



POURRIEL

COMMENT LE **RECONNAÎTRE**
ET MIEUX **VOUS PROTÉGER**

Qu'est-ce que le pourriel?

Le pourriel est considéré comme un message électronique commercial non sollicité. Il est souvent la source d'escroqueries, de virus informatiques et de contenu offensant qui font perdre beaucoup de temps et augmenter les dépenses des consommateurs, des entreprises et des gouvernements.



Vous pouvez prendre diverses mesures pour lutter contre le pourriel et limiter la quantité que vous recevez. Il est important de faire tout ce que vous pouvez pour vous protéger, mais également de savoir comment gérer adéquatement les pourriels que vous recevez.

La clé pour prévenir et gérer les pourriels est de protéger :

- *votre ordinateur*
- *votre courriel*
- *vous-même*

La meilleure façon de prévenir et de gérer les pourriels est d'appliquer les lignes directrices suivantes.

Protégez votre ordinateur

N'ouvrez jamais de pièces jointes à un courriel provenant d'un inconnu ou d'une personne à qui vous ne faites pas confiance.

Une pièce jointe peut contenir un logiciel qui pourrait nuire à la performance de votre ordinateur et rendre vulnérables vos renseignements personnels. Un logiciel malveillant peut corrompre votre ordinateur ou s'emparer de votre compte de courrier électronique pour envoyer des virus à d'autres personnes. Sachez que les polluposteurs peuvent faire en sorte que les messages semblent parvenir de personnes que vous connaissez – c'est ce qui est appelé la « mystification ». Si vous avez des doutes quant à une pièce jointe, renseignez-vous auprès de son expéditeur avant de l'ouvrir.

Installez des logiciels anti-pourriel, anti-virus et pare-feu.

Le pourriel renferme souvent des programmes nuisibles comme des virus. Il est recommandé d'utiliser les trois types de protection qui suivent :

- 1) Un **logiciel anti-pourriel** balaie les courriels avant qu'ils n'atteignent votre ordinateur et se débarrassent automatiquement des pourriels connus. La plupart des fournisseurs de services Internet (FSI) offrent un tel service, moyennant quelquefois des frais mensuels. De nombreux services de courriels gratuits offrent ce genre de services anti-pourriel.
- 2) Un **logiciel anti-virus** peut vous aider à protéger votre ordinateur contre les virus informatiques. Il peut aussi vous aider à retirer des virus connus d'un système informatique infecté. Assurez-vous de choisir un logiciel anti-virus à jour et qui reconnaît les anciens virus et ceux plus récents.
- 3) Un **pare-feu personnel** est un progiciel qui vous aide à contrôler l'information qui est reçue et envoyée de votre ordinateur. Assurez-vous de choisir un pare-feu qui protège votre ordinateur de l'information que vous recevez (qui entre) et l'information que vous envoyez (qui sort).

De nombreux fournisseurs de services Internet (FSI) au Canada fournissent gratuitement à leurs clients un logiciel de protection. Renseignez-vous auprès de votre FSI s'il peut vous offrir un logiciel que vous pourrez installer.

Mettez à jour votre logiciel anti-virus et votre pare-feu personnel régulièrement.

De nouveaux virus informatiques sont découverts tous les jours. De nombreux progiciels vous permettent de repérer les virus et de télécharger automatiquement des mises à jour (mise à jour automatique). Vous pouvez trouver plus de détails sur la façon de mettre à jour votre logiciel dans les renseignements qui accompagnent chaque progiciel.

Débranchez et fermez votre ordinateur lorsque vous ne l'utilisez pas.

De nouveaux programmes de pourriel et d'autres menaces peuvent apparaître en tout temps, et aucun progiciel de protection n'est entièrement sécuritaire. De nombreux polluposteurs se servent de programmes compliqués qui repèrent et profitent d'ordinateurs non protégés qui sont laissés allumés et connectés à Internet. Si vous fermez votre ordinateur et que vous le déconnectez d'Internet, vous empêcherez des programmes malveillants de se brancher à votre système informatique et de l'infiltrer.

Mettez à jour votre navigateur Web régulièrement.

Assurez-vous de vérifier régulièrement si de nouvelles mises à jour de votre navigateur Web sont disponibles. Les entreprises qui conçoivent des navigateurs Web cherchent constamment à rendre leurs logiciels plus sécuritaires afin de protéger leurs clients.

Protégez votre courrier électronique

Supprimez le message pourriel sans l'ouvrir.

Souvent, les pourriels peuvent contenir du code de programmation invisible qui permet aux polluposteurs de valider une adresse électronique lorsqu'un message est ouvert. Une adresse électronique validée recevra vraisemblablement plus de pourriels qu'une autre qui ne l'est pas; alors, assurez-vous de supprimer le courriel avant de l'ouvrir. Toutefois, si vous recevez des courriels d'une organisation légitime auprès de laquelle vous avez enregistré votre adresse électronique et que vous ne désirez plus recevoir des courriels de sa part, vous pouvez vous servir de son service de « désabonnement », plutôt que de supprimer les messages. Les organisations légitimes sont heureuses d'aider à réduire la quantité de courriels non désirés.

Fermez le volet de visualisation de votre logiciel de courrier électronique.

Le volet de visualisation est une fenêtre qui permet de prendre connaissance du contenu d'un courriel sans avoir à l'ouvrir. Le code de programmation invisible dont se servent souvent les polluposteurs peut être activé au moyen du volet de visualisation. La plupart des programmes de courrier électronique vous donnent la possibilité de fermer le volet de visualisation. Vous trouverez plus d'information sur ce sujet dans la documentation qui accompagne votre programme de courrier électronique.

Établissez des options de filtrage dans votre logiciel de courrier électronique.

En établissant des options de filtrage dans votre logiciel de courrier électronique, vous aurez de meilleures chances de contrôler les pourriels que vous recevez. Consultez la documentation relative à votre logiciel pour obtenir plus d'information.

Créez une adresse électronique « *alphanumérique* ».

En créant une adresse électronique qui contient à la fois des chiffres et des lettres, il sera plus difficile pour les polluposteurs de deviner votre adresse. (Exemple : jean72robert@_____.ca)

Servez-vous de plus d'une adresse électronique.

Il est préférable d'avoir une adresse électronique dont vous vous servirez uniquement pour communiquer avec vos amis et votre famille, une autre que vous utiliserez pour communiquer avec des entreprises dignes de confiance et une troisième pour les activités telles que les abonnements, les messages sur un babillard électronique, les sites de réseautage social et d'autres services en ligne qui requièrent une adresse électronique. L'utilisation d'une troisième adresse pour les autres activités peut réduire le nombre de pourriels reçus dans les comptes de courrier électronique utilisés pour communiquer avec les entreprises dignes de confiance ainsi qu'avec vos amis et votre famille. Renseignez-vous auprès de votre fournisseur de services Internet (FSI) pour savoir comment vous pouvez créer des adresses électroniques supplémentaires. Un certain nombre de services de courrier électronique gratuits sont également disponibles sur Internet.



Protégez-vous

Ne répondez jamais à des courriels vous demandant de fournir des renseignements personnels.

Les hameçonneurs envoient souvent des courriels qui paraissent authentiques et qui semblent provenir d'entreprises légitimes bien connues pour demander des renseignements personnels ou vous demander de confirmer des renseignements personnels qui servent ensuite à la fraude. Ne répondez pas à des courriels qui proviennent prétendument, par exemple, de votre institution financière ou d'autres organisations légitimes et vous demandant de fournir votre mot de passe, vos renseignements financiers ou d'autres renseignements personnels. Votre banque ne devrait jamais vous envoyer un courriel vous demandant de fournir cette information. Même si un représentant de votre banque vous appelle parce qu'il soupçonne une activité frauduleuse dans votre compte bancaire ou de carte de crédit, il ne devrait jamais vous demander de fournir vos mots de passe ni vos numéros de comptes verbalement ni en vous servant du clavier téléphonique.

Si on vous demande ce type de renseignements, appelez l'organisation pour vous assurer que la demande est valide, mais **n'utilisez pas** l'adresse électronique ni les coordonnées téléphoniques fournies dans le courriel parce qu'elles pourraient bien également être fausses. Cherchez plutôt les coordonnées de l'organisation sur son site Web, dans l'annuaire téléphonique ou dans la correspondance imprimée que vous aurez reçue de celle-ci.

Ne composez jamais un numéro interurbain que vous recevez dans un courriel non sollicité.

Certains polluposteurs vous enverront un courriel faisant la promotion d'un service ou d'un produit que vous n'avez jamais demandé. Le message peut contenir un numéro de téléphone que l'on vous demande de composer pour retirer votre adresse de la liste de diffusion. Ne composez pas ce numéro puisque les fraudeurs pourraient tenter de vous voler votre service d'interurbains, ce qui est appelé de la fraude touchant les appels interurbains.

Faites attention aux numéros de téléphone 1-900 qui sont connectés à des services tarifés à l'appel. Les services tarifés à l'appel comprennent les services en direct et les services préenregistrés comme les lignes de bavardage pour adultes, l'enregistrement de votes, la consultation de voyants, l'horoscope, la couverture de téléromans, des jeux, la collecte de fonds, des résultats sportifs, des prévisions météorologiques, de la traduction ainsi que des services de médias, juridiques ou gouvernementaux. Il faut comprendre que vous devez payer pour tous les appels faits à partir ou facturés à votre compte téléphonique peu importe qui a fait les appels ou a accepté de payer les frais. Cela signifie également que si vous êtes victime de fraude touchant les appels interurbains, vous êtes responsable des coûts.

Créez des mots de passe composés à la fois de caractères et de chiffres.

Plus un mot de passe est complexe, plus il sera difficile à deviner par d'autres personnes. Si possible, créez des mots de passe composés d'au moins huit caractères comportant à la fois des chiffres, des lettres et des caractères spéciaux.

Changez vos mots de passe.

Vous réduirez ainsi le risque que vos mots de passe soient découverts.

Mémorisez vos mots de passe.

À moins que vous n'utilisiez un logiciel de gestion de mots de passe sûr, conserver vos mots de passe dans un fichier sur votre ordinateur n'est pas sécuritaire. Votre ordinateur pourrait être infiltré ou volé. Mémoriser ses mots de passe constitue la meilleure protection. Si vous décidez de noter vos mots de passe alors :

- Ne conservez pas votre nom d'utilisateur et votre mot de passe au même endroit.
- N'incluez pas d'en-têtes évidents sur la page comme « mon mot de passe » ou « mes noms d'utilisateur ».
- Ne placez pas cette information près de votre ordinateur.