Paramount Unified School District

Educational Services

Curriculum, Instruction and Assessment

Malware Guidelines

EMails

- Do Not click on **attachments in emails** in which you are not familiar with the sender
- Do Not click on **links in emails** in which you are not familiar with the sender
- Be especially cautious of emails that look like they are from banks, the IRS, a lottery, the "Paramount IT Department", a package delivery company, etc. Most of these are fake.
- Be especially cautious of emails that encourage immediate action, like an account is disabled, password is compromised, a bill is delinquent, taxes are due, etc. All of these are fake.
- The spam filter catches the majority of spam coming into the District, but less than 1% do get through. This 1% can be dangerous !

Web Browsing

- Do not leave multiple internet browser windows open for extended periods of time
- Do not download and install **free wallpapers, screensavers, icons, games, or other "free" things on the internet.** These types of downloads often will infect the computer.
- Do not click on links or respond to pop-up windows in the browser, especially **pop-up windows that state that your computer is infected with something**. Clicking on pop-up windows usually results in the computer becoming infected. The only legitimate messages come from the District virus software, Sophos. If you receive a message indicating some type of malware is present, stop and consider contacting the Technology Department immediately. If this is not possible, close the pop-up window by clicking on the X in the top right corner of the window. Save any open work, close all programs, and restart the computer. Run a complete scan in Sophos (second page).

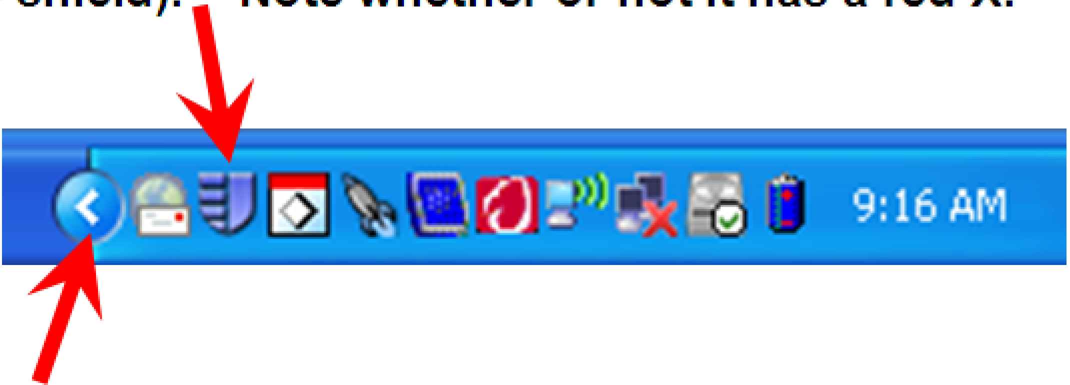
USB Drives

It is recommended that all USB drives are scanned frequently, especially if you transfer data from one computer to another.

Thank you for your attention to computer security. Please contact the Technology Department at x2000 if you have any questions.

Checking Sophos and Performing a Scan

In the lower right-hand corner of your screen (near the time) look for the Sophos icon (it looks like a blue shield). Note whether or not it has a red X.



You may need to click this button to display hidden icons.

If a red "X" is displayed, it is imperative that you contact the Technology Department Help Desk immediately at extension 2000. This indicates that the Sophos Virus protection is not running[1] and the computer is especially vulnerable to infection!

If there is no red "X" on the Sophos icon then Sophos is running fine and the computer is protected. Periodically you will want to scan the computer's hard drive for added safety.

To scan your computer, follow these steps:

1. Right-click on the Sophos icon (see above)
2. Choose "Open Sophos Anti-Virus"
3. Click on "Scan my computer"

[1] Perform this test inside the District. Sophos may show a red "X" outside the District.