Canadian Judicial Council

Ten Things Judges Can Do Now to Improve the Security of Judicial Data

Ten Things Judges Can Do Now to Improve the Security of Judicial Data

Originally prepared by the Security Subcommittee of the Judges Technology Advisory Committee of the Canadian Judicial Council, May 15, 2002. Second edition, July 26, 2006.

1. **Portable devices.** Keep all portable devices such as laptops, Blackberries, PDAs and removable media such as USB flash drives with you when traveling. Otherwise, keep these items securely locked with a safety cable, in a desk drawer, hotel room safe, or in the trunk of your car.
2. **Passwords.** For any computer account, choose a strong password, for example, at least six characters, not a dictionary word or proper noun, combining upper and lower case letters, numbers and symbols. (For example, “FtLYd%7”.) Change your passwords frequently and never share them with anyone. To keep track of all these passwords, use password management software that keeps your passwords readily accessible but encrypted. Never write your passwords down where they can be seen by others.
3. **Backup**. Always make a secure backup of important files if you are not connected to the network. You can use a USB flash drive, an external hard drive, tape device or recordable CD or DVD, as long as you ensure the backup itself is either encrypted, locked up or both.
4. **E-mail**. Never open e-mail attachments from unknown sources, and never click on a link in an e-mail from an unknown or suspicious source, especially if the e-mail is requesting personal information. Such e-mails could be attempts at “phishing,” or dangerous hoaxes masquerading as legitimate messages. Configure and use spam filters to reduce the risk of unwanted intrusions..
5. **Anti-virus and spyware**. Make sure you use available anti-virus and anti-spyware software. Spyware, and its close relative adware, are very persistent examples of malicious software code that take control of web browsers, pop up unwanted ads, and even spy on your computer activities. Always ensure that the protective software signatures are updated on a regular basis, and that the software is set to automatically scan uploaded or downloaded files, websites and e-mail.
6. **Metadata.** Never send computer files (such as draft judgments) outside a secure court environment without making sure that any hidden information such as revisions and deletions from previous drafts, or private personal information (“metadata”) has been cleansed. See “Avoid the Metadata Trap,” forthcoming, *Computer News for Judges*.
7. **Encryption**. Use reliable encryption technology to secure particularly sensitive information stored on your computer whether it is being transmitted or not. You may need to ask your System Administrator for assistance.

8. **Home Operating System**. When prompted periodically by Microsoft Windows to install security patches and fixes to your operating system, confirm the legitimacy of the prompt, and then install the patch to ensure your operating system is current. Prompts from Microsoft are never sent by e-mail. For more information, visit the Microsoft home computing security website: http://www.microsoft.com/athome/security/email/default.mspx
9. **Home wireless networking**. Wireless networks are notoriously weak when it comes to security, but improper installation makes an already poor situation untenable. Make sure you implement all the available security controls on any wireless network. Use the most current equipment to take advantage of recent updates in the wireless security standard.
10. **Monitoring.** Monitoring of judges' computer use raises serious issues about privacy, confidentiality and judicial independence. Chief Justices should identify the appropriate System Administrator and ask for details about the extent to which and ways in which judges' and judicial staff computer use is monitored.

For more information please contact the Canadian Judicial Council by e-mail at info@cjc-ccm.gc.ca or by telephone: (613) 288-1566.