

Computing on the Road

As more and more people travel with their computers, it is important to know about common wireless practices, particularly because of the ways in which wireless can hinder checking email. Here are a few tips and reminders to take with you on the road.

- Most free wireless is not secure- be very careful where you login, and what files are on your computer. (Don't know why this is important? See "Why Secure Matters" below)
- Keep confidential files and files with personal information stored on a flash drive rather than on your laptop, if you must have them with you.
- Commercial establishments (airports, hotels, coffee shops, etc) require you to check in and agree to their terms and conditions. Ask at the front desk or the employees for how to register if you are not redirected to the gateway page.
- You must open the browser first and register or agree to the terms and conditions before any other program will be able to connect to the internet (such as mail programs, chat programs, online help resources for Word and other programs, etc)
- You will probably have to register every day in hotels, etc, since they traditionally reset everything once a day (usually in the afternoon for hotels, since checkout is late morning).
- Unless you know the wireless is high-speed and has little traffic, try using the basic client of Zimbra, by clicking on the link that says basic on the login page, or go to <https://mail.carleton.edu/h/> . This will load much faster than the advanced client.
- If you are using a public computer in a business, keep in mind that these computers are monitored, but that it is still easy for people to get information from the computers about previous users.
- When free wireless is advertised, make sure that there is a named provider and that it isn't always listed as free wi-fi. Recently, there have been a rash of businesses that are providing free wireless, and the provider is monitoring all that occurs on the network. Big name wireless providers are still the most trustworthy.
- Always remember to logout!

If you want to know more about how to enable and connect to a wireless connection, Wellesley College has thorough documentation on how to do so from a [Mac](#), and also for [Windows](#) computers.

Why Secure Matters

These days, wireless is one of the easiest ways to get confidential information from someone else's computer. Insecure wireless can very easily be hacked: what you do online can be monitored and replicated, files on your computer can be copied and read, and other information taken from your computer. If you have a file that you would prefer not to be public, it is recommended that you do not have it on your laptop when traveling and using wireless (store it on a flash drive and use the file when you aren't online). Be particularly mindful of documents of any type that list your usernames and passwords to specific sites. Even a small bit of personal information in the hands of a skilled hacker can reveal far too much information about you and allow them to steal your identity and cause all sorts of problems.