How to Combat Spam

SPAM

Everyday, millions of people receive numerous unsolicited e-mail messages, known popularly as "spam." Some users see spam as a minor annoyance, while others are so overwhelmed with spam that they are forced to switch e-mail addresses.

Because the content of spam e-mail often offers get-rich-quick schemes or pornographic Web sites, it is easy to assume that the activity of sending a spam must be illegal. The truth is that, in most cases, it is legal.

Common Types of Spam

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRODUCTS</td>
<td>Offers or advertises general goods and services. Examples: devices, investigation services, clothing, make-up</td>
</tr>
<tr>
<td>FINANCIAL</td>
<td>Contains references or offers related to money, the stock market or other financial opportunities. Examples: investments, credit reports, real estate, loans</td>
</tr>
<tr>
<td>ADULT</td>
<td>Contains references to products or services intended for persons over the age of 18; often offensive or inappropriate. Examples: pornography, personal ads, relationship advice</td>
</tr>
<tr>
<td>SCAMS</td>
<td>Suggests fraudulent, intentionally misleading, or known to result in fraudulent activity on the part of the sender. Examples: Nigerian investment, pyramid schemes, chain letters</td>
</tr>
<tr>
<td>HEALTH</td>
<td>Offers or advertises health-related products and services. Examples: pharmaceuticals, medical treatments, herbal remedies</td>
</tr>
</tbody>
</table>

Sources of Spam

Spammers use software-harvesting programs such as robots or spiders to record e-mail addresses listed on Web sites, including both personal Web pages and institutional Web pages. Some spam is generated through attacks on mail servers—a method that doesn't rely on the collection of e-mail addresses at all. In "brute force" attacks and "dictionary" attacks, spam programs send mail to every possible combination of letters at a domain, or to common names and words. While these attacks can be blocked, a high number of messages still get through.
Damage

Organizational

Network administrators can spend more than an hour a day combating spam, an organization’s bandwidth usage can be taken up by spam, and employees spend time reading and reacting to these messages. If an organization ends up spending one dollar on each spam, the amount can add up pretty quickly.

Personal

End users have incurred financial loss by reacting to spams that are fraudulent or misleading. Some may be put in an incriminating position, for example, by responding to spams that offer child pornography. Spam has made users less trusting of e-mail. In trying to block such messages, a user may be rejecting legitimate mail if the filter is too stringent.

How to Mitigate

Here are some things that end users can do to combat spam.

1. Do not give out your e-mail address to suspicious sites.
2. Avoid getting on mailing lists unless you expect information that will meet your need.
3. Program filters in the e-mail program to place spam messages in a special folder, which the user can empty periodically.
4. Web-mail users can take advantage of the junk mail folder offered by the mail Web site.
5. Do not respond to spams—just delete them. Response can be recognized by the sender as interest.

Organizations should do the following:

1. Educate users on how to deal with spam.
2. Implement spam filtering at the e-mail gateway.
3. Provide a process for employees to report spam.
4. Take action with organizations that persistently send spam.
5. Report illegal messages to the authorities.

VIRUSES AND WORMS

Almost every PC user has heard about computer viruses and at least vaguely understands their effects. The number of viruses and their disruptive abilities continue to grow. It is costing organizations and individual users money and time to protect their systems and
data from infection. Viruses are often called worms and the two terms are used by a lot of people interchangeably. They are indeed very similar.

McAfee, a major anti-virus software developer, defines virus and worm as follows: "A virus is a manmade program or piece of code that causes an unexpected, usually negative, event. Viruses are often disguised games or images with clever marketing titles such as "Me, nude." A worm is a virus that resides in the active memory of a computer and duplicates. It may send copies to other computers through e-mail or Internet Relay Chat (IRC)."

A growing method for worms to distribute is by means of Window's file-sharing feature. Thus an infected computer can spread a worm to thousands and thousands of computers on the Internet in a matter of minutes.

Another similar term is Trojan horse. A Trojan horse is a malicious program that pretends to be a benign application; it also does something the user does not expect. Trojans are not viruses since they do not replicate, but they can be just as destructive. Many people use the term to refer only to non-replicating malicious programs, thus making a distinction between Trojans horses and viruses.

Here are some recent viruses and what they can do.

- The Blaster worm came out in August 2003 to take advantage of a Remote Procedure Call vulnerability in a number of late versions of Windows and infected about 30 000 computers worldwide within a day. Besides system crashing, other symptoms include:
  - inability to cut/paste
  - inability to move icons
  - add/Remove Programs list empty
  - errors in most Microsoft Office programs
  - generally slow, or irresponsive system performance

- The Slammer worm infected 75 000 computers in 10 minutes on January 25, 2003. Although it did not have a destructive payload, its intensive scanning of computers on the Internet for vulnerabilities tied up many networks and caused some firewalls to fail from overloading, thus resulting in denial-of-service. Some ATMs were forced to be out of business for a day.

- Code Red appeared in July 2001 and took advantage of a Microsoft Internet Information Server security flaw. The worm is programmed to spread for the first 19 days of each month, after which infected machines launch a day-long denial of service attack against the White House domain.

How do worms and viruses infect computers? It used to be through shared diskettes. Although that is still possible, it is now an infrequent cause because diskettes are used
much less often than online file transfers. The two prevalent ways of infection are e-mail and network connection. E-mail transmission can be hard to avoid, but a conscious user who is on guard about opening unknown attachments can play an important prevention role. The most dangerous channel is by network connection. This means that as long as your computer is connected to a network, you can be exposed to worm infection from a computer in another organization or another country, even if you are not connected to the Internet directly. This is an unpleasant by-product of global connectivity.

How can we prevent infection? Well, although viruses and worms are very similar, the former is more easily defined and traced because of its longer history. A virus takes advantage of the necessary functions of a computer to wreak havoc. Even healthy computers (i.e., computers whose operating systems are up-to-date and tightly configured) are infectable. Anti-virus software vendors track new viruses everyday and update their list of signatures. New lists are available to subscribers several times a month for them to install on their computers. When a virus attempts to infect a computer equipped with anti-virus software, the computer checks the virus to the list of signatures. If there is a match, the infection will not be successful. A signature is really a unique pattern used by a virus, similar to DNA. A virus uses that to reproduce itself and propagate. Because anti-virus software is always playing catch-up, organizations are taking some proactive measures.

One proactive measure is to configure the e-mail gateway and firewall to reject certain file types, types that are commonly used by viruses, for example, .exe and .vbs. The downside is rejecting legitimate files. To compensate for false positives, certain users who have frequent need to receive or download files of these types can be given exemptions by the systems.

Because viruses can hit from e-mail, Internet download, and file transmission through a LAN or a diskette, it would be prudent to implement more than one layer of anti-virus protection. The common approach is to have a layer at the corporate e-mail gateway, one at a local e-mail gateway, and another on the desktop or laptop. It would also be prudent to use different vendors to spread the risk as vendors do not always update their signature files at the same time.

Worms are harder to guard against. On the other hand, if a computer's system software and the organization's firewall are tightly configured, worms will hardly succeed. A typical worm takes advantage of a vulnerability in the operating system or other systems software like the Web hosting system. It is, without intent, the norm these days for software to be released that is far from fool-proof. As time goes on, security researchers and hackers identify vulnerabilities, and hackers then write worms to propagate on the Internet, then infect and compromise computers. An infected computer in turn will spread the worm to other computers that are reachable. Although a typical worm is less destructive to the target computer than a typical virus is, the speed of worm propagation and the typical high volume of network traffic it generates quite often result in denial-of-service to networks.
To guard against worms, organizations should harden their system software configuration, implement software patches in a timely manner, and tightly configure their firewalls. For example, a port should be open only if it is needed for business purpose. A port is a logical connection place and specifically, using the Internet's protocol, TCP/IP, the way a client program specifies a particular server program on a computer in a network. A common port is 80, which is used for ordinary Web surfing; encrypted Web traffic uses port 443. There are tens of thousands of ports available for communication between two computers; worms quite often use high-order ports, so an effective preventive measure would be to close all ports higher than a certain number, say 1200.

**SPYWARE**

Spyware is defined on [http://www.whatis.com](http://www.whatis.com) as follows:

"In general, spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet, spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program. Data collecting programs that are installed with the user's knowledge are not, properly speaking, spyware, if the user fully understands what data is being collected and with whom it is being shared.

A cookie is a well-known mechanism for storing information about an Internet user on their own computer. However, the existence of cookies and their use is generally not concealed from users, who can also disallow access to cookie information. Nevertheless, to the extent that a Web site stores information about you in a cookie that you don't know about, the cookie mechanism could be considered a form of spyware. DoubleClick, a leading banner ad serving company, changed its plans to combine cookie information with database information from other sources to target ad campaigns directly to individuals without their permission. DoubleClick's current policy is not to collect personally-identifiable information about a user without their explicit permission."

A Trojan horse is spyware, but spyware that does not even serve a purpose purported to be useful to the target. Trojan is simply hidden malicious software.

Spyware is similar to virus in that it can harm the computer or the user. Here are some things spyware can do:

- Steal your information
- SPAM your e-mail account
- Send pop-up ads to you
- Slow down your computer
- Crash your computer

It has been said that some peer-to-peer programs for music file swapping are spyware.
How to Guard Against Spyware

To prevent spyware, users should be judicious in downloading software, especially freeware. The browser's security level can be set to high and the browser can be configured to reject or alert the users of programs using extensive interactive features such as Java applications. Abstaining from unnecessary surfing or being selective of Web sites to visit would also help, because quite often spyware is installed without the user downloading software.

To find out whether spyware exists on your computer, you can purchase a product that scans your computer. It costs about $50. However, these products are not fool-proof, especially for identifying malicious software that identifies your computer applications and configuration. They also do not undo the damage that has been done by spyware.

CONCLUSION

The final word of advice for combating spams, virus, worms and spyware is "safe surfing" and limit your presence on the Internet.