



Conseil canadien de la magistrature

La protection en dix points des renseignements judiciaires informatisés

La protection en dix points des renseignements judiciaires informatisés

Guide établi à l'origine par le Sous-comité sur la sécurité informatique, Comité consultatif sur la technologie, Conseil canadien de la magistrature, le 15 mai 2002. Deuxième édition, 26 juillet 2006.

1. **Les appareils portatifs.** Gardez tous vos appareils portatifs (par exemple ordinateur portable, téléphone mobile, Blackberry, assistant numérique personnel, support d'information amovible comme les unités de mémoire Flash USB) en votre possession lorsque vous voyagez. Autrement, verrouillez ces appareils au moyen d'un câble anti-vol et rangez-les dans le tiroir d'un bureau fermé à clé, dans le coffre-fort de l'hôtel ou dans le coffre de votre voiture.
2. **Les mots de passe.** Choisissez un mot de passe compliqué pour n'importe quel compte informatique. Utilisez au moins six caractères, quelque chose qui ne soit ni un nom propre ni un mot du dictionnaire. Utilisez également une combinaison de lettres (majuscules et minuscules), de chiffres et de symboles, par exemple « FtLYd%7 ». Changez vos mots de passe régulièrement et ne les divulguez à personne. Pour conserver tous vos mots de passe, servez-vous d'un logiciel de gestion de mots de passe qui les protège tout en vous permettant de les récupérer facilement. N'écrivez jamais vos mots de passe à des endroits où d'autres personnes peuvent les voir.
3. **La sauvegarde.** Lorsque vous n'êtes pas connecté au réseau, veillez toujours à sauvegarder les fichiers importants. Vous pouvez utiliser une unité mémoire Flash USB, une unité de disque dur externe, une unité de bande magnétique, ou un CD ou DVD inscriptible. Assurez-vous que les fichiers sauvegardés soient chiffrés ou verrouillés, ou les deux.
4. **Le courriel.** N'ouvrez jamais des pièces jointes à un courriel d'une source inconnue et ne cliquez jamais sur un lien dans un courriel d'une source inconnue ou suspecte, surtout si l'auteur du courriel vous demande des renseignements personnels. De tels courriels pourraient être des tentatives d'« hameçonnage » ou de dangereux canulars se faisant passer pour de légitimes messages. Utilisez un filtre de pourriel pour réduire les risques d'intrusion.
5. **La protection contre les virus et les logiciels-espion.** Assurez-vous d'utiliser un logiciel anti-virus et anti-logiciel-espion. Les logiciels-espion, qui s'apparentent aux logiciels publicitaires, sont des exemples de codes malveillants qui prennent le contrôle des navigateurs Web, qui affichent des annonces publicitaires non sollicitées, et qui peuvent même épier vos activités informatiques. Assurez-vous de faire une mise à jour régulière du logiciel de protection et de configurer le logiciel de manière à vérifier automatiquement le courriel, les sites Web et les fichiers téléchargés.

6. **Les métadonnées.** Avant d'expédier des fichiers informatiques (comme des projets de jugement) à l'extérieur de l'environnement sécurisé de la cour, assurez-vous toujours de supprimer toutes les données cachées (les « métadonnées »), par exemple les révisions d'un texte, le texte supprimé de versions antérieures, ou des renseignements personnels. Voir l'article « Évitez le piège des métadonnées », paru dans le numéro d'octobre 2006 du bulletin *Actualités technologiques pour les juges*.
 7. **Le chiffrement.** Utilisez une technologie de chiffrement fiable pour protéger les données particulièrement sensibles qui sont stockées dans votre ordinateur, que vous les transmettiez ou non. Demandez au besoin l'aide de l'administrateur de système.
 8. **La sécurité du système d'exploitation.** Lorsque vous recevez un message d'incitation de Microsoft Windows vous invitant à installer des pièces ou des correctifs sur votre système d'exploitation, confirmez la légitimité du message et installez ensuite la pièce ou le correctif pour vous assurer que votre système d'exploitation soit à jour. Les messages d'incitation de Microsoft ne sont jamais envoyés par courriel. Pour plus de renseignements à ce sujet, consultez le site Web de Microsoft sur la sécurité de l'informatique à l'adresse suivante : <http://www.microsoft.com/canada/fr/athome/security/default.mspx>.
 9. **La sécurité de la réseautique sans fil.** Les réseaux sans fil sont d'une faiblesse notoire lorsqu'il s'agit de sécurité, mais une installation incorrecte peut vous exposer à des risques encore plus élevés. Assurez-vous de prendre toutes les mesures de sécurité possibles lorsque vous utilisez n'importe quel réseau sans fil. Utilisez l'équipement le plus récent de manière à bénéficier de la protection la plus actuelle en matière de sécurité de la réseautique sans fil.
 10. **La surveillance.** La surveillance des ordinateurs des juges soulève de sérieuses questions concernant la vie privée, la confidentialité et l'indépendance des juges. Les juges en chef devraient s'adresser à l'administrateur de système compétent pour savoir dans quelle mesure et de quelle façon l'usage des ordinateurs par les juges et par le personnel judiciaire fait l'objet d'une surveillance.
-

Pour plus de renseignements, veuillez communiquer avec le Conseil canadien de la magistrature par courriel à info@cjc-ccm.gc.ca ou par téléphone au (613) 288-1566.