Les courriels

La sécurité des informations, j'y veille! *Volume 2, Numéro 2, Mars 2012*

Le courriel est maintenant le moyen de communication par excellence sur Internet entre collègues, parents et amis. Il permet une communication beaucoup plus rapide et efficace que la poste régulière, et ce, quelle que soit la distance qui sépare l'expéditeur du destinataire. Par contre, comme il est le moyen de communication probablement le plus utilisé, nous devons tous être très vigilants dans l'utilisation que l'on en fait, puisque plusieurs malfaiteurs tenteront de l'utiliser comme porte d'entrée.

La sélection des adresses courriel est importante!

Normalement, avec tout abonnement à Internet, le fournisseur octroie au moins une adresse de messagerie qui est, en quelque sorte, votre adresse courriel principale.

L'adresse courriel principale, la plus importante, ne doit **jamais** être communiquée en dehors du cercle familial et des amis proches. En aucun cas elle ne devrait être fournie sur Internet (dans un formulaire d'inscription ou une liste de diffusion, par exemple) ou par d'autres biais (par téléphone, afin de recevoir une confirmation de réservation d'une compagnie aérienne). Toute adresse confiée de bonne foi à une base de données est susceptible de se retrouver, un jour pas si lointain, entre les mains d'un polluposteur.

Lorsque vous naviguez sur le Web, il est préférable d'utiliser une adresse courriel spécialement créée à cet effet, une adresse jetable. Idéalement, vous pouvez la créer à partir d'un service de messagerie électronique gratuit (hotmail.com, yahoo.fr, google.fr, etc.). Vous pourrez donc la changer facilement en cas de besoin.

Pour les achats ou réservations en ligne, il est recommandé de créer une deuxième adresse avec le fournisseur d'accès Internet.

Qu'est-ce que les pourriels?

À l'image des prospectus papier qui inondent les boîtes aux lettres situées dans les rues ou dans les halls d'immeubles, les pourriels (également appelés « spams ») encombrent les boîtes aux lettres électroniques.

Un pourriel est un message non sollicité, de nature commerciale ou promotionnelle, provenant d'un expéditeur inconnu. Le principal problème posé par le pourriel réside dans sa propension à inonder une boîte aux lettres et à la polluer, jusqu'à saturation.

Règles et bonnes pratiques

⇒ Ne cliquez pas sur les liens proposés dans les pourriels.

⇒ Ne répondez jamais à un pourriel, même pour vous désabonner.

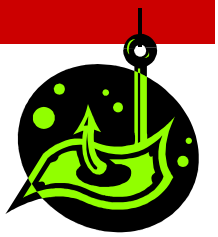
⇒ N'achetez pas de produits ou de services annoncés dans les pourriels. Saisissez directement l'adresse Web d'un site de commerce électronique dans la barre d'adresse. Cela vous évitera peut-être de tomber sur un site « cloné ».

⇒ N'ouvrez jamais les fichiers joints provenant d'expéditeurs que vous ne connaissez pas.

⇒ N'entrez pas dans des « chaînes ».

Agence de la santé et des services sociaux de la Côte-Nord
Québec

Éviter l'hameçonnage!



L'hameçonnage (ou pishing) est une tentative d'escroquerie qui vise à obtenir des renseignements personnels et financiers d'internautes, afin de les utiliser pour détourner des fonds.

Dans le courriel hameçon typique, un message au caractère urgent vous demande de cliquer sur un lien menant à un site Web qui imite l'apparence d'une institution reconnue, où vous êtes invité à divulguer des renseignements confidentiels sur votre compte bancaire, vos cartes de crédit, etc.

Méfiez-vous des courriels demandant des informations personnelles. Les entreprises sérieuses ne demandent jamais de renseignements importants par le biais d'un simple courriel.

L'utilisation adéquate du courrier électronique au travail

L'utilisation du courrier électronique peut présenter certains risques et ces risques ne nous permettent pas d'assurer totalement la confidentialité et l'intégrité des renseignements circulant dans le réseau Internet. Internet est une autoroute d'information.

Rappelez-vous également que cette autoroute à une capacité limitée et que nous partageons tous la même autoroute. Donc, il est important de limiter le partage de fichier lourd (document PowerPoint, photo, etc.) qui surcharge l'autoroute de l'information et empêche la circulation des données cliniques.

N'ouvrez jamais les courriels suspects. Un courriel suspect pourrait être considéré comme :

* un courriel non relié au travail (blague, image, etc.);
* un fichier joint que vous n'attendez pas;
* un fichier joint avec un nom de fichier suspect (*.exe, *.vbs, *.bin, *.com ou *.pif);
* un courriel qui vous enjoint à cliquer sur un lien Web.

Ouvrez une pièce jointe à un courriel SI ET SEULEMENT SI vous êtes sûr à 110 % que le courriel provient d'une source sûre.

Les techniques de chiffrement modernes permettent d'assurer la confidentialité et l'intégrité des courriels.

Écrivez et adressez prudemment, car une fois le courriel envoyé il peut être gardé longtemps.

Même si vous effacez un courriel sur votre poste, il y a plusieurs copies en circulation (ex. : serveur, archives, receveur, etc.).

Lors de l'envoi de courriels, vous devez être préoccupé par la confidentialité, les aspects légaux, la fuite d'information, le matériel offensant, etc.

Respecter la Nétiquette

* Utilisez le champ CCC dans Lotus Notes si vous envoyez un courriel à un groupe sans divulguer qui fait partie du groupe.
* Évitez de retransmettre les chaînes de courriels
* N'abusez pas de la fonction « répondre à tous »
* Utilisez un sujet significatif dans l'objet du courriel.
* Évitez d'écrire des phrases ou des mots en MAJUSCULES.

Anne Paquet
Officier de sécurité régional
Direction régionale des ressources informationnelles (DRRI)
Pour questions ou commentaires : anne.paquet.09siles@ssss.gouv.qc.ca

Dépôt légal
Bibliothèque et Archives nationales du Québec, 2012
ISSN : 1927-7911

Source : ***Formation générale sur la sécurité de l'information et la protection des renseignements personnels****, Ministère des Services gouvernementaux du Québec / ISIQ / 2010*
L'Internet + sûr, ça s'apprend*, sur le site www.protegetonordi.com, par Augustin GARCIA et David MARTIN*
Éliminer les pourriels et Éviter l'hameçonnage*, ISIQ pour la sécurité de l'information, http://monidentite.isiq.ca*