

PROTECT YOURSELF ON A PUBLIC COMPUTER

Most of us will occasionally have to use a public computer for one reason or another. Maybe it's an emergency situation (your own computer crashes or you get caught without your laptop when traveling) or perhaps the opportunity is just too convenient to pass up. But whatever your reasons, using public computers will always carry an inherent risk of exposing your personal data. Here are some things you can do to protect yourself and lessen that risk.

#1: Delete your Browsing History

This should be the first step you take to protect your privacy when Web surfing on a public computer. When you've finished browsing, it's a good idea to delete your cookies, form data, history, and temporary Internet files. In Internet Explorer 7, you can do this all at once under Tools | Delete Browsing History. In older versions of IE, each of these must be deleted separately, under Tools | Internet Options.

In Mozilla Firefox, go to Tools | Options, click the Privacy tab, and select Always Clear My Private Data When I Close Firefox. By default, this erases your browsing history, download history, saved form information, cache, and authenticated sessions. Click the Settings button and select the options to erase your cookies and saved passwords, too.

#2: Don't save files locally

When you're using a computer other than your own, even if it's a trusted friend's machine, it's polite to avoid saving files locally if you can help it. This is basically equivalent to not cluttering up another person's home with your junk. On a public machine, though, this goes beyond politeness and is an important security practice. 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 a flash drive and save files there when necessary. It's also a good idea to attach the flash drive to your key ring so you'll be less likely to misplace it and create a new security problem.

#3: Don't save passwords

This should be obvious when using a public computer, but if the option is already turned on, you might forget about it. To make sure passwords are not saved in Internet Explorer 7, go to Tools | Internet Options | Content. In the AutoComplete panel, click the Settings button and verify that the Prompt Me To Save Passwords check box is deselected. None of the other AutoComplete features needs to be enabled either, so deselect them as well. In Firefox, choose Tools | Options | Security and deselect Remember Passwords For Sites.

#4: Don't do online banking

You should remember that ultimately, a public computer is never going to be anywhere close to completely secure, so there are some things you just shouldn't use them for. If you really need to check your balance on the road, you're much better off finding a branch office or ATM or using your phone.

#5: Don't enter credit card information

As with online banking, public computers are not the place for online shopping. Your purchases from eBay or Amazon.com can and should wait until you can browse from a more secure location. A little added convenience isn't worth the trouble of having your credit card hijacked.

#6: 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.

These files are usually 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 Shift, they'll usually be sent to the Recycle Bin, which you would then have to empty.)

#7: Clear the pagefile

The pagefile is the location on the hard disk that serves as virtual memory in Windows. Its purpose is to swap out data from RAM so that programs can operate as if they have more RAM available than you actually have installed in the computer. Anything that can be stored in memory could also be stored in the pagefile. To have this automatically cleared on shutdown, you need to use Local Security Policy.

To access Local Security Policy, open Control Panel, double-click on Administrative Tools, and double-click on Local Security Policy. Then, click Security Options in the right-hand pane and scroll down to Shutdown: Clear Virtual Memory Pagefile. Double-click that item and make sure it's enabled.

Note: On many public machines you won't have the rights to get to Local Security Policy, and while this task can also be accomplished from the registry, on these machines you likely won't be able to use regedit either. In this case, you can delete the page file manually. First you'll have to change the settings in Windows Explorer. Click View | Folder Options and the View tab, then scroll down and click Show Hidden Files And Folders. Deselect the Hide Protected Operating System Files check box. Now, find the file named pagefile.sys. It is usually (but not always) on the C: drive. Delete it; a new one will be created when the system reboots. Speaking of which...

#8: Reboot

When you're finished using the public computer, 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).

#9: Boot from another device

This is a fairly advanced option, and one that is often overlooked. If you boot from either your own USB drive or from a CD, many of the problems mentioned above can be avoided. Today, many Linux distributions have the option of running completely in memory after booting from a CD. If a public computer has had its BIOS options left at default (which happens more often than you would think), this could be an option. If you are able to do this and remember not to save any other files to the local hard drive, everything will be gone when you reboot.



#10: 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 any truly sensitive documents you couldn't bear for 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.

Most important, 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.