Ten Things Judges Can Do Now to Improve the Security of Judicial Data[1]

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. Third edition, May 2009, Fourth Edition August 2009. Fifth edition, January 17, 2014.

1. **Mobile devices**. Keep all mobile devices such as laptops, tablets and smartphones with you when traveling. Keep these items securely locked with a safety cable, in a desk drawer, hotel room safe, or in the trunk of your car. To protect your privacy and the privacy of others, when travelling across international borders consider using devices configured with wired or wireless connectivity but no sensitive data stored locally.
2. **Passwords**. Use a different password for every account. For all accounts, 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". If the system allows only letters, a long compound word is also an excellent choice: "movethecheesealong".) Change your passwords frequently and never share them with anyone. To keep track of all your 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. Popular password management software packages include RoboForm[2] and Password Safe[3].
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 or an external hard drive, as long as you ensure the backup itself is either encrypted, locked up or both. Use cloud services such as Dropbox, Google Drive, or Skydrive only for non-sensitive files, as these systems are not encrypted.
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.
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

[1] Please note: Specific examples of software are provided for you convenience and all judges are encouraged to research and seek out software appropriate for their needs. Software mentioned here has not been officially tested, recommended or approved by the Canadian Judicial Council.
[2] http://www.roboform.com/
[3] http://passwordsafe.sourceforge.net/index.shtml

scan uploaded or downloaded files, websites and e-mail. Consider programs from reputable vendors such as McAfee[4], Symantec[5], Trend Micro[6] and Kaspersky[7].

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. Newer versions of word processing software contain metadata cleansing tools. Metadata Assistant[8] is a popular commercial metadata cleansing program.
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. Judges may wish to try Truecrypt[9], PC-Encrypt (for free) or encryption tools from Symantec[10] (which are also available for Blackberries and are US-government approved).
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/protect/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.
    a. Use WPA2 not WEP encryption
    b. Change the default network name
    c. Turn off SSID broadcasting
    d. Try to place the wireless router so as to limit signal "leakage" to neighbours
    e. Consider using MAC address filtering (get help if necessary)
    f. Consider using static IP addresses (get more help)
10. **Wireless networking on the road**. By definition public Wi-Fi hotspots (i.e. in hotels, conference centres, coffee shops and airports) are *not* secured. This means that what you transmit over a public wireless network - including the content of an e-mail, your web-browsing to unsecured (non-SSL) sites, and login passwords - can easily be monitored and then used to compromise the security of your personal and judicial information. When using wireless on the road,
    a. Use only court-provided VPN connections to access network data
    b. If you are not connecting through a VPN, connect only to secure websites (e.g. https://...)
    c. If you are not connecting through a VPN, make sure any services you use are secured (for example, Judicom is secured, Yahoo Mail is not)

---

[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

d. Disable sharing of services, folders and files on your laptop - this is usually enabled by default (get help)
e. Use personal firewall software (you may need help with this)

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