Best Practices for SPAM Reduction

ABS Computer Technology, Inc.

SPAM Zapper - SPAM Stops Here - www.No-JunkMail.com

Developed in Pittsburgh, PA and used Internationally, the SPAM Zapper is multi-layered approach to Security, Spam and Viruses we encounter on the Internet daily.

The amount of SPAM we receive, effects our ability to communicate effectively. Our Multi-Layered approach provides the greatest protection available.

The SPAM Zapper stops SPAM and Viruses. Our Best Practices guide is intended to assist you in Reducing (even eliminating) the amount of SPAM you are exposed to on a daily basis.

Please visit us on-line for more information on the SPAM Zapper.

Corporate Sponsor of the Pittsburgh FBI—InfraGard.

Founding Member & Sponsor.

ABS Computer Technology, Inc.

519 Nichols Road
Pittsburgh, PA 15237

Phone: 412-635-7488
Fax: 412-635-2546
Email: aewhale@ABS-CompTech.com
www.ABS-CompTech.com

ABS Computer Technology, Inc.

Best Practices for SPAM Reduction

The SPAM Zapper™

http://www.No-JunkMail.com

1. **DO NOT** Click on the Unsubscribe link on HTML Based Email, it only serves to confirm that they have a valid Email Address.
2. **DO NOT** Put your Email address on the Internet (without some protection of course). If you do, Be prepared to answer questions (as I do) from over the world. Be prepared to receive Hello Messages (which you should IGNORE).
3. **DO NOT OPEN ATTACHMENTS** from Email without a Scanner. If necessary, Change your Email Reader. There are many tools which will not load the attachments (which MAY contain Dangerous Viruses). A Few of the more Well Known Email readers are Netscape, Eudora, Evolution, Pine ....
4. **Use a Pop-Up Blocker** on your Web Browser. Netscape includes one for free. You can configure it by selecting Edit -> Preferences -> Privacy & Security -> Pop-up Windows.
5. **Do not Load the Images on the HTML Files** unless you know the Sender. Preloading the images leaves a trail from you to the Spammers, and only encourages them to send more spam because they get paid on the number of Web Hits that they generate.
6. **Verify the DNS Address of the Sender** (more for ISPs and Businesses). If provide Email Delivery as a Service, verifying that the Sender has a Valid DNS Entry is a good start.
7. **Reject Email Delivery from Unknown Sources**. Most Sendmail (server based software) installations provide a means to Reject or otherwise block unwanted sources.
8. **Subscribe to a DNS RBL** (Relay Block List Service). These lists have an been developed to identify the SPAMMERS. Be selective, some are better than others.
9. **Restrict Access to the Mail Servers to nodes in your Network**. By eliminating the ability to relay to only the sources in your network reduces the number of free range machines available for the Spammers to use.
10. **Report the offenders** to the Abuse @ Domain.com address for the provider of the Service. You can use the whois service to validate the registration of the Domain Name.
11. **Don't put your Email address or personal Information on the Internet** to identify yourself. There are many Web Spiders which collect this information for the SPAM Lists, and other activities.
12. **Use a Proxy (or a Firewall) to connect on the Internet whenever possible**. This isolates your connection information, and inhibits the ability for someone to penetrate your connection.
13. **Use an SSH Tunnel** to Encrypt your password for POP3 and IMAP connections. These protocols transmit your Email Address and Passwords in Clear Text.
14. Email Providers should **implement an Acceptable Use Policy** which prohibits abuse, and permits the service provider to disconnect access to the offending user(s).
15. **Avoid Mailing Lists**, while it may be a necessity, it is also a security risk which may expose you to unacceptable levels of SPAM. Even though you may get great information from the Mailing List, they may sell your contact information, or their security on their facility may permit others to obtain your personal information.
16. **Eliminate HTML from your EMAIL** as this it the main delivery mechanism for Viruses and SPAM. Who needs to transmit 30k of data for a 1k message? If you need fancy text, send it in an attachment. Plain Text Email does not transmit Viruses, but HTML Formatted Text certainly can!
17. When you subscribe or register on a site on the Internet, be sure to indicate that you wish to **keep your information Private**. This includes the check box that says that they want to permit third parties to send you information. In essence, you are permitting them to sell your contact information.