CJC CCM

Canadian Judicial Council

Conseil canadien de la magistrature

La protection en dix points des renseignements judiciaires informatisés[1]

La première version a été préparée le 15 mai 2002 par le Sous-comité de la sécurité du Conseil consultatif sur la technologie du Conseil canadien de la magistrature. Deuxième version : le 26 juillet 2006. Troisième version : mai 2009. Quatrième version : août 2009.

1. **Les appareils portatifs.** Lorsque vous voyagez, gardez toujours avec vous vos appareils portatifs tels que les ordinateurs portatifs, les BlackBerry, les assistants numériques personnels (ANP) et les supports amovibles, comme les clés USB à mémoire flash. Sinon, verrouillez-les à l'aide d'un câble antivol et rangez-les dans un tiroir de bureau, un coffre-fort d'hôtel ou le coffre de votre voiture. Dans le but de préserver votre vie privée et celle des autres lors de vos déplacements à l'étranger, utilisez des appareils qui sont munis d'une connexion avec ou sans fil, mais qui ne referment aucune donnée confidentielle dans leur mémoire locale.
2. **Les mots de passe.** Choisissez un mot de passe complexe pour chacun de vos comptes informatiques. Un tel mot de passe devrait compter plus de six caractères et comprendre des majuscules, des minuscules, des numéros et des symboles (p. ex., « FtLYd%7 »). N'employez aucun mot du dictionnaire ou nom propre. Changez vos mots de passe fréquemment et ne les divulguez à personne. Pour ne pas oublier vos mots de passe, utilisez un gestionnaire de mots de passe vous permettant de les

[1] Nota : Les logiciels cités en exemple sont proposés pour plus de commodité. On invite les juges à trouver les logiciels qui répondront à leurs besoins. Le Conseil canadien de la magistrature n'a éprouvé, recommandé ni approuvé aucun logiciel mentionné dans le présent document.

chiffrer tout en les rendant aisément accessibles. Ne conservez jamais vos mots de passe à un endroit où d'autres personnes pourraient les voir. RoboForm et Password Safe sont deux progiciels de gestion de mots de passe populaires.

3. **Les copies de sauvegarde**. Faites toujours une copie de sauvegarde de vos fichiers importants lorsque vous n'êtes pas branché au réseau. Vous pouvez utiliser une clé USB à mémoire flash, un disque dur externe, un périphérique à bandes ou bien des CD ou des DVD inscriptibles, à condition que la copie de sauvegarde soit chiffrée, verrouillée ou les deux. Microsoft Backup est inclus dans Windows.
4. **Les courriels**. N'ouvrez aucune pièce jointe d'un courriel provenant d'une source inconnue et ne cliquez jamais sur un lien contenu dans un courriel provenant d'une source inconnue ou suspecte, surtout si son auteur vous demande des renseignements personnels. Il pourrait s'agir d'un courriel d'« hameçonnage » ou d'un canular dangereux présenté sous la forme d'un message légitime. Configurez et utilisez des filtres antipourriel pour réduire les risques d'intrusion indésirable. Certains programmes de messagerie électronique comprennent des détecteurs de pourriel. Vous pourriez aussi choisir des programmes conçus par des fabricants réputés, comme McAfee, Symantec, Trend Micro et Kaspersky.
5. **Les antivirus et les anti-logiciels espions**. Assurez-vous d'utiliser un antivirus et un anti-logiciel espion. Les logiciels espions et les logiciels publicitaires, leurs proches parents, sont des exemples très persistants de programmes malveillants qui prennent le contrôle des navigateurs Web, font surgir des publicités indésirables et surveillent même l'usage que vous faites de votre ordinateur. Assurez-vous de mettre régulièrement à jour les signatures de protection et de configurer vos logiciels pour qu'ils analysent automatiquement les fichiers téléchargés ou téléversés, les sites Web et les messages électroniques. Choisissez des programmes conçus par des fabricants réputés, comme McAfee[2], Symantec[3], Trend Micro[4] et Kaspersky[5].
6. **Les métadonnées.** N'envoyer aucun fichier informatique (comme des projets de jugement) à l'extérieur de l'environnement sécurisé de la cour sans d'abord vous assurer de supprimer tout renseignement caché, comme les révisions, les versions antérieures ou les renseignements personnels confidentiels (les « métadonnées »). Les derniers traitements de texte comprennent des outils de nettoyage des métadonnées. Metadata Assistant[6] et SendShield[7] sont deux programmes disponibles sur le marché.
7. **Le chiffrement.** Utilisez une technologie de chiffrement fiable pour protéger les données particulièrement sensibles qui sont enregistrées dans votre ordinateur, que vous les transmettiez ou non. Au besoin, demandez l'aide de votre administrateur de système. Vous pourriez essayer PC-Encrypt (gratuit) ou des outils de chiffrement comme PGP[8] (qui sont aussi disponibles pour les BlackBerry et approuvés par le gouvernement américain).
8. **Le système d'exploitation**. Lorsque Microsoft Windows vous invite à installer des correctifs de sécurité pour votre système d'exploitation, vérifiez d'abord la pertinence

---

[2] http://www.mcafee.com
[3] http://www.symantec.com
[4] http://us.trendmicro.com
[5] http://www.kaspersky.com
[6] http://www.payneconsulting.com/products/metadataretail
[7] http://www.sendshield.com
[8] http://www.pgp.com

de l’invitation, puis installez les correctifs pour vous assurer de toujours utiliser un système d’exploitation à jour. Microsoft n’envoie jamais ces invitations par courriel. Pour de plus amples renseignements, veuillez visiter le site Web de Microsoft sur la sécurité informatique individuelle au http://www.microsoft.com/protect/default.mspx.

9. **Le réseautage sans fil à domicile**. On sait que la sécurité des réseaux sans fil est faible, mais une installation inadéquate peut aggraver davantage cette faiblesse. Assurez-vous d’activer tous les dispositifs de sécurité disponibles pour votre réseau sans fil. Utilisez les appareils les plus récents pour tirer avantage des dernières mises à jour des normes de sécurité sans fil.
    a. Utilisez le chiffrement WPA plutôt que le chiffrement WEP.
    b. Modifiez le nom par défaut du réseau.
    c. Désactivez la diffusion du nom de réseau sans fil (SSID).
    d. Déposez le routeur sans fil à un endroit qui permet de limiter les « fuites » de signal vers vos voisins.
    e. Activez le filtrage d’adresses MAC (demandez de l’aide au besoin).
    f. Utilisez des adresses IP statiques (demandez de l’aide supplémentaire).
10. **Le réseautage sans fil en déplacement.** Par définition, les points d’accès sans fil publics Wi-Fi (c.-à-d., dans les hôtels, les cafés et les aéroports) ne sont *pas* sécurisés. Cela signifie que les renseignements que vous transmettez au moyen d’un réseau sans fil public, ce qui comprend le contenu de vos courriels et des sites non sécurisés (sans protocole SSL) que vous consultez ainsi que vos mots de passe, peuvent être facilement interceptés, puis utilisés pour compromettre la sécurité de vos renseignements personnels ou judiciaires. Lorsque vous utilisez un réseau sans fil en déplacement :
    a. utilisez seulement les connexions de réseau privé virtuel (RPV) fournies par la Cour pour accéder aux données du réseau;
    b. branchez-vous seulement à des sites Web sécurisés (p. ex., https://...) si votre connexion n’est pas établie au moyen d’un RPV;
    c. assurez-vous d’utiliser des services sécurisés (p. ex., JUDICOM est sécurisé, mais Yahoo Mail ne l’est pas) si votre connexion n’est pas établie au moyen d’un RPV;
    d. désactivez le partage des services, des dossiers et des fichiers sur votre ordinateur portatif. Cette option est généralement activée par défaut (demandez de l’aide);
    e. utilisez un coupe-feu personnel;
    f. installez les correctifs de sécurité recommandés afin de tenir à jour votre système d’exploitation.

Pour de plus amples 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.