Title:
Danger, Danger: 5 Tips for Using a Public PC

Word Count:
994

Summary:
Internet cafes are great when you're travelling. But before you log on, consider these hints for protecting your private information.

Keywords:
Small Business Ideas, Small Business Start Ups, Small Business Software

Article Body:
There's a guy in New York who may have got into your personal business. If he did, he probably looted your online bank account.
Juju Jiang is serving time now after pleading guilty. But for a couple years, he bugged public computers with software that logged keystrokes. He used it to capture usernames and passwords. Some he used to steal money; others he sold on the web.
He got caught when he manipulated a victim's home computer while she was present. She watched incredulously as he methodically searched her computer. He was using GoToMyPC, which allows travellers to manipulate their computers from afar. The victim had used GoToMyPC previously from a public machine. Jiang stole her username and password.
Spying software can easily be placed on public computers, such as those in Internet cafés, airports, libraries and other public places.
With spying software, a criminal can grab your passwords and usernames. Ultimately, you could lose your money or have your identity stolen. That should tell you enough to be wary of public PC terminals.
Software is Unobtrusive
Spies usually use software because it is invisible to the untutored eye. Hardware to do virtually the same thing also can be used, by placing it between the keyboard and computer. But using it is too obvious in a public place.
The software programs, however, can record a victim's every keystroke. The keystroke loggers can then e-mail the collected information on a set schedule. Or it can be downloaded. Other software programs take screen shots of places you go. These, too, send their collected information via e-mail.
The spying programs are inconspicuous. Unless you know how to look for them, you'll never see them.
But don't forget there are other threats besides spy programs. Here's how to

stay safe:
Here are five things to consider when you sit down in front of a strange computer:
Check for Spy Programs
Download X-Cleaner Spyware Remover at spywareinfo.com. Put it on a floppy disk. If the public computer you use has a floppy drive, insert the disk and run X-Cleaner from the floppy to check the hard drive. You do not have to install X-Cleaner.
Erase Your Tracks
When you use an internet browser, it keeps records of where you went. When you finish surfing with Microsoft Internet Explorer, click Tools > Internet Options. On the General tab, click Delete Files and Delete Cookies. Then click Clear History.
If you're using Netscape Navigator, it's a little more complicated. Follow these steps.
• Check the settings before going online. Click Edit and Preferences. Click the arrow next to Navigator and select History. On the right, find Browsing History. Change "Remember visited pages" to 0.
• Click on the arrow next to Privacy and Security. Select Disable Cookies and Disable Cookies in Mail and Newsgroups.
• When you finish surfing, click Edit and Preferences. Click the arrow next to Navigator. Click Clear History and Clear Location Bar. Go to Privacy and Security on the left side and click the arrow. Select Cookies. Click Manage Stored Cookies. On the Stored Cookies tab, click Remove All Cookies.
• Now go to Advanced, in the left-hand panel. Click the Arrow and click Cache. Click Clear Memory Cache and Clear Disk Cache. Protect Your Passwords
Browsers also track passwords. Before going on the web, if you're using Internet Explorer, click Tools > Internet Options . On the Content tab, click AutoComplete. Clear the four boxes.
When you finish surfing, again click Tools > Internet Options . Go to the Content tab and click AutoComplete . Click Clear Forms and Clear Passwords.
If you're using Netscape, click Edit and Preferences . Click the arrow next to Privacy and Security . Click Passwords . Clear the box next to Remember Passwords . When you finish browsing, click Passwords again, under Privacy and Security. Click Manage Stored Passwords. Select the Passwords Saved tab and click Remove All.
Netscape has a feature similar to AutoComplete. It saves data entered into forms. To disable that, under Privacy and Security, click Forms. Uncheck "Save form data from Web pages when completing forms." When you finish browsing,

return to the Forms page. Click Manage Stored Form Data. Click Remove All Saved Data.
Cleaning out the browser will ensure that no one can track your surfing or grab your passwords with saved data. But a keystroke-logging program will still catch your passwords.
Probably the best password protection is a temporary password. Use it while you're on the road, then discard it.
Don't Rely on Encryption
There are a number of encryption packages on the market. They can be used to encrypt email. However, they encrypt the mail when the Send button is clicked. That's too late if a key-logging program is on the computer. It will make a record of the password and message as it is being written.
Use Some Common Sense
Public computers may be secure. But you really have no way of being sure. You can secure your home or business computer, but you can't be certain of what has been done with a public machine.
Approach these machines with care. Don't do any banking or stock trading on them if you can avoid it. Avoid credit-card transactions. Use a temporary password if you must check your email. And ask your system administrator how to "expire page views."
If you're just surfing, that should not be a problem. But avoid sensitive business if you can. There might be a Juju Jiang watching.