# EXHIBIT N

College of Liberal Arts AUBURN UNIVERSITY

Search Departments Site Map Directory Calendar

*You are here:* Liberal Arts Home > Faculty > Technology > Information/Policies > **Spyware/Adware**

Critical Updates

Information and Policies

Spyware and Adware

Mac Adobe Problems and Solutions

## Spyware and Adware

There's a new type of software out there that you may have heard about. It's called Spyware and the most common way it gets on your computer is when you are downloading something else that claims to be free. The purpose of this page is to provide you with some information regarding **Spyware and Adware**.

Spyware and Adware are two examples of "deceptive" software. Deceptive software includes programs which take over your home page or search page without first getting your permission. There are a number of ways deceptive software can get on your system. A common trick is to install the software covertly during the installation of other software you want such as a music or video file sharing program.

Whenever you are installing something on your computer, make sure you carefully read all disclosures, including the license agreement and privacy statement. Sometimes the inclusion of Adware in a given software installation is documented, but it may appear at the end of a license agreement or privacy statement.

### Symptoms

Deceptive software such as Spyware or unauthorized Adware on your computer can cause you to experience any one or more of the following symptoms:

- When you start your computer, or when your computer has been idle for many minutes, your Internet browser opens to display Web site advertisements.
- When you use your browser to view Web sites, other instances of your browser open to display Web site advertisements.

- Your Web browser's home page unexpectedly changes.
- Web pages are unexpectedly added to your Favorites folder.
- New toolbars are unexpectedly added to your Web browser.
- You cannot start a program.
- When you click a link in a program, the link does not work.
- Your Web browser suddenly closes or stops responding.
- It takes a much longer time to start or to resume your computer.
- Components of Windows or other programs no longer work.

**Identification**

You can identify if you have deceptive software on your computer by looking in one of the following locations:

**Add or Remove Programs:**

1. Click *Start*, *Settings*, *Control Panel*
2. Click *Add or Remove Programs*.
3. In the Currently installed programs list, see if there are any programs that you do not recognize or if there are any of the programs listed in the "Examples of Spyware" list below.

**Start Menu:**

1. Click *Start*, *Programs* and see if there are any programs that you do not recognize or if there are any of the programs listed in the Examples of Spyware list.

We recommend that you **do not uninstall or remove any programs yourself**. If you have excessive deceptive software on your computer please contact Lisa Taylor at taylols@auburn.edu for help with removal.

**Examples of Spyware**

AccessPlugin ActualNames ACXInstall AdBreak

| | | | |
|---|---|---|---|
| AdRoar | AdultLinks | AproposMedia | Aornum |
| ASpam | AutoSearch | AutoStartup | BargainBuddy |
| BDE | BookedSpace | BrowserAid | BrowserToolbar |
| Bulla | ClearSearch | ClickTheButton | ClientMan |
| CnsMin | CometCursor | Comload | CommonName |
| CoolWebSearch | CrackedEarth | CustomToolbar | Cytron |
| DailyToolbar | DailyWinner | DialerOffline | DialerActiveX |
| DownloadPlus | DownloadReceiver | DownloadWare | E2Give |
| eStart | eXactSearch | ezCyberSearch | ezSearching |
| FavoriteMan | FlashTrack | FreeScratchAndWin | Gratisware |
| GAMsys | Gator | GlobalNetcom | HotBar |
| Httper | HuntBar | IEAccess | IEDriver |
| IEMonit | IEPlugin | IETray | IGetNet |
| ILookup | InetSpeak | InternetOptimizer | InternetWasher |
| IPInsight | ISTbar | KeenValue | LinkReplacer |
| lop | MagicControl | MarketScore | MasterDialer |
| MatrixDialer | MediaUpdate | Meridian | MoreResults |
| MoneyTree | MyPageFinder | MySearch | NavExcel |
| nCase | NetPal | Network Essentials | NewDotNet |
| NewtonKnows | NowBox | Onflow | OnlineDialer |
| PerfectNav | PerMedia | PowerStrip | Pugi |

RapidBlaster
RelatedLinks
Roimoi
SaveNow
SCBar
SearchAndBrowse
Searchex
SearchSprint
SearchSquire
SearchWWW
ShopAtHomeSelect
ShopNav
Sidesearch
SmartBrowser
SpyBlast
StarDialer
StripPlayer
SubSearch
Surfairy
SuperBar
SVAPlayer
TinyBar
ToolbarCC
TopText
TOPicks
Transponder
TVMedia
Wazam
webHancer
Whazit
Wink
Winshow
Winupie
Wonderland
WurldMedia
XDialer
XDiver
XLoader
Xupiter
ZeroPopUp
Zipclix
Zyncos

Questions about this page
Last updated September 28, 2004

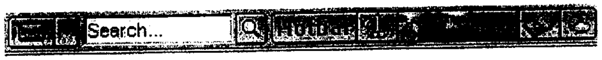
College of Liberal Arts
2046 Haley Center
Auburn University, AL 36849
Phone (334) 844-4026
FAX (334) 844-2378

Protect your computer -- Highlighted 'Ware Archive -- Hotbar Removal Instructions

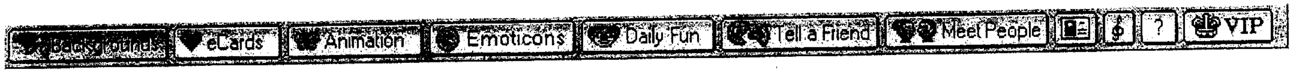
## How to Remove Hotbar

Hotbar is a popular program that installs a new toolbar into Outlook and Internet Explorer that allows you to use 'smilies' and other graphical features in e-mail. What you might not know about Hotbar is that it also installs a plethora of spyware onto your computer, which tracks your surfing habits and pops up advertisements. This Spyware can be a threat to your privacy and will also cause your computer to run much more slowly.

How do you know whether or not you have hotbar? If you see this toolbar in Internet Explorer:

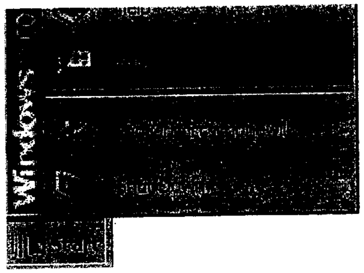


And / Or this one in Outlook:

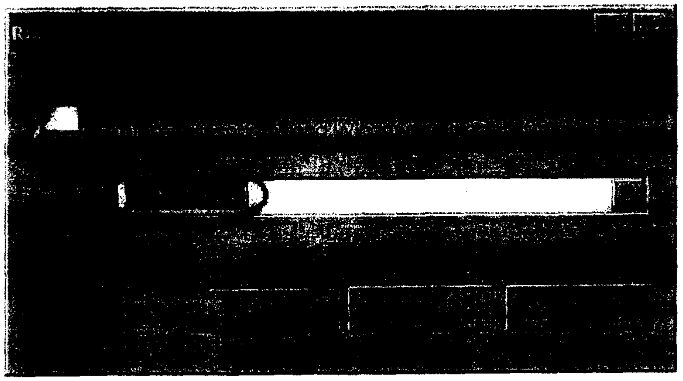


Then you have hotbar and should remove it as soon as possible. The removal process is quite simple:

Click "Start" and then select "Run":

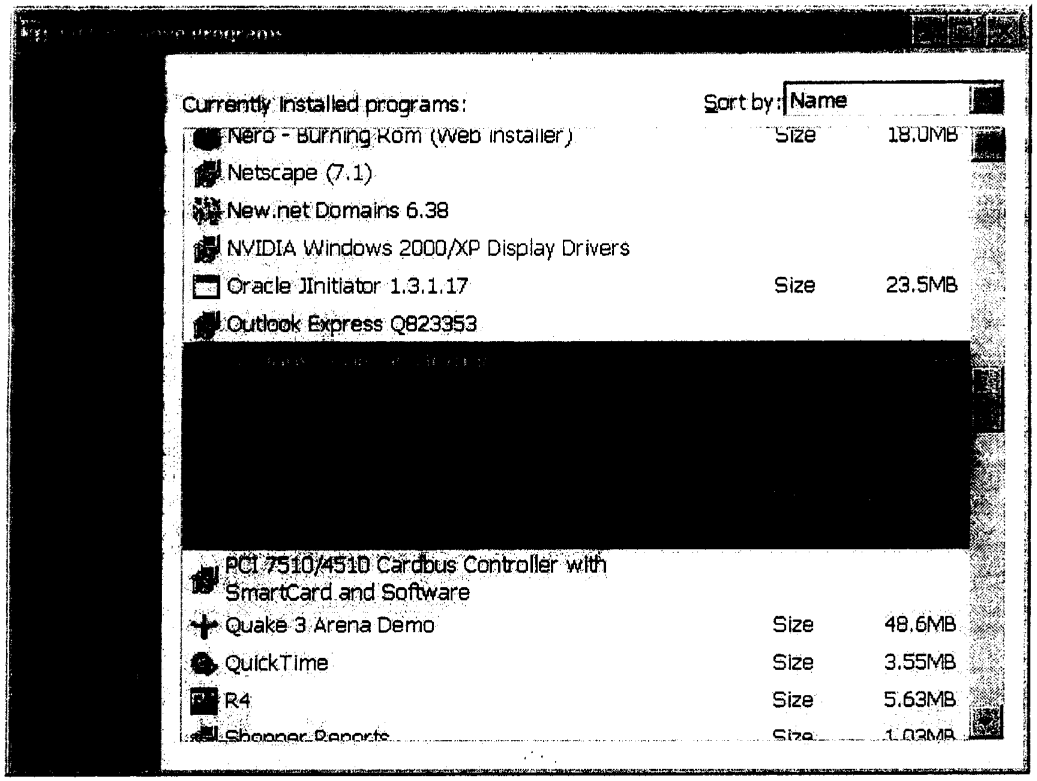


Type "control panel" and click "OK":



Select "Add/Remove Programs" from the list of control panel options:

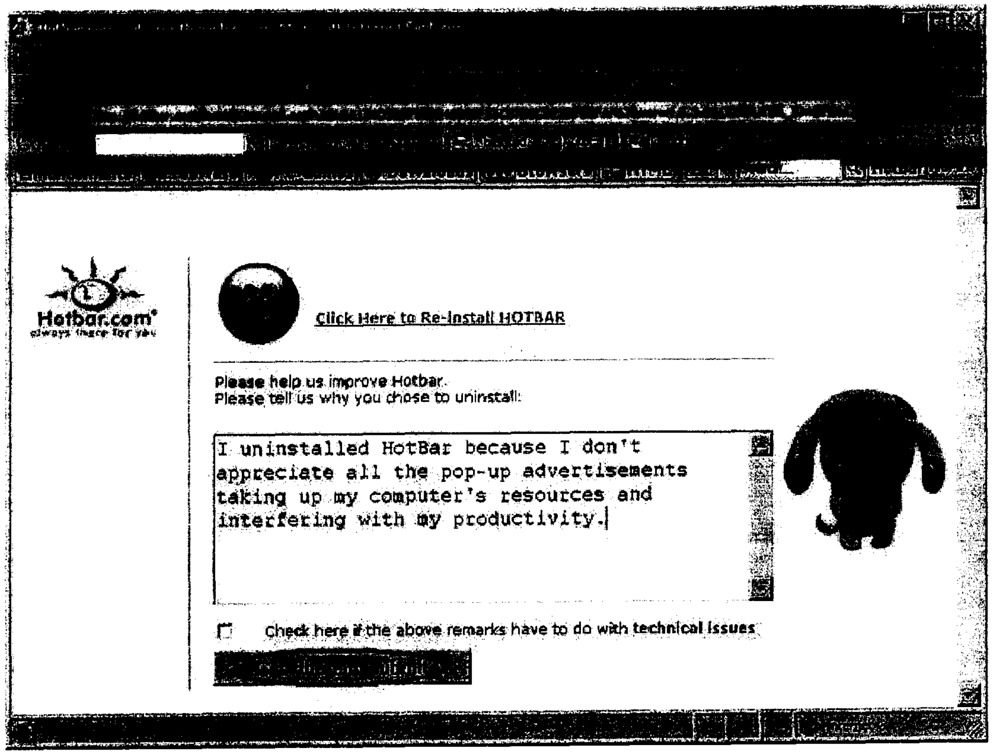
Scroll down the list of programs until you find "Outlook Tools by Hotbar" and then click "Change / Remove":



Currently installed programs: Sort by: Name

| | | |
|---|---|---|
| Nero - Burning Rom (Web installer) | Size | 18.0MB |
| Netscape (7.1) | | |
| New.net Domains 6.38 | | |
| NVIDIA Windows 2000/XP Display Drivers | | |
| Oracle JInitiator 1.3.1.17 | Size | 23.5MB |
| Outlook Express Q823353 | | |
| [redacted] | | |
| PCI 7510/4510 Cardbus Controller with SmartCard and Software | | |
| Quake 3 Arena Demo | Size | 48.6MB |
| QuickTime | Size | 3.55MB |
| R4 | Size | 5.63MB |
| Shopper Reports | Size | 1.03MB |

After telling it you are sure you want to uninstall, the following webpage will come up. Enter whatever reason you wish, or simply type a few random characters into the field and then click "Click here to submit":



Click Here to Re-Install HOTBAR

Please help us improve Hotbar.
Please tell us why you chose to uninstall:

I uninstalled HotBar because I don't appreciate all the pop-up advertisements taking up my computer's resources and interfering with my productivity.

□ Check here if the above remarks have to do with technical issues

That's it! Now reboot your computer and Hotbar will be gone.

*NOTE* The Help Desk also recommends running a spyware scan to remove any vestiges of Hotbar that may remain after the uninstallation, and also to clean up any other spyware you may have. Click Here for instructions on performing a spyware scan.

Last Updated 02/14/05

Back to Top

# Dakota Wesleyan University-Helpdesk

1200 West University Ave.·Mitchell, SD 57301·www.dwu.edu
605-995-2697
email: helpdesk@dwu.edu

## Spyware

Common Files of File Sharing & Adware/Spyware

### What is spyware?

- Spyware is any software that covertly gathers user information through the user's Internet connection without their knowledge. It is generally used for advertising. It is often included within freeware or shareware programs that are downloaded off the Internet.
- Spyware can invade your privacy. It can monitor keystrokes, scan harddrives, read cookies, install other software, load advertisement, and constantly relay information back, and forth to the author of the spyware. It can gather information about email addresses, the users' activities on the Internet, and even password and credit card numbers. This information then can be passed along undetected to someone else.
- Spyware robs the user of memory resources on their computer. It can make your computer system and browser unstable and cause your system or browser to crash. It can also make your system run slower.
- The bad news is there are hundreds of these types of programs out there. Some common spyware programs include: Hotbar, Comet Cursor, Xupiter, Gator, Offer Companion and BonziBuddy. RealAudio Player can also put "data mining" software on your system to "track preferences" and report back to the mothership. Even free CD games from a cereal box or fast food kid's meal can put "adware" on your system.

### Symptoms

- browser crashes
- computer instability
- high CPU utilization
- unexplained freezing
- slowness
- slow boot time

- "blue screen of death"
- illegal operation errors
- signature lines change
- pop-up/under advertisements appear when the user is online and offline
- default homepage of the browser changes

**Spyware categories**

- **Adware networks**
  The backbone for big time spyware are ad serving networks that pay publishers of games, utilities and music/video players per download, to include their ad serving programs. As serving networks are DoublClick, Web3000, Radiate, SaveNow, GAIN.

- **Stalking horses**
  A number of programs that enable the adware networks to function on desktops are bundled in many popular programs and often (not always) presented in installation disclosure screens as desirable add-ons to their Trojan horse hosts. All collect information. Included in TopText, Cydoor, OnFlow, Medialoads, Delfin, WebHancer, New.net

- **Trojan horses**
  These popular Internet downloads usually come with ad serving network basic software and at least one stalking horse. Included in KaZaa, Grokster, Morpheus, Limewire, AudioGalaxy, iMesh, DivX.

- **Backdoor Santas**
  Stand-alone programs that incorporate similar approaches have no links to ad serving networks and collect information from users. Included in Alexa, Hotbar, Comet Cusor, eWallet, CuteFTP, BonziBuddy.

- **Cookies**
  Netscape Navigator and Internet Explorer will still send out existing cookies even after disabling cookies in the browser settings. You must manually delete any/all cookie files on your system to eliminate being tracked by third party ad networks or spyware or adware providers.

**How do you get rid of Spyware?**

Many anti-Spyware products are available for free download, such as Ad-aware and Spybot. These products scan for Spyware and allow you to remove it.

In Ad-aware, the Scan now option will search default or selected drives for Spyware files. When the scan is finished, click Next to view display results for the objects found. Double-click on any object to view its details and decide whether you want it to stay on your computer. To remove objects, click their checkbox and then click Next.

In Spybot, the Search for Problems option will perform a system scan for Spyware. When the scan is finished, results will appear in the white box. Click the fix selected problems button to delete the checked files. Spybot also has an Immunize option to block problem files.

### How do you keep from getting Spyware?

- Always install from trusted sources and make sure to read the End User License Agreement.
- Set your browser not to allow third-party or session cookies For Internet Explorer (5 and above), this is done in Tools-->Internet Options-->Privacy.
- Delete temporary Internet files and set History to 1 day. For Internet Explorer (4 and above), this is done in Tools-->Internet options-->General.
- Use anti-virus software and keep it up-to-date.
- Use a personal firewall such as Zone Alarm and/or an Internet filter such as DNSKong.
- Avoid using Peer-2-Peer file sharing programs or "freeware."
- Do not click on banners that appear at the top of web pages even if they look like a fun game, they say you are a winner or they are going to help you correct a potential problem on your computer (your clock is wrong, you have spyware, ect.). Do not download free software. If you must use free software, be as selective as possible and only install that which is completely necessary. Use trustworthy web sites.
- Do not follow links in spam e-mail messages. They often take you to sites that install spyware on your computer.
- Music/file sharing software is illegal. It is also a pipeline to spyware, viruses and hackers.

### Are cookies considered spyware?

- Cookies are used in a manner similar to adware and spyware. They report information about you back to the publisher of the cookie. Many, many web sites use cookies. Respectable sites, such as Amazon.com, use cookies responsibly. They only store information directly related to the use of their web pages. Other sites gather more information than they should. Cookies can easily be deleted and they can recreated when you revisit the site.

### How to detect and remove spyware

- There is no one software product that will detect and remove all spyware. Until better anti-spyware software is developed the best you can hope for is to manage the problem. Try using free products and use them in tadem. Neither product is known to install spyware or adware. They are Adware and Spybot.
- Removing spyware may disable the software it tagged along with. In some cases the spyware cannot be removed until the free software it came with is also removed.

**Back to Top**

DUKE UNIVERSITY

oit ATS

Academic Technology Services

Home About Computer Labs Multimedia Project Studio Training SWAT Community Outreach Site Map Contact

Spyware > iMesh

# SUPPORT DOCUMENTS

Spyware
- Audiogalaxy Satellite
- BearShare
- Global DiVX Player
- GolZilla
- Grokster
- iMesh <
- Kazaa
- LimeWire

Students
- Lab locations
- Printing
- Training options & topics
- Register for a workshop
- Request a tutorial

Faculty
- Lab schedules
- Reserve a lab
- Request lab software
- Training showcase
- Request student training

## iMesh

iMesh installs three pieces of spyware without consent.

| Name of Spyware | Program function | Known issues | Automatically Installed |
|---|---|---|---|
| Gator | Assists with forms by remembering usernames, passwords, etc. of sites you frequently visit. | Very dangerous in that it can also "assist" you by remembering credit card numbers. | No |
| OfferCompanion | Offered with the Gator installation, it tracks your web habits and transmits the data back to Gator.com. | | No |
| SaveNow | Advertising toolbar that monitors what sites you visit and pops up sponsored "deals" when products/shopping/etc. appears on those sites. | | No |
| iMesh Ads Support | It is unknown what this software does. We can only assume it serves up ads when you are using iMesh. | Does not un-install when iMesh is un-installed. Must be un-installed separately. | Yes |
| New.net | Filters all web address requests through the DNS servers of New.net. | Can cause your internet connectivity to stop altogether. The New.net plugin is known to have compatibility problems with some other products. Also, it leaves a new.net .dll file on your computer, which may interfere with your internet connection after the program has been removed. | Yes |
| Hotbar | Gathers and stores information about the web pages you visit and the data you enter in search engine search fields. Places ads in the toolbar of your browser. | | No |

| | | | |
|---|---|---|---|
| Bonzi Buddy | An icon to install this software is placed onto your desktop. This "software companion" places a talking purple cartoon character on your desktop that purportedly helps you find items easier on the Internet. | This software is embedded deep in your operating system and is very difficult to remove. A re-installation of Windows may be necessary to completely remove it. (Not to mention that its cuteness wears off after 3 or 4 restarts and it just becomes a nuisance when you use your computer.) | Yes |

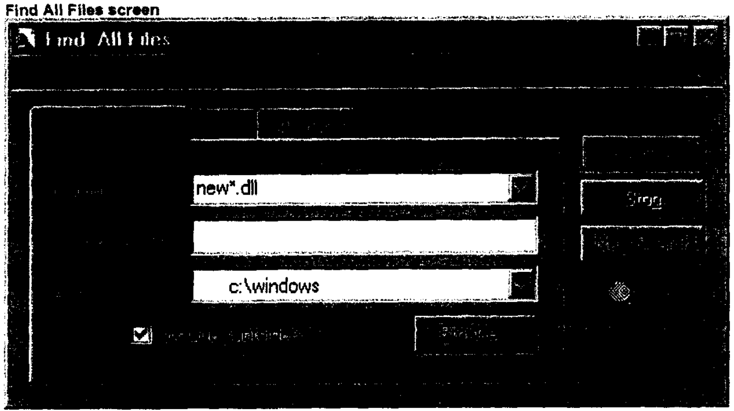
Should you decide to un-install iMesh, the following spyware components are left on your computer.

| Registry Keys | Files | Folders | Miscellaneous |
|---|---|---|---|
| 2 for SaveNow<br>3 for Hotbar<br>2 for Gator | 1 for Web3000<br>5 for Gator | 4 | 0 |

In addition to these files, the folder NewDotNet should be removed from C:\Program Files. You should also perform the following steps:

1. Select Start > Find > Files or Folders
When the following screen appears, fill in the appropriate fields on your screen with the values shown and click Find Now.

Find All Files screen



new*.dll

c:\windows

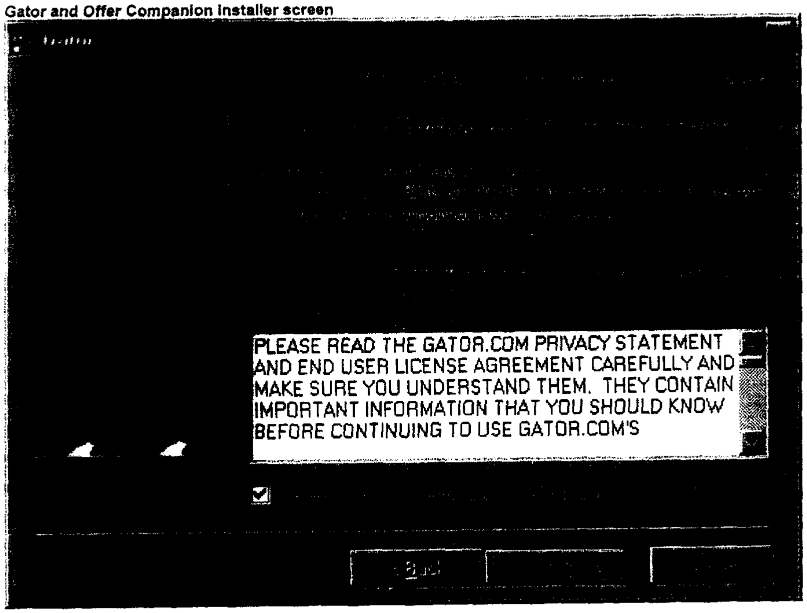
2. If any files are found, right click on each file and select Rename.

3. Replace the last three letters of the filename, dll with the letters old.

4. Close the window by clicking the X in the upper right corner of the window.

Recognizing the following screens and taking the prescribed action minimizes the amount of spyware/adware installed onto your machine

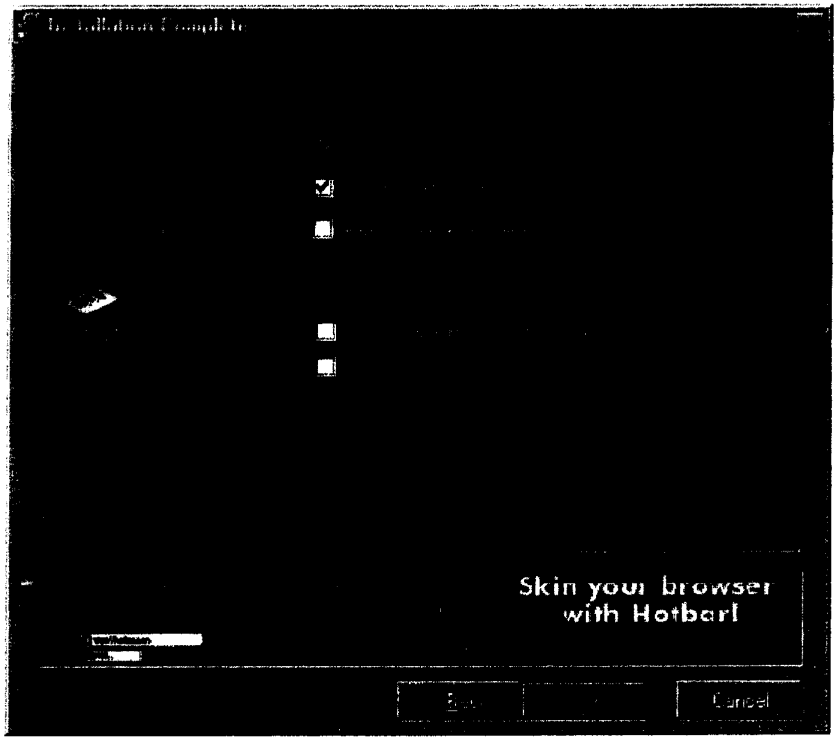
**Gator and Offer Companion installer screen**



PLEASE READ THE GATOR.COM PRIVACY STATEMENT AND END USER LICENSE AGREEMENT CAREFULLY AND MAKE SURE YOU UNDERSTAND THEM. THEY CONTAIN IMPORTANT INFORMATION THAT YOU SHOULD KNOW BEFORE CONTINUING TO USE GATOR.COM'S

Uncheck the check box and then click I Accept/Next.

**iMesh main installer screen**

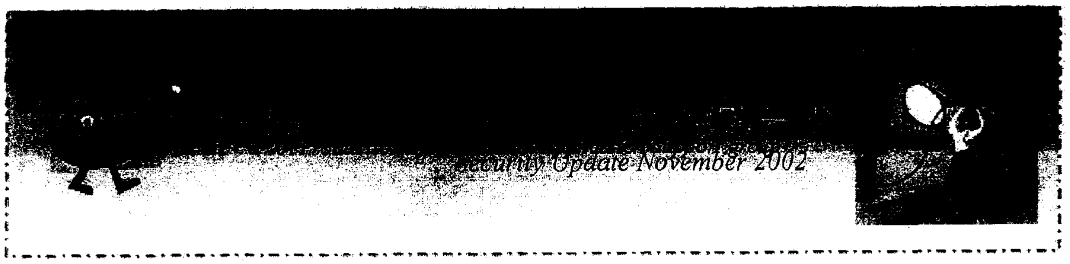


Deselect HotBar and SaveNow options as shown above and click Finish.

OIT HOME | HELP DESK | SITE INDEX | SEARCH OIT | DUKE

OIT Home | Help Desk | Site Index | Search OIT | Duke Home

**Last updated: 09/22/2003 12:08:32**
Questions/Problems? Let us know.

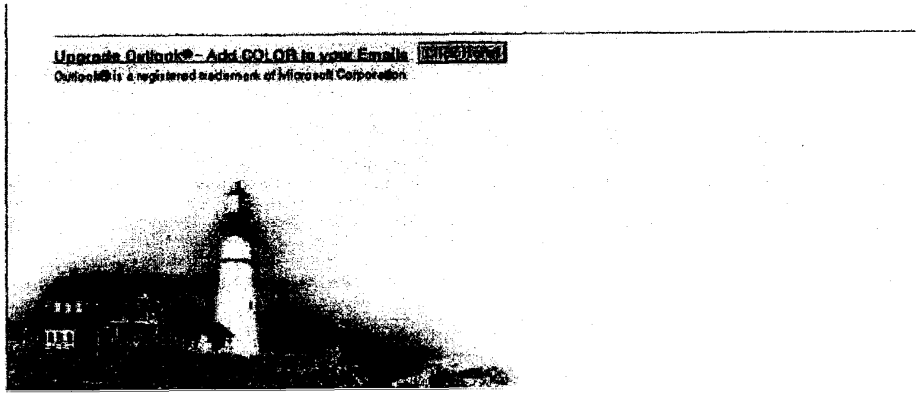


*In an effort to help educate faculty and staff, ITCS critical application support group will be providing the west campus with a security tip of the month. These tips will be focused on all areas of system security.*

If you have a tip request or comments please e-mail Lisa Ezzell at ezzelll@mail.ecu.edu

## Topic: Hotbar and other spyware

At first glance the scene below appears to be an official upgrade. Actually, it will install Hotbar on your system. What is hotbar? Their website says it enhances and personalizes your internet and email applications. While this may be true, there are a few facts that you should know about this software.


Upgrade Outlook® - Add COLOR to your Emails
Outlook® is a registered trademark of Microsoft Corporation.

1. This is not an official upgrade from Microsoft Outlook.
2. Hotbar is considered Adware / Trackware. It is a program that adds graphical skins to Internet Explorer toolbars. It monitors all websites you visit to add link buttons to its toolbar dependant on the websites you visit.

Is Hotbar violating your privacy? Yes, it spies on websites visited and forms filled in, even when the toolbar is disabled.

3. Is Hotbar a security violation? Yes. Hotbar has a silent update feature, which means, that without your knowledge or approval. this software will go to its home website and download newer versions automatically.
4. Does Hotbar cause problems with the computer system? Yes, it can slow down you computer or cause lockups when you are using your web browser or email.

How to remove Hotbar

1. Click on Start, Control Panel (or Start, Settings, Control Panel)
2. Click on add/remove programs
3. Locate hotbar, click on it one time (so it is highlighted)
4. And choose remove
5. You will be asked to check which programs you wish to have it removed from choose both outlook and internet explorer.

Please note there is other adware / trackware otherwise known as "spyware" - some of the most common are Gator, Offer Companion and BonziBuddy.

Check out these websites if you would like more information on the different types of "spyware" that is out there.
http://www.accesscomm.ca/internet/security/spyware.html

http://www.pdxtc.com/200201-spyware.htm
http://grc.com/oo/spyware.htm
http://virgolamobile.50megs.com/spyware/spyware.htm

**Training opportunity!!**

We are offering training opportunities on a work group basis. If you or your office mates at Brody School of Medicine need training on particular topics, please forward your requests to Tim Hester at hestert@mail.ecu.edu.

[redacted]

## Prohibited and Undesirable ("Bad") Software

**SUMMARY - Please do NOT download or install *any* freeware or software. If it is specifically related to your job duties, we request that you call the OIT Help Desk and request assistance first!**

**Spyware, Scumware, Adware, Malware, Parasitic, Prohibited, and Undesirable Software**

This page was developed to provide definitions and information on the types of software that may have been installed on the workstation in your office. In addition, a list of prohibited and undesirable software, as referred to in the memo by Dr. Stanton on January 17, 2002, is posted.

**Spyware** - There is considerable debate, even among the experts, on what exactly constitutes Spyware. One characteristic in common is the ability of these types of programs or technology to gather information about a person or organization without their knowledge. It can get onto a workstation through a virus or through the installation of a program. If you install a program and agree to the EULA (End User Licensing Agreements), this would not necessarily be considered Spyware since you agreed to the EULA in order for the program to install itself on the workstation. Most people will not read through a lengthy EULA, particularly when it is full of legal-sounding terms - they will just click Next or OK to get the program quickly installed.

**Be very careful** of shareware or freeware, know exactly what type of information it intends to gather about you, the web sites you visit and the ad banners you click on, as well as what they intend to do with that information and who they intend to share it with! Some common examples of software that may be considered Spyware include Gator, DoubleClick, Yo Mama, Osama (game), Aureate Media, Hotbar, Comet Cursor, Conducent Timesink, Cydoor, Flashpoint/Flashtrack, GoHip, Mattel Brodcast, SongSpy, Web3000, WebHancer, and RadLight. For more information, visit http://netsecurity.about.com/

**Scumware** - Scumware most often will disguise itself as Adware, when in actuality, it can track what you are doing on the web, and even alter the contents of a web page without your knowledge, or the knowledge of the site's owner! Common scumware programs include OfferCompanion (it comes installed with Gator, you just aren't informed), EZula, TopText, Surf+, and others.

For more information and updates, visit http://www.scumware.com.

**Adware** - As defined at http://whatis.techtarget.com, Adware is "any software application in which advertising banners are displayed while the program is running. The authors of these applications include additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on a computer screen. The justification for adware is that it "helps recover programming development cost and helps to hold down the cost for the user." In addition, some Adware programs will send personal information to third parties without the user's knowledge or consent (see Scumware). Some of the more common programs are BonziBuddy and Tsadbot.

For more information, click here:
http://whatis.techtarget.com/definition/0,289893,sid9_gci521293,00.html

**Malware** - Malware (malicious software) is any program or file that will alter or delete files on the hard drive of a workstation. It is developed for the purpose of doing harm. Included in this category are viruses, Trojan horses, and Trojan worms.

**Parasitic Software** - Most often, this software is installed via freeware without the user's knowledge, it latches itself onto the web browser. It can cause numerous, annoying, pop-up banner ad windows, report what you do online back to marketing companies, leave security holes in the system, add advertising links to web pages, cause system degradation, use enormous amounts of bandwidth, and cause system errors. Most often, virus scanning software will not detect this type of program, they are technically Trojans and not viruses.

Many of the parasitic programs identified by OIT so far are bundled with other freeware programs. We have made every attempt to identify these freeware programs and block them through the firewall.

**Prohibited Software** - **Any form** of pornography is prohibited on campus computers. Policies have been written for the exact procedures to implement when pornography is identified. (See Enforcement of this Policy (Employees) at http://www.etsu.edu/humanres/ppp/PPP-44.htm. Child pornography is a federal offense. Anyone with knowledge of child pornography on any campus computer is legally obligated to report it to the proper authorities.

**Undesirable Software** - There are certain programs, mostly likely available as freeware or shareware, that have proven to be "bandwidth suckers", that is, they will use the workstation as a peer-to-peer server for webcasting, therefore using huge amounts of campus bandwidth. When this happens, the network slows down for everyone on campus. Normally, these programs will show as spikes on the bandwidth management program and may send alerts. In the cases that OIT has investigated, the user was totally unaware of what was occurring. As usual, be very careful of what you are downloading and installing on the computers in your department. Some of the peer-to-peer sharing programs identified and disabled through the campus firewall are Napster, Morpheus, KaZaA, Radlight, MarketScore, and Chaincast. In addition, the OIT Code of Ethics prohibits the intentional use of viruses for the purpose of infecting any campus computer. Please review the Code of Ethics at this time.

Normally, these programs will show as spikes on the bandwidth management program and may send alerts. Some have been identified and blocked at the firewall. However, more are developed and released everyday, so an extensive, up-to-date list is virtually impossible to maintain.

**We request that you NOT install HotBar on your computer! If you already have it, please uninstall it now.**

ICQ, AOL Instant Messenger, Yahoo Instant Messenger and any other instant messaging programs should not be used.

In addition, there are programs that send continuous packets across the network, once again, slowing things down and using bandwidth unnecessarily. The most popular ones OIT has encountered include **WebShots**, and any of the **stock-ticker update** programs. We request that you uninstall any of these applications from the workstation in your office.

There are tools to help you identify and remove some of these applications. Although OIT cannot promote any, you are free to visit the web sites and use any removal tools that are available free of charge. Please see:

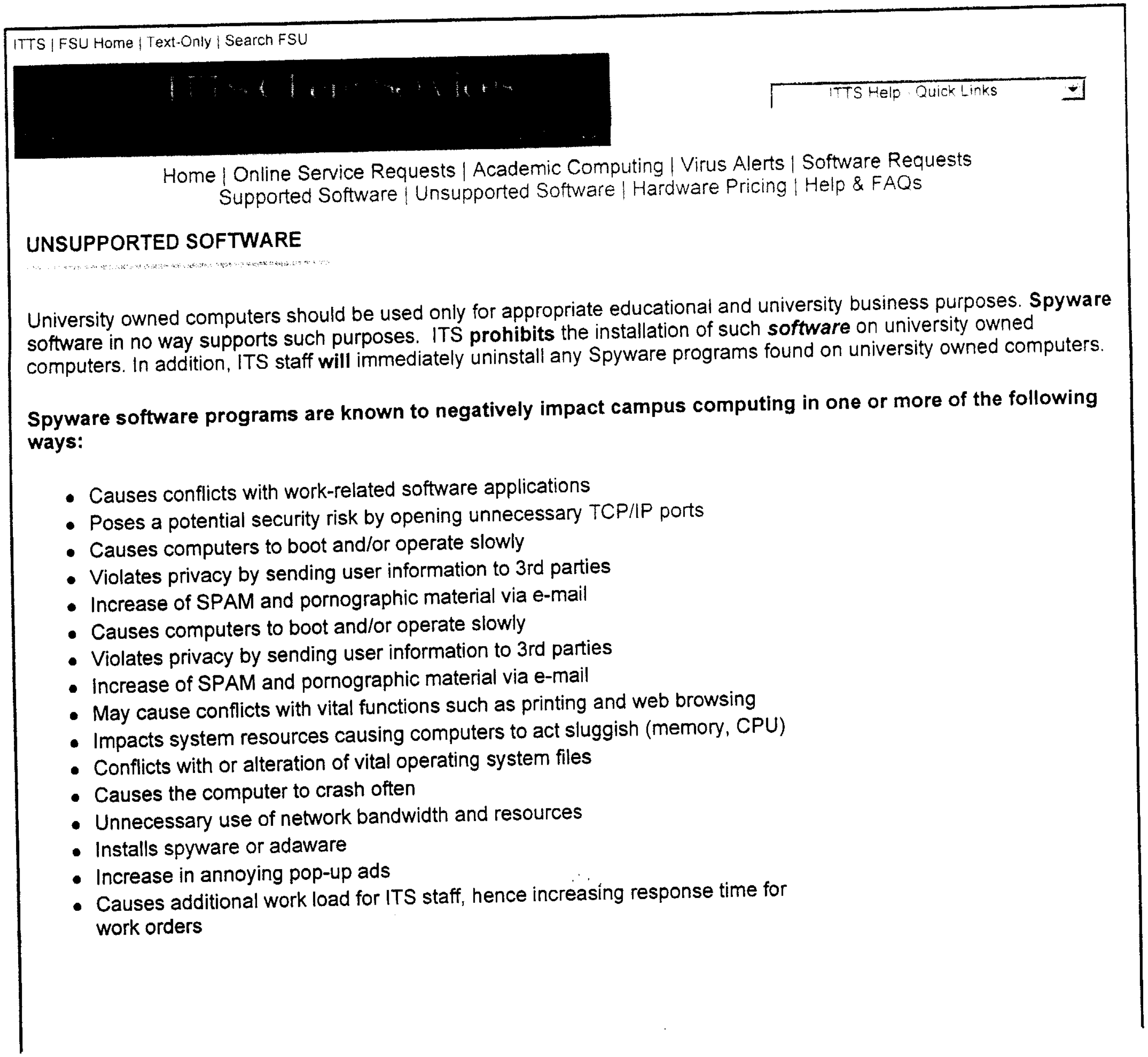
Pest Scan from Pest Patrol™: http://www.pestscan.com/ScanOrTrial.asp
SpyBot Search & Destroy: http://beam.to/spybotsd
Ad-Aware: http://www.lavasoft.de
PC Tools' SpyWare Doctor: http://www.pctools.com/spyware-doctor/?ref=trial_google

Also visit:

http://www.spywareremoversreview.com/
http://antivirus.about.com/od/spywareandadware/

Some of the information on this page is a compilation from several reputable sites on the Internet. If you have comments, questions, or concerns about the information you find here, please contact the OIT Help Desk by phone (x94648, on campus, or (423) 439-4648 if you are calling from off campus) or send email to oithelp@etsu.edu

last updated 06/24/04



ITTS | FSU Home | Text-Only | Search FSU

Home | Online Service Requests | Academic Computing | Virus Alerts | Software Requests
Supported Software | Unsupported Software | Hardware Pricing | Help & FAQs

## UNSUPPORTED SOFTWARE

University owned computers should be used only for appropriate educational and university business purposes. **Spyware** software in no way supports such purposes. ITS **prohibits** the installation of such ***software*** on university owned computers. In addition, ITS staff **will** immediately uninstall any Spyware programs found on university owned computers.

**Spyware software programs are known to negatively impact campus computing in one or more of the following ways:**

- Causes conflicts with work-related software applications
- Poses a potential security risk by opening unnecessary TCP/IP ports
- Causes computers to boot and/or operate slowly
- Violates privacy by sending user information to 3rd parties
- Increase of SPAM and pornographic material via e-mail
- Causes computers to boot and/or operate slowly
- Violates privacy by sending user information to 3rd parties
- Increase of SPAM and pornographic material via e-mail
- May cause conflicts with vital functions such as printing and web browsing
- Impacts system resources causing computers to act sluggish (memory, CPU)
- Conflicts with or alteration of vital operating system files
- Causes the computer to crash often
- Unnecessary use of network bandwidth and resources
- Installs spyware or adaware
- Increase in annoying pop-up ads
- Causes additional work load for ITS staff, hence increasing response time for work orders

Please contact the ITS Helpdesk at extension 2085 for assistance in the removal of any of the following programs which are considered Spyware. You will be notified as we discover additional ***Spyware*** software.

**Alexa**
**Web Search tool (adware)**
http://www.thestandard.com/article/display/0,1151,9599,00.html

**ATTune**
Sponsored pop-up ads (e.g. "Buy toner") when using your printer (spyware)

**AudioGalaxy**
File Sharing (spyware, copyright infringement, high bandwidth use, banned in CCLs)
http://security.uchicago.edu/peer-to-peer/no_fileshare.shtml

**Aureate / Radiate**
Spyware "bundled" with many free downloads, screen savers, web sites, etc.

**Bargain Buddy**
Advertising (spyware, bandwidth use, computer resources)

**BearShare**
File Sharing (spyware, copyright infringement, high bandwidth use, banned in CCLs)
http://security.uchicago.edu/peer-to-peer/no_fileshare.shtml

**Bonzai Buddy**
PC "Pet" (resource drain, application conflicts, no university related purpose)
http://www.cord.edu/dept/computing/news/newsletters/2001/03/26_2.html

**Brilliant Digital**
Brilliant Plan to Usurp Internet Bandwidth
UC-Berkeley - Security Risks and Bandwidth Hijacking
http://news.com.com/2100-1023-875274.html

**Comet Cursor**
Animated cursor (probable spyware, waste of resources, possible application conflicts)
http://wwwnew.towson.edu/cans/faculty/policy/software/problematic.asp

**CommonName**
Targeted advertising (spyware, resource drain)
http://www.safersite.com/PestInfo/C/CommonName.asp

**CyDoor**
http://www cexx.org/cydoor htm (spyware, resource drain)

**DLDER**
http://www.cexx.org/dlder.htm (spyware trojan)

**Gator, OfferCompanion, Trickler, GAIN**
Very intrusive spyware that auto-fills web forms. Dangerous because it caches and "remembers" credit card numbers.
http://www.cexx.org/gator.htm

**GoZilla**
Download accelerator (slows boot time, drains resources, multiple spyware)
http://www.oit.duke.edu/ats/support/spyware/gozilla.html

**HotBar**
http://www.safersite.com/PestInfo/h/hotbar_adware.asp

**Kazaa**
Stealth Network Hides Inside Kazaa
http://security.uchicago.edu/peer-to-peer/no_fileshare.shtml

**OnFlow**
Targeted advertising bundled with many "free" applications (spyware)
http://www.slyck.com/newsjan2002/010602a.html

**Spinner (Not Spyware)**
As with many of the other programs listed here, it is an unnecessary application that uses up valuable system resources, especially memory and network bandwidth. One problem that sets Spinner apart from others is that, by default, it starts automatically after logon. Many necessary system services are loading at this time - so the less there is, the quicker the system boots, and the sooner you can start using the system. If ITS finds that Spinner is installed on your PC and causing conflicts, it will be removed immediately by ITS staff.

**Weatherbug**
Continuous, real-time weather reports (high bandwidth use, potential security risk, slows boot time, can disable printing, spyware)
"Spyware" catches school tech directors by surprise
Weatherbug - Bandwidth Use and Questionable Behavior
UWM School of Education: Conflicts, Not Supported, Banned in Labs
Duke University: list of troublesome software

**Web3000**

Advertising spyware that overwrites the important wsock32 dll system file (spyware, potential security risk)

**WebHancer**
Extremely intrusive spyware, can disable internet connection
http://www.cexx.org/webhancer.htm

**Webshots**
Wallpaper rotation utility (spyware, slows boot time and system operation, application and operating system conflicts)
U of AZ: Webshots Causes Computer Performance Problems

**Xupiter**
Xupiter, like Gator, is spyware that can be installed on your computer without your knowledge if your Internet security settings are not set correctly. It can be installed when you visit a web site or click on an advertising link. Applications that install in this manner are also referred to as "drive-by downloads." (This term was probably derived from a similar term, "drive-by hacking", which describes a practice hackers employ to hack into wireless networks. In the case of spyware, the term "drive-by" is figurative; in the case of hackers, the term is literal.) If you suspect that you may have Xupiter installed on your computer or you find that your web browser is running very slow, please submit a service request thru FootPrints to have it removed from your computer.

"Fayetteville State University is a member institution of The University of North Carolina, which is committed to equality of educational opportunity and does not discriminate against applicants, students, or employees based on race, color, national origin, religion, sex, age, or disability."

Page Contact: Linda Mitchell
Last Updated: 05/27/05 03:30 PM

Gettysburg College Information Technology Department

# IT Bits

[illegible]

## HotBar Users

Please be aware of the following security risk for ***Hotbar*** users.

Hotbar, an add-on program for Microsoft Outlook, has become a heavily used application across campus. While we understand the desire to make e-mails friendlier, this application has some definite drawbacks.

The first of these drawbacks is that this program is considered Spyware. Like Comet Cursor, it records information from your computer and then sends that information to a centralized database. The type of information being sent is unknown to us in Computing Services, however it could be personal information that you do not wish to have known. This information could be responsible for some of the Pop-ups

## About IT Bits

IT Bits is a new weekly newsletter offering the Gettysburg College faculty & staff the latest in campus IT news. The newsletter will be published on a weekly basis. You will be able to read IT bits online at http://www.gettysburg.edu/it/itt/itbits. In addition, a link to IT Bits and contents will be published in the CNAV Faculty, Support-Staff, and Administrative digests.

## IT Bits Archives

Did you miss last weeks edition? Check out ITBits historical archives at:

**ITBits Archives:**
http://www.gettysburg/edu/it/itt/itbits/archives

Interested in other archives?

U.S Archives:
http://www.archives.gov/

Internet Archives:
http://www.archive.org/

## *Computing Tip* - Changing Passwords

**Time to change your password?**

**go to:**

**http://www.gettysburg.edu/passwords**

**IT Links**

- ■ Gettysburg College
- ■ IT Homepage
- ■ Computing Services
- ■ Instructional Technology & Training
- ■ WebTech
- ■ MIS
- ■ IO

advertisements and Spam email that plagues your computer and reduces productivity.

The second problem with this application is that it can cause several problems within Outlook! We have seen instances where Outlook fails to open at all, instances where the "Send" button disappears, and instances where other basic options appear grayed out, and several other problems.

This application gets sent to you from a person who has already installed Hotbar. Inside of their message, there is a section at the bottom that says, "Upgrade Outlook – Add Icons to your e-mails". We are recommending that you do not click any link as it will install the Hotbar application and is likely to cause problems with Outlook. Installing the application will surely install a Spyware component that will begin tracking your computer use.

If you have already installed Hotbar or know of someone who has done this who works for you, and would like this removed Computing Services recommends the installation of AdAware (see below). This is a product that Computer Services uses when we visit a machine on campus to remove Hotbar as well as other Spyware.

Alan Griffin
Computing Services

Back to top

### Preparing for the Upcoming Semester (Blackboard)

If you are planning to use Blackboard next semester, it would be to your advantage to begin development as soon as possible. Developing your course site in advance will save you a great deal of hassle during the upcoming semester by reducing technical problems and reducing the workload of uploading documents, creating discussion boards, and generating quizzes.

New Blackboard course sites for the upcoming spring semester will not be generated until mid-August. However, this does not mean that you cannot begin developing your Blackboard course site for this fall. If you are planning on using Blackboard next semester you have several options for creating a course site and begin working on adding content into the site immediately.

1. **You can reuse one of your old course sites**
   Reuse an existing course site during the summer months for development. Once your fall semester course site is generated, you can have your development site copied into the new fall semester course site. Contact James Rutkowski to have your development site copied into your fall semester course site after your course site has been generated in mid-August.

2. **Create a development site**
   Contact James Rutkowski if you would like to create a separate development course site to work on during the summer. You can then have this course site copied into the new fall semester course site in mid-August by contacting James Rutkowski before the semester begins.

If you would like help on getting started with Blackboard, please contact James Rutkowski at x 6198.

Back to top

**Ad-Aware - Get Rid of Spyware**

Computing Services has begun using a program called AdAware to search your computer for what is known as Spyware. Spyware includes applications such as Hotbar, Comet Cursor, and Gator. These are programs that collect data on your machine and send it back to a centralized database. These programs can increase the inflow of pop-up ads and spam and are also responsible for slowing down a computer.

To download AdAware,

go to: http://lavasoft.element5.com/support/download/ or if you are here on campus (windows Users)

-Click the **Start** Button

-Select **Run** from the Start menu
-Type *\\responsems\data\Utilities\adaware\AdAware6* in the *Open* field and press **OK**
-Install AdAware by double-clicking the **aaw6.exe** file

Once AdAware has been installed, an icon will be placed on your desktop allowing you to start and run the application. Computing Services recommends that you use the default settings for scanning your computer.

To run the program:

- Open AdAware program and click **Start** button in the lower right hand corner
- Click the **Next** button to begin scanning your computer.
- When the scan is done, click **Next** again
- You will see a list of the found items (items that are considered SpyWare) with corresponding checkboxes.
- Simply check all the boxes and click the **Next** button.
- A confirmation dialog box will appear, click **OK**.
- The files will be removed from your system and you will be sent to the beginning screen. You can now close out of the application and continue working.

Please Note** While it is possible to work on other things while AdAware is scanning, it is not recommended because the Spyware could be working in conjunction with the other applications you have open at the time and not be allowed to be removed.

Computing Services recommends that the application be run once every two weeks, or whenever an influx of pop-up ads, spam, or slowness occurs.

For more help with AdAware, please contact Computing Services at x7000

Back to top

**About IT Bits**

IT Bits is a new weekly newsletter offering the Gettysburg College faculty & staff the latest in campus IT news. The newsletter will be published on a weekly basis. You will be able to **read IT bits online at** http://www.gettysburg.edu/it/itt/itbits. In addition, a link to IT Bits and contents will be published in the **CNAV Faculty**, **Support-Staff**, and **Administrative digests**.

Back to top

Questions/Comments about this site?

HOME | CALENDARS | DIRECTORIES | SEARCH | CONTACTS

Information Systems & Services

HOWARD UNIVERSITY

Students | Faculty | Staff | Departments | IT Glossary | Contacts

You are at: HU Home > Computing & Technology >

# Hotbar

Page Index:

**See Also...**

- Spyware/Adware Removal Guide

## What is Hotbar?

According to their web site, Hotbar enhances and personalizes your internet and e-mail applications. Most people use Hotbar to add smiley faces to their e-mail or to add colorful backgrounds to Internet Explorer (aka: "skins"). However, there are a few important facts you should be aware of:

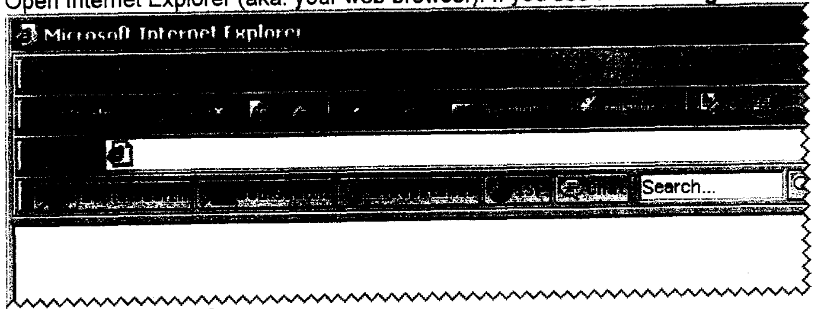
1. **Hotbar is adware/spyware.** It monitors all web sites you visit, collects information about your interests and habits, displays pop-up ads, and provides buttons and advertisements in its toolbar.
2. Hotbar automatically updates itself from their web site without your approval. These updates can include new functionality that can by-pass security/privacy protection programs, and update the way it gathers information about you.
3. Hotbar is **not an official upgrade** from Microsoft for Internet Explorer or Outlook.

## How do I know if I have Hotbar?

There are several ways to tell if Hotbar is installed If any of the following steps show that you have Hotbar, go to the How do I remove Hotbar? section on this page.

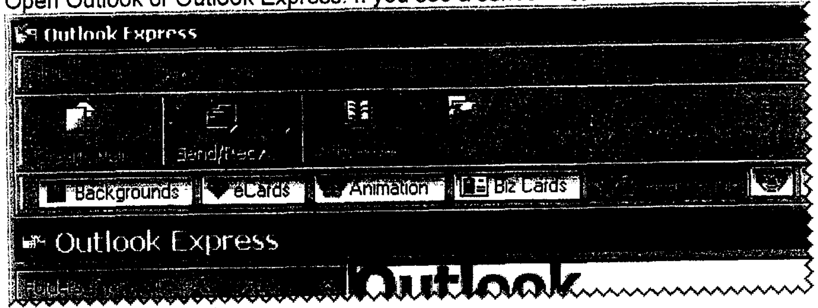
**Note:** If you have changed the "skin" for Hotbar, the buttons may look different. If that is the case, you may want to jump to step 3 to see if Hotbar is installed.

1. Open Internet Explorer (aka: your web browser). If you see a series of **gold buttons**, like in the picture below, you have Hotbar installed.



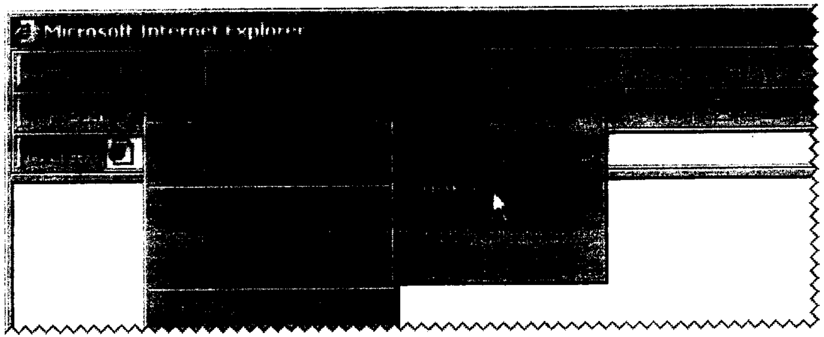
[Click image to zoom in]

2. Open Outlook or Outlook Express. If you see a series of **silver buttons**, like in the picture below, you have Hotbar installed.



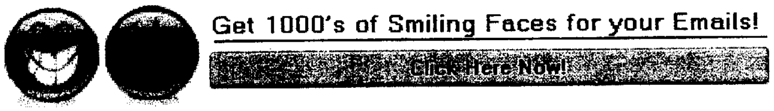
[Click image to zoom in]

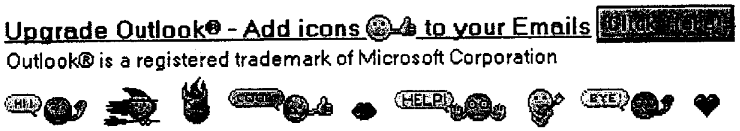
3. Open Internet Explorer. Go to the "View" menu and then click "Toolbars", like you see in the picture below. If you see "Hotbar" in the Toolbars menu, you have Hotbar installed.



[Click image to zoom in]

4. If you send an e-mail to someone, an image similar to one of the following **may** be automatically appended to the bottom. However, if someone sends you an e-mail, and at the bottom there is an image similar to one of the following, then the sender may have Hotbar.




Upgrade Outlook® - Add icons to your Emails
Click Here
Outlook® is a registered trademark of Microsoft Corporation
HI!
COOL
HELP!
BYE

## How do I remove Hotbar?

The following instructions are taken from Hotbar's web site:

**To uninstall Hotbar from your computer please follow these steps:**

1. Click "Start", "Settings" and choose "Control Panel".
2. Choose "Add/Remove Programs".
3. Find "Web Tools by Hotbar".

4. Click the "Add/Remove" button at the bottom right of the window.
5. **Check both browser and email toolbars**
6. Press the "Uninstall" Button.

**If the steps above do not work:**

You can also try using Hotbar's uninstaller which can be downloaded from http://hotbar.com/downloads/HbUninst.exe

After download is complete, locate the file "HBUnInst.exe." on your computer. Double-click this file to start the uninstall process and follow the on-screen instructions.

If the instructions provided by Hotbar do not work, you can try one of the following 3rd party adware/spyware removal tools.

- Ad-Aware
- Spybot

More tools are available at http://www.spychecker.com/topdownloads.html

**Note:** Howard University does not officially support the 3rd party adware/spyware removal tools above. Technical support for the tools will not be provided by the University helpdesks or by the University webmasters.

## Is Hotbar violating your privacy?

Yes. It monitors web sites you visit, forms you fill in, and searches you make on the internet. This can happen even when the toolbar is hidden/disabled.

## Is Hotbar a security risk?

Yes. Hotbar's silent update feature gives the intruding company the ability to add any functionality they wish on your computer at any time, without notification.

### Does Hotbar cause problems with my computer?

Yes. Hotbar slows down your computer and can cause lockups (aka: crashes) when you are using Internet Explorer or Outlook.

---

### What information does Hotbar track/collect?

- Web sites you visit, in what order you visit them, and how often you visit them.
- What you search for on the web using search engines.
- Personally identifiable information such as your full name, postal address, zip code, age or e-mail address.

The information above is taken from the Hotbar privacy policy at http://hotbar.com/site/privacy.htm

---

### Does Hotbar use pop-up ads?

Yes. Hotbar monitors your use of web sites and uses pop-up ads on a regular basis. In many cases, you do not need to be browsing the web for pop-ups to appear.

---

### Doesn't Hotbar have a privacy policy?

Having a privacy policy does not mean Hotbar will respect your privacy to the degree you would hope for. Their license agreement also states that they are free to change their policy or software at any time, without notification.

Policy links:
http://hotbar.com/site/privacy.htm
http://hotbar.com/site/license.htm

---

### Where can I find more information about Hotbar?

- http://www.doxdesk.com/parasite/HotBar.html
- http://www.unf.edu/compserv/articles/spyware-1.html

- http://www.gettysburg.edu/it/itt/itbits/archives/8-04-03.html

---

## Where can I find lists of spyware/adware?

- http://www.spywareguide.com/product_list_full.php
- http://virgolamobile.50megs.com/spyware/spyware.htm
- http://www.cexx.org/adware.htm

---

## About this page:

Information on this page was gathered from the Hotbar policy and terms of use, and from various security/university web sites. Screen captures on this page were created by Howard University web staff.

For questions about installing/uninstalling software, please contact the Helpdesk using the contact information at http://www.howard.edu/technology/.

Comments, corrections, or concerns in regard to this page should be submitted using the webmaster contact form at http://www.howard.edu/webcenter/contact.asp?ref=Hotbar

2301 Georgia Avenue, NW, Suite 334, Washington, DC 20059. Phone: 202-806-2940
Webmaster / Contacts - WWW Disclaimer