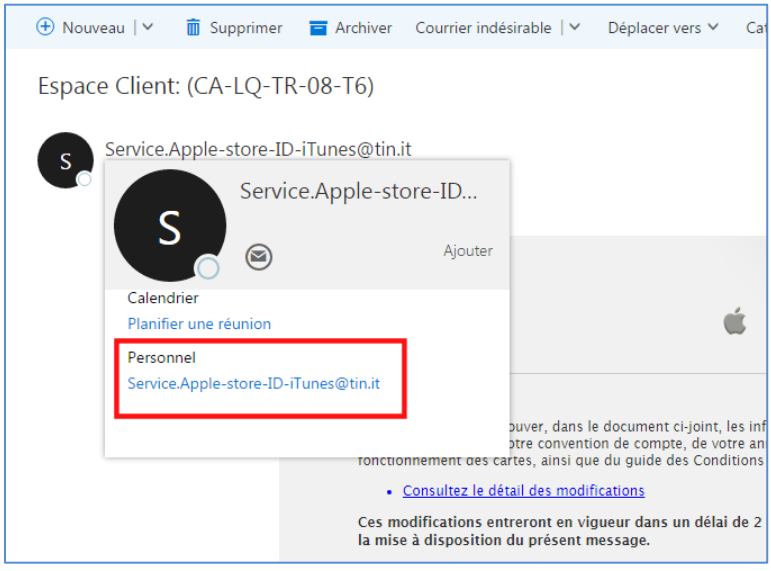
L'adresse du lien

Il est possible de vérifier l'adresse du lien sans cliquer dessus. Pour cela, placez votre curseur sur le lien dans le courriel et regardez dans la barre en bas pour vérifier si le lien est vraiment celui de l'organisation. Cette barre que nous voyions dans l'encadré rouge est présente à chaque fois que vous passez votre curseur sur un lien et elle vous indique le site que vous allez visiter si vous cliquez sur le lien. Il est donc important de le vérifier avant de cliquer sur un lien dans un courriel. Ici, il est bien clair que le lien est vers le site Internet de l'organisation Bouclair et n'est pas une tentative de hameçonnages.



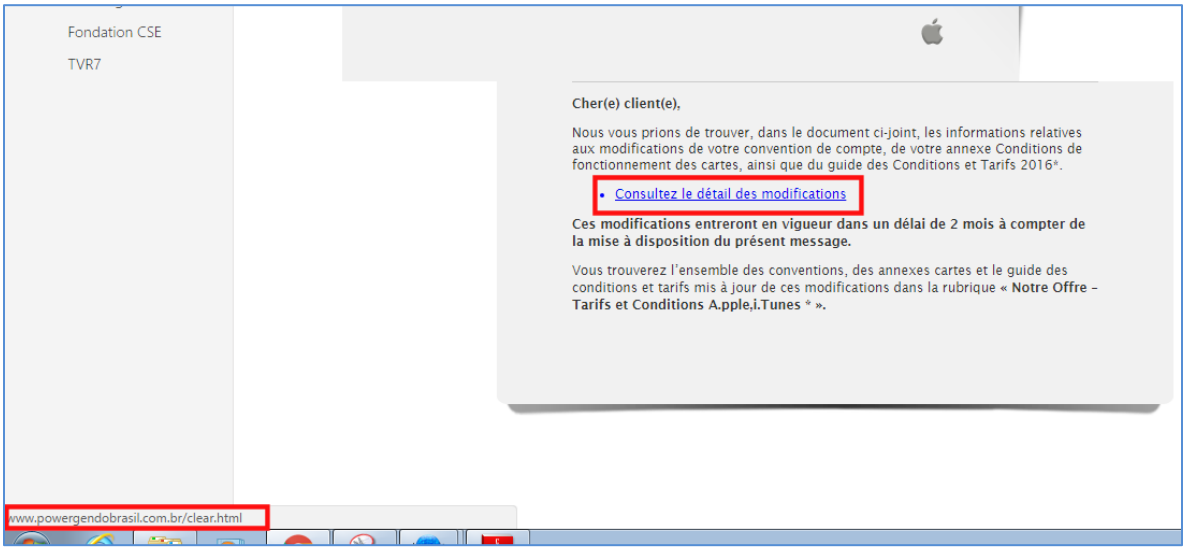
Exemples de courriels frauduleux

Exemple 1 :



Dans l'encadré rouge, nous voyons bien que l'adresse courriel n'est pas normale.

Exemple 2 :

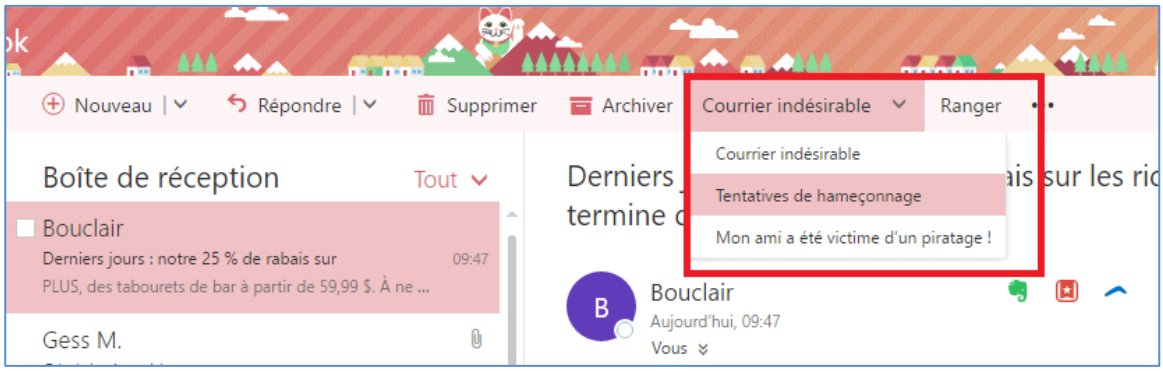


Dans l'exemple 2, nous voyons qu'en passant notre curseur sur « Consultez *le détail des modifications* » dans le premier encadré rouge que l'adresse dans le deuxième encadré rouge du bas n'est pas celle du site d'Apple. Il ne faut donc pas cliquer sur ce lien.

Un autre élément important est l'aspect vide du courriel, sans publicité pour la marque supposée (Apple ou autre produit de la marque). Un courriel qui ressemble à celui de l'exemple 2 est considéré comme louche.

Comment s'en débarrasser

La plupart des boites de réception de courriel comme Outlook (ou encore Hotmail, Gmail, Sympatico, etc.) ont des systèmes de sécurité pour vous protéger de ces tentatives de hameçonnage. Cependant, comme la technologie et l'imagination des pirates évoluent très vite, il est difficile pour ces systèmes de rester à jour. C'est pour cette raison qu'ils ont souvent un onglet « Indésirable » où vous pouvez choisir tentative de hameçonnage, comme dans l'encadré rouge pour Outlook.



Exemple : pour Gmail, il est possible de signaler les courriels comme un « spam » qui est similaire à « indésirable » comme dans l'encadré rouge.

Indiquez à votre système de messagerie que ce courriel particulier est une tentative de hameçonnage ou un pourriel (spam) aide le système de sécurité à mieux gérer ces courriels et ainsi vous éviter de futures tentatives. Cela aide aussi à mieux filtrer les courriels que vous recevez et vous éviter de devoir vous demander à chaque fois si vos courriels sont des tentatives de hameçonnages.

Conseils de base

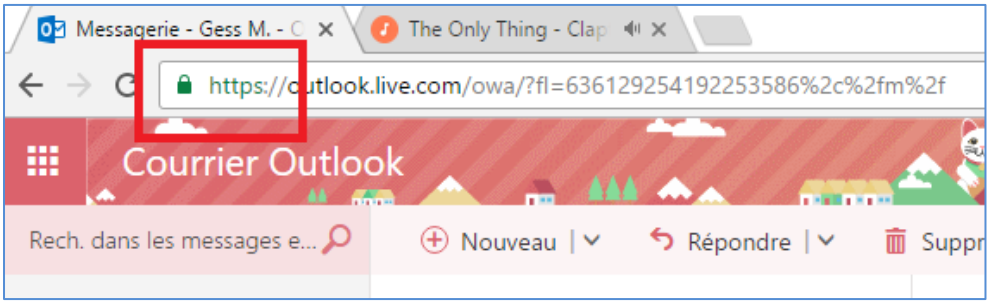
Liens dans un courriel

La meilleure façon d'éviter de vous faire hameçonner est de ne jamais cliquer sur un lien dans un courriel si vous avez le moindre doute qu'il n'est pas sécuritaire. Il vaut mieux aller directement sur le site que vous voulez visiter que de cliquer sur un lien dans un courriel. Vous devez donc être sûr à 100 % de la sécurité du lien avant de cliquer dessus.

Demande de mot de passe

Les organisations ne demandent jamais de mot de passe dans un courriel, ils les connaissent déjà. Si vous recevez un courriel d'une banque ou caisse, d'Apple ou de Paypal, vous demandant de confirmer votre mot de passe, c'est automatiquement une tentative de hameçonnage.

La meilleure chose à faire est d'aller directement sur le site Internet de l'organisation que vous voulez visiter en vous assurant que le cadenas vert de protection est présent dans votre barre de



navigateur. Si ce cadenas n'est pas présent, il y a un risque que le site que vous visitez ne soit pas sécuritaire.

Comment se débarrasser des courriels publicitaires?

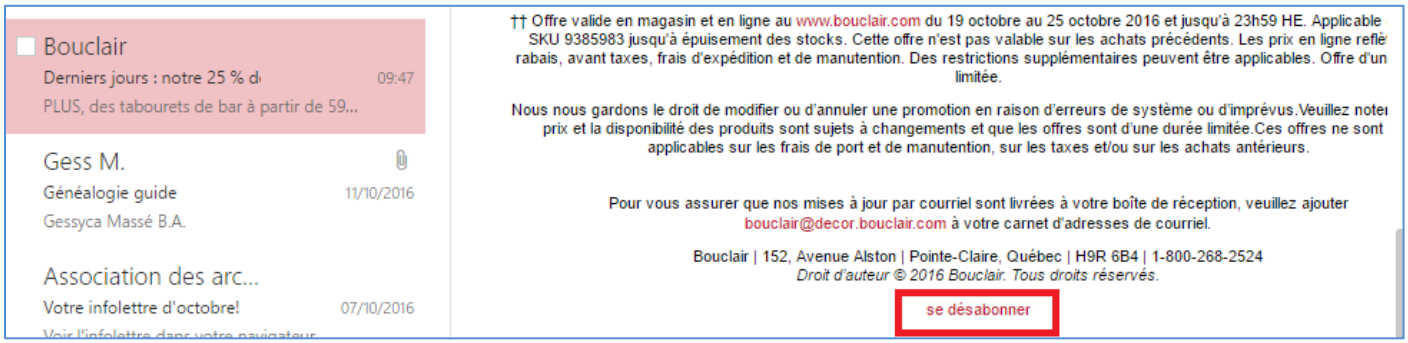
Vous êtes automatiquement inscrit à la liste d'envoi de courriel d'une organisation avec qui vous entrez en contact sur Internet en :

- participant à un concours;
- achetant sur leur site Internet;
- vous inscrivant volontairement à leur liste d'envoi;
- etc.

Les organisations sont obligées par la loi de mettre un lien qui vous permet de vous désabonner de façon sécuritaire de leur courriel publicitaire. Vous avez souvent deux façons de le faire : soit directement avec Outlook ou dans le courriel publicitaire directement.

1. Avec Outlook comme dans l'encadré rouge :

2. Dans le courriel publicitaire, cette version est celle de Bouclair, mais peut varier selon les organisations. En général, il sera inscrit « *se désabonner* » dans le bas complètement du courriel, comme dans cet exemple, dans l'encadré rouge :



Si vous ne voyez pas le lien pour vous désabonner de la liste dans le bas du courriel, il est certain que votre système de messagerie vous le proposera comme Outlook le fait.

Se souvenir...

Pour terminer, la chose la plus importante à retenir est d'être le plus prudent possible avec les liens dans les courriels. La meilleure chose à faire est donc d'aller directement sur le site de l'organisation plutôt que de cliquer sur un lien dans un courriel. Si vous avez le moindre doute, il vaut mieux ne pas cliquer sur le lien.

En toute circonstance, vous ne devez communiquer vos mots de passe et numéro de compte de banque ou de caisse à personne. Vous devez garder ces informations de façon sécuritaire.

Dites-vous que les organisations avec qui vous faites affaire connaissent déjà ces informations, elles ne vous les demanderont pas.

Bonne navigation!

SADC
Société
d'aide au développement
de la collectivité
DE LA HAUTE-CÔTE-NORD