

PROBLEM:

Webmasters, Site Owners and Internet E-mail Users... it is time to take the fight to the senders of all that unsolicited E-mail that clogs your in-box.

Unsolicited E-mail messages are referred to as UCEs or sometimes as spam, the name spam comes from a famous Monty Python skit that was set in a restaurant specializing in dishes involving lots of Spam. A group of Vikings sitting in the corner would sing Spam, Spam, Spam, lovely Spam. Wonderful Spam!, drowning out the waitress and all conversation in the restaurant... See: <http://www.detritus.org/spam/skit.html>
Since unsolicited E-mail is seen as drowning out all other communication, it made sense then to call it spam (with a lowercase "s" to differentiate it from the Hormel meat product).

In 1994 the first large-scale spamming occurred with the infamous Green Card spam. See: http://www.urbanlegends.com/legal/green_card_spam.html

Two attorneys trying to drum up some clients hired a programmer to flood every USENET newsgroup with this letter. This unsolicited E-mail made people so angry that recipients began referring to it as spam.

Today more than ever, spam is more than annoying to most Internet users. Research shows that from 2002 to 2003 there was a 77% increase in UCEs. To Internet Service Providers, it uses up valuable resources needed to run their networks, degrading services and running up the total cost of operations. Current legislation (See: <http://www.spamlaws.com/federal/108s877.html>) will do nothing to stop unscrupulous senders of UCEs, as the law is written it gives businesses that follow "the letter of the law" the green light to flood your in-box.

Spammers send unsolicited E-mail via three common methods;

1. From their own servers...
2. Relayed off of unsecured (open relays) SMTP servers...
3. Relayed while spoofing (falsifying) header information...

In case #1, The sender will have legitimate removal routines and will honor such requests so they cannot be prosecuted under certain State and Federal laws. See: <http://www.spamlaws.com/>

In cases 2 and 3, Any bounced messages will never effect the spammer, because the spammer could care less if the TO: address is legitimate or not, they are playing a numbers game and non-deliverables are just a drop in the ocean. You can try using SpamCop (<http://spamcop.net>) to help notify the network administrator of the open relay server who just delivered spam to you... but who is willing to take time and spend resources to do this. But, in case # 3, The spoofed sender's Postmaster will receive the bounced message, making extra work for an innocent 3rd party... for which the spammer couldn't care any less about as well.

"Unsubscribing" is not an option since email lists are purchased for pennies an address and are distributed quickly and widely, it's impossible to be removed from a list once you make it onto one. Therefore, replying to an email and asking to be removed from a group list will never get you anywhere, in most cases it only verifies to the sender of the UCE that your address is a valid working box.

E-mail users eventually loathe and procrastinate downloading their E-mail because of all the junk in it. Worse, your staff is loosing productive time every day! The average E-mail user filters through unsolicited mail for .5 hours per day. If one of your staff is responsible for receiving E-mail sent to an address posted on a Web page or through an on-line form... he or she will spend a full hour each day with a finger on the delete key... it adds up, 30 minutes in the morning (spammers don't seem to sleep) and then a few minutes each hour until the end of the work day. Tomorrow the routine starts all over again!

It seems that even with the help of filtering techniques and Federal legislation, you can't turn the tables against spammers. How can you fight back? With Luminatch's [EClean](#) you can! >>> and at \$29.99 it's a bargain, the first three hours of saved productivity pays the ROI.

The information above is the reasons we developed the [EClean](#) application...

The information below is some advise for how to make the best use of [EClean](#).

SOLUTION:

First, if you do not know what our software will do for you... it will protect your address from being harvested by using a special encoded HTML mailto: link. Your Webmaster will need to add these to your Website for you... then when visitors click the link on your site to send you mail, their default E-mail client will open, the special link they clicked adds a unique code (specific only to *your* E-mail address) to the subject line of the message being sent...

In the body of the message is displayed some short instructions... that they should not alter the subject line, but they can safely delete the text in the body and replace it with their own.

Then you run our software installed on your PC or workstation, it searches the messages on your E-mail server for the special code added to the subject line of legitimate business or personal transmissions from your Website. It also checks to see if the sender and / or sending Domain is an entry in your "trusted" section of the installed software. The software then sorts your mail for you, separating the good from the bad, giving you an opportunity to view the messages that are suspected UCEs. Later, after you have been using this new system for a while, you can optionally turn on an additional feature "automatically" deleting the UCEs.

Now, you just open your regular E-mail client and it downloads your E-mail like usual... but the in-box is *clean* except for legitimate correspondences. Once our software has been setup for a while and you trust this new system...a couple of clicks of the mouse and you and your staff save valuable time... every day!!!

FEES:

All fees are one-time fees based on the E-mail address being protected. Encoded links can be placed on as many Web pages or forms as you like. The software is free and can be used by more than one user on more than one PC, as you are paying for the encoded link and the right to protect the E-mail address with the software. The software can also process more than one E-mail box, each additional E-mail box needs a code, the cost for additional encoded addresses varies depending on volume. The software will need to be registered twice to use 2 boxes, thrice to use 3, etc...

TCO: One small business with 10 employees: Needs to purchase 10 encoded addresses (\$27.74 x 10 = **\$277.40 total cost of ownership**) ... if 1/2 of an hour is saved per employee per day @ 220 working days in a years time @ \$12 per hour salary @ 10 employees = **\$13,200 in saved productivity** over the coming year!

The software is being sold at an introductory price. Luminatech reserves the right to pull the introductory pricing at any time. Buy now before the software goes up to our intended retail price. See our Website for details.

TIPS:

- Use the encoded link on your Website as soon as possible.
- Put verbiage on your Website, explaining this filtering system... so senders know not to alter the subject line. Links to our site (<http://luminatech.com/eclean/>) are authorized in advance, and appreciated.
- Have your Webmaster add the special subject code to your on-line forms. This can be done in plain text.
- Turn on trusted senders and import a list of your clients addresses, personal contacts, etc...
- Turn on the add valid senders to trusted senders feature.
- Broadcast a message to current business contacts asking them to visit the URL with the encoded link and to send you a short message so they can be added to the trusted senders, or import a list of addressees.
- Add the Domain names of your frequent correspondences and / or your own Domains to the trusted Domains section, then add the Domains of the local Internet Service Providers in your metro area to the same.
- Use more than one E-mail address and the forwarding feature to consolidate messages in a secret (not posted on any site and not used for normal correspondences) box that gets no UCEs.
- Use the URL of the Web page that has your encoded link on it instead of E-mail addresses on your Business cards, brochures, letterheads, etc...
- Monitor the messages cued for deletion for a period of time ... right click to view suspect messages that you think are business or personal messages.
- If your E-mail address has already been harvested by spammers or if yours is a new E-mail address, a new Domain or a new on-line form handler ... [EClean](#) will work to pre-sort your messages for you.
- Add a link to [EClean](#) in the startup folder on your administration PC and you'll never forget to run [EClean](#) prior to your default E-mail client.
- It is true, you are \$29.99 (or less) and a short setup from a spam-free workspace! [Buy EClean now...](#)
- See the Software's help file for info on setting up features and other tips.