http://www.chtu.org/Tech/technologist.html

aft Local 795

the Union Technologist

Volume 10 Number 1 | Cleveland Heights Teachers Union | September 2003

Computer Viruses on the Loose

There have been a rash of viruses and worms making the news recently and it is worth revisiting the methods of protecting your computer. The most common means of infecting your computer is from an e-mail attachment that you run by double click on it. A number of viruses or worms use a computer user's address book to send itself to other people—attempting to make it look like an e-mail from someone you know so you will be more likely to open the attachment. Others fake a return address, including microsoft.com. You should never trust a program sent as an attachment.

Many e-mail services routinely scan attachments for viruses and do not let them through to your mailbox. That is the case with the CH-UH school's mail system. Attachments with a virus will be quarantined automatically. You should make sure your computer's virus detection program also checks all e-mail attachments before allowing you to open them.

In the past you could feel confident that you would not get a virus or worm by running a virus detection program on your computer, and not opening e-mail attachments, inserting floppy disks or running programs from anyone you did not trust. The new Blaster Worm can infect your computer simply because it is connected to a network. You do not do anything but turn your computer on. If the worm has infected another computer on your network, it scans the network for connected computers and tries to infect them.

The Blaster Worm takes advantage of a programming error that was discovered in Windows 2000/XP earlier this summer. Microsoft released a patch to fix the bug in July. By early August the first worm to take advantage of the bug appeared. If you have not yet installed the patch on your Windows 2000 or XP computer, it could be affected even if you are running a virus detection program. Without the patch and up-to-date virus definitions, these worms could cause problems on your Windows 2000/XP computer and attempt to infect other computers on your home network.

How you connect your computer to the Internet, will determine how likely you will be affected by the Blaster Worm and others of this type. Laptops are most susceptible because they are designed to move from network to network. **The school district network is infected, but many computers have been updated or use Windows 95/98 (which are not affected)**

If you have a home network, it is important to have some type of firewall protecting your computers from your Internet provider's network Check with your Internet provider to see what they provide or recommend.

You can find out if your computer is infected by running a free program provided by Symantec Corporation, the makers of Symantec Anti-Virus: Connect to **securityresponse.symantec.com** and look for advisories and removal tools. The Microsoft security patches are at **windowsupdate.microsoft.com/** or using auto-update.

Do not open e-mail attachments unless you are expecting them

Do not run software that is downloaded from the Internet unless it has been scanned for viruses.

Keep up with security updates (patches) for your Internet browser and operating system. (windowsupdate.microsoft.com)

Install and keep up-to-date a virus detection program.

Note: this advise is for your home computers, the CH-UH MIS department manages updates on school computers. 397-5910 or support@staff.chuh.org

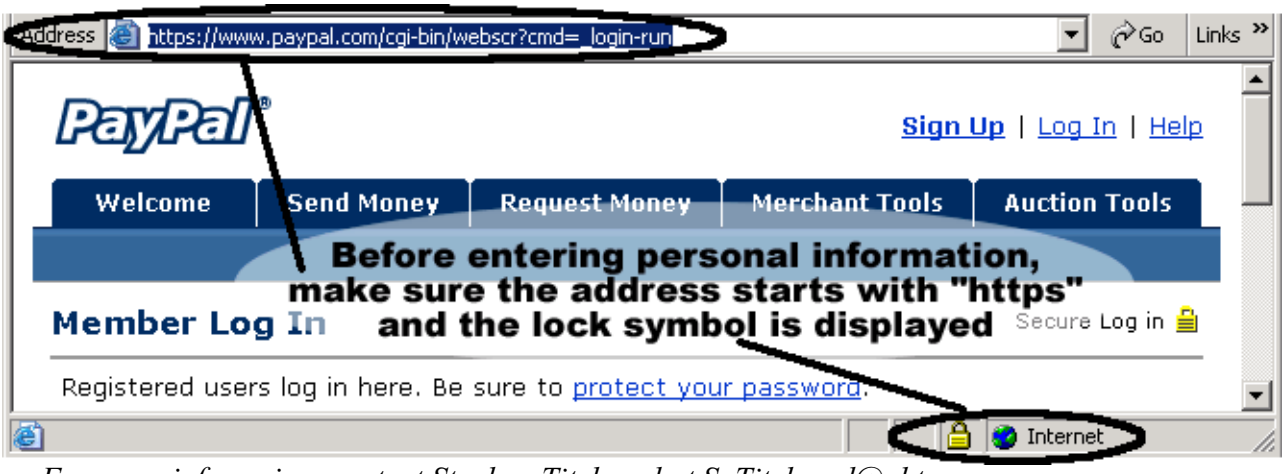
Fake E-mail and Security of Your Personal Information

If you are very active on the Internet, it is likely that you get more junk mail (SPAM) than legitimate mail. As more and more people use the Internet to transact business, criminals are also becoming more prevalent. I recently received a convincing e-mail purportedly from ebay asking me to "verify" my account. It is a good example of both the increasing sophistication of criminals and the things to watch out for when you receive mail. Because it is so easy to fake a return address, never assume that a message is from whomever it claims to be from. The first clues are misspelled words and grammatical errors. Often the criminal does not have a good command of the English language and does not have anyone editing/approving the message before it is sent out.

The second clue is a little more difficult to notice, but even more important — the link that you click on takes you to a different website than what is shown in the e-mail. You should make it a habit to observe the website address (URL) of any website you go to. The url can be seen in the location or address bar...

http://scgi.ebay.com|SAW-CGI|eBayUPDATE**@isapi.dll.go.ro**/VerifyInformation

Notice that the actual url includes "@isapi.dll.go.ro". **The website you are going to is actually "go.ro" NOT ebay.com.** Also note that "https" has been changed to "http". The "s" indicates a secure website that has been authenticated and will encrypt the information you send. The criminal does not have such a site. Once you get to the web page, you will find a request for personal and credit card information. You are not verifying information already known to ebay, you are filling in a blank document — that is another clue that this is not really ebay.com. You may want to re-type in the address of a website requesting personal information (and then login if necessary) rather than click on a link in an e-mail or another site. Never provide credit card or other private information to a web page that does not have "https://" at the start of the url in the location bar.



You may also want to check the Privacy Policy of the company you are going to do business with. How will they use your personal information?

For more informaion, contact Stephen Titchenal at S_Titchenal@chtu.org

AFL-CIO

CLEVELAND HEIGHTS TEACHERS UNION
local 795 — american federation of teachers
democracy in education • education for democracy

Fairmount Office Building
3473 Fairmount Boulevard
Cleveland Heights, Ohio 44118

2155 Miramar Boulevard
University Heights, Ohio 44118

Telephone
216-321-0020
Fax
216-321-0786

www.chtu.org