

## **Spyware, Adware, and Peer-to-Peer File Sharing Applications**

The security risks posed by spyware, adware, and peer-to-peer file sharing applications are not clearly understood by many computer users. The purpose of this document is to provide some background information about these applications and to communicate Arts and Humanities Academic Computing Services policy for responding to problems caused by such software. The information provided here is just a summary of a complex and quickly evolving issue. You are encouraged to research this topic further to gain a full understanding of the issue.

### **What is it and how does it work?**

Adware is defined as any software that is supported by advertising revenue. On the surface and in its purest form, this is not necessarily a bad thing. Software developers can get revenue from advertisers, allowing them to make their software available to users for free. Often the developer will provide two versions of the software: a professional version for a fee and a freeware version supported by advertising. Users can decide to use the freeware version and put up with the often minor irritation of pop-up ads or ad banners. Unfortunately, the visible advertisements are often not the only added features in the freeware version of the application. In order to provide targeted advertising, the capability of tracking individual users' Internet usage has been added to many adware programs, making them spyware. This software tracks where you go and what you view on the Internet and sends that information back to the ad server to allow the advertiser to send the banners and pop-up ads that will be most attractive to you.

There is nothing illegal about spyware provided the user knows what the software is doing. The information about spyware processes is normally included in the end user licensing agreements provided when the software is installed. The information is rarely stated clearly and is typically buried deep within a lengthy document. Most users simply click "I accept" without looking carefully at the terms of the agreement. As a result, most users are unaware that they have software on their computers that tracks and reports on their Internet usage.

As long as the software is collecting and transmitting information that is not highly personal, such as browser histories, many people are not concerned that information is being transmitted without their knowledge. The greater danger is that some of this software does not limit itself to browser histories but also collects and transmits personal information such as email addresses, passwords, card numbers, and account details. A link has been

made between the increase in SPAM and spyware, as advertisers can use spyware to collect email addresses and sell them to other companies that use SPAM to advertise their products or services.

Peer-to-peer applications became well-known when Napster was regularly in the news. KaZaA and Grokster currently are the two dominate applications in this category. Peer-to-peer applications allow users to connect directly with other users to share files. Although such applications facilitate the illegal sharing of copyrighted materials, the applications themselves are not illegal. The problem is that both KaZaA and Grokster come bundled with adware. By accepting the terms of the software license, users agree to accept various advertisements and promotions. Many of the files that are shared are also adware, Trojan Horses, or are infected with viruses and worms.

Adware and spyware represent a real threat to the operation of computers and networks, and they create personal privacy and security risks. Because spyware is often designed to be secretly loaded at system start-up and to run continuously, and because there are often multiple spyware applications loading on a system, the cumulative effect to the operation of the system can be dramatic. The increase in network traffic caused by these applications continually sending information back to their source consumes bandwidth, slowing down the overall operation of the network. Although adware in its purest form is not a security threat, it is clear that we cannot trust it to remain pure. It is easy to imagine how the capability to collect personal information from your computer and covertly send it back to the ad server could be abused. Because this information is transmitted secretly, we cannot be certain exactly what information is being sent.

### **How do you know you have it?**

Often it is impossible to tell that adware or spyware have been installed on your computer. When problems become obvious symptoms include unexplained slowness of the operating system, redirection of your web browser's home page to another web site, new icons appearing on your desktop when you haven't installed new software, and new bookmarks or favorites appearing in your web browser. Spyware and adware are frequently installed with freeware applications such as games and utility applications, so avoiding such applications will help reduce the possibility of having spyware installed on your computer. Of course, there are many freeware applications that do not include spyware. In some cases, adware or spyware can be installed by visiting a web site and downloading a plug-in application or by Internet shopping, with the most noticeable symptom frequently being an increase in the amount of SPAM you receive. It is no

longer possible to completely avoid behaviors that could result in spyware being installed on your computer.

### **How can you get rid of it?**

There are a number of applications available to detect and remove spyware and adware. Computing Services currently recommends Spybot Search and Destroy for use on Windows systems. We hope to have a recommendation for Macintosh systems soon. If you suspect a problem with spyware or adware on your University-owned computer, contact ACS at extension 52104. In some cases, the best course of action for solving problems caused by adware and spyware will be to replace the computer's operating system.

There is a lot of information available on the Internet about adware and spyware and the privacy and security threats they present. If you are interested in learning more about the capabilities of this software and some of the most dangerous applications, you can start by reading the document available on the Federal Trade Commission's site (<http://www.ftc.gov/os/comments/spyware/040329howes.pdf>), visiting the counter exploitation web site (<http://cexx.org/>), or visiting Steve Gibson's site (<http://grc.com>).

### **Academic Computing Services policy in response to problems caused by adware, spyware, and peer-to-peer file sharing software**

Arts and Humanities Academic Computing Services has established the following policies and procedures for responding to problems on computers caused by adware, spyware, and peer-to-peer sharing applications:

- ACS currently recommends Spybot Search & Destroy for identifying and removing spyware and adware from computers.
- In response to problems caused by spyware and adware, ACS staff will first try to remove the offending applications
- Because it is impossible to tell what malicious applications may have been installed as a result of installing freeware, Computing Services reserves the right to replace the operating system by re-imaging any computer on which a user has installed freeware (e.g., games, media players, utilities, peer-to-peer file sharing applications). User-installed applications and locally stored data will be removed through the re-imaging process.
- In cases where spyware and adware have caused significant problems, re-imaging the computer will be the preferred solution.