EXHIBIT A

symantec.

security response

united states

- global sites
- products and services
- purchase
- support
- security response
- downloads
- about symantec
- search
- feedback

security risks

Symantec AntiVirus products allow users to protect themselves from a variety of potential software and Internet risks. These include malicious code such as viruses and Trojans, as well as security risks, which include Spyware, Adware, and Dialers.

Symantec classifies potential risks based on a number of characteristics. Once categorized, they can be detected by our products, and users can choose whether to keep or remove them based on their personal needs.

General Criteria for Security Risks >>

Security Risk Dispute Submission
Symantec provides a submission form for disputing Security Risk classifications and detections.
More Info

Adware
Programs that facilitate delivery of advertising content to the user through their own window, or by utilizing another program's interface. In some cases, these programs may gather information from the user's computer, including information related to Internet browser usage or other computing habits, and relay this information back to a remote computer or other location in cyber-space.

Adware can be downloaded from Web sites (typically in shareware or freeware), email messages, and instant messengers. Additionally, a user may unknowingly receive and/or trigger adware by accepting an End User License Agreement from a software program linked to the adware or from visiting a website that downloads the adware with or without an End User License Agreement.
More info

Dialers
Programs that use a computer or modem to dial out to a toll number or internet site, typically to accrue charges. Dialers can be installed with or without a user's explicit knowledge, and may perform their dialing activity without a user's specific consent prior to dialing. More info

Hack Tools
Tools that can be used by a hacker or unauthorized user to attack, gain unwelcome access to or perform identification or fingerprinting of your computer. While some hack tools may also be valid for legitimate purposes, their ability to facilitate unwanted access makes them a risk. Hack tools also generally:

- Attempt to gain information on or access hosts surreptitiously, utilizing methods that circumvent or bypass obvious security mechanisms inherent to the system it is installed on, and/or
- Facilitate an attempt at disabling a target computer, preventing its normal use

One example of a hack tool is a keystroke logger -- a program that tracks and records individual keystrokes and can send this information back to the hacker. Also applies to programs that facilitate attacks on third-party computers as part of a direct or distributed denial-of-service
More info

Joke Programs
Programs that alter or interrupt the normal behavior of your computer, creating a general distraction or nuisance. Joke programs generally do not themselves engage in the practice of gathering or distributing information from the user's computer. More info

Remote Access
Programs that allow one computer to access another computer (or facilitate such access) without explicit authorization when an access attempt is made. Once access is gained, usually over the Internet or by direct dial access, the remote access program can attack or alter the other computer. It may also have the ability to gather personal information, or infect or delete files. They may also create the risk that third party programs can exploit its presence to obtain access. Such remote access programs generally:

- Attempt to remain unnoticed, either by actively hiding or simply not making their presence on a system known to the user, and/or
- Attempt to hide any evidence of their being accessed remotely over a network or Internet

Means by which these programs provide access may include notifying a remote host of the machine by sending its address or location, or employing functionality that wholly or partially automates access to the computer on which the program is installed. More info

Spyware
Programs that have the ability to scan systems or monitor activity and relay information to other computers or locations in cyber-space. Among the information that may be actively or passively gathered and disseminated by Spyware: passwords, log-in details, account numbers, personal information, individual files or other personal documents. Spyware may also gather and distribute information related to the user's computer, applications running on the computer, Internet browser usage or other computing habits.

Spyware frequently attempts to remain unnoticed, either by actively hiding or by simply not making its presence on a system known to the user. Spyware can be downloaded from Web sites (typically in shareware or freeware), email messages, and instant messengers. Additionally, a user may unknowingly receive and/or trigger spyware by accepting an End User License Agreement from a software program linked to the spyware or from visiting a website that downloads the spyware with or without an End User License Agreement. More info

Viruses, Worms and Trojan Horses
A virus is a program or code that replicates itself onto other files with which it comes in contact; that is, a virus can infect another program, boot sector, partition sector, or a document that supports macros, by inserting itself or attaching itself to that medium. Most viruses only replicate, though many can do damage to a computer system or a user's data as well. More info

A worm is a program that makes and facilitates the distribution of copies of itself; for example, from one disk drive to another, or by copying itself using email or another transport mechanism. The worm may do damage and compromise the security of the computer. It may arrive via exploitation of a system vulnerability or by clicking on an infected e-mail. More info

A Trojan Horse portrays itself as something other than what it is at the point of execution. While it may advertise its activity after launching, this information is not apparent to the user beforehand. A Trojan Horse neither replicates nor copies itself, but causes damage or compromises the security of the computer. A Trojan Horse must be sent by someone or carried by another program and may arrive in the form of a joke program or software of some sort. The malicious functionality of a Trojan Horse may be anything undesirable for a computer user, including data destruction or compromising a system by providing a means for another computer to gain access, thus bypassing normal access controls. More info

Other
Risks that do not meet the definitions of Viruses, Trojan horses, Worms, or other security risk categories, but which may present a risk to a computer and its data, an unwanted nuisance to the user, or exhibit other unexpected or unwanted results when the risk is present and functioning. This category includes programs that encrypt or otherwise attempt to obfuscate some of their

functionality, making it difficult to determine whether they fall into one of the other categories. More info

EXHIBIT B

searchSMB.com Definitions - powered by whatis.com

adware

1) Generically, adware (spelled all lower case) 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.

Adware has been criticized because it usually includes code that tracks a user's personal information and passes it on to third parties, without the user's authorization or knowledge. This practice has been dubbed spyware and has prompted an outcry from computer security and privacy advocates, including the Electronic Privacy Information Center.

Noted privacy software expert Steve Gibson of Gibson Research explains: "Spyware is any software (that) employs a user's Internet connection in the background (the so-called 'backchannel') without their knowledge or explicit permission. Silent background use of an Internet 'backchannel' connection must be preceded by a complete and truthful disclosure of proposed backchannel usage, followed by the receipt of explicit, informed consent for such use. Any software communicating across the Internet absent of these elements is guilty of information theft and is properly and rightfully termed: Spyware."

A number of software applications, including Ad-Aware and OptOut (by Gibson's company), are available as freeware to help computer users search for and remove suspected spyware programs.

2) AdWare is also a registered trademark that belongs to AdWare Systems, Inc. AdWare Systems builds accounting and media buying systems for the advertising industry and has no connection to pop-up advertising, spyware, or other invasive forms of online advertising.

>> Find white papers, products and vendors related to adware.

Read more about it:

>> Counterexploitation provides a detailed explanation of "advertising spyware" and related security issues.
>> SearchSecurity.com contains links to numerous articles and commentaries explaining how spyware and adware work.

SMB RELATED LINKS

Ads by Google

Which Spyware Remover?
5 Side-by-side Comparisons of Top Spyware Virus Removers. Free Scans.
CompareSpywareRemovers.com

Spyware Remover Download
Free Scan, awarded Spyware and Adware killer - 5 Stars Rated.
www.pctools.com

Free Adware/Spyware Scan
Search and Remove Trojans, Spyware, Adware and other Intruders. aff
www.Anti-Adware.net

Free Spyware/Adware Scan
Detect and Remove Spyware & Adware from your PC. Recommended by Users!

WHAT'S NEW
on searchSMB

1. FAQs on Spyware and Malware
2. Spyware theme month for SMBs
3. The Trouble with Next-Gen IT Leaders
4. Bakery samples ERP flavors

Join our community

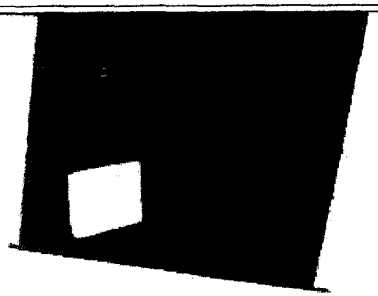
Last updated on: Jul 09, 2004

<< **Back to previous page** **Go to whatis.com home page** >>

EXHIBIT C

OIT Help Desk

Fighting Malware



Protecting your computer from Spyware, Adware and Viruses

Malware (short for **mal**icious software) is a term coined to describe programs which are ultimately detrimental to the computing experience. Viruses are the most visible and publicized malware but there are other types, specifically adware and spyware, which are less obviously a threat but perhaps even more of a nuisance. This page will describe the various types of malware and what steps should be taken to remove them or, if possible, prevent their installation.

Viruses and Worms
A virus is a computer program designed to install itself on a computer without the user's knowledge and then perform some task. Most commonly viruses will try to infect other machines, open up the infected machine to outside access or cause damage to files. A worm typically is installed when a user launches an infected e-mail attachment. The worm then uses the mail system (and address books) of the infected computer to send infected e-mails to other users.

This type of malware is very high-profile with several companies such as Network Associates (McAfee) and Symantec (Norton) actively working to combat it. Using a virus-scan product and keeping current with Windows Updates are the best methods available to prevent infections. Users should also be wary of unexpected e-mail attachments, even if they come from someone they know.

More information on viruses and methods of prevention can be found at the OIT Virus and Security Alerts website.

Adware and Spyware
Adware is software which is free to the user or available at a reduced cost because it displays advertisements either in the software window itself or in separate pop-up windows. By itself adware is merely irritating as the user must contend with unwanted pop-up windows while running the ad-supported software.

Spyware is any software which utilizes the bandwidth of the machine on which it is installed to communicate with the parent company. Statistics about one's browsing habits, installed software and other information

ISU COMMUNITY

PROSPECTIVE STUDENTS

ALUMNI & FRIENDS

PARENTS & FAMILY

BUSINESS & COMMUNITY

ISU A-Z

MyISU

SEARCH

are collected by these companies and then either sold as market research or used by the company itself to target ads at the user.

Together (often a program works as both adware and spyware) they represent a serious invasion of the user's privacy and could use up considerable bandwidth and processor resources communicating with the developer and downloading ad content

It is often difficult to identify this software without a thorough reading of the end user license agreement. Companies which distribute this software use many tricks to entice users to install their programs. Two common channels by which malware is installed are pop-ups which look like a security warning and opt-out installers. Users should familiarize themselves with these methods and use discretion when agreeing to anything on the web.

Spoofed Security Warnings – Some malware installation requests are designed to look like a typical security request from the browser. The tendency is for people to accept anything that pops up which they feel is restricting them from viewing a particular page. When a user clicks yes, thinking they are accepting a security certificate, they actually are giving permission to install whatever software the distributor wishes to push to their computer. To prevent these installations one only has to read carefully any requests that pop-up while browsing and make sure they are indeed required. If you are unsure, answer no and then if you have problems with that particular web page, go back and answer yes when the request appears.

Opt-out Installers – Some web-sites which require a user registration include opt-out installers for various pieces of adware and spyware. An opt-out installer is one such that if you do not explicitly decline whatever software they are offering, it will be installed by default once you complete your registration for the site. The tools to decline the installation are often deliberately inconspicuous and typically the installation happens without the user's knowledge. Opt-out installers are also seen quite often in the installation packages for "free" software such as screen-savers, download managers, games, shopping assistants and web accelerators.

Prevention/Removal

Users are not often aware that their machine is host to malware until it begins to affect performance. Excessive pop-ups or slow network access may be the only indication that the computer has been "infected".

As the old saw goes, an ounce of prevention is worth a pound of cure. Users should take the following steps to be sure their machines are as secure as possible:
- Keep Windows up to date – Use the Windows Update feature of your operating system to be sure you have all of the most recent security and functionality updates.
- Keep anti-virus software current – Users should be running an anti-virus package such as McAfee VirusScan which continually scans the computer for viruses and other threats. It is vital that the virus information be kept up to date; otherwise its effectiveness will be greatly diminished.
- Install and configure a firewall – Install a personal firewall product such as ZoneAlarm or enable Internet Connection Firewall under Windows XP to monitor and block internet traffic.

For the removal of spyware, OIT recommends and uses a program

called SpyBot Search and Destroy. Freely available from http://security.kolla.de, users may install and run this software which scans their machine for known spyware, adware and tracking information. It works similarly to a virus scanner and will recognize and eliminate the vast majority of spyware programs.

Other Resources

New malware threats appear almost daily so it is important that users take the time to become familiar with the information and tools which are available to combat the problem. Below is a list of links to many resources related to the problem of malware.

http://simplythebest.net/info/spyware.html
Here you will find a more thorough definition of spyware and adware as well as links to many other resources for dealing with this problem.

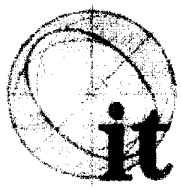
http://www.nai.com
The official website for McAfee VirusScan carries alerts about current threats, a virus information library and many other tools and articles which will assist one in fighting viruses.

Please see the Common Malware Programs page for a partial list of software which is known to include spyware elements. A comprehensive list would not be possible to produce as new spyware is produced almost daily. Users should view this list as a warning of the prevalence of this problem and take steps to keep their machines free from this latest threat to privacy and productivity.

Last modified: 04-Nov-04 Maintained by: IT-Help@indstate.edu

200 North Seventh Street, Terre Haute, Indiana, USA 47809-9989

EXHIBIT D



Princeton University

Office of
Information Technology

Search the KnowledgeBase

New Solutions
OIT Services A-Z
FAQs
Headlines
Outage History
KnowledgeBase
Business App Help

Performance Stats
Online Forms
Video Series
Contact Us
About Us
OIT Home

From the KNOWLEDGE BASE

Title: What is Spyware/Adware? How do I safeguard myself against Spyware?

Synopsis:
What is Spyware/Adware? How do I safeguard myself against Spyware?

Solution:
Spyware is the generic term for computer software that gathers information about you and your Internet surfing habits for marketing purposes; Adware refers to programs which gather information about you for marketing purposes in order to target your computer with advertisements (often in the form of pop-up windows.) These programs are often difficult to uninstall through traditional un-installation programs and will interfere with the normal performance of your computer's software and/or networking protocol.

Fortunately, there are many options for prevention and the safe removal of Spyware/Adware from your computer.

Preventing Spyware / Adware
Choose programs carefully. Often free or trial programs downloaded from the Internet contain spyware/adware to fund the creators of the programs. The most common Spyware/Adware programs are installed with peer-to-peer sharing software such as Kazaa, Bearshare, and Limewire. Reading the license agreement and "Read Me" files of these programs will often indicate the installation of additional programs. Protect yourself by knowing your

options. Some programs will allow you to customize the installation, whereas others such as Kazaa's latest version cannot be installed without Spyware/Adware.

Protect yourself by knowing that there are other dangers for users of these programs; particularly for those who do not understand how the software is structured to operate or for those who are not careful to share only files they own legally. Please see: Copyrighted music, film, video files: Are they illegal to have on my computer?

Do not click on unfamiliar links in pop-up windows. Spyware/Adware creators will disguise links in their pop-up windows. The safest way to close a pop-up windows is to right-click on it in your taskbar and choose **Close** or select the active window and use **Alt + F4** on your keyboard.

Removing SpyWare / Adware
Many Spyware/Adware removal programs are free to download and use. The Solution Center has found success with a free program called Spybot available from http://www.safer-networking.org as well as Microsoft's AntiSpyWare. OIT advises that novice users request technical assistance when installing and using these programs. See "Obtaining Technical Assistance" below. Should you choose to use Spybot without assistance, read the directions online which remind you to back up your registry first, and then update the Spybot definition files before scanning your hard drive.

Obtaining Technical Assistance

Call the OIT Help Desk at 8-HELP (4357 press option #1) for more information

1. Contact an RCC for assistance - Available to students only

2. Contact SCAD or DCS Staff - Available to staff and faculty only

3. Visit the OIT Solution Center - Available to all University affiliates

Last Updated: February 2, 2005

Solution ID: 9538

EXHIBIT E

Adware

From Wikipedia, the free encyclopedia.

Adware or **advertising-supported software** is any software application in which advertisements are displayed while the program is running. These applications include additional code that displays the ads in pop-up windows or through a bar that appears on a computer screen. The Opera web browser is a popular example. Adware helps recover programming development costs, and helps to hold down the price of the application for the user (even making it free of charge)—and, of course, it can give programmers a profit, which helps to motivate them to write, maintain, and upgrade valuable software.

Some adware is also shareware, as such it may be used as term of distinction used to differentiate between types of shareware software. What differentiates adware from other shareware is that it is primarily advertising supported. Users may also be given the option to pay for a "registered" or "licensed" copy, which typically does away with the advertisements. Other types of shareware include demoware, nagware, crippleware, freeware, loyaltyware, and even spyware.

Some adware programs have been criticized for occasionally including code that tracks a user's personal information and passes it on to third parties, without the user's authorization or knowledge. This practice has been dubbed spyware and has prompted an outcry from computer security and privacy advocates, including the Electronic Privacy Information Center [1] (*http://www.epic.org*). Other adware programs do not track a user's personal information. Often, spyware applications send the user's browsing habits to an adserving company, which then targets adverts at the user based on their interests. Kazaa and eXeem are popular programs which incorporate software of this type.

A number of software applications are available to help computer users search for and modify adware programs to block the presentation of advertisements and to remove spyware modules. To avoid a backlash, as with the advertising industry in general, creators of adware must balance their attempts to generate revenue with users' desire to be left alone.

See also: spyware, malware

This article is part of the series: forms of software distribution

Adware | Beerware | Careware | Crippleware | Donateware | Free software | Freeware | Hostageware | Nagware | Open source | Postcardware | Shareware | Shovelware | Vaporware |

Categories: Advertising | Software

- This page was last modified 03:29, 23 May 2005.

- All text is available under the terms of the GNU Free Documentation License (see **Copyrights** for details).