

Spyware and spam are all a big scam!

By Bruce A. Love

*Spyware and spam!
They're both such a scam!
I do not like
that spyware and spam!*

*"Do you want those larger?"
"Do you want that bigger?"
"Here's a pretty foreign girl,
I think that you'll dig her!"*

*I don't like your scams
I don't like your spams
And I really don't want
To see you on cams!*

*"You can get a mortgage,"
"a Russian girl for marriage"
"Prescription drugs are no problem!"
"Send cash, and you'll get them."*

*An oil guy from Nigerya
wants to share millions with ya.
To get your share's easy
"Mail your bank numbas to me!"*

*If an offer sounds great,
Too good to be true
It probably is
Not a good one for you.*

*Make laws that do ban
This new form of scam
Do what you can
to can all this spam!*

*Take my advice,
Remember this verse,
Don't read the foul spam
Their attachments are worse.*

*Delete it right now
Delete it I say,
Take no more chances,
Just throw it away!*

Ok, I am no Dr. Seuss, but the onslaught of spyware and spam can make anyone feel as miserable as a Grinch. Spam is unsolicited "junk" e-mail sent to large numbers of people to promote products or services. Spam can be a huge time waster and is one of the biggest threats to personal privacy and security today.

Unlike junk mail that arrives at the curb, spam can contain software that burrows deep into your computer and steals email address lists, passwords, and personal information that could cost you, or your friends, dearly. Your best defense against such personal violations is to educate yourself about good e-mail and web surfing practices, and get a few tools to assist you in your efforts.

Spam has become such a problem, that legislators have enacted laws against it. The CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing) was signed into law in December 2003. This was a good gesture, but has done little to eliminate the barrage of spam launched against our wired society. What it has done, however, is provide law enforcement professionals the legal footing they need to prosecute the vermin that send this trash (if and when they are located).

As an e-commerce web store developer, I recognize the value of mailing lists generated by the e-stores that I build. I view the use of promotional e-mail as a service to the customers. However, in fully complying with the CAN-SPAM Act, the subject lines of promotional mail generated by my stores clearly identify the commercial content of the e-mail, and contact information and opt-out instructions are always provided. These are legitimate uses of commercial e-mail.

Illegal uses of email often are easy to spot. Their subject lines frequently have nonsensical words, or the sender is unfamiliar. These are the first clues that should alert recipients to potentially destructive spam. The misspelled words are not necessarily the product of an uneducated sender. They are attempts to evade programs designed to block spam. Anti-spam programs look for certain words and the proportional use of those words in the subject lines and content of e-mails. I worry that some spam blockers filter mail coming from a guy named Love. The best thing to do with suspected spam is delete it without opening it. Above all, do not open attachments or click on links contained in the e-mail.

Anyone who does any amount of web surfing will eventually stumble upon web sites requesting e-mail information. If you fill out these forms, use a disposable e-mail address just in case the website sells your contact information to spammers. There are free services that serve as buffers between real e-mail addresses and ones that are given to others (see sneakemail.com or mailinator.com).

You can minimize the threat of spam by observing the following:

1. Do not open suspicious e-mail.
2. Do not respond to a bulk email EVER!
3. Use throwaway e-mail addresses when filling out online forms, and when joining newsgroups.
4. Use spyware blockers (Spy Sweeper, Ad-Aware, and/or Spybot Search and Destroy)
5. Keep your Anti-virus software up to date.
6. Keep Windows up to date.
7. Consider using a firewall.

If you think you've been a victim of online fraud, you should contact the FBI's Internet Fraud Complaint Center (www.ifccfbi.gov)