5 ways to be safe when using public computers

Are public computers safe in libraries, Internet cafes, airports or in stores? It depends on how you use them! Follow the tips below to stay safe c

Are public computers safe in libraries, Internet cafes, airports or in stores?

It depends on how you use them! Follow the tips below to keep your personal and account information safe.

1, Do not save access information

Always log out of the logged-in websites by clicking 'log out' or 'Exit' on the website. It is not safe if you simply close the browser window or enter another web address, because you really have not exit the system you have accessed.

Many programs (especially instant messaging programs - like Yahoo Messenger, etc.) have automatic access features by saving user and password names. Please disable this feature before you visit.

2, Do not leave the computer when sensitive information still appears on the screen . If you are not using a public computer, exit all programs before you leave and close all windows that display sensitive information.

3, Delete the saved information

Web browsers such as Internet Explorer always keep password information on the pages you have visited, even if you have closed the browser window or logged out.

Disable password storage

Before going to the web, turn off the feature that can save your password on Internet Explorer by following these steps:

- In Internet Explorer window, click **Tools** > **Internet Options**

- Select the **Content** tab and click **AutoComplete** (in IE7 is in the **AutoComplete** section click **Settings**)

- Completely remove all relevant fields of user, password.

Delete temporary Internet files and history on the browser

When not using a public computer, you should delete all temporary files and history on your browser by:

- Go to Internet Explorer, select **Tools** > **Internet Options**

- On the **General** tab, under **Temporary Internet files** , click **Delete Files** , then **Delete Cookies** .

- Under **History** , click **Clear History** .

Delete other files saved from company information (like Sharepoint Portal Server)

If you use the company's corporate website to allow internal company documents to be viewed, you can casually save sensitive computer memory. Follow these steps to remove them from your computer

- Delete all files located in the temporary folder of the account in use, this folder is located in the path **C: Documents and SettingsusernameLocal SettingsTemp**

- If your company uses Microsoft Office SharePoint Portal Server, delete the temporary folder of this section (**My DocumentsSharePoint Drafts**)

4, Watch out for those snooping over your shoulder

When using a public computer, you must always watch out for information thieves by watching you enter sensitive passwords, to collect your information, as this is the simplest and most effective way. Pay attention, be on the lookout or behind you!

5, Do not enter sensitive information into public computers

This method is intended to prevent those who accidentally get information, who use the computer behind you.

But there are also a few "diligent" thieves who use the installation of sophisticated software on public computers. These software will retrieve all information through keyboard typing and then email address information for the installer.

Nothing will happen if you don't save important information or delete all sensitive information according to the steps above.

If you really want to be safe, avoid entering credit card information, financial information or any other sensitive information on any public computer.