



## Adopter de bonnes pratiques en sécurité de l'information

### Contexte

L'objectif de ce guide sur la sécurité dans les technologies de l'information et des télécommunications est d'établir les bonnes pratiques concernant autant l'usage personnel que l'usage corporatif d'un ordinateur et de l'Internet.

### Principe

Il faut reconnaître que dans le domaine de l'informatique et de l'Internet, il n'y a pas de sécurité absolue. Cependant, on peut adopter des pratiques qui peuvent nous fournir une sécurité raisonnable.

### Règles et bonnes pratiques

#### 1. Pratiques générales

- Il faut toujours se rappeler que tout ordinateur, et plus spécialement ceux utilisés dans le cadre d'une fonction officielle (poste de travail d'un travailleur autonome, d'un conseiller, d'un trésorier, d'un directeur, etc.), sont susceptibles de contenir des informations sensibles. Il faut être alors attentif et prudent dans l'utilisation de cet ordinateur pour des motifs personnels (messages échangés, sites Internet visités, logiciels installés, etc.).
- TOUS les ordinateurs, et plus spécialement les ordinateurs de travail devraient être protégés par des logiciels antivirus efficaces (voir section : Ordinateurs 2.2).
- Les logiciels ou services (adresse électronique, site Web, etc.) offerts gratuitement sur l'Internet doivent être utilisés avec prudence.

#### 2. Les ordinateurs

- TOUT ordinateur DOIT avoir un Antivirus à jour. (Symantec, McAfee, etc.). Les virus peuvent autant provenir de l'Internet que d'une unité de stockage tel que des clés USB ou des disques durs externes.
- Tout ordinateur branché sur l'Internet DOIT AUSSI avoir un anti-espioniciel (contre les logiciels espions) et pare-feu logiciel à jour. (Symantec, McAfee, etc.).

- Tout ordinateur ou réseau possédant un lien Internet haute vitesse DOIT être relié à l'Internet par un pare-feu matériel (Linksys, DLink, SMC, etc.).
- Faire une copie de sécurité des fichiers (« back-up ») et la remettre dans un lieu sécuritaire différent (éventuellement un autre édifice). Un disque dur USB externe est un moyen simple et peu dispendieux de réaliser ses copies de sauvegarde.
- Fermer complètement les ordinateurs liés à l'Internet lorsqu'ils ne sont pas utilisés sur une longue période (soir, nuit, week-end, etc.).
- Pour les ordinateurs portables :
  - a) Ne pas y conserver d'information sensible ou personnelle.
  - b) Si vous devez y placer de l'information personnelle, une solution est de la conserver dans une section chiffrée (crypté) du disque dur. On peut chiffrer un disque dur, en totalité ou en partie, à l'aide d'un logiciel spécialisé pour un coût modique.
  - c) Certains ordinateurs portables vous permettent de les configurer pour que leur accès ou que l'accès au disque dur se fasse à l'aide d'un mot de passe.  
 Il faut noter que cette protection peut être contournée par un technicien.
  - d) Dans tous les cas, toujours conserver une copie de sécurité à jour de vos fichiers.
- Formatez toujours les disques durs des ordinateurs dont vous avez à vous départir. Cela servira à effacer minimalement toutes les données qu'ils contiennent.  
 Il faut noter que les données ainsi effacées pourraient être retrouvées par un technicien.
- Si votre ordinateur contient des informations sensibles ou personnelles, il est recommandé, avant de s'en départir, d'utiliser un logiciel spécialisé pour effacer de manière sécuritaire toutes les informations qui y sont inscrites.

### 3. Les mots de passe

- Un bon mot de passe doit contenir au moins 8 caractères.
- Il est constitué d'un mélange de chiffres et de lettres majuscules, minuscules et possiblement des symboles.
- Il doit être facile à mémoriser tout en ne contenant pas des informations facilement associables à une personne (nom, coordonnées, etc.).

Un exemple de mot de passe serait : « \_Toyota07verte\_ » pour une personne possédant une voiture Toyota verte 2007, ou encore : « +Rikia2ans+ » pour une personne possédant un animal de deux ans nommé Riki. Il est à noter que ces deux mots de passe commencent et se terminent par des caractères spéciaux, soit le trait de soulignement « \_ » pour le premier mot de passe, ou le plus « + » pour le second.

### 4. Les renseignements personnels

- La prudence à l'égard des renseignements personnels veut parer contre le vol d'identité. Le vol d'identité est l'un des principaux problèmes liés à l'Internet : attention aux informations personnelles inscrites dans les messages, informations qui peuvent être cumulées.
- Ne pas inscrire de renseignements personnels dans les messages envoyés par Internet, ni sur aucun site web où l'on présente les personnes, bénévoles et professionnelles, travaillant pour la communauté, comme par exemple : numéro d'assurance sociale,

numéro de carte de crédit, date d'anniversaire, adresse, codes d'accès.

- N'hésitez pas à utiliser le téléphone ou le télécopieur pour transmettre des informations confidentielles demandées. Ces médiums de communication assurent davantage la confidentialité des informations échangées. Assurez-vous que la personne à qui vous destinez ces informations soit bien celle avec laquelle vous parlez, ou qu'elle attende près du télécopieur.

## 5. Le courrier électronique, le blogue et les messageries instantanées

- Il faut toujours se rappeler qu'en envoyant un message sur l'Internet (courriel, clavardage, etc.), c'est l'équivalent d'un message énoncé dans un ascenseur bondé. Prenez pour acquis qu'un message envoyé sur l'Internet est public et peut être intercepté de multiples façons.
- Ne pas répondre aux sollicitations non-désirées, demandes non-habituelles. Cela inclut les prix gagnés sans que vous ayez participé à quoi que ce soit, les héritages ou les montants à transférer à partir de pays étrangers avec un pourcentage en commission, les messages qui sollicitent des aides et des services financiers sans référence précise ou avec des références douteuses, etc. **Effacer simplement ces messages.**
- Ne pas répondre par courriel à des demandes de confirmation de renseignements personnels qui semblent venir d'organismes avec lesquels vous faites affaire (exemple : votre institution financière, etc.). En cas de doute, vous pouvez toujours leur téléphoner.

Ne **jamais utiliser les hyperliens de ces messages** : les hyperliens de courriels peuvent vous conduire à des sites différents de ceux qu'ils annoncent. Dans ces cas, il faut vérifier si l'hyperlien correspond au site qui apparaît au bas du fureteur avant de cliquer sur lui.

- Effacer les pourriels (*spam*) sans les consulter.
- Ne pas ouvrir le fichier attaché d'un courriel dont on ne connaît pas la source.
- Attention aux fichiers avec des photos, des diapositives, des animations, etc. qui peuvent transporter facilement des virus. Votre antivirus doit toujours être à jour car un virus pourrait même provenir d'un courriel d'une personne que vous connaissez et qui a été infecté à son insu.
- Désactivez l'exécution automatique de macros de votre logiciel de courriels pour ne pas qu'il exécute lors de son ouverture une commande cachée dans le contenu du message que vous venez de recevoir. Demandez l'aide de votre service technique en cas de doute.

## 6. Les sites Web et les achats en ligne

- Consigne de navigation : faire des achats en ligne sur les sites de compagnies reconnues dont vous avez écrit vous-même l'adresse dans votre fureteur.

Si vous utilisez vos favoris, assurez-vous que l'adresse est bien celle du site que vous voulez visiter.

Faites attention, vérifiez toujours l'adresse du site dans la barre du fureteur car certains virus peuvent changer les adresses de vos favoris. Votre antivirus doit toujours être à jour afin de vous aider à vous protéger contre ce désagrément.

- Ne pas accepter que votre fureteur web mémorise le nom d'un site, votre mot de passe et votre nom d'utilisateur.

À la limite, si vous avez peur de les oublier, notez ces informations dans un carnet que vous rangerez dans un endroit sécuritaire.

- Avoir une carte de crédit dédiée aux achats en ligne, avec une limite basse de crédit.

## 7. La connexion à l'Internet via un routeur sans-fils

- Pratiques concernant la **configuration du routeur sans-fils** de la communauté ou de l'organisation :
  - a) Changer le mot de passe d'administration par défaut et en choisir un nouveau (qui respecte les bonnes pratiques des mots de passe décrites ci-dessus).
  - b) Changer le SSID (nom d'identification de ce routeur sans-fils) par défaut et en choisir un plus significatif et facile à retenir.
  - c) Désactiver l'émission du SSID par le routeur, afin que seuls ceux qui le connaissent puissent s'y connecter.
  - d) Activer le chiffrement de la liaison sans-fils (idéalement choisir le chiffrement : WPA2)
  - e) Limiter l'accès à votre routeur sans-fils à l'aide du numéro de chaque ordinateur. (Inscrire l'adresse MAC de chaque ordinateur autorisé dans le routeur).
  - f) Activer l'APIsolation, afin de s'assurer que les ordinateurs utilisant la connexion sans-fils ne se voient pas entre eux.
  - g) Ne pas autoriser l'administration du routeur via le lien sans-fils.
- Pratiques concernant l'utilisation d'une **connexion sans-fils publique** avec son portable
  - h) ATTENTION ! N'échangez aucune information confidentielle quand vous êtes branché à un réseau sans-fils public, tel que celui d'une bibliothèque, d'un restaurant ou d'une école.
  - i) L'ordinateur portable devrait être configuré afin de ne pas se connecter automatiquement à un réseau sans-fils public, sans la demande préalable de l'utilisateur. Cette connexion devrait toujours être provisoire (quelques heures).
  - j) Avant d'écrire quelque information sensible, s'assurer que vous êtes bien connecté à un site web chiffré (petit cadenas dans le bas de l'écran du navigateur) lorsque vous utilisez un réseau sans-fils public. Sans cette précaution, un autre utilisateur du réseau pourrait écouter votre communication et intercepter, par exemple, votre nom d'utilisateur et le mot de passe de votre boîte de courriel, ou le numéro de votre carte de crédit que vous aurez utilisée pour effectuer un achat.

## 8. Le soutien technique

- Soutien technique à distance :
  - a) Si vous utilisez les services d'une firme pour faire la gestion de vos systèmes informatiques à distance : ne pas leur permettre un accès automatique à votre système.  
Exigez plutôt un mécanisme qui nécessitera une autorisation manuelle préalable de votre part.  
Par exemple, lorsqu'un technicien voudrait faire une intervention à distance sur votre système, il aurait à vous téléphoner afin que vous lui remettiez le numéro d'autorisation unique nécessaire pour établir la connexion.

- Soutien technique sur place, dans l'organisation ou à domicile :  
Vérifier l'identité du technicien. En cas de doute, téléphoner à la personne qui aurait fait la demande ou encore à la firme pour laquelle cette personne est supposée travailler. Ne jamais laisser le technicien avoir accès aux ordinateurs, ou tout autre matériel informatique de la communauté, ni le laisser emporter d'appareil avec lui, surtout si le technicien insiste notamment en évoquant des délais pressants.

Dernière mise à jour : 21 août 2007