

ANTIVIRUS SAFETY AND YOU

Operating securely in the college environment

Viruses are a significant problem in any college environment. The South Seattle Community College IT Department has put together a best effort antivirus system, but cannot be responsible for the integrity of your personal data. We have put together this sheet to help you protect yourself from the threat of viruses.

What IT is doing to protect you

We have installed Microsoft's Forefront antivirus security software on our workstations, and locked down our servers and network so that viruses that infect individual workstations will not spread to either the servers or other workstations via the network. We cannot guarantee that these steps we have taken will be 100% effective, as viruses evolve over time to exploit new vectors. However, we have taken every reasonable step we can to prevent viruses from spreading in that method. In addition, we schedule regular antivirus scans of the workstations, and wipe them clean in between quarters.

In addition, we are utilizing Citrix's virtualization technology in TEC125 and the library computer labs. Each time these machines are rebooted, all the software on those machines (along with any viruses that may have infected those individual workstations) is removed, and replaced with fresh software that is clean of viruses.

Even with these steps, your personal data is still at risk from viruses. We cannot guarantee a virus-free environment, and we need your cooperation to keep the network free of viruses.

How you can protect yourself

Utilize home antivirus software

There are many home antivirus packages available. Microsoft's Security Essentials is available for free at http://www.microsoft.com/Security_Essentials/, and AVG is also available for free from <http://free.avg.com/>. If you had antivirus that came with your computer that you have not updated or subscribed to, remove it from your system before installing the free antivirus packages.

Don't install unauthorized software

South Seattle Community College has gone to great length to prepare a large quantity of software for your usage. If you find that a software package is needed, please request it through proper channels or use your own computer instead of trying to install outside software on our computers. Besides possibly being a conduit for viruses, it could potentially be illegal and open both you and us to lawsuits by the software manufacturer.

Use Google Docs and webmail accounts to transmit files

Google Docs (<http://docs.google.com>) and webmail accounts (Yahoo, Hotmail, and GMail for example) can be used to safely transfer data from home to school and back with a reduced chance of viral transmission. You can attach files to an e-mail draft, or send it to yourself via e-mail. This will reduce your chances of losing data due to a virus. In addition, the webmail services have their own antivirus scanning features.

Limit web browsing to educational usage only

The internet is a dangerous place! While we have made attempts to tighten up web-based antivirus screening without limiting your ability to access the internet, realize that many web sites (especially social networking sites, warez/pirate websites, and pornographic sites) make money by infecting your machine with software of dubious value, including sometimes viruses. By limiting your school web usage to research, you limit the chances of you catching a virus from other websites.


Limit your usage as much as possible to the virtualized labs

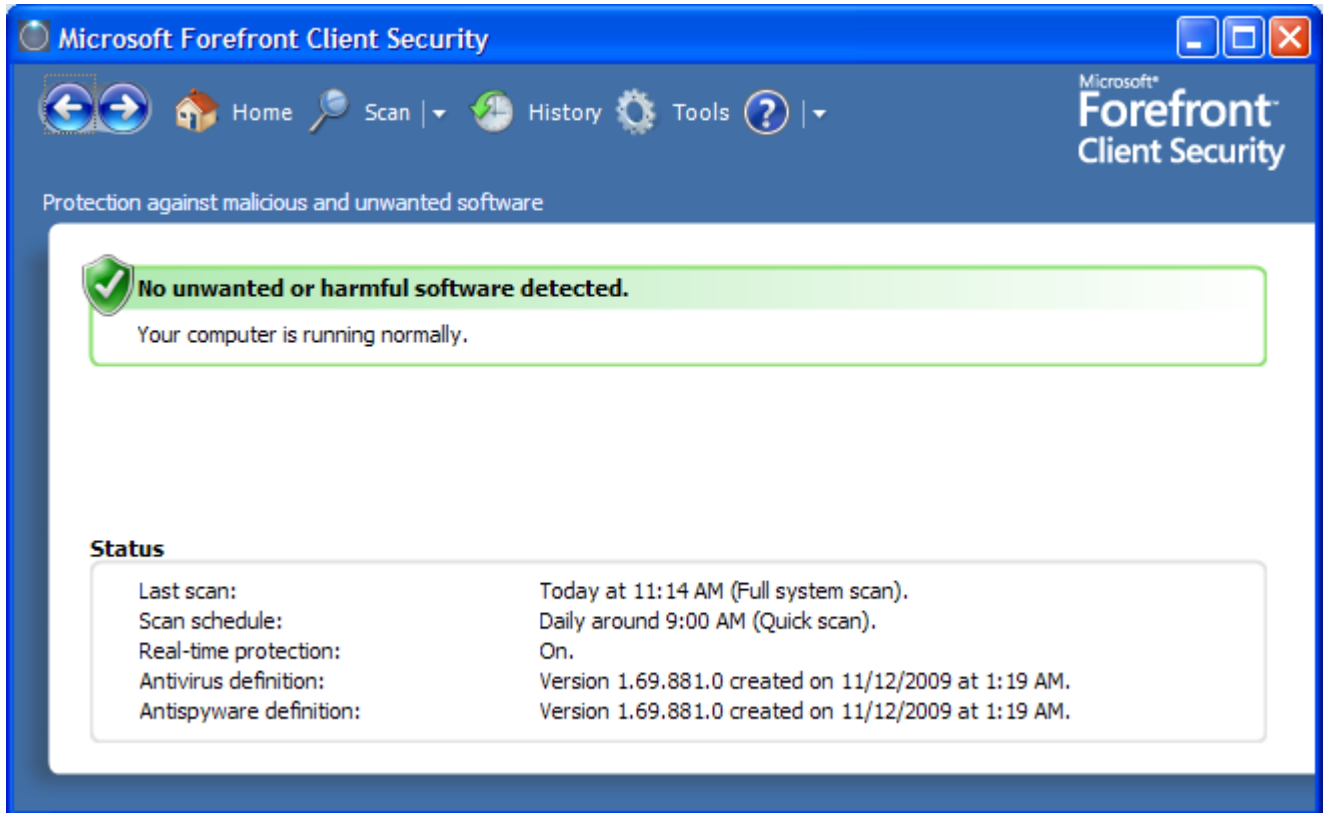
To be as safe as possible, utilize the computers in TEC125 or the Library computer lab. These computers are using the latest Citrix desktop virtualization technology to help protect you from viruses. Every time you restart the workstation, it wipes out the machine and starts over with a fresh image of the workstation. However, rebooting a machine does take 2-3 minutes for it to complete the refresh, so this does require some patience.

Scan your thumb drives

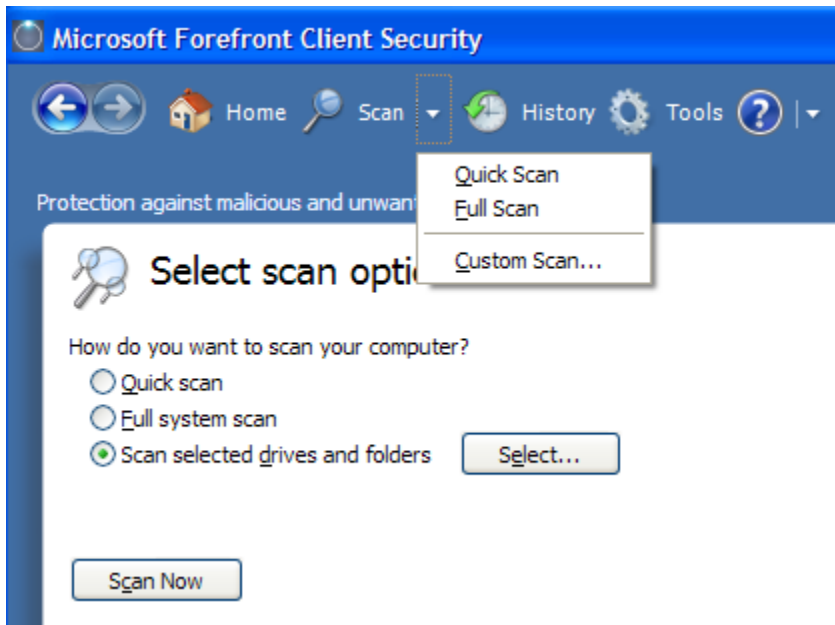
We utilize Microsoft Forefront Security on our workstations. To scan your thumb drive, take the following steps:

1. Insert your thumb drive into the computer.
2. Double click on the Forefront Security icon on the taskbar in the lower righthand corner of your screen.

It looks like this:  This will start the Forefront Security application.



3. Select the dropdown arrow next to scan, select custom scan, press the select button, and select the drive that has been mapped to your thumbdrive.



4. Press the "Scan Now" button. Forefront will scan your thumbdrive and alert you to any viruses that might be present on your thumbdrive.

If you need further assistance in scanning your thumb drive, please ask for assistance from a lab aide.