Dix choses que les juges peuvent faire pour améliorer la sécurité des renseignements judiciaires informatisés[1]

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. Troisième édition, mai 2009. Quatrième édition, août 2009. Cinquième édition, 17 janvier 2014.

1. **Les appareils mobiles.** Gardez tous vos appareils mobiles (par exemple ordinateurs portatifs, tablettes électroniques et téléphones intelligents) avec vous lorsque vous voyagez. Autrement, verrouillez ces appareils au moyen d'un câble antivol et rangez-les dans le tiroir d'un bureau, dans le coffre-fort de l'hôtel ou dans le coffre de votre voiture. Pour protéger vos renseignements personnels et ceux des autres, lorsque vous voyagez à l'étranger, pensez à utiliser des appareils équipés pour la connectivité câblée ou sans fil sur lesquels aucune information sensible n'est conservée localement.
2. **Les mots de passe**. Utilisez un mot de passe différent pour chaque compte. Pour tous les comptes, utilisez des mots de passe forts, comportant au moins six caractères, quelque chose qui ne soit ni un mot du dictionnaire ni un nom propre, combinant des majuscules et des minuscules, des chiffres et des symboles (par exemple, « FtLYd%7 »; si le système ne permet que des lettres, un long mot composé constitue aussi un excellent choix « passemoilesel »). 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. Les logiciels de gestion des mots de passe populaires comprennent RoboForm[2] et Password Safe[3].
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 ou une unité de disque dur, mais assurez-vous que les fichiers sauvegardés soient chiffrés ou verrouillés, ou les deux. N'utilisez les services d'archivage en nuage comme Dropbox, Google Drive ou Skydrive que pour les fichiers non confidentiels, puisque ces systèmes ne sont pas chiffrés.

---

[1] Remarque importante : les exemples de logiciels sont présentés à titre informatif. Les juges sont encouragés à faire leurs propres recherches et à choisir les logiciels appropriés à leurs besoins. Les logiciels mentionnés dans cet article n'ont pas été officiellement testés, recommandés ou approuvés par le Conseil canadien de la magistrature.

[2] http://www.roboform.com/

[3] http://passwordsafe.sourceforge.net/index.shtml

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 que vous pourriez prendre pour de légitimes messages.
5. **La protection contre les virus et les logiciels-espions**. Assurez-vous d'utiliser un logiciel antivirus et anti-logiciel-espion. Les logiciels-espions et les publiciels, qui leur sont étroitement apparentés, sont des exemples de codes malveillants très persistants qui prennent le contrôle des navigateurs Web, affichent des annonces publicitaires non sollicitées et peuvent même épier vos activités informatiques. Assurez-vous que le logiciel de protection soit mis à jour sur une base régulière et qu'il soit configuré de manière à vérifier automatiquement les fichiers téléchargés, les sites Web et le courriel. Considérez les logiciels offerts par des fournisseurs réputés, comme McAfee[4], Symantec[5], Trend Micro[6] et Kaspersky[7].
6. **Les métadonnées.** N'expédiez jamais de fichiers informatiques (comme des projets de jugement) à l'extérieur de l'environnement sécurisé de la cour sans en avoir supprimé toutes les données cachées, par exemple les révisions d'un texte, le texte supprimé de versions antérieures, ou des renseignements personnels (les « métadonnées »). Les versions récentes des logiciels de traitement de texte comportent des outils permettant de supprimer les métadonnées. Metadata Assistant[8] est un logiciel commercial populaire pour la suppression des métadonnées.
7. **Le chiffrement**. Utilisez une technologie de chiffrement fiable pour protéger les données particulièrement délicates qui sont stockées dans votre ordinateur, que vous les transmettiez ou non. Au besoin, demandez l'aide de votre administrateur de système. Les juges pourraient faire l'essai de Truecrypt[9], PC-Encrypt (offerts gratuitement) ou des outils de chiffrement offerts par Symantec[10] (qui sont aussi offerts pour les appareils Blackberry et qui sont approuvés par le gouvernement des États-Unis).
8. **Le système d'exploitation de l'ordinateur à la maison**. 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/security/default.aspx
9. **Le réseau sans fil à la maison**. 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

---

[4] http://www.mcafee.com/
[5] http://www.symantec.com
[6] http://us.trendmicro.com
[7] http://www.kaspersky.com
[8] http://www.thepaynegroup.com/support/faq/metadata/
[9] http://www.truecrypt.org/
[10] http://www.symantec.com/products-solutions/families/?fid=encryption

plus récent de manière à bénéficier de la protection la plus actuelle en matière de sécurité de la réseautique sans fil.

a. Utilisez le chiffrement WPA2 plutôt que le WEP
b. Changez le nom par défaut du réseau
c. Désactivez la diffusion du SSID
d. Efforcez-vous de placer le routeur sans fil de manière à limiter les « fuites » vers les voisins
e. Envisagez la possibilité d'utiliser le filtrage par adresse MAC (demandez de l'aide, au besoin)
f. Envisagez la possibilité d'utiliser des adresses IP statiques (demandez aussi de l'aide)

10. **La réseautique sans fil en voyage**. Par définition, les points d'accès Wi-Fi publics (p. ex. : dans les hôtels, les centres de conférences, les cafés et les aéroports) *ne sont pas* sécurisés. Cela signifie que tout ce que vous transmettez sur un réseau sans fil public – incluant le contenu des courriels, vos recherches sur les sites Web non sécurisés (non SSL) et vos mots de passe d'accès – peuvent être facilement surveillés et ensuite utilisés pour compromettre la sécurité de vos renseignements personnels et des renseignements judiciaires. Lorsque vous utilisez un réseau sans fil en voyage :
    a. utilisez uniquement les connexions d'un réseau privé virtuel (RPV) fourni par la cour pour accéder aux données du réseau;
    b. si vous n'êtes pas branché par l'entremise d'un RPV, branchez-vous uniquement à des sites Web sécurisés (p.ex. : https://...);
    c. si vous n'êtes pas branché par l'entremise d'un RPV, assurez-vous que les services que vous utilisez sont sécurisés (par exemple, Judicom est sécurisé, Yahoo Mail ne l'est pas);
    d. désactivez le partage des services, des dossiers et des fichiers conservés sur votre ordinateur portable – ceci est habituellement la configuration par défaut (demandez de l'aide);
    e. utilisez un logiciel pare-feu personnel (vous pourriez avoir besoin d'aide pour cela).

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.