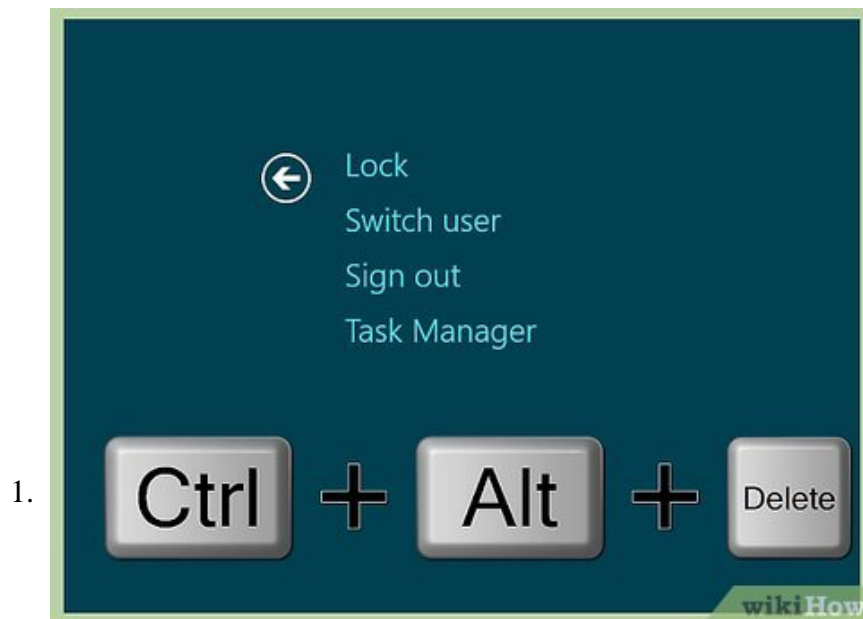


# How to Hack Lanschool

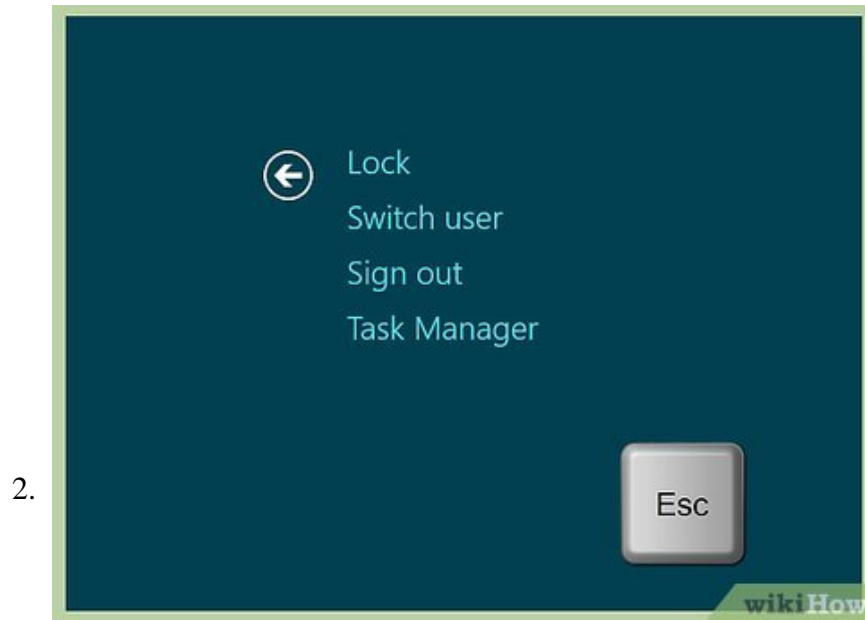
Lanschool is 'classroom software' used by various schools to ensure that students are appropriately using school computers. Unfortunately, the vast array of features Lanschool has is very open to abuse. Malicious users can steal usernames...

Method 1 of 6:

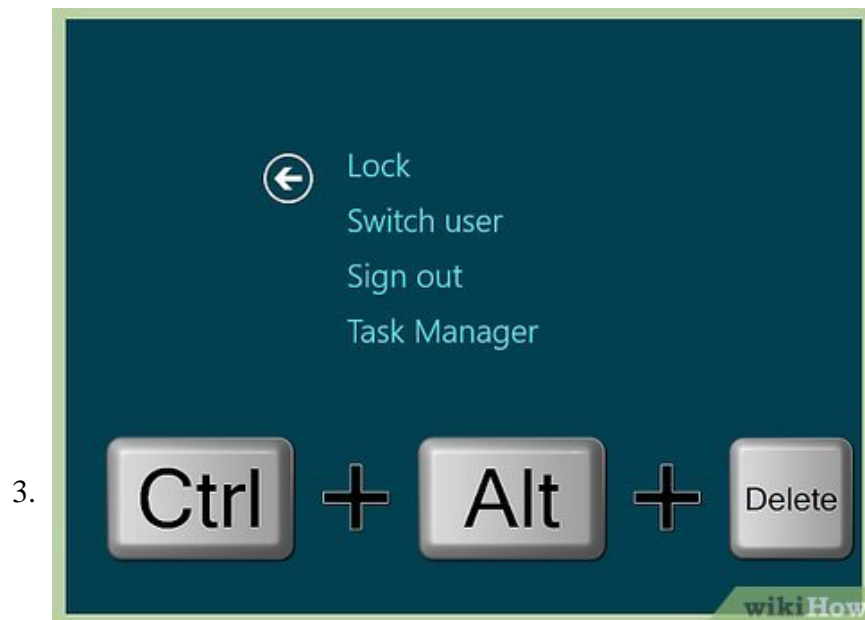
## Retaining Control with "Show Student" Enabled



Once the teacher has enabled "Show Student" press ctrl-alt-delete to bring up the screen that has the buttons to get to the task manager, lock computer, etc.



**While that is open, press esc multiple times while releasing ctrl-alt-delete to ensure you hit it right as the menu is disappearing**

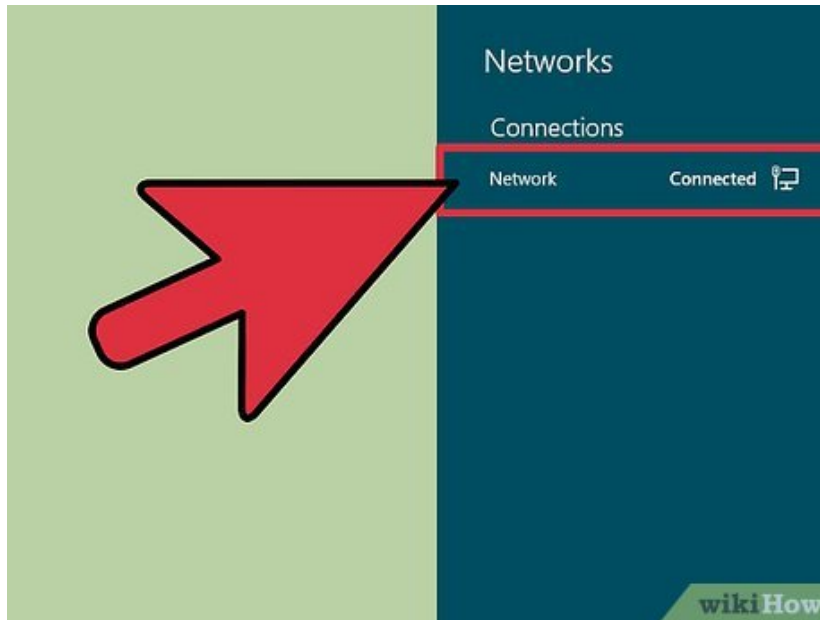


**press ctrl-alt-delete once again and you will have control of the computer's mouse for 2-3 seconds**

Method 2 of 6:

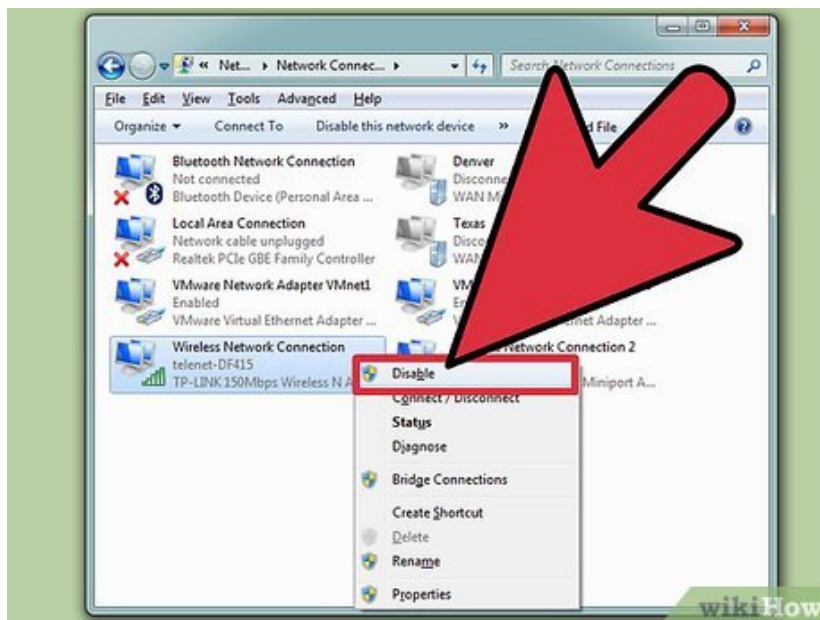
## **Disconnecting From the Network**

1.



An alternative method of gaining control, and for an indefinite time, is to remove the network cable from the back of the computer. "Show student" ceases to be broadcast to the disconnected computer.

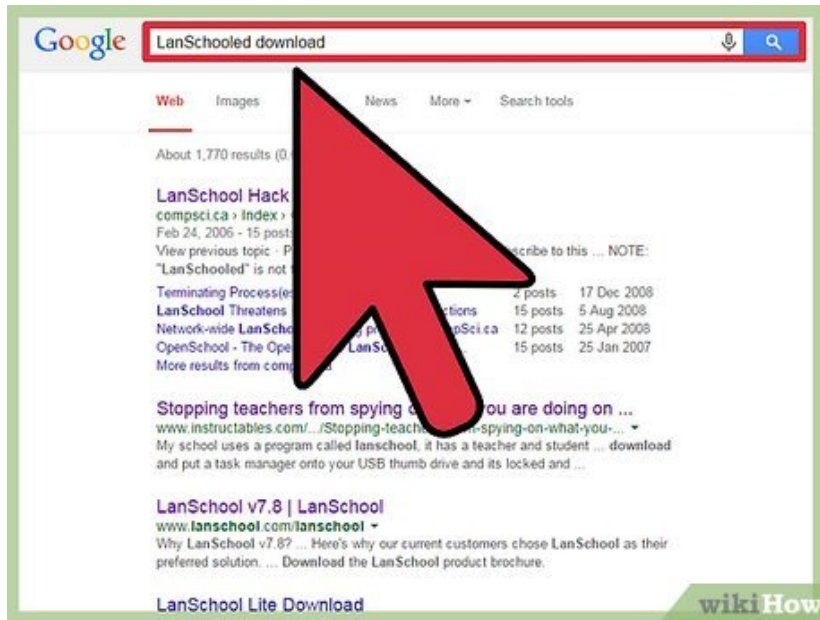
2.



The above method also applies to computers connected wirelessly, especially laptops with an external "Turn off wifi" switch.

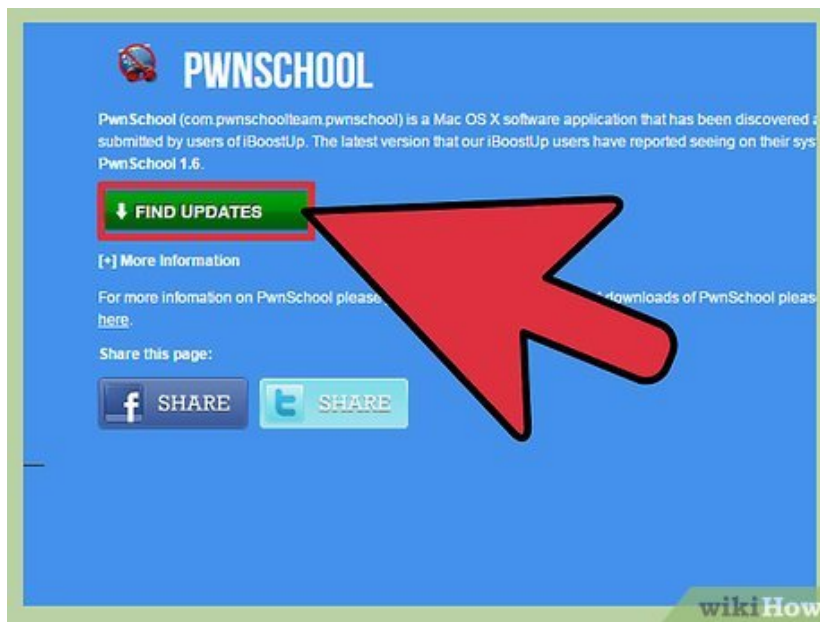
Method 3 of 6:

**Using Software Tools**



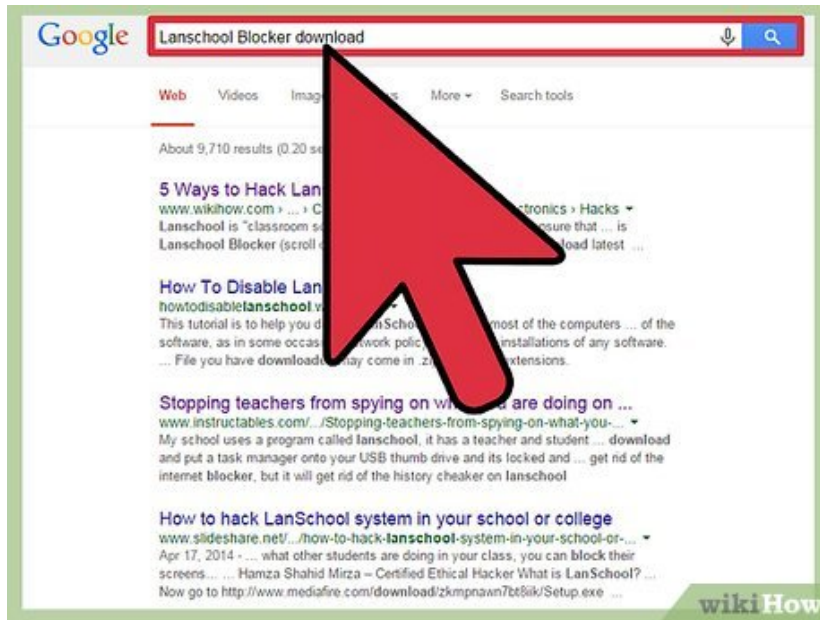
1.

For Lanschool 6 or below, "LanSchooled", a piece of software which spoofs Lanschool broadcasts, allows you to perform teacher functions such as shutdown people's screens etc.



2.

On Mac OS X, PwnSchool allows you to stop the Lanschool process and render it useless. It is also effective for stopping Apple Remote Desktop and Screen Sharing. Note Pwnschool is a dead project and newer versions of Lanschool are unaffected by Pwnschool.

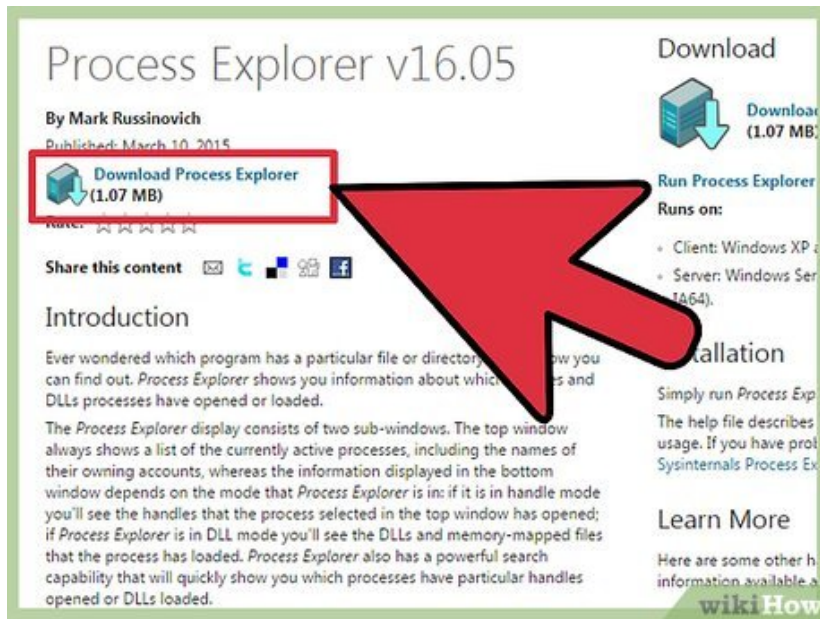


3.

**Another piece of software available for Mac users is Lanschool Blocker (scroll down to Download Packages, and download latest Version.zip)**

Method 4 of 6:

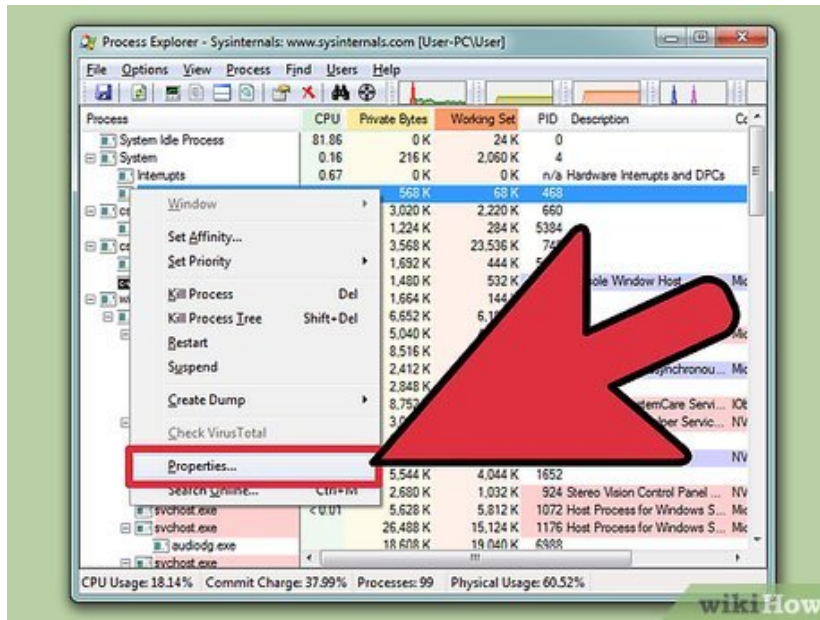
### Using Microsoft Process Hacker



1.

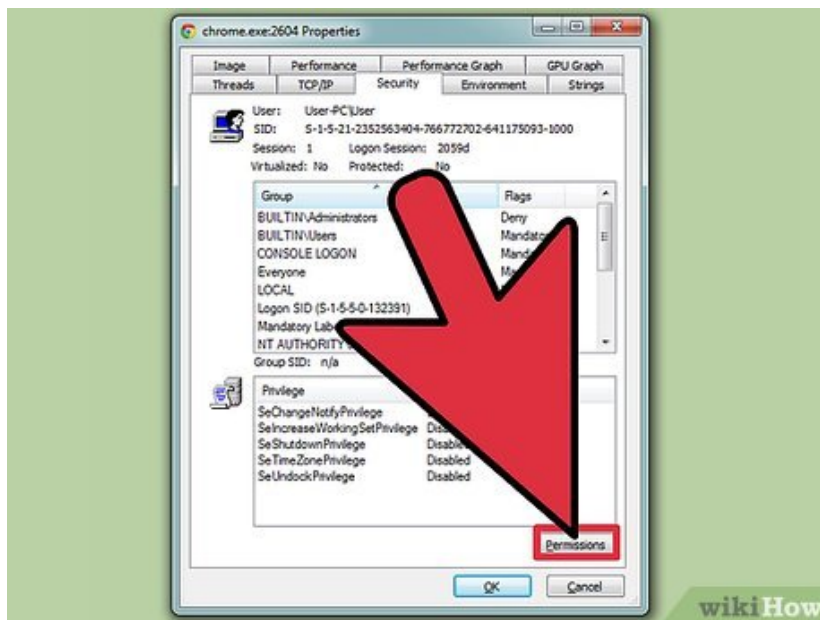
**Download and run Microsoft Process Explorer or Process Hacker**

2.



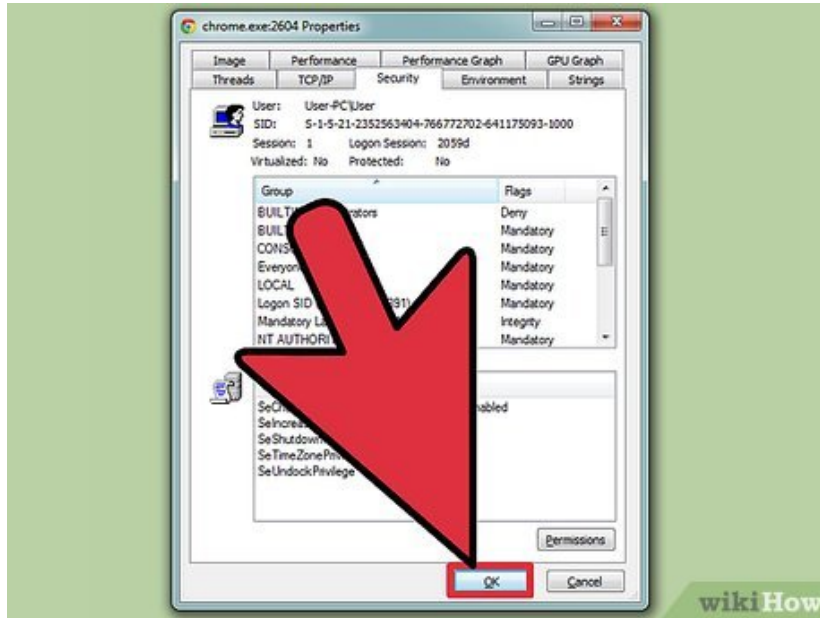
Right click "student.exe" and go to "Properties".

3.



**Remove all permissions from SYSTEM.** If a member of staff is currently monitoring you, go to the bottom of the permissions list. Your name should have a tick on the terminate permission. You can give yourself permission to terminate student.exe.

4.



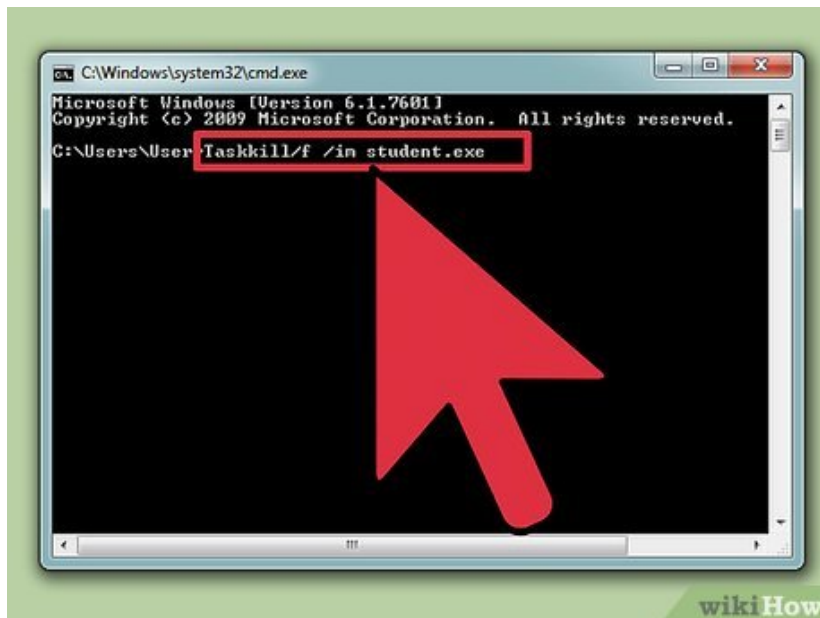
Click "Apply" to save the changes.

Method 5 of 6:

## Using Command Prompt

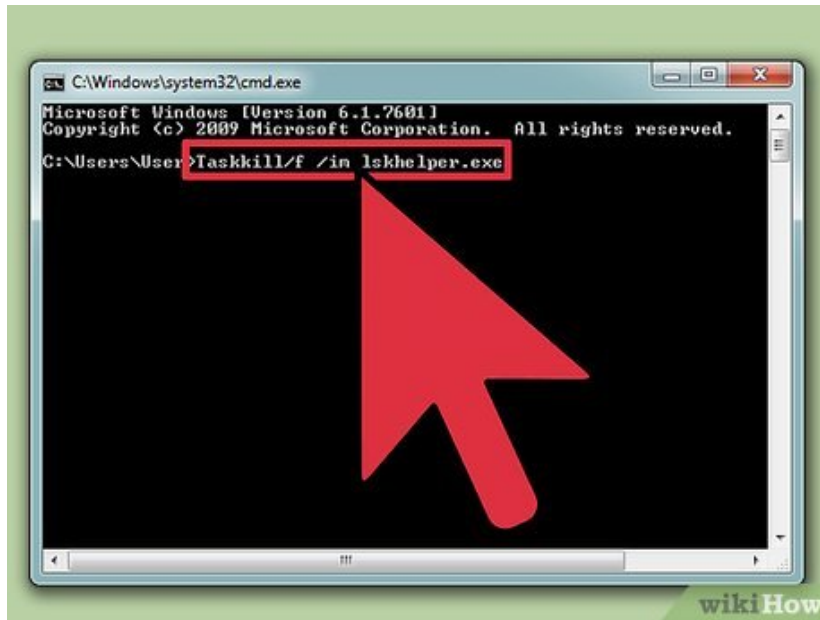
Find some way to get onto Windows Command Prompt.

1.



Then type in the command "Taskkill/f /im" and student.exe. The file will be terminated.

2.



Then use the next command line with Taskkill/f /im and "lskhelper.exe". That file will be terminated as well. Do the same with lskhlpr64.exe

Method 6 of 6:

## Using LinuxLive USB

### 1. Burn a Linux ISO to a USB flash drive.

1. Using a computer at home, follow the instructions on [Make a Bootable Ubuntu with USB Drive Using UNetbootin](#)
2. You probably do not have to pay too much attention to system requirements. When choosing between 64-bit and 32-bit, try 64-bit. If that fails to work, try 32-bit.

### 2. After having inserted the flash drive, restart the computer you want to bypass LanSchool on.

1. If the computer boots into windows, try again, pressing F12 to choose a boot device as the computer is starting up. When a menu appears, select your USB flash drive.

### 3. Choose options to boot Linux live, avoiding any options to install

1. **Do not install Linux on the computer you are using! Make sure you choose an option such as "Try Ubuntu without installing"!**
2. Some of the other steps can be prevented by your instructor, but this one can not, so long as the computer has a USB port.
3. This will leave no traces as long as you **do not actually install** the operating system.

You finished reading the article "[How to Hack Lanschool](#)" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.