Montana State University - Northern
Information Technology Services

ITS Home Page

Inside ITS
Mission, Plans & Projects
Services/Training
How To...
News
Search

How To...

Security:
Spyware & Adware

11 Signs of Spyware | How to Avoid Spyware
What can you do?

Return to Security

Pages in this section:
What you can do
Privacy
>Spyware & Adware
Spam
Spam Filtering @ MSUN

Additional Information
Viruses & Protection
Bandwidth Issues
Password Guidelines
MSU Security Web Site

Many freeware programs (and even some commercial ones) come with and abundance of hidden programs call ***Spyware***. Spyware is software that installs itself without your knowledge, or pretends to be an innoccous "media helper" program. With these programs, the developers collect personal information from you and your computer including websites you go to, and items you buy. They then use that information to send back pop-up ads to your desktop.

In addition to invading your privacy, these programs are also a security risk to your computer. They access the internet to send your data, but hackers can utilize their connections to hack into your computer. These programs are not written with any regard for speed and effiency - they slow down your computer and your network connection.

In one particular example, a feature (B3D projector) installed by default with KaZaA includes in its user license a clause that allows it to legally use your computer to help it's ad network by using your processor and memory to send information to other computers. This significantly slows down your machine and sucks up bandwidth.

Examples of Known Spyware

Flyswat	Hotbar	Webhancer	Comet Cursor	Doubleclick
Gator	eZula	TimeSink	Web3000	Transponder

Spyware installed by KaZaA

Cydoor Commonname B3D projector New.net OnFlow Savenow

11 Signs of Spyware

By Neil J. Rubenking
PC Magazine, March 2, 2004

1. You find a new finger-size hardware device connected between your keyboard cable's plug and the corresponding socket on the back of your computer. Or maybe someone recently offered you "a better keyboard."
2. Your phone bill includes expensive calls to 900 numbers that you never made—probably at an outrageous per-minute rate.
3. You enter a search term in Internet Explorer's address bar and press Enter to start the search. Instead of your usual search site, an unfamiliar site handles the search.
4. Your antispyware program or another protective program stops working correctly. It may warn you that certain necessary support files are missing, but if you restore the files they go missing again. It may appear to launch normally and then spontaneously shut down, or it may simply crash whenever you try to run it.
5. A new item appears in your Favorites list without your putting it there. No matter how many times you delete it, the item always reappears later.
6. Your system runs noticeably slower than it did before. If you're a Windows 2000/XP user, launching the Task Manager and clicking the Processes tab reveals that an unfamiliar process is using nearly 100 percent of available CPU cycles.
7. At a time when you're not doing anything online, the send or receive lights on your dial-up or broadband modem blink just as wildly as when you're downloading a file or surfing the Web. Or the network/modem icon in your system tray flashes rapidly even when you're not using the connection.
8. A search toolbar or other browser toolbar appears even though you didn't request or install it. Your attempts to remove it fail, or it comes back after removal.
9. You get pop-up advertisements when your browser is not running or when your system is not even connected to the Internet, or you

get pop-up ads that address you by name.

10. When you start your browser, the home page has changed to something undesirable. You change it back manually, but before long you find that it has changed back again.
11. And the final sign is: Everything appears to be normal. The most devious spyware doesn't leave traces you'd notice, so scan your system anyway.

How to Avoid Spyware
By Sean Carroll
PC Magazine, March 2, 2004

1. **Make sure to run an antispyware application.** Perform on-demand scans regularly to root out spyware that slips through the cracks. Reboot after removal and rescan to make sure no ticklers, which are designed to reinstall spyware, have resurrected any deleted apps. Additionally, even though we are not overly impressed with any app's real-time blocking abilities, activate whatever your app of choice offers; it's nearly always better than nothing.
2. **Give your antispyware some backup.** In addition to an antispyware app, make sure to run both software and hardware firewalls and antivirus applications to protect yourself against Trojan horses (and viruses, naturally).
3. **Beware of peer-to-peer file-sharing services.** Many of the most popular applications include spyware in their installation procedures. Also, never download any executables via P2P, because you can't be absolutely certain what they are. Actually, it's a good idea to avoid downloading executables from anywhere but vendors or major, well-checked sites.
4. **Watch out for cookies.** While they may not be the worst form of spyware, information gathered via cookies can sometimes be matched with information gathered elsewhere (via Web bugs, for example) to provide surprisingly detailed profiles of you and your browsing habits. PC Magazine's Cookie Cop 2 (www.pcmag.com/utilities) can help you take control of cookies.
5. **Squash bugs.** Web bugs are spies that are activated when you open contaminated HTML e-mail. Get rid of unsolicited e-mail without reading it when you can; **turn off the preview pane** to delete messages without opening them. In Outlook 2003, **Tools** |

Options, click on the **Security** tab and select **Change Automatic Download Settings**. Make sure **Don't download pictures or other content automatically in HTML e-mail** is checked.

6. **Don't install ANYTHING without knowing exactly what it is.** This means reading the end-user license agreement (EULA) carefully, as some EULAs will actually tell you that if you install the app in question, you've also decided to install some spyware with the software. Check independent sources as well, as some EULAs won't tell you about spyware.
7. **Protect yourself against drive-by downloads.** Make sure your browser settings are stringent enough to protect you. In IE, this means your security settings for the Internet Zone should be at least medium. Deny the browser permission to install any ActiveX control you haven't requested.
8. **Keep up to date on the ever-changing world of spyware.** Knowing the threat will help you defeat it. There are several great sites you can visit to keep abreast of this issue. PestPatrol's Research Center (www.pestpatrol.com/pestinfo) has one of the most comprehensive lists of spyware and related threats we've seen. SpywareInfo is another good online source of information. Finally, PC Magazine's Security Scout utility (www.pcmag.com/utilities) aggregates dozens of security-specific news feeds and brings them right to your desktop.

What Can You Do?

Spyware Stoppers - ratings by *PC magazine* (March 2004)
Links to spyware stopper software vendors

ITS@
MSU-Northern
P.O. Box 7751
Havre, MT 59501

Last Update: 30-Dec-2004
Site Index
Feedback

Antivirus - Trend Micro OfficeScan v6.5 Client

posted on 24 Nov 2004

The newer antivirus client will include the detection of spyware and adware. We have received queries that hotbar has been classified as a adware. Note that hotbar monitors your web activites. It captures the web sites that you have visited and tracks your web usage habits. As such, OfficeScan will prompt of such adware.

You are advised to uninstall hotbar. To do so,

1. goto Control Panel
2. click on Add/Remove Programs
3. remove the following programs

Outlook Tools by Hotbar.
Shopper Report by Hotbar.
Web Tools by Hotbar.

More information is available at http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=ADW_HOTBAR.A.

Should you encounter any problem or have any query, kindly contact NUS IT Care at ITCare@nus.edu.sg, or call 6874 2080.

IT Help Desk

Northern Virginia Community College
(703) 426-4141 Option 1
Email: ithelpdesk@nvcc.edu

Search

GO

Student:
- Email Support
- Lan/Web Accounts
- Blackboard Login
- Remote Library Access
- Grades/Schedules
- Computer Purchases
- Nova Connect
- Nova Connect FAQs
- Wireless LAN

Faculty/Staff:
- LAN Accounts
- Email Support
- Web Access
- Mainframe Support
- Nova Connect
- Virus Support
- Wireless LAN
- College Phone System
- NVCC Forms
- Blackboard
- Online Training
- Remote Library Access
- Working Calendar
- FAQs

Technology Policies:
- Home Use of Software
- NVCC/VCCS Policies
- User Account Policy
- About the Help Desk

Computer Slowdown - Spyware Software 4/7/2003

Spyware is becoming an increasing problem throughout the college. Spyware is free software that is downloaded from the Internet, and it can cause numerous problems for your computer, including:

- Dramatic PC slowdown - Spyware slows down your computer because it keeps a log of all of your Internet activity.
- More frequent PC lockups - Your computer will lock up more because the Spyware software drains a lot of your system resources.
- More junk mail - This software results in more junk mail, or spam mail, because companies now have your e-mail address and any other information you have entered into a website.
- More pop-up ads - Spyware programs launch pop-up ad windows from Internet Explorer because the software is programmed to do so.

There are several different Spyware programs that we have noticed in the college, including Hotbar, Date Manager, Precision Time, Gator, Bonzi Buddy and Offer Companion.

Please be aware that just because software that you install is free does not mean it is harmless. Some software may just run in the background, making your computer run slower. Spyware is a little more problematic because it has a legitimate function but a hidden agenda. Not only does it run in the background, but also it keeps track of the all the unsecured web sites you visit and any information you have entered into a website. It then transmits this information back to its server. For example, Hotbar is software that lets users add graphics to e-mail, and it has a nice customizable toolbar in Internet Explorer and Outlook. However, Hotbar records the websites you visit. Although this may seem illegal, it is not because when the software is installed, it states that by installing it you agree to allow their company to gather information about you and websites you visit.

You can check to see if the software you are downloading is Spyware by going to the website www.spychecker.com.

To remove Spyware software yourself, click on "Start" on your start menu, then click on "Settings", and then click on "Control Panel". Click on "Add/Remove Programs" next. You will need to single click on the Spyware component you would like to uninstall and then click on "Add/Remove".

If you have Spyware software installed on your computer please remove it.

You can either call the Help Desk at 703-426-4141 or e-mail them at ithelpdesk@nvcc.edu and request to have it removed.

Last updated on 9/23/04

ithelpdesk@nvcc.edu
(703) 426-4141
Comments to: ithelpdesk@nvcc.edu
NVCC Privacy Statement and Ethics Agreements

Hours of Operation:
Mon-Fri: 8AM to 9PM
Sat: 8AM to 5PM
Annandale, VA 22003

Spyware and Adware Information Policy

Viruses are only one type of malicious or troublesome software that proliferates over the high speed access that is available at CSB/OSB. There are numerous other programs, many of which seem to be helpful or serve some useful purpose that pose serious problems. These web enhancements and freeware are often accompanied by independently installed software that runs unobserved to collect data from you and your computer and transmit it to a third party.

In many cases this hidden software is not intended to be malicious and can be considered the price for the free software that you have downloaded. This software is often referred to as Adware, because it can create pop-up ads or ads within the software that you have installed. Other types are called Spyware, because they run hidden in the background and collect and share information about the websites you visit, email addresses, and other personal data. These sorts of software are objectionable for a variety of reasons, most especially privacy, bandwidth, security, and local performance.

When software is installed that collects data from your computer, you have no control over what data is collected or where it is sent. While most of us might not mind if advertisers collect our Zip Code, it might be considered more serious if they also wanted to know the websites you prefer, your telephone number, the hours that you work, credit card numbers, birth date, passwords, etc. Any data you enter while these programs are running can be collected. These programs can potentially transmit any of the data on your computer or from the areas of the network to which you have access. The distributor of the software has essentially the same rights to and control of your computer that you do.

Your access to the internet and our campus network is a shared resource. There is a physical limit to the amount of data that the network can carry. Programs that keep open data transfers between a local computer and a computer on or off campus degrade the overall performance of the entire network and your specific connection to it.

Because there is no local control over the software installed, frequently no way to remove it without complicated registry edits, no control over the data shared, and no information about what the software is doing, it represents a security threat to everyone on the network. Not only can such software collect data about your computer and your use of it, it can collect information about other users and computers on the

network. It can serve as a point of access for a variety of intrusive actions against the network and other users. Compromised machines can be used to steal or vandalize local machine data and as a platform to attack other computers and networks, including those off-campus.

These programs reside in the background on your computer, consuming a significant proportion of the memory and CPU activity. Every active process on your computer consumes a certain amount of its resources. Adware, spyware, and other web enhancement software deplete the available resources and slow down your computer. The applications interfere with operating system files as well as consuming lots of computer resources. Often these adware applications install a separate component that runs in the background whenever your computer is on. The applications usually remain active even after the associated application has been removed. Spyware applications have been linked to computer problems including system slowdown, Illegal operation errors, and browser crashes. An inordinate amount of network bandwidth and resources is constantly usurped by the software for the transmission of data from your machine to a remote location. The constant flow of data from the advertisers to your machine and vice versa results in decreased bandwidth and internet slowness. This means that the normal software you have to use in the course of your work does not perform at its maximum efficiency. Often the software is poorly written, with no consideration given to compatibility or co-existence with other software, the operating system, or your particular computer hardware. This can lead to frequent crashes, lockups, and failures of your computer.

The following software applications should not to be installed on any CSB/OSB owned workstation:

180Search Assistant	Bullseye	EverAd	IEPlugin	MyDailyHoroscope	Smirk	Xolox
AdDestroyer	CashBack	Expedioware	ILookup	Napster	Soulseek	
Aimster	Comet Cursor	EzUla	Imesh	Ncase	Spinner	
Alexa	Cydoor	Filetopia	Internet Optimizer	Netpal Games	TimeSink	
Audio Galaxy	Direct Connect	Flyswat	IWon	Netscape Radio	Transponder	
Aureate	Doubleclick	Freenet	Kazaa	OneMX	Virtual Bouncer	
Bad Blue	DSSAgent	Gator	Kazaa Media Desktop	OnFlow	Weather Bug	

Bearshare	Earth Station 5	Gnotella	Keenvalue	Phex	Web 3000
BitTorrent	Edonkey	Gnucleus	Limewire	Qtella	Web Shots
BlazeFind	Edonkey 2000	Gratisware	Mactella	Shareaza	Webhancer
Blubster	Emule	Grokster	Madster	ShopAtHome	WebRebates
Bonzi Buddy	E-Mule	HotBar	Morpheus	Slyck	WinMX

This list is subject to change.

New programs of this nature are being created continuously. If you are unsure whether you should install a new program or if you need assistance removing spyware and adware software, please contact the **Help Desk** or 2228. Please note that in some instances spyware and adware programs may not be easily removed from the workstation and a reimage of the workstation would be necessary.

For information on spyware on your personal computer, see **Spyware Removal**.

Spyware and Adware

What is spyware?

"Also known as 'adware,' this hidden software program transmits user information via the Internet to advertisers in exchange for free downloaded software." ZDNet

So what is the downside? Advertising companies may also install additional tracking software on you computer which continuously talks to their servers. This obviously can use your bandwidth, and frequently causes instability on your system resulting in multiple "blue screens." So you want to remove this free application using Windows to Add/Remove it from your desktop? The spyware will remain on your computer, often buried within the Windows System Registry.

OIT maintains a list of spyware and adware programs that have crossed to eating bandwidth, causing lots of desktop problems or being very intrusive of your privacy. The list is below and we recommend that you not allow any of these programs on your computer. Its difficult to stay current, so check out Counterexploitation for the latest programs.

- AudioGalaxy Satellite installs aureate, DoubleClick, Bonzi Buddy, WebCelerator, Hotbar, Gator and OfferCompanion
- Beare Share installs new.net, SaveNow, Bonzi Buddy icon, and n-Case
- Claria (formerly known as Gator)
- Global DiVX Player installs SaveNow
- Grokster installs Gator, OfferCompanion and SaveNow
- iMesh installs Gator, OfferCompanion, SaveNow, New.net, Hotbar and Bonzi Buddy
- KaZaA Media Desktop installs software from Brilliant Digital Entertainment that it plans to use to create its own hidden P2P network. It also installs New.net, SaveNow, Cydoor, Common Name Toolbar and B3D
- Limewire

FSPs
Work Securely
Top priorities
Prepare to recover
Backup
Patching
Desktop security for:
Macintosh
Unix/Linux
Windows

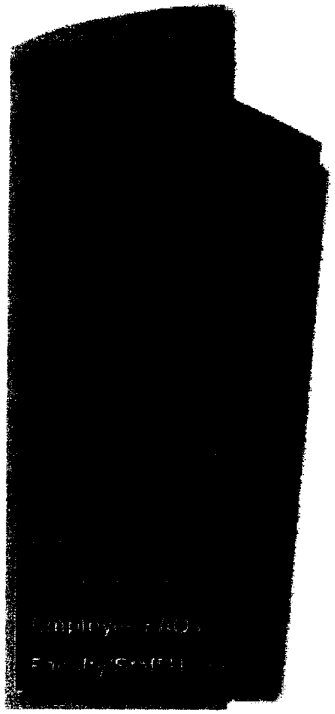
Tools
Anti-Virus
Privacy
SpyWare
Security Templates
SANS Sec Guides

Security Library
Links and documents

- Morpheus
- Radlight 3.0 a multimedia player will delete Adaware upon install
- Webhancer
- Xupiter

Tools for identification and removal

- Ad-aware... free utility
- Spybot Search & Destroy
- SpyChecker ... a database of spyware and the programs they are downloaded with.
- WebWasher ... free utility for Windows and Macs, uses proxy to block cookies, etc. Not for the feint of heart, when this is installed or uninstalled incorrectly it can totally block TCP/IP.



INTERNET SECURITY (Safe Use of the Internet)

Privacy Rights | Identity Theft | Spam | Spyware | "Hotbar" and Other Spyware

Privacy Rights

http://www.privacyrights.org/
The Privacy Rights Clearinghouse is a nonprofit consumer education, research, and advocacy program. Our publications empower you to take action to control your personal information by providing practical tips on privacy protection.

Identity Theft

http://www.consumer.gov/idtheft/index.html
Welcome to the U.S. government's central website for information about identity theft. This site is maintained by the Federal Trade Commission. Please continue to visit this site often and share the information with your family, friends and colleagues. More information will be added to the site regularly, including government reports and Congressional testimony, law enforcement updates, and links to other sites with helpful information about identity theft.

Spam

http://songseek.com/spamorg/index.htm
Spam.org Info about reducing spam, or junk e-mail on the internet. Our goal is the dispersal of accurate and useful information. The special project underway at this time is a comparison of spam filters, the page is a work in progress.

http://www.uakron.edu/vpcio/opsys/spamfaq.php
The University of Akron FAQ on spam (unsolicited bulk email)

Spyware

http://spybot.safer-networking.de/
Spybot - Search & Destroy can detect and remove spyware of different kinds from your

computer. Spyware is a relatively new kind of threat that common anti-virus applications do not yet cover. If you see new toolbars in your Internet Explorer that you didn't intentionally install, if your browser crashes, or if you browser start page has changed without your knowing, you most probably have spyware. But even if you don't see anything, you may be infected, because more and more spyware is emerging that is silently tracking your surfing behaviour to create a marketing profile of you that will be sold to advertisement companies. Spybot-S&D is free, so there's no harm in trying to see if something snooped into your computer, too :)

http://www.lavasoft.nu/
Get Rid of Spyware now. Ad-aware is a free multi spyware removal utility designed for all Win9x / ME / NT40 / W2000 platforms It scans your system for components of known spyware parasites and lets you remove them safely.

"Hotbar" and Other Spyware

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.

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 your computer or cause lockups when you are using your web browser or email.

Hotbar also tracks information entered into web forms, which may include names, addresses, passwords, credit card numbers, phone numbers, social security numbers, or any other text strings which a user might type into a web form. Although the hotbar end user license agreement states that they intend to respect your privacy, it also states that they are free to change the licensing terms at will. Additionally, computers with hotbar installed will automatically download and install the latest program updates without notification or user intervention. Please take a look at the pages below:

http://www.ouhsc.edu/it/security/security-rules.asp
http://www.ecu.edu/itcs/cas/newsletter/st2002-NOV.htm
http://www.usq.edu.au/its/newstaff/Hotbar.htm

http://www.doxdesk.com/parasite/HotBar.html
http://www.cexx.org/adware.htm

This last link makes for some good reading. It is at the zdnet download site and features the opinions/reviews of people who have installed hotbar. Apparently it has caused some real headaches for people working in the computer support field.

http://downloads-zdnet.com.com/3302-2366-10156187.html

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

Wayne College 1-800-221-8308 or 330-683-2010

1901 Smucker Road, Orrville, OH 44667 • FAX (330) 684-8989
The University of Akron is an Equal Education and Employment Institution
This page is maintained by WayneWebEditor@uakron.edu

ABOUT ITS

ITS Home
Contact Info
Mission
News
Other Tech Info Links
Policies/Procedures

QUICK LINKS TO

Blackboard
Classroom AudioVisual
Computer Accounts
Hardware/Software
Dial In Access
E-Mail
Self Service Forms
ITS Support Center-Tech Support
Internal Docs (restricted)
Manuals/Handouts
Osprey ID
Passwords
PIN Guidelines
Security
Statistics/ Maintenance Hours

SPYWARE

Hotbar

What is it?

Marketed as a program to add graphical skins to IE toolbars, it also adds its own toolbar. It monitors all URLs you visit to add link buttons to its toolbar dependent on the site.

It will also add toolbars to Microsoft Outlook and provide the ability to add graphics and animations to e-mails sent within Outlook which could cause severe problems and security risks.

How could I have gotten it on my compuer?

Bundled with older releases of iMesh and other free software; more recently, advertised through junk e-mail purporting to be a Microsoft upgrade to Outlook.

What can it do to my computer?

Will it put annoying advertisements on my computer?

Yes. If HotBar's toolbar is not removed (form View/Toolbars), it will add buttons on the left-hand side leading to advertisers' sites, often competitors of the site you are on.

Could it violate my privacy?

Yes. HotBar spies on sites visited and forms filled in, even when its toolbar is disabled.

Are there any security risks in using Hotbar?

Yes. Hotbar has a silent-update feature which will connect automatically to different sites.

Could it cause my computer to crash?

Absolutely. The program uses extra computing resources that may be needed to perform day to

Telephone Support
Web Publishing
Wireless

day operations.

This product also increases the size of each e-mail that you send. This will cause you to exceed your quota at a much faster rate.

Gator

What is it?

Gator is a software product that can automatically fill in passwords and other form-elements on Web pages. But its main purpose is to load an advertising spyware module called OfferCompanion, which displays pop-up ads when visiting some Web sites. Gator boasts that since it's software is always running, it can spam users with "Special Offers" and other ads anywhere they go--even competitors' sites--with remarkable targeting capabilities, since it can spy on what sites the user is visiting.

There are some variants to this software:
Gator/A covers all versions of Gator before it became 'GAIN'. These old variants have not been researched, so the removal instructions here may not work for them.

Gator/GAIN includes versions (3.1.x-4.0.x) of the current system, an independent adware network.

Gator/Trickler is an installer program which fetches Gator/GAIN gradually, using only a small part of the bandwidth available.

Gator/PDP is an ActiveX control used to install Gator.com applications which bundle Gator/Trickler. When Gator itself has started loading, the installer control is removed.

How could I have gotten it on my compuer?

The Gator/A variant was distributed as part of 'Gator eWallet', an application used to fill in web forms. eWallet is now a separate program.

Gator/Trickler (and hence Gator/GAIN) is now distributed with all Gator.com applications, including eWallet and Precision Time/Date Manager. It is also widely bundled with third-party software, particularly peer-to-peer file-sharing programs.

Gator/PDP is included as a drive-by download on web pages, particularly hidden pop-ups.

What can it do to my computer?

Will it put annoying advertisements on my computer?

Yes. Pop-up windows (both Internet Explorer windows and Gator's own non-browser windows) appear periodically while IE is in use.

Could it violate my privacy?

Yes. Every time a new site is visited, the address of the site (though not the full URL) is reported to Gator's servers, with a unique user ID which can be used to track your web usage.

Are there any security risks in using Hotbar?

Yes. Gator/GAIN can download and execute arbitrary code from its controlling server (as an update feature).

Gator/PDP, the installer control, can be directed by any web page to install code from Gator's servers.

Gator/PDP/3061, an early version of the installer control, has a critical security flaw: it allows any web page to download and execute code from anywhere, with no security checks.

Could it cause my computer to crash?

At the moment it just seems to crash your internet browser.

Xupiter

What is it?

Xupiter consists of an Internet Explorer toolbar containing link buttons to one of Xupiter's search engines and a task run at Windows startup which downloads updates to the software and may launch pop-ups. It also contains functionality to hijack your home page and address bar searches, and add Xupiter links to your bookmarks.

How could I have gotten it on my compuer?

Installed by ActiveX drive-by-download in affiliate pages. Known sources include the site www.freewebupgrades.com (which is advertised by junk e-mail) and pop-up adverts on sites such as FortuneCity.

More recently also bundled with Grokster.

One of Xupiter/Sqwire's ActiveX drive-by-download pages has been advertised by junk e-mail (spam) offering a 'Free Christian Toolbar'.

What can it do to my computer?

Will it put annoying advertisements on my computer?

Yes. Apart from the hijacking and added links, the software periodically opens pop-under advertisements as directed by its controlling servers. (These may appear in windows with only an 'exit' menu.)

Could it violate my privacy?

The privacy policy states that the software may track all web usage. However this behaviour has not been observed.

Are there any security risks in using Hotbar?

Yes. The software contacts its servers to ask for update code, which is executed without checks. It has also been known to download third-party software (for instance a casino loader app).

Could it cause my computer to crash?

In the initial variants, the update-checking task tries to connect to xupiter.com to download updates whether or not you are connected. If it fails it may cause a crash in 'RunDownload.exe'. Some versions of Xupiter can cause the Windows Explorer to crash when opened under Windows XP.

Useful links:

(some information from the following pages are included on this site)

http://www.cexx.org/adware.htm
http://www.doxdesk.com/parasite/
http://www.spychecker.com

ResNet @ Wellesley College

ResNet News and Alerts:

05-18-2005: Seniors: Urgent Technology Tips
02-08-2005: Second semester brings new software and more!
12-20-2004: Home For The Holidays!

Getting Help
Computing Help Forms
Computing First Aid

Incoming Students
Guide to Evaluating IT
Student Computing FAQ
Purchasing a Computer
Computer Purchase Program
Windows XP (Pro Vs. Home)

Hot Topics
ResNet News and Alerts
ResHall Computer Rooms
Wireless at Wellesley

Documentation and Troubleshooting
Getting Connected
Using Your Computer
Peer-To-Peer Etiquette
Domain Accounts
Tips and Tricks

Helpful Links
Virus Protection
Spyware Protection
Computer Security
FirstClass
Information Services Training
ElementK

iMesh (Version 3.1 build 130 for Windows)

Using iMesh Wisely

Note: *Because iMesh automatically installs a large number of "Adware" and "Spyware" applications, and because it is not possible to completely disable iMesh's server function, Information Services strongly recommends against using iMesh.*

To restrict iMesh's server function, limit simultaneous downloads to one, and prevent iMesh from launching automatically at startup:

1. Launch iMesh.
2. From the **Preferences** menu, choose **Options**.
3. Under *Category*, choose **General**.
4. Uncheck **Launch on startup**.
5. Under *Category*, choose **Traffic**.
6. Set *Maximum concurrent downloads* to **1**.
7. Under *Upload*, set *Maximum concurrent uploads* to **1**. Set *Maximum bandwidth (in KB/s)* to **24**.
8. Click **OK**.
9. Under *iMesh Windows*, click **Media Manager**.
10. In the list of folders on your computer, click each "+" mark to list all subfolders. Scroll through the list and remove all check marks to un-share all shared folders.

Please exit iMesh whenever you are not actively using it. To exit, from the **File** menu choose **Exit**.

Removing Adware and Spyware

iMesh automatically installs a number of applications which monitor your Internet usage and display advertisements. These may include GAIN, Cydoor, Hotbar, eZula TopText, New.net, CommonName, SideStep, NetPal, FavoriteMan, VX2, FlashTrack, BonziBuddy, Defender, FirstLook Portal, eAnthology, and other adware and spyware applications. Uninstalling iMesh does not automatically remove these applications.

To uninstall some of these programs:

1. Double-click on the **My Computer** icon on your desktop.
   *Note: If you are running Windows XP and the My Computer icon does not appear on your desktop, choose **My Computer** from the Start menu.*
2. Double-click on **Control Panel**.
3. Double-click on **Add/Remove Programs**.
4. Remove each of the following items by selecting its name, then clicking **Add/Remove** and following the instructions on your screen:
   - CommonName
   - FirstLook Portal
   - FT remove
   - Hotbar - Email and Browser enhancer
   - SideStep
     *Note: When you are asked whether you want to keep SideStep available, click **No**.*
   - Top Text iLookup
   - eAnthology
   - New.net Domains 4.50
5. Close all open windows.
6. Double-click on the **My Computer** icon on your desktop.
   *Note: If you are running Windows XP and the My Computer icon does not appear on your desktop, choose **My Computer** from the Start menu.*
7. Double-click on the icon for your hard drive.
8. Open the **Program Files** folder.
9. Delete the following folders:
   - CommonName
   - FirstLook
   - NewDotNet

Certain components of these programs may remain after uninstallation. You should run a spyware removal tool such as Ad-aware to remove any remaining components of these and any other advertising or monitoring programs installed by iMesh.

Uninstalling iMesh

1. Double-click on the **My Computer** icon on your desktop.
   *Note: If you are running Windows XP and the My Computer icon does not appear on your desktop, choose **My Computer** from the Start menu.*
2. Double-click on **Control Panel**.
3. Double-click on **Add/Remove Programs**.
4. Select **iMesh**. Click **Add/Remove**.
5. Follow the instructions on your screen to remove iMesh.
6. Close all open windows.

7. Double-click on the **My Computer** icon on your desktop.
   *Note: If you are running Windows XP and the My Computer icon does not appear on your desktop, choose **My Computer** from the Start menu.*
8. Double-click on the icon for your hard drive.
9. Open the **Program Files** folder.
10. Right-click on the **iMesh** folder. From the menu which appears, choose **Delete**.
11. When you are asked If you are sure you want to remove the folder, click **Yes**.
12. Double-click on the **My Computer** icon on your desktop.
    *Note: If you are running Windows XP and the My Computer icon does not appear on your desktop, choose **My Computer** from the Start menu.*
13. Double-click on **Control Panel**.
14. Double-click on **Add/Remove Programs**.
15. In the Add/Remove Programs Properties window, select **iMesh Ads-support**. Click **Add/Remove**.
16. Follow the instructions on your screen to remove advertising support for iMesh.

After uninstalling , you should remove any adware or spyware installed with iMesh.

Matt Shelton
ResNet Manager
Information Services
Last modified: June 1, 2005
Expires: August 31, 2005

[redacted]

WINONA STATE UNIVERSITY

HOTBAR

Hotbar is a program that is used to enhance and personalize 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:

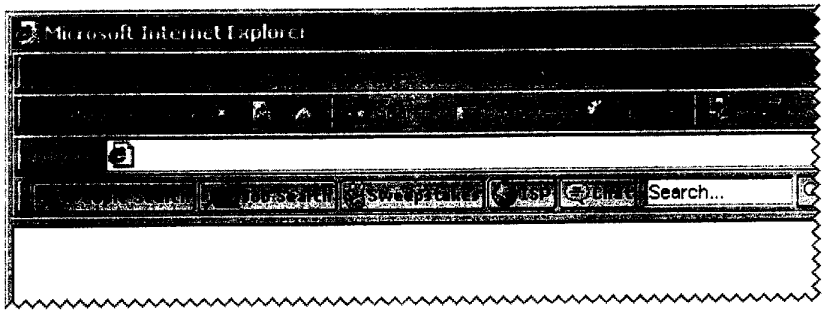
1. **Hotbar is considered spyware**. It monitors all web sites you visit to add link buttons to its' toolbar dependant on the websites you visit and will display pop-up ads. It spreads itself through email as an advertisement to coax your friends, family, and co-workers to install it as well.
2. **Hotbar is a security violation**. 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.
3. Hotbar is **not an official upgrade from Microsoft** for Internet Explorer or Outlook.
4. Hotbar **slows down your computer** and can cause lockups when you are using Internet Explorer or Outlook.

How to Tell if Hotbar is Installed?

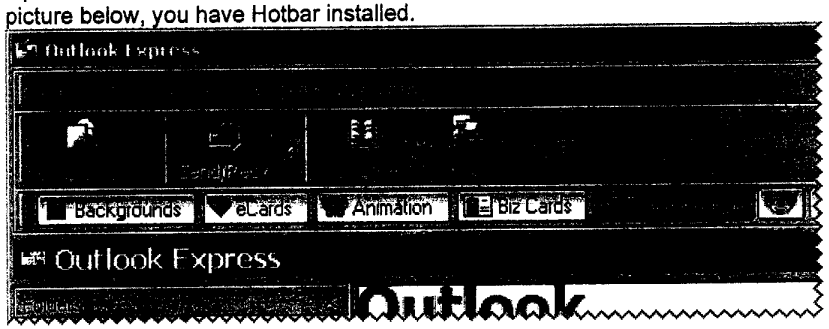
If any of the following steps show that you have Hotbar, see the section below on how to remove Hotbar.

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.

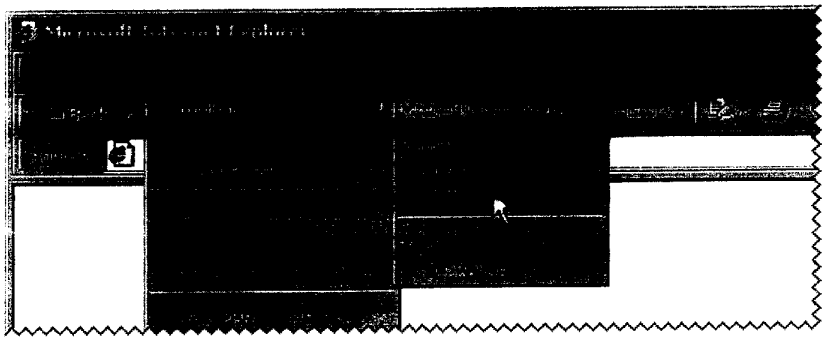
1. Open Internet Explorer (aka: your web browser). If you see a series of gold buttons, like in the picture below, you have Hotbar installed.



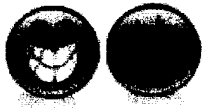
2. Open Outlook or Outlook Express. If you see a series of silver buttons, like in the picture below, you have Hotbar installed.



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.



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.



Get 1000's of Smiling Faces for your Emails!

Click Here Now!

Upgrade Outlook® - Add icons to your Emails Click Here!!!

Outlook® is a registered trademark of Microsoft Corporation

Remove Hotbar from your system:

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 above steps do not work:

You can also try using Hobar'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

---

Additional links:

- 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

Spyware/Adaware lists:

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