M E M O R A N D U M

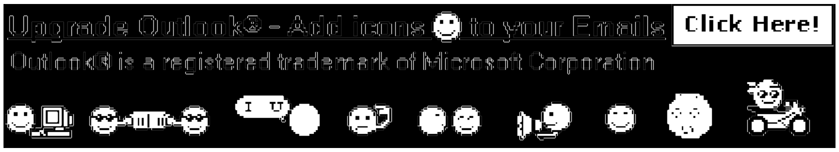
February 19, 2003

TO: All Locations

FROM: Information Technology Services

SUBJECT: ***** URGENT *** HOTBAR SOFWARE ALERT**

In recent weeks the use of an e-mail product called Hotbar has become popular in the school system. E-mails sent from users having Hotbar may have advertising lines at the bottom that look like this:


Upgrade Outlook® - Add Icons ☺ to your Emails
Click Here!
Outlook® is a registered trademark of Microsoft Corporation
I U

All of the icons are animated.

We have discovered that Hotbar is a "spyware" product. This means that it sends information about you, your machine, the web pages you view and the searches you perform via your Internet connection back to the Hotbar database. Although they say in their End User License Agreement (EULA) that they do not keep your personal information in a way that could be identified with the web use or search information, the fact that the information is being taken from your machine and stored elsewhere on a regular basis should be a danger flag to all users.

Based on this and the information listed below, Hotbar software on district computers should not be used and all Hotbar software should be removed as soon as possible. The Hotbar site will be blocked by the district's Internet Content Filtering package and the spyware agent will be blocked at the firewall. Newer versions of the software can be removed by using the Start button/Settings/Control Panel/Add-Remove Programs function in all Windows machines. Older versions are more difficult to remove and may require a visit from a technician. There are also spyware identification and removal products on the market, since there is so much spyware being loaded on computers everywhere. Information Technology Services (ITS) is researching what needs to be done to remove the product completely and will send more information as it becomes available.

The following quote from the EULA explains the danger:

> *"By using the Internet and/or the Software and/or the Service and/or the Content,* ***Licensee may be exposed to contaminated files, computer viruses, eavesdropping, harassment, electronic trespassing, hacking and other harmful acts or consequences that might lead to unauthorized invasion of privacy, loss of data and other damages****. Furthermore, by installing the Software on Licensee's computer, Licensee understands that: (i) certain system non-personally identifiable information, including Statistical Data, stored on Licensee's computer will be made available and transmittable to Hotbar servers; (ii) other information available now or in the future on the Service including links, services, messages advertisements, cookies and the like may be installed on Licensee's computer and; (iii) Hotbar may automatically transmit to and install on Licensee's computer, Software improvements, corrections, adaptations, conversions to more recent Software versions or any other changes to the Software."*

Please note the following:

- Many of the district network administrators, techs and users have reported problems related to the Hotbar software.

- The Hotbar icons and pictures are entertaining, but that is the “hook” they use to get you to install their software. Their real purpose is to get you on their lists to send you advertising of all sorts.
- Hotbar takes information from your machine and sends it to an outsider’s database whenever they wish to receive it.
- Hotbar can install other agents, links, services, advertisements, cookies, etc. on your machine whenever they wish.
- Hotbar is also sending advertising to the e-mail address of the user. This “spam” advertising will eventually overwhelm your inbox if you get on enough lists. You may even begin to receive offensive material, like advertising for pornographic sites. As an example of how they work, if Hotbar sees you doing financial work on your machine, they may decide to start sending you advertising for dozens of stock brokers and analysts, credit card offers, loan companies and “get-rich-quick” schemes of all sorts. **If you begin to receive this kind of “spam” e-mail, do not respond to it. Responses will confirm that the e-mail address is a valid one and they will begin to inundate you with everything imaginable. This even includes responding to say you want to be removed from their list. This again confirms the validity of the e-mail address and in many cases spam senders will ignore your wishes and continue to send advertising.** The district is looking at ways to intercept and delete “spam” before it gets to users.
- Although Hotbar currently promises not to do anything with the information they collect except to send you advertising and icons based on how they see you using your computer, there is no guarantee that a change in management would not decide otherwise.
- The software agent Hotbar installs on your machine may be used by unauthorized hackers to take the data Hotbar collects or load their own executable hacker code on your machine.
- At some point the hackers may be able to modify the Hotbar agent to take any other information they wish from your machine.
- Spyware agents can slow your machine down as they send and receive data and install software as they please. Many people have had their machines rendered virtually unusable because they had multiple spyware products running in the background, mostly without their knowledge, all sending and receiving data without any participation by the user.
- Hotbar currently appears to be incompatible with Internet Explorer 6 and Outlook 2000/XP. A number of users downtown have had to get their computer serviced because of this incompatibility.
- Other users have reported that when you send an e-mail in Outlook that has the Hotbar advertising, the user receives it as an HTML file rather than a standard Outlook message. This means that the standard format has been changed to a web specific format. Also, the user can only save it off their machine as HTML.

It is important to understand that Hotbar is not a virus, but a software package that require that you consent to load the software on your machine. However, newer versions are now appearing in pop-ups from the Internet that are installing themselves without your consent. This is the way most of the spyware packages get on people’s computers. Hotbar appears to be run by a legitimate vendor, but the possible repercussions are the same as if you had gotten a virus or had some other hacker software, like keystroke loggers, surreptitiously installed on your machine.

If you have any questions regarding this memo, please call Support Services at 305-995-3705(0).