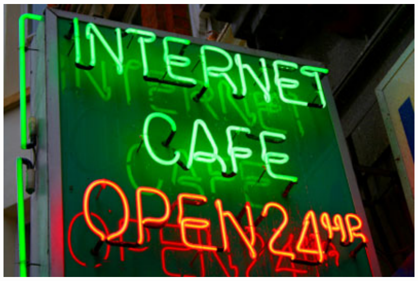
BRITISH COLUMBIA | Office of the Chief Information Officer

Public Computers - Protect Your Personal and Confidential Information



Working on confidential and/or personal information in public areas and on public computers is not recommended. Computers in public locations can be used by a variety of individuals throughout the course of a day and, therefore, security cannot be verified. Users typically don't have the authority to install software or change settings, however, the following steps should be taken to protect your privacy when you have finished working on a public computer:

Delete your Browsing History

Web browsers such as Internet Explorer keep a record of your passwords and every page you visit, even after you've closed them and logged out.

To remove stored passwords or other stored information in Internet Explorer 8 or 9:

1. From the **Tools** menu, select **Internet Options**.
2. On the **General** tab, under **Browsing history**, click **Delete.**
3. Check the item(s) you want to delete:
   - **Temporary Internet files**: Copies of web pages, images, and media that are saved for faster viewing
   - **Cookies**
   - **History**: A list of visited sites
   - **Download history** (Internet Explorer 9 only): A list of downloaded files
   - **Form data**: Saved information you entered in forms
   - **Passwords**
   - **ActiveX Filtering and Tracking Protection data** (Internet Explorer 9) or **InPrivate Filtering data** (Internet Explorer 8): Saved data to detect where web sites may be automatically sharing details about your visit
   - To delete everything, uncheck **Preserve Favorites website data** and check all the other options.
4. Click **Delete**.

To remove passwords or other stored information in Mozilla Firefox:

1. Go to Tools/Options/Privacy/select Clear history when Firefox closes. Click the Settings button and select all the options under History and Data. Click OK.

If you are using a corporate website, such as SharePoint Portal Server and Outlook Web Access, that allows you to open and view internal work-related documents, this will result in storing the documents locally as temporary files. Best practice is to view files through DTS and not to save documents when using a public computer. Do not download, save to the local hard drive or print confidential and/or personal information accessed electronically when using a non-government computer. Refer to Working Outside the Workplace Policy for more information.

Don't save files locally

Do not download, save to the local hard drive, or print confidential and/or personal information accessed electronically when using a non-government computer. Many of the files you would normally save locally, such as e-mail attachments, can contain private or sensitive information. An easy way to protect this data is to carry an encrypted flash drive and save files on it when necessary.

Delete temporary files

Temporary files (often abbreviated to “temp files”), as opposed to temporary Internet files, are created when you use programs other than a Web browser. For instance, when you create a Word document, in addition to the actual document file you save, Word creates a temporary file to store information so memory can be freed for other purposes and to prevent data loss in the file-saving process. Similarly, when video clips are being viewed, temporary copies are placed in the default temporary file location.

On Windows 7 and Vista:

> To clear all temporary files from the temporary file locations navigate to C:\Users\[USERNAME]\AppData\Local\Temp, where [USERNAME] is the name used to log on to the computer. Once in this folder, select all files and folders and delete them.
>
> In the case where the C:\Users\[USERNAME]\AppData\Local\Temp is not visible, ensure the option to display operating system and hidden files is enabled by going to:
>
> 1. Click on the Start button and select Control Panel
> 2. Click on Folder Options and select the View tab
> 3. In the Advanced Settings area, locate the Hidden files and folders category
> 4. Click the radio button for Show hidden files, folders and drive, click the radio button
> 5. Click OK at the bottom of the Folder Options window and close the Control Panel window

Certain files are supposed to be deleted automatically when the program is closed or during a system reboot, but unfortunately they often aren’t. To find these files, do a search on all local drives (including subfolders, hidden, and system files) for: ***.tmp,*.chk,~*.*** This will bring up all files beginning with a tilde or with the extensions .tmp and .chk, which are the most common temp files. Once the search is complete, highlight all and Shift + Delete to remove them. (If you don’t hold down the Shift key, they’ll usually be sent to the Recycle Bin, which you would then have to empty.)

Reboot

When you’re finished using the public computer, if possible, the final thing you should do is a hard reboot. This will not only clear the pagefile, if you’ve enabled that option, but it will also clear out everything you did from the physical memory (RAM).

Pay attention to your surroundings and use common sense

Finally, you need to remember to pay attention to things outside of the actual computer that could be a risk. Be aware of strangers around you (potential shoulder surfers) and remember that a public computer is just that — public.

Don’t view sensitive documents you couldn’t bear others to see. Remember the security camera over your shoulder. Cover your hands from view when entering any login information to prevent any casual spying. Don't leave the computer unattended, especially with sensitive information on the screen. If you have to leave the public computer, be sure to have done all tasks listed here.

Most importantly, remember that there is nothing you can do to make a public computer completely secure. A truly malicious owner or user could install a hardware keystroke logger that would be impossible to detect without actually opening the case and inspecting it. With that less-than-comforting thought, use common sense and use public computers only for non-sensitive tasks.

Useful Links:

Get Cyber Safe
http://www.getcybersafe.gc.ca/

Web Source
http://www.web-source.net/pc_security/pc_security_safe_public_computer_use.htm

Stay Smart Online
http://www.staysmartonline.gov.au/home_internet_users/protect_yourself2/using_public_computers

EarthLink Security Centre
http://www.yoursecurityresource.com/earthlink/feature/emerging_threats/safe_public_computer_use/index.html#axzz32TsOGSvs

Working Outside the Workplace Policy
https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/policies-procedures/working-outside-workplace/working_outside_the_workplace_policy.pdf