BRITISH COLUMBIA | Office of the Chief Information Officer

Tip Guide:
How to Protect Your Home Computer

May, 2010
Updated November 2016

Table of Contents

This Tip Guide is intended to provide Government employees with some tips and tools to protect their home computer. Examples of free software tools are identified in this Tip Guide to demonstrate that cost does not have to be a barrier to securing a home computer.

1. Why is it important to protect a home computer?

It is important to protect your home computer system to prevent computer viruses and malware (malicious software) from compromising the security of your computer. Viruses and malware on a compromised computer may be used by criminals to steal your personal information (your identity) and banking information, or gain unauthorized access to confidential and personal information.

If you are approved to use your home computer for government work you are required to ensure that you have adequately protected your computer. Please refer to the Working Outside the Workplace policy and the Home Technology Assessment for more information. Also read the government's Appropriate Use Policy. **Only in extenuating circumstances may a home computer be used for working on GOVERNMENT'S confidential, sensitive and/or personal information.**

2. What kinds of software should be used to protect (secure) a home computer?

There are four essential types of security software that should be active on your computer. They are available as standalone (commercial or freeware products), as part of certain Operating Systems (OS), or bundled as part of a Security Suite product/service. The four types of security software are:

1. **Anti-virus Software** – used to prevent, detect, and remove malicious software (malware), including computer viruses, worms, keyloggers and Trojan horse programs. Such software may also prevent, detect and remove adware, spyware, and other forms of malware.
2. **Firewall** – used to block unauthorized access to or from the Internet while permitting authorized communications. Firewalls are available as software programs installed on the personal computer or as separate hardware devices.
3. **Specialized File Deletion Software –** used to securely delete files created by a variety of software on your computer. The deleted files are erased in a manner that does not allow them to be easily recovered. **NOTE: Files deleted using the file *delete* function (Recycle Bin) in the operating system are still easily recoverable.**
4. **Encryption software** – used to transform (encrypt) plain-text information so that it is unreadable and secured until decrypted or changed (transformed) back to its original form. Encryption can be applied to an entire hard drive, folder, file or storage device (e.g. USB Flash Drive). Best practice dictates the use of encryption, especially when working with confidential and/or personal electronic information.

3. Is government providing software or support for a home computer?

Government provides support for specific remote access options to the government network. In addition, government has entered into a Home Use Offer agreement with Microsoft (Canada), Ltd. to enable employees to download Microsoft 365 at a nominal cost for up to ten installations (up to five on desktops and laptops, and up to five on mobile devices, such as iPads, iPhones and Android). *See the link in section 12 for more information on this offering.*

Government does not provide helpdesk support or tools for securing your home computer. This Tip Guide is intended to help the employee become self-sufficient by providing the knowledge on what tools can be used to protect their computer and where to find information about those tools.

Note that the use of Web-based products (word processors, spreadsheets, presentation software, form software, and data storage services – for example, Google Docs) is prohibited when working with government information, especially if the information is confidential, sensitive or personal.

4. 10 things you can do to secure your home computer

Protecting your home computer system from computer viruses and malware can keep your personal information from being compromised. Doing the following actions will help to ensure that your home computer is secured as much as possible. More detailed information is provided in the Tip Guide sections below.

1. Defend your computer in depth by using anti-virus software and firewalls (hardware devices and/or software). **These two components are absolutely essential and no computer system should be operated without anti-virus and firewall software**. *See section 6 and section 7 for details.*
2. Keep your operating system and software programs up-to-date with the latest security patches. Ensure that updates are applied regularly to the operating system and **ALL** the software programs installed on the computer. Ensure that automated updating features of the operating system and various software programs are enabled and scheduled. This is necessary as vulnerabilities in software programs are discovered daily. *See section 8 for details.*
3. Use secure file deletion software to permanently erase files. *See section 5 for details.*
4. Use encryption when storing data locally on your computer hard drive or on removable (portable) devices. Store sensitive files in an encrypted folder or in an encrypted virtual drive only. *See section 9 for details.*
5. Create a separate user profile/account on your home PC for your work activities (or personal identity activities such as banking) to isolate them from activities of other people using the same computer. For assistance in completing the suggested action, please refer to the HELP section of your operating system.
6. Set the screen saver to come on automatically after 15 minutes of computer inactivity with a password to resume computer activity. For assistance in completing the suggested action, please refer to the HELP section of your operating system.
7. Remember to change your password(s) periodically. One way to remember is to change your password at home when you have had to change it at work. Immediately change it if you suspect that it has been compromised. *See section 11 for details.*
8. If you use a wireless network at home or have a Wireless Network Router, ensure the default device configuration password is changed. Restrict access to the wireless network with a password and ensure the network transmissions are encrypted. *See section 10 for details.* Do not enable the web browser features that allow you to 'remember my password' and 'auto fill' forms as it increases the risk of losing information if your machine is compromised. For assistance in completing these suggested actions, please refer to the HELP section of your operating system.
9. Disable file and printer sharing as it enables other computers on the network you are connected into to access resources on your computer. When you use your mobile PC in a Wi-Fi hotspot, ensure that the file and printer sharing feature is disabled. When it is enabled, your computer will be vulnerable to hackers. For assistance in completing the suggested action, please refer to the HELP section of your operating system.

10. Educate yourself about the types of threats that can affect your computer and the associated tools available to protect your computer. Refer to the Information Security Awareness website for resources on the protection of information.

5. What is specialized file deletion software and why is it needed?

When computer files are deleted using the file delete function that comes with the operating system, the files are not actually deleted from the hard drive on your the computer. To describe how files are stored on the hard drive of your computer, think of books on a library bookshelf. Each book is labelled with a unique call number that is referenced in the card catalogue or index – even when the library book is checked out (or gone from the shelf) the unique call number still exists.

If specialized deletion software is not used, only the identification numbers for the files are erased, and not the contents of the file (the library book, or data still exists, the unique call number is erased). Using file recovery software, new numbers can be easily re-assigned to the 'deleted' files. Once this has been done, the files and their contents can be recovered. With specialized file deletion software, both the files and their index/reference numbers are deleted and then overwritten so that they cannot be easily recovered. Many of the secure deletion products in the marketplace provide extra security by also deleting the 'temporary' files created by many software programs and stored indefinitely on the computer hard drive. These temporary files may also contain sensitive information.

There are a variety of commercial general security and dedicated file erasure products available for use. Some operating systems feature built-in secure file erasure utilities. There are also freeware tools available, including: CCLeaner (http://www.piriform.com/ccleaner/) and Delete Files Permanently.

- For Microsoft Windows operating systems (Windows 7) there is the built-in "Cipher" utility that is available as part of the operating system.
    - To use the built-in operating system "Cipher" utility:
        - Delete the file as normal
        - Empty the Recycle Bin as normal
        - Bring up a Command Prompt window as the Cipher utility is a command line utility. Press **Start**, type **CMD** in the "Search Programs and Files" field and press return.
        - At the command line type:
            - **cipher /W:"*directory*"** ; where the word "directory is replaced with the name of the directory from which the files have been deleted. For example, to securely delete all the files from your default document directory on Windows 7 you would type:
                - **cipher /w:C:\Users\"*your user account name*"\Documents**.
            - For ease of use, the command can be run on the root of the local drive, and as such it will sanitize all the free space on the drive. For example, to securely erase all free space on local drive C: and therefore permanently erase all files that have been deleted from C: drive, the command to execute would be:
                - **cipher /w:C:**

- For Apple OSX, the operating system has "Secure Empty trash" built in.
    - For Apple OSX :
        - delete a file as normal
        - then select the Trash icon
        - Select "**Finder**" in the menu bar and press "**Secure Empty Trash**". This overwrites the files using 32 data passes.

Note that the above mentioned file deletion software does not delete temporary files or cookies. For step-by-step instructions on deleting cookies, please visit the AllAboutCookies.org (http://www.allaboutcookies.org) website. For information on how to delete your browsing history and temporary internet files, visit http://www.bnl.gov/itd/webapps/browsercache.asp.

6. Anti-virus software

Anti-virus software is an essential component and no computer system should be operated without it installed.

The following are base requirements in the configuration of the anti-virus software:

- Ensure that the anti-virus software installed is active. Typically, anti-virus software provides a visual status indicator via an icon in the taskbar usually found at the bottom of the screen.
- Ensure that the anti-virus software is configured to check and download definition updates daily. Periodically check the date when the definition files were last updated, to ensure that updates are being automatically installed.
- Ensure that a virus scan job is configured to scan the entire computer for viruses on a weekly basis.

There is a variety of commercial and freeware products in the marketplace and consumers need to make an informed choice about what is best for them. This can be done by conducting an Internet search using 'review' and the type of software, for example, 'anti-virus review' and reading the reviews. Wikipedia (http://en.wikipedia.org) is also a good starting point for general information and there are a number of computer magazines that maintain websites with reviews and comparisons of computer hardware and software. For example:

- Microsoft offers a free anti-virus security solution for Windows 7, and it can be downloaded from http://www.microsoft.com/security_essentials/
- PC Magazine provides reviews on commercial and free anti-virus software at http://wwwpcmag.com/category2/0,2806,4796,00.asp
- PC Magazine has identified 'The Best Free Software', by year, at http://www.pcmag.com/article2/0,2817,2381528,00.asp

It is important to take the time to check reputable sources such as those mentioned above and read reviews to ensure that you choose good software. Simply searching for anti-virus software on the Internet and picking one randomly is dangerous, since there are thousands of poorly designed products advertised on the Internet. Many are fake versions (called 'rogue software') used by cybercriminals to infect and gain access to computers.

7. Firewalls

A firewall is a protective system that lies, in essence, between your computer network and the Internet. When used correctly, a firewall prevents unauthorized use and access to your network. The job of a firewall is to carefully analyze data entering and exiting the network based on your configuration. It drops information that comes from an unsecured, unknown or suspicious location. A firewall plays an important role on any network as it provides a protective barrier against most forms of attack coming from the outside world.

Firewalls can be either hardware or software. The ideal firewall configuration will consist of both.

Software-based firewalls are available as part of some Operating Systems (e.g. Windows 7 and Apple OSX), as standalone products (e.g., Zone Alarm, Comodo Firewall), or as part of various security suites (e.g., Norton Internet Security, McAfee Internet Security, Kaspersky Internet Security). Reviews of Security Software are available at http://www.pcmag.com/reviews/software

Most routers and wireless network routers currently available commercially provide firewall services on the devices themselves. These are hardware-based firewalls that provide an additional layer of protection to computer systems. Hardware-based firewalls will shield the computer system or the computer network (LAN - several computer systems hooked up together) within the home from malicious attacks from the Internet by closing down all incoming ports by default.

It is recommended that both software-based firewalls and hardware-based firewalls/router devices are implemented on each personal computer.

The computer's operating system firewall needs to be enabled and active. To check this setting and to enable it, if necessary, confirm your operating system and then perform the following steps.

- Microsoft Windows 7
  - go to "*Control Panel*"
  - select "*Windows Firewall*" (in Classic View) **or** select "*System and Security*" then "*Windows Firewall*" (in Category View)
  - ensure that the "*ON*" option is selected.
- Apple OSX:
  - select "*System Preferences*", "*Security*" then "*Firewall*."

If a separate software-based firewall has been implemented instead of the built-in operating system firewall, check the settings within the security suite software to ensure that the firewall is active.

Hardware-based firewalls in the form of routers are recommended, in addition to software-based firewalls, as they provide additional protection from Internet based attacks. Low-cost home routers are available from many vendors such as Linksys, NetGear, D-Link and more. If the hardware-based firewall/router features wireless connectivity as well, follow instructions in the *secure your home wireless system* in *section 10*.

8. Software Updates

Since vulnerabilities in software programs are discovered daily, it is essential to have patches applied regularly and promptly to the operating system and all applications installed on the computer system.

Most operating systems and many software applications feature automatic patch updating capabilities via the Updates feature. Ensure these automated updating features are enabled and scheduled. Manual updates should be done on a regular basis for software programs that do not have this feature.

Operating System Security Updates

To check current settings and to enable if necessary:

- Microsoft Windows 7

- go to "*Control Panel*"
- select "*Windows Update*" (in Classic View) **or** select "*System and Security*" then "*Windows Update*" (in Category View)
- Select "*Change Settings*"
- Ensure that under "Important Updates" the "*INSTALL UPDATES AUTOMATICALLY*" option is selected.
- Ensure that under the "*Recommended Updates*" the "*Give me recommended updates the same way I receive important updates*" option is selected.
- Ensure that under the "*Microsoft Updates*" the option "*Give me updates for Microsoft Products*" is selected. If the "*Microsoft Updates*" section is not displayed in the "*Change Settings*" window, it must be installed and enabled first. This is achieved by clicking on the "*Get Updates for other Microsoft products. Find Out More*" link in the "*Windows Update*" main window. This will include security updates for all Microsoft products, including Microsoft Office.

- Apple OSX:
  - For OSX you can enable automatic updating from "*System preferences*" then "*Software Update*".

Application Software Patches

Most of the software used today has an integrated automatic update feature.

For Microsoft Office products, please ensure that Windows Updates is enabled for the operating system as well as any other Microsoft Products to ensure Microsoft Office products are kept updated automatically on a regular basis.

- Microsoft Windows 7
  - go to "*Control Panel*"
  - select "*Windows Update*" (in Classic View) **or** select "*System and Security*" then "*Windows Update*" (in Category View)
  - Select "*Change Settings*"
  - Ensure that under the "*Microsoft Updates*" the option "*Give me updates for Microsoft Products*" is selected. If the "*Microsoft Updates*" section is not displayed under the "*Change Settings*" screen it must be installed and enabled first. This is achieved on the "*Windows Update*" main window by clicking on the "*Get Updates for other Microsoft products. Find Out More*" link. This will enable the automatic download and install of patches for all Microsoft products, including Microsoft Office.

Alternatively, you can download and install the updates manually by checking Microsoft's support pages for product updates. For example, for Microsoft Office, go to http://office.microsoft.com/en-ca/support/?CTT=97.

For other non-Microsoft software, such as Adobe, Apple, Mozilla and so on, ensure that the software default for updating software automatically is enabled at the point of install. If you are unsure if the automatic update has been enabled, you can usually check the current setting by selecting the "Options" or "Preferences" menu option in the software. Ensure that under the "Updates" section, the software is configured to download and install updates automatically, on a daily or weekly basis.

For software that does not have a built-in automatic update feature, please visit the vendor's support website on a regular basis and install updates as they are made available.

If you are unsure or cannot find out how to update your software then download and install the most recent version of the software for your operating system. This will mean that the very latest version of the software, which typically includes the latest security patches for these programs, is installed on your computer. Alternatively, investigate the use of Patch Status Checking Software described below.

Web Browser Patching

Since more and more computer systems are compromised via the web browser, it is very important to ensure that the web browser used is up-to-date and patched.

Internet Explorer receives its necessary patch updates via Microsoft Windows Updates.
If you are using Internet Explorer as your web browser, please ensure that the Windows Updates is enabled for the operating system as well as other Microsoft Products updates.

If you are using other web browsers, such as Firefox, Opera, Chrome, Safari and so on, ensure that the defaults for updating software automatically are enabled at the point of install. The current settings for the automatic updates can usually be checked by selecting the "Options" or "Preferences" menu option in the software. Ensure that under the "Updates" section the software is configured to download and install updates automatically, on a daily or weekly basis. Mozilla Firefox is automatically set to search for updates by default at the point of install. For Apple OSX Safari, enable automatic updates from "System preferences" then "Software Update".

Software Patch Status Check

Commercial and free tools are available to check the status of software patches for all installed software programs as well as for the operating system.

One such utility that is available free for home use is the Secunia Personal Software Inspector available at http://secunia.com/vulnerability_scanning/personal. This utility greatly simplifies the process of checking the patch status of the entire system. It also offers an easy updating option for all software applications as well as alerts for newly announced vulnerabilities.

Another free utility that checks the status of missing patches (Microsoft product patches only) is the Microsoft Baseline Security Analyzer, available at http://technet.microsoft.com/en-us/security/cc184924.aspx. Patch status checking utilities can be used to ensure that there is no vulnerable software present on your system.

"Patch Tuesday" is the second Tuesday of each month, on which Microsoft releases security patches. Starting with Windows 98, Microsoft included a "Windows Update" system that would check for patches to Windows and its components, which Microsoft would release intermittently. With the release of Microsoft Update, this system also checks for updates to other Microsoft products, such as Office, Visual Studio, SQL Server, and others.

9. Encryption

Encryption is a way to protect sensitive information from unauthorized disclosure, alteration or loss. The encryption process makes information unreadable unless decrypted by an authorized user with the correct

key or password. Encryption can be applied to an entire hard drive, folder, file or storage device (e.g., USB Flash Drive). Encryption can also be applied to a virtual disk within an encrypted file to securely store data.

Encryption can be added to individual files with information that needs to be protected. To use the file encryption function from within Windows 7, modify the file properties:

- Open Windows Explorer
- Right-click the file that you want to encrypt, and then click *Properties*
- On the General tab, click *Advanced*
- Select the **'***Encrypt contents to secure data'* check box

For additional assistance on the encryption function, please refer to the HELP section of your operating system.

If you routinely work with electronic files at home containing sensitive information, it may be helpful to create an encrypted folder to store all sensitive files. All files stored in the folder would then be automatically encrypted. Microsoft operating systems feature a folder encryption technology called Encrypting File System (EFS) which is only available on certain versions of Windows operating system:

- Windows 7 Professional, Enterprise and Ultimate

EFS is **not** available on:

- Windows 7 Starter and Home Premium

To use the EFS folder encryption function, create a new folder. Modify the folder properties (under the advanced attributes section and select "Encrypt Contents" option) to enable encryption. Store files containing sensitive information in this folder only. For additional assistance on the encryption function, please refer to the HELP section of your operating system.

To use the folder encryption function on Apple OSX:

- Enable AES 256 encryption on your at home work account by selecting "*System Preferences*", "*Security*", then "*FileVault*".

The use of a virtual encrypted disk within an encrypted file to securely store data is another viable option for providing encryption for the sensitive data. There are a number of open source and commercial software products that provide the use of a virtual encrypted disk within an encrypted file to securely store data.

There are many encryption software packages available, some of them free or open source. Be sure to research products and read reviews to ensure that you choose a good product, and ensure that the product mentions that it uses the AES 256 (or better) encryption standard, which complies with the government's Cryptographic Standard for Information Protection. Products that use a lower level of encryption do not provide adequate protection.

10. Secure your home wireless system

Setting up a home wireless system securely requires a number of changes to the default state. Wireless routers/firewall devices have default passwords that are published on the Internet. If you do not change the password on your device, it will allow a hacker to gain access to your device and re-configure it without your permission. Therefore, the default password should be changed.

Your Internet Service Provider should be able to offer wireless setup support and you can also search the Internet for assistance with setting up security measures associated with home wireless systems.

Wireless routers/firewall devices typically come pre-configured from the manufacturers with the wireless connectivity enabled and set to no-encryption. These defaults should be changed as follows:

- If wireless connectivity is available on the home router/firewall but is not needed, you are recommended to disable it in the router/firewall configuration
- If wireless connectivity is used, then the settings should be as follows:
    - "WPA2-Personal" encryption is strongly recommended. The "WPA-Personal" setting is acceptable but not as secure. "WEP" encryption must not be used. The option of "No-encryption" must never be used
- In order for a wireless device to connect to a wireless network it must know the network name, or SSID (service set identifier), of the wireless network in question. If you plug in your wireless router or access point and leave the default SSID, it won't take long for an attacker to determine what the SSID is. Ensure that the default SSID for the wireless settings has been changed. Ensure that the new SSID is at least 8 characters in length and is composed of a combination of letters and numbers.
- Ensure that the Pre-Shared Key used for the wireless authentication is at least 13 characters in length and is composed of a combination of letters, numbers and special characters. A pre-shared key, or PSK, is a secret which is shared between two parties using a secure channel before it needs to be used. The PSK term is used in Wi-Fi encryption such as WEP or WPA, where both the wireless access points (AP) and all clients share the same key.

How to Secure Your Wireless Home Network (includes a 5 minute video)
http://www.wikihow.com/Secure-Your-Wireless-Home-Network
Home Wireless Security Settings Tips
http://wirelessdefence.org/Contents/Home%20Wireless%20Security%20Tips.htm

11. Are there any methods available to ensure I have created a strong password?

Employees are asked to create and manage lengthy and complex passwords. This is necessary because encryption algorithms are only as strong as the password used to encrypt and to open the file. Short passwords (even complex passwords of 8 characters in length) are relatively easy to break as the attack technology for password guessing has dramatically improved recently. Large complex passwords may seem daunting, but they can be quite easy to create, and more importantly, easily remembered without the need to write them down. Although the method offered below will not create a password as strong as one using truly random characters, it will help you create and use lengthy and complex passwords when needed.

The goal is to remember the starting phrase of your password and then the rules used to convert it into a password.

Step 1. Think about a phrase, book title or famous quote that you can easily remember. For example:

- The quick brown fox jumped over the hedge
- To be or not to be

Step 2. Create some rules to modify the phrases based on the types of characters used to create strong passwords (e.g., upper and lower case letters, numbers and special characters (e.g., !@#$%)); some samples are provided below. For this example the rules include:
Rule 1: Capitalization – Capitalize the first letter of every second word
Rule 2: Numbers - Replace the vowels with numbers e.g., o's with the number 8, e's with a 5, and etc.

Rule 3: Special Characters - Put a special character in the spaces between words (e.g., @, #, !)

Applying Rule 1: Capitalization **-** Capitalize the first letter of every second word.

- **T**he quick **B**rown fox **J**umped over **T**he hedge
- **T**o be **O**r not **T**o be

Applying Rule 2: Numbers - Replace the vowels with numbers e.g., o's with the number 8, e's with a 5, u's with a 3, i's with a 1, a's with a 2.

- Th**5** q**31**ck Br**8**wn **f8x** J**3**mp**5**d **8**v**5**r Th**5** h**5**dg**5**
- T**8** b**5** **8**r n**8**t T**8** b**5**

Applying Rule 3: Special Characters - Put a special character in the spaces between words

- Th5**!**q31ck**!**Br8wn**!**f8x**!**J3mp5d**!**8v5r**!**Th5**!**h5dg5 (Using a single character (!) to replace the spaces)
- T8**&**b5*****8r**&**n8t*****T8**&**b5***** (alternating & and * to replace the spaces)

Step 3. Check the Length – you now have a long complex password that you can recreate easily, rather than having to remember a long, complex series of characters.

- The quick brown fox jumped over the hedge - became
  Th5!q31ck!Br8wn!f8x!J3mp5d!8v5r!Th5!h5dg5 - 42 characters
- To be or not to be- became
  T8&b5*8r&n8t*T8&b5* - 20 characters

A short phrase can be repeated to create a longer password. Similarly, part of a long phrase can be pared down to create a shorter password.

12. General Information

Employees who have been approved to work at home are accountable for taking reasonable security measures to protect the information they are dealing with. Typically, Internet Service Providers (such as Telus and Shaw) are able to provide a fully supported suite of Internet security services for personal computers. This product suite may include Virus Protection, Internet Shield (Firewall), anti-spyware, e-mail Scanning, System Control, Parental Control, Spam Control and Auto-Update features. Employees need to ensure that due diligence is performed and policies and best practices are observed.

Employees are also reminded that if they have used the remote access service to connect to work from their home computer, they must completely log out and disconnect from the remote access session once their work is completed. If they do not log out and proceed to carry out personal Internet transactions, their personal Internet data traffic will traverse the Government network. These personal Internet activities on the Government network could result in a government policy violation, a security (or privacy) investigation and possible legal repercussions.

Employees must comply with policy and are aware of best information security practices by referring to the OCIO Information Security and Information Security Awareness websites.

NOTE: There is no actual or implied endorsement or recommendation made for any of the vendors or products listed in this document. The BC government is also not liable for any loss or damage to employee's home computer or personal files arising from the use or installation of these products and services. Employees are also solely responsible for reviewing the licence agreement

terms of any software they choose to use on their home computers and ensuring that their intended use complies with the agreement.

Resource Links

Effectively Erasing Files
http://www.us-cert.gov/cas/tips/ST05-011.html

Good Security Habits
http://www.us-cert.gov/cas/tips/ST04-003.html

Understanding Anti-Virus Software
http://www.us-cert.gov/cas/tips/ST04-005.html

Understanding Encryption
http://www.us-cert.gov/cas/tips/ST04-019.html

Understanding Firewalls
http://www.us-cert.gov/cas/tips/ST04-004.html

Understanding Patches
http://www.us-cert.gov/cas/tips/ST04-006.html

Using Wireless Technology Securely
https://www.us-cert.gov/sites/default/files/publications/Wireless-Security.pdf

Understanding Your Computer: Operating Systems
http://www.us-cert.gov/cas/tips/ST04-021.html

Understanding Your Computer: Web Browsers
http://www.us-cert.gov/cas/tips/ST04-022.html

Government links:

Microsoft Home Use Offer
https://ssbc-client.gov.bc.ca/servicenews/service_bulletin_557.html

Information Security Branch
http://www.gov.bc.ca/InformationSecurity

Information Security Awareness
http://www.gov.bc.ca/InformationSecurityAwareness

Working Outside the Workplace policy
http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/working-outside-workplace

Home Technology Assessment
http://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/policies-procedures/working-outside-workplace/home_technology_assessment.pdf

Remote Access Information
https://ssbc-client.gov.bc.ca/rao/RemoteAccessOptions.html