

The term spam comes from the 1970 Monty Python sketch in which a café customer is told that it's impossible to order anything that doesn't include Hormel's canned meat product Spam. During the sketch, a chorus of Vikings repeatedly chanted the word "spam," eventually drowning out the conversation. In the 1980's, the term was given to "attacks" on electronic bulletin boards and in chat rooms, where a user or a group of users attempted to drown out others by posting long text messages and often included material from the original Monty Python sketch.

Commercial email spamming started around 1990 as people flocked to email and the www, and its reach and volume have been growing ever since. In 1994, the first large-scale spam was sent to around six thousand newsgroups and reached millions of users who were accessing the newsgroups. In June, 2005, 30 billion pieces of email spam were sent each and every day. The number of spam pieces have increased more than 80% today. Typically more than ½ of a person's email today is spam!

Email spam comes in a number of flavors or formats.

1. **Advertising Spam.** Advertising Spam is the most common flavor and include "come-on's" for pornography websites, prescription drugs, sexual-enhancement potions, printer cartridges and even counterfeit items such as name-brand watches and popular software, mortgage offers, phony diplomas, and penny stocks.
2. **Advance-Fee Fraud Flavor.** Mostly known by the infamous "Nigerian scam," advance-fee spam is supposedly sent from a foreign government minister or a relative of a wealthy person and offers you a percentage of a large sum of money if only you would pass along private information that ends up with your bank account being emptied.
3. **Phishing Flavor.** These are emails or messages that claim to be from source that you trust; for example your bank, your stockbroker, an online service like PayPal, eBay, or Amazon. These emails ask you to go to an *authentic-looking* website and give out your password, account numbers, credit card numbers, or some other private information in order to continue to use their service or to update your account settings. The information given to these sites is then used to access your bank checking/savings account and your credit cards. Identify theft can be the result of responding to these emails.
4. **Virus Spam Flavor.** Emails that contain viruses as attachments are often sent by infected PC's without the knowledge of the computer's owner. These computer viruses turn unwilling Pc's into 'zombies.' Later these zombie computers are used to relay spam or conduct "denial-of-service" attacks. Denial-of-service attacks launch massive amounts of data at an Internet domain with the intent of

overwhelming its servers and shutting the service down; for example the IRS, eBay, Microsoft and many other famous sites are targets of these attacks. Even Macs today are subject to these kinds of attacks and in fact Macs are becoming more popular with virus and spyware (spying programs) writers.

5. Web Bugs. Spammers began creating HTML (Internet coded) spam for the purpose of including Web bugs. Web bugs are invisible HTML image tags that report that a message has been read by the receiver. Often this process is used to validate email addresses to be good ones. Spam can also be formatted as plain text as well as Rich Text (text that can support more formatting options). Using graphics in spam is being done to make the email more appealing and to get by spam filters that are designed to look for wording and not graphics.

You can avoid a lot of spam by not giving out your email address to people you don't know. You shouldn't reply to spam ever! Many email clients (programs that you read and send email with) have spam filtering options; you should use them. Outlook 2003 and 2007 have a very good one built in. You can also do some searching for programs to run to intercept spam before it gets to you. Installing and running these programs can help with the spam problem.

We Computer Tamers keep telling our customers that SAFE and SMART COMPUTING begins with "reading before clicking" and being careful where you go on the Internet. Understanding what spam is and how harmful it can be is a start to safer and smarter computer usage.

Allen is one of JASAsolutions' Computer Tamers who host The Computer Club heard every Wednesday after the 5 o'clock news on WILI AM 14. You can learn more about getting your unruly computer under control by visiting www.TheComputerTamers.com and explore the free information compiled there for you. Earlier columns are also available at the website. Be sure to visit the Computer Tamers Sales and Service Center at River Plaza, 75 Bridge Street Willimantic. The phone number is 860-456-1310. You can call us toll-free 1-877-456-1310.