

[Microsoft.com Home](#)[Site Map](#)

Search Microsoft.com for:

 Microsoft[Security At Home](#)[Microsoft At Home](#)[Microsoft At Work](#)**Protect Your PC**[Security Essentials](#)[Updates & Maintenance](#)[Viruses & Worms](#)[Spyware](#)**Protect Yourself**[Personal Information](#)[Online Activities](#)[E-Mail & Spam](#)**Protect Your Family**[Child Safety](#)**Resources**[Videos](#)[Downloads](#)[Support](#)[Community](#)[Worldwide Sites](#)

Need Security Help Now?

Help Protect Your PC or get support for viruses and other security issues
AT NO CHARGE
Get started

[Security At Home](#) > [Personal Information](#)

5 safety tips for using a public computer



Public computers at libraries, Internet cafes, airports, and copy shops are convenient, cheaper than buying your own laptop, and sometimes even free to use. But are they safe? Depends on how you use them.

Here are 5 tips on using public computers without compromising your personal or financial information.

1

Don't save your login information

Always logout of Web sites by pressing logout on the site, instead of by closing the browser window or by typing in another address. This will help keep other users from accessing your information.

Many programs (especially instant messenger programs) include automatic login features that will save your username and password. Disable this option so no one accidentally (or on purpose) logs in as you.

2

Don't leave the computer unattended with sensitive information on the screen

If you have to leave the public computer for any amount of time, logout of all programs and close all windows that may include sensitive information.

3

Erase your tracks

When you're done using a public computer you should delete all the temporary files and your Internet history.

To delete your temporary Internet files and your history

1. In Internet Explorer click **Tools** and then click **Internet Options**.

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

Related Links

- [7 ways to protect your laptop on the road](#)
- [Use public wireless networks more safely](#)
- [Danger, danger: 5 tips for using a public PC](#)

3. Under **History**, click **Clear History**.



Watch for over-the-shoulder snoops

Because there's so much in the news about how hackers can digitally sneak into your personal files, we sometimes forget about the old fashioned version of snooping. When you're using a public computer, be on the look out for thieves who collect your information by looking over your shoulder or watching as you enter sensitive passwords.



Don't enter sensitive information into a public computer

The measures listed above will provide some protection against casual hackers who use a public computer after you have. However, an industrious thief may have installed sophisticated software on the public computer that will record every keystroke and then e-mail that information back to the thief. Then it doesn't matter if you haven't saved your information or if you've erased your tracks. They still have access to this information.

If you really want to be safe, avoid typing your credit card number or any other financial or otherwise sensitive information into a public computer.

Was this information useful?

Yes

No

[↑ Top of page](#)



[Printer-Friendly Version](#)



[Send This Page](#)



[Add to Favorites](#)

[Manage Your Profile](#) | [Contact Us](#) | [Free Newsletter](#)

© 2005 Microsoft Corporation. All rights reserved. [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)