

Protecting Yourself and Your Computer

<u>Topic</u>	<u>Page</u>
SPAM.....	2
Pop-Up Ads.....	4
Virus.....	4
Worms	5
Browser High-Jacking...	5
Adware.....	5
Spyware/Adaware.....	6
Phising.....	8

Version 1.1

Created by Alan Swarts and Don Campbell, Information Services, Johnson County Community College

What is 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. However, some online services have instituted policies to prevent spammers from spamming their subscribers.

There is some debate about the source of the term, but the generally accepted version is that it comes from the Monty Python song, "Spam spam spam spam, spam spam spam spam, lovely spam, wonderful spam..." Like the song, spam is an endless repetition of worthless text. Another school of thought maintains that it comes from the computer group lab at the University of Southern California who gave it the name because it has many of the same characteristics as the lunchmeat Spam:

- Nobody wants it or ever asks for it.
- No one ever eats it; it is the first item to be pushed to the side when eating the entree.
- Sometimes it is actually tasty, like 1% of junk mail that is really useful to some people.

Message Statistics: 12/25/04 to 1/23/05

Number of message received: **2,453,152**

Number per month from JCCC (Internal): **224,162**

Average per day: **81,772**

Average per day from JCCC (Internal): **7,472**

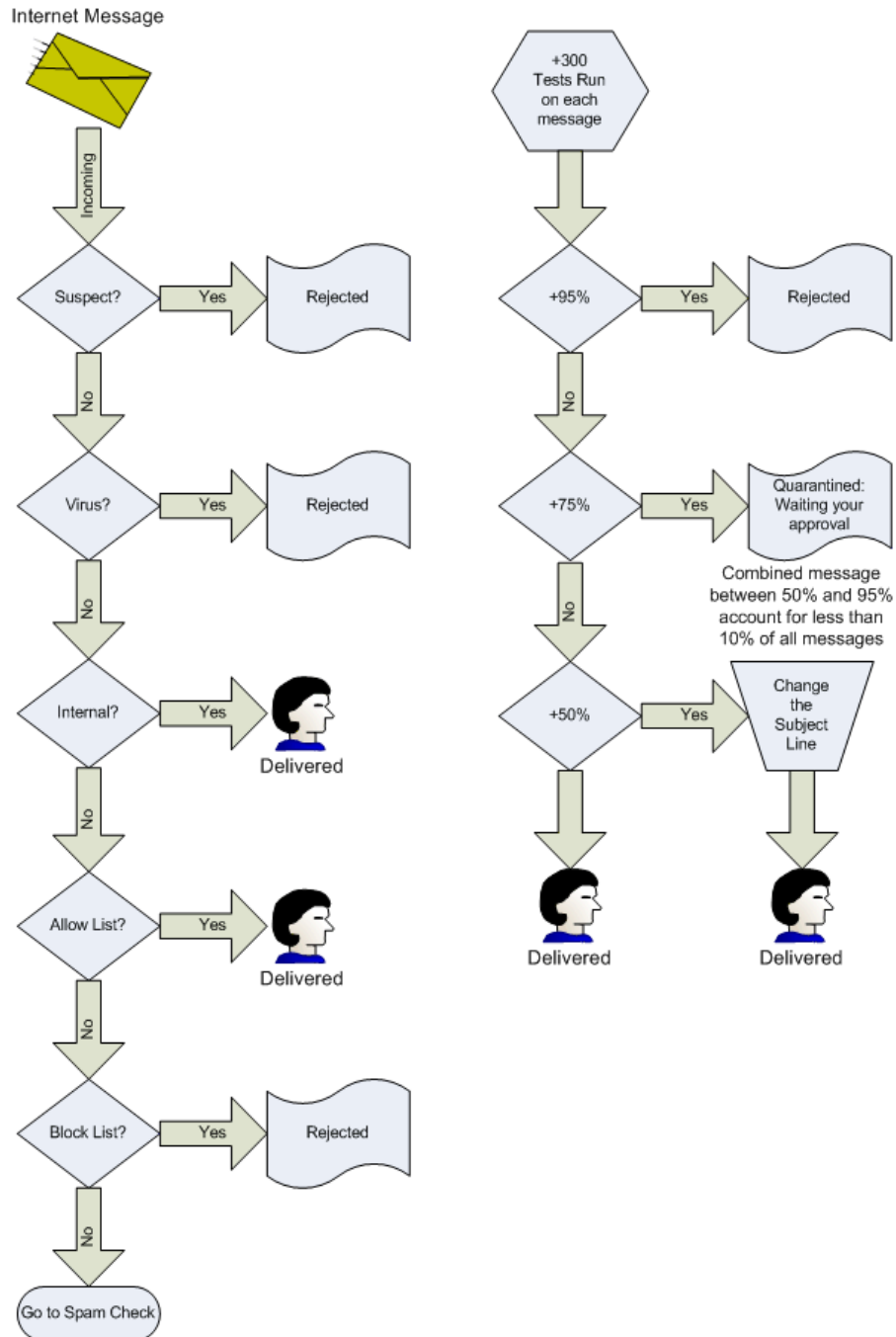
Number of blocked (90% level): **1,664,741- 68%**

Messages with Viruses: **14,114 - .6%**

How to protect yourself:

SPAM is usually controlled by the system administration staff of your e-mail service provider. If you believe messages should be blocked or messages are inappropriately being blocked, please contact the Help Desk and report the problem.

How the JCCC SPAM Filer Processes E-mail Messages



What is a Pop-Up Ad?

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.

A pop-up ad is also referred to as a pop-up.

How to protect yourself:

Warning: Some time when you close a pop-up ad by clicking the **X** button in the upper right hand corner of the screen or by answering either No or Yes to a question in the window, software may be installed on your computer. Select and hold the **Alt** key then press the **F4** key should close the window safely.

Installation of pop-up blocker software is the normal action taken to avoid these nuisance message windows. There are several products available and for Windows users, the Service Pack 2 (SP2) upgrade implements a pop-up blocker in Internet Explorer. However, please note, pop-up blockers will cause problems with both WebCT and the current version of the web based Outlook Web Access (OWA) software.

What is a 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. Since 1987, when a virus infected ARPANET, a large network used by the Defense Department and many universities, many antivirus programs have become available. These programs periodically check your computer system for the best-known types of viruses. Some people distinguish between general viruses and worms. A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.

How to protect yourself:

Have the current version of anti-virus software installed and keep your virus definitions up-to-date. In the event of suspicious workstation activities, please contact the Help Desk for assistance.

What is a Worm?

A worm is 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. A worm tends to differ from a virus in that a worm's intent is to attack your computer and the resources on it.

How to protect yourself:

Have the current version of anti-virus software installed and keep your virus definitions up-to-date. In the event of suspicious workstation activities, please contact the Help Desk for assistance.

What is High-Jacked?

High-jacking a browser is the reconfiguration of your browser including the setting of a new home page. Even though you replace the home page entry, the browser will still be redirected/high-jacked to the other location. In addition, it is likely software, spyware, or other malicious code has been installed threatening the security of your systems.

How to protect yourself:

Contact technical support at the Help Desk immediately and avoid using your system until someone has responded and analyzed the system. This problem is very difficult to repair and may require several hours of a technical support staff member time to recover.

What is Adware?

Adware is considered a legitimate alternative offered to consumers who do not wish to pay for software. Programs, games or utilities can be designed and distributed as freeware. Sometimes freeware blocks features and functions of the software until you pay to register it. Today we have a growing number of software developers who offer their goods as "sponsored" freeware until you pay to register. Generally most or all features of the freeware are enabled but you will be viewing sponsored advertisements while the software is being used. The advertisements usually run in a small section of the software interface or as a pop-up ad box on your desktop. When you stop running the software, the ads should disappear. This allows consumers to try the software before they buy and you always have the option of disabling the ads by purchasing a registration key.

In many cases, adware is a legitimate revenue source for companies who offer their software free to users. A perfect example of this would be the popular e-mail program, Eudora. You can choose to purchase Eudora or run the software in sponsored mode. In sponsored mode Eudora will display an ad window in the program and up to three

sponsored toolbar links. Eudora adware is not malicious; it reportedly doesn't track your habits or provide information about you to a third party. This type of adware is simply serving up random paid ads within the program. When you quit the program the ads will stop running on your system.

[How to protect yourself:](#)

Avoid installing free or shareware. Examples are: Weatherbug, Yahoo instant messaging, possible free screen saver software

Regularly execute an adware/spyware removal utility program to remove the software from your system. System recommendations can be obtained by contacting the Help Desk. It is very important to regularly update the spyware definitions. Examples of removal software are:

Spybot: Spybot - Search & Destroy: Can detect and remove a multitude of adware files and modules from your computer. Spybot also can clean program and Web-usage tracks from your system, which is especially useful if you share your computer with other users. Modules chosen for removal can be sent directly to the included file shredder, ensuring complete elimination from your system. For advanced users, it allows you to fix registry inconsistencies related to adware and to malicious program installations. The handy online-update feature ensures that Spybot always has the most current and complete listings of adware, dialers, and other uninvited system residents.

Version 1.3 adds enhanced immunization features, an improved interface, and integration of BrowserManager for spyware detection, plus the new Hosts File feature and bug fixes.

<http://www.download.com> Search for: Spybot – Search & Destroy

Adaware: Ad-Aware is designed to provide advanced protection from known Data-mining, aggressive advertising, Parasites, Scumware, selected traditional Trojans, Dialers, Malware, Browser hijackers, and tracking components. With the release of Ad-Aware SE Personal edition, Lavasoft takes the fight against Spyware to the next level.

<http://www.lavasoftusa.com/software/adaware>

What is Spyware/Adaware

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; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. 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.

[How to protect yourself:](#)

Regularly execute an adware/spyware removal utility program to remove the software from your system. Recommended system can be obtained by contacting the Help Desk. It is important to regularly update the spyware definitions. Examples of adware/spyware removal software are:

Spybot: Spybot - Search & Destroy: Can detect and remove a multitude of adware files and modules from your computer. Spybot also can clean program and Web-usage tracks from your system, which is especially useful if you share your computer with other users. Modules chosen for removal can be sent directly to the included file shredder, ensuring complete elimination from your system. For advanced users, it allows you to fix registry inconsistencies related to adware and to malicious program installations. The handy online-update feature ensures that Spybot always has the most current and complete listings of adware, dialers, and other uninvited system residents.

Version 1.3 adds enhanced immunization features, an improved interface, and integration of BrowserManager for spyware detection, plus the new Hosts File feature and bug fixes.

<http://www.download.com> Search for: Spybot – Search & Destroy

Adaware: Ad-Aware is designed to provide advanced protection from known Data-mining, aggressive advertising, Parasites, Scumware, selected traditional Trojans, Dialers, Malware, Browser hijackers, and tracking components. With the release of Ad-Aware SE Personal edition, Lavasoft takes the fight against Spyware to the next level.

<http://www.lavasoftusa.com/software/adaware>

What is Phishing

Phishing or Phishing pronounced “Fishing” is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user’s information. For example, 2003 saw the proliferation of a phishing scam in which users received e-mails supposedly from eBay claiming that the user’s account was about to be suspended unless he clicked on the provided link and updated the credit card information that the genuine eBay already had. Because it is relatively simple to make a Web site look like a legitimate organizations site by mimicking the HTML code, the scam counted on people being tricked into thinking they were actually being contacted by eBay and were subsequently going to eBay’s site to update their account information. By spamming large groups of people, the “phisher” counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with eBay legitimately.

Phishing, also referred to as brand spoofing or carding, is a variation on “fishing,” the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting.

How to protect yourself:

Never open a web link included in an e-mail message from a company. While the link may look correct, reputable companies do not send e-mail and ask you to confirm user-id, password, account numbers or credit cards.

Warning: Some time when you close a webpage by clicking the **X** button in the upper right hand corner of the screen or by answering either No or Yes to a question in the window, software may be installed on your computer. Select and hold the **Alt** key then press the **F4** key should close the window safely.