

Internet User Safety Guide

How to avoid the problems related with spyware, pop-ups and other Internet Nasties



The problem with excessive pop-up ads, spyware/adware, viruses and spam continue to plague the Internet. In some cases, their effects become more than annoyances. This type of programming can sometimes choke valuable system resources to the point of rendering a workstation (personal computer) useless. When the situation gets this bad, the best solution is often a total system reimage (basically erasing your hard drive and reinstalling everything from scratch). This process is very time consuming. The following are tips for the office as well as at home to help educate as well as combat this growing problem.

1. Spyware

Also called *adware*, spyware is any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers. Spyware is similar to a Trojan horse in that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today. Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability. Because spyware exists as independent executable programs, they have the ability to monitor keystrokes, scan files on the hard drive, snoop other applications, such as chat programs or word processors, install other spyware programs, read cookies, change the default home page on the Web browser, consistently relaying this information back to the spyware author who will either use it for advertising/marketing purposes or sell the information to another party. Licensing agreements that accompany software downloads sometimes warn the user that a spyware program will be installed along with the requested software, but the licensing agreements may not always be read completely because the notice of a spyware installation is often couched in obtuse, hard-to-read legal disclaimers.

Some common examples of spyware that are extremely prevalent throughout the Internet include:

- 1. Kaza**
 - 2. Gator**
 - 3. BonziBuddy**
 - 4. HotBar**
 - 5. eXactSearch**
- And Many More....**

This is by no means a complete list of spyware. There are over 370 known types of spyware / adware software that can find its way on to your workstation.

(Source: <http://www.spyware-guide.com> - 4/2/2004)

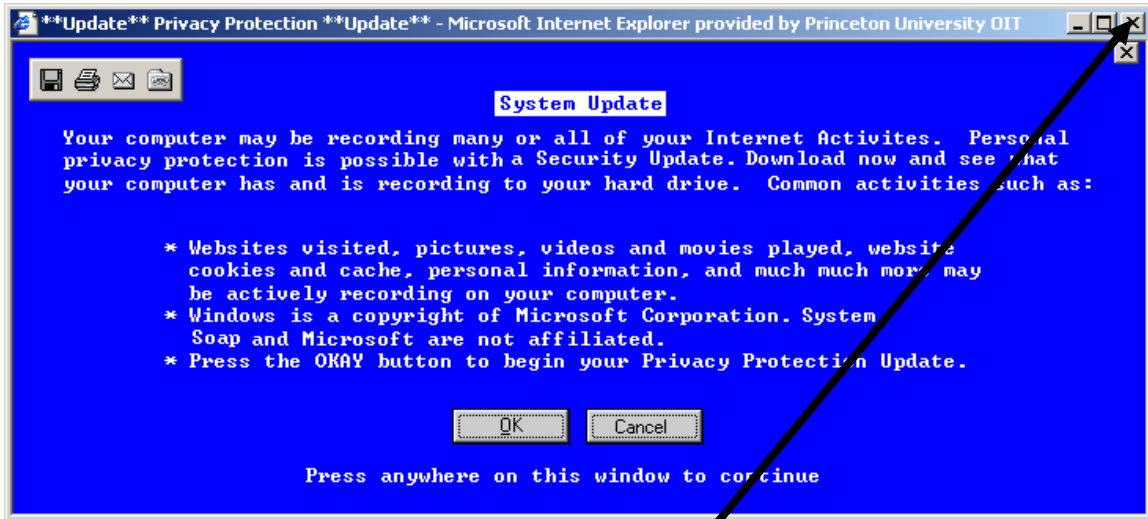
In addition to causing large amounts of pop-ups to appear, spyware can trigger many insidious actions against your workstation which may negatively impact you. While some spyware displays innocent ad messages from your web browser, other types of spyware can record how you surf the web, your chat clients and even record your keystrokes and harvest your e-mail addresses (stored on the workstation). The main point to remember, is that your workstation could potentially (and unknowingly) be transmitting sensitive data while you are logged on during the day.

2. Pop-up ads

A pop-up ad is a type of window that appears on top of (over) the browser window of a Web site that a user has visited. In contrast to a pop-under ad, which appears behind (in back of) the browser window, a pop-up is more obtrusive as it covers other windows, particularly the window that the user is trying to read. Pop-ups ads are used extensively in advertising on the Web, though advertising is not the only application

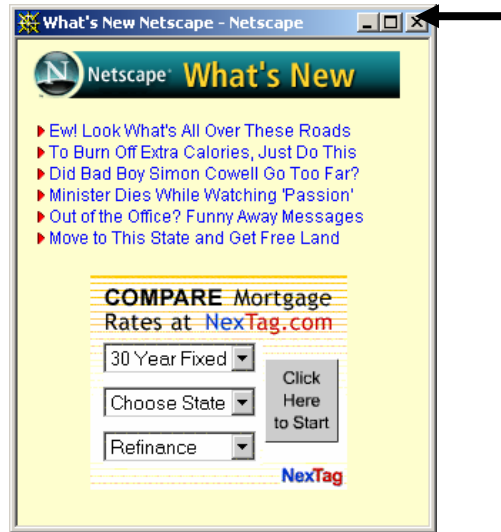
for pop-up windows. Some legitimate web based applications use pop up windows (such as OnBase, the Last saved by edwardyne new version of Peoplesoft, and Works). The pop-ups that you should be concerned with are of the advertising variety. Some of pop-up adds are crafted in a purposely deceitful manner. Often, pop-up ads (if activated) can inadvertently install spy ware on a workstation. Pop-up blocker software is available but sometimes conflicts with legitimate University Systems applications.

When a pop-up ad appears on your window **NEVER** use the close button or anything else that is located within the window/ad. Instead, use the "X" button located at the very top of the ad. This "X" button is Windows close command. Many ads fashion a close button (within the add) that actually installs spyware on the workstation. To be safe always close pop-up ads by using the "X" button. Below is an example of a very sneaky pop-up ad:

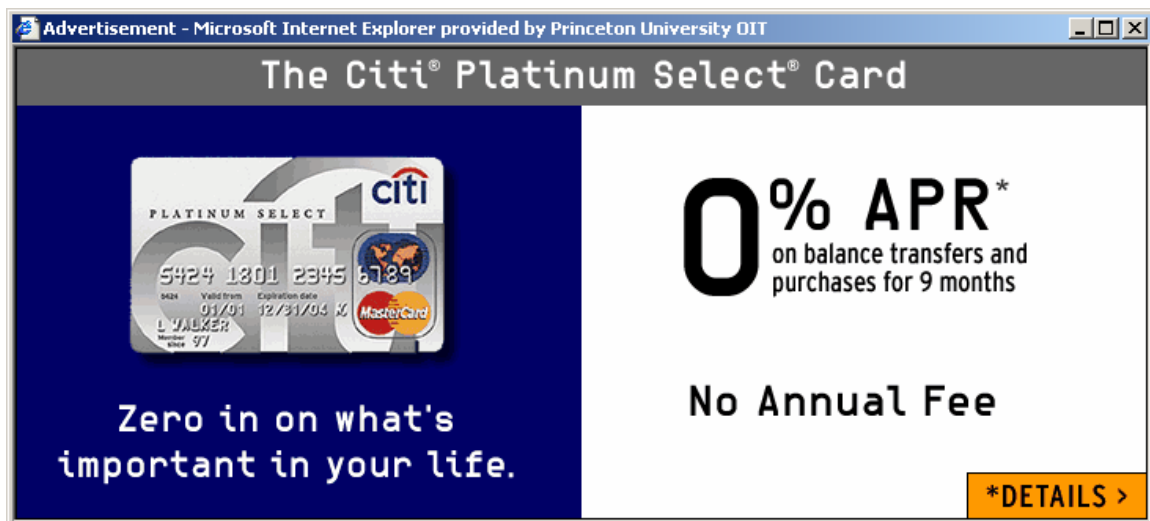


To nullify this ad use the "X" button at the very top of the ad. Also, know that OIT nor Operations Support use pop-ups in this manner (relating to system problems).

Sometimes pop-ups appear when a browser is launched. The example below shows a common pop-up ad when Netscape is initially launched. Notice the advertisement for the mortgage company? If you accidentally click on that portion of the screen you would be sent to that website, and possibly more. To avoid possibility, simply click on the "X" button to safety close the pop-up window down.



Other pop-ups are not so tricky, like the one listed below. Again, click the “X” button at the very top portion of the ad to safely close it.



3. Hijacking

A trend that is becoming more and more common is where the browser settings of web surfers are being forcibly hijacked by malicious web sites and software which changes your default start and search pages. Sometimes internet shortcuts will be added to your favorites folder or desktop without asking. The purpose of this is to force you to visit a web site of the hijacker's choice so that they can artificially inflate their web site's traffic for higher advertising revenues. In some cases, these changes are reversible simply by going into internet options and switching them back. This is not always the case though and sometimes it's necessary to edit the windows registry to undo the changes made. There is even a combination of registry setting and files placed on your hard drive that redo your settings every time you reboot the computer. No matter how often you change your settings back, they are changed again the next time you restart your system. There have even been cases where internet options have been removed from the tools menu by registry hacking to prevent you from controlling your own computer!

4. Spam

Electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited e-mail. However, if a long-lost brother finds your e-mail address and sends you a message, this could hardly be called spam, even though it's unsolicited. Real spam is generally e-mail advertising for some product sent to a mailing list or newsgroup. In addition to wasting people's time with unwanted e-mail, spam also eats up a lot of network bandwidth. Consequently, there are many organizations, as well as individuals, who have taken it upon themselves to fight spam with a variety of techniques. But because the Internet is public, there is really little that can be done to prevent spam, just as it is impossible to prevent junk mail. To cut down on your spam exposure, be careful of who you give your e-mail address to. Whenever you fill out a form online prior to downloading "free" software be mindful, and realize that this online entity now has your e-mail address and will most likely sell it to advertisers. One of the trickier methods used by spammers is to create a link within the body of the spam e-mail (or ad) stating something like, "If you wish to be removed from this list click here". **NEVER** do this! Spammers send out e-mail by the millions and quite blindly. When you respond in this manner you are literally telling the spammers that you have a live, active e-mail address. The result of this action will be MORE spam not less! OIT offers spam filtering software. Although not 100% foolproof it can significantly cut back on this kind of annoying e-mail.

5. Viruses, Worms and Trojan Horses

Virus: A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

WORM: A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down.

Trojan Horse: A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

Methods of Delivery: One of the most recent examples of virus proliferation was roughly a month ago. Users were receiving e-mails reporting to be from OIT or Princeton University telling users to update their e-mail account information or warning that their e-mail account is sending out viruses. The e-mail went on to instruct on running a piece of software attached to the message which was supposed to remove the infection. These types of message (with attachments) should be ignored and deleted! OIT or members of the Operations Support Staff will **NEVER** send a message of instruction in this manner! Nor would such e-mails be directly sent from vendors, financial institutions, law enforcement agencies, lawyers, etc. Keep in mind that hackers can easily forge the "From:" field on any piece of e-mail, so you never really know whether the source is legitimate. Also, some viruses or worms can replicate themselves and use your address book as a source to send messages to others. The bottom line is simple, **NEVER OPEN AN UNSOLICITED E-MAIL ATTACHMENT**, even if it appears to be from a trusted source! If you receive an e-mail with an attachment call or e-mail the source and confirm that an e-mail was actually sent before opening the attachment(s).

6. Conclusions

The best way to avoid many of the things described within this document is to avoid unknown websites, opening unconfirmed e-mail attachments and especially avoid installing free software downloaded off the Internet onto your computer. When a program is offered as being “downloadable for free” often the hidden price is spyware or your system being hijacked by this “free” software. Some advertisers exploit people’s trusting nature and entice users to download a free game or service only to surreptitiously get into their system and create headaches. Problems described within this document are growing in severity all the time. Lawmakers simply can not keep ahead of this rapid moving technological curve and legislation to control this is slow in coming. There are tools currently available that can combat some of the effects of this annoying/destructive programming, but the best method remains education and a general understanding of how computers, e-mail and the Internet work. If you have any further questions or actually have problems that are described within this document, please contact Joe Keane at 8-6847 or e-mail at jkeane@princeton.edu.