**Using Shared Computers**

* Many of us access the Internet from different locations — a friend's house to check email, an Internet café to check a stock quote, or the library to research a term paper. Sharing a computer is a great convenience, but you must take extra precautions to safeguard your personal information.
* These tips can help protect your Yahoo account when you use a shared or public computer.

**Use an on-demand password**

[On-demand passwords](https://help.yahoo.com/kb/SLN25781.html) let you sign in to your account without using a memorized password. We will send you a new password to your phone when you need to sign in

**Do not check the "Keep me signed in" box**

Many sites, including Yahoo, offer this remember option. When a computer keeps you signed in, it usually sets a persistent [cookie](https://help.yahoo.com/kb/cookies-sln20532.html) on the computer that allows the website to identify you so you don't have to sign in. If you check this option, you'll remain signed in after you close your browser. This is a convenient option if you are the only who uses a computer, but if you share a computer, do not check this option.

**Never leave a computer unattended while you are signed in**

If someone uses the computer in your absence, the person can easily access your account information.

**Always sign out completely**

If you use a public or shared computer, it's especially important to sign out completely. Always click the "Sign Out" link when you have finished accessing your Yahoo account.

**Clear the browsing data**

The browser keeps a cache that contains a copy of websites that you have visited, your download history, cookies, passwords, and similar information. The cache may be stored on the computer's local drive. Clearing the cache is simple and will prevent subsequent people who use the computer from seeing the sites you have visited. See your browser's help for details on how to clear the cache.

**Watch for "shoulder surfers**"

Use caution — sneaky thieves may try to watch your fingers as you type your password.

**Avoid confidential transactions**

Do not use a public or shared computer to log in to a bank account or other online service that accesses confidential information. You should access these websites only on a trusted computer.

**Be wary of spyware**

Any computer that you do not personally control is hard to trust. It could have spyware, such as keystroke loggers, or other malicious software installed. Think about the precautions you would take on your own computer and consider if other computers have the same safeguards. If a computer is infected with spyware, even clearing the browser cache or closing the browser and opening it again will not protect you, because spyware programs record everything you type.  
Check with the computer's owner or administrator before using it to learn what security precautions have been taken. Find out if antivirus and antispyware software are installed, how often the computers are scanned for vulnerabilities, and whether security updates are current.

**Never save passwords, and change them often!**

If you do decide to use a password, be careful on public computers. Many web browsers and other programs will automatically offer to save passwords for you — do not use this feature on a shared computer! If you use shared computers frequently, change your password often, in case you use a computer that's been compromised by spyware or malware.  Be sure that you change your password only on a trusted computer, preferably one that is not shared.