

Eight Cost-Effective Tips for Fighting Spam

Contributed by the Information Technology Solution Providers Alliance

Revised February 2007

The AIA collects and disseminates Best Practices as a service to AIA members without endorsement or recommendation. Appropriate use of the information provided is the responsibility of the reader.

SUMMARY

There are steps you can take to protect your computer from potential spam. Eight steps are listed below to help prevent spam infiltration.

FIGHT SPAM

Fighting spam is a top priority for America's 8 million small to midsize businesses (SMBs). The typical employee receives more than 13 unwanted e-mail messages daily, according to a recent study by Nucleus Research. That results in 6.5 minutes per person per day managing spam, which costs almost \$1,000 per employee each year in lost productivity.

The best way to fight spam is to keep your e-mail address away from spammers and keep them out of your mailbox. Protecting your address can be handled through basic workplace policies.

PREVENTING SPAM

Preventive measures are the best and cheapest. ITSPA's advisory board members, who include executives from the nation's most successful IT solution providers, offer these useful and, in most cases, free measures to help SMBs reduce spam:

1. Avoid responding to spam. By responding to spam or sending a remove request, the recipient confirms receipt and validates his or her e-mail address.
2. Avoid posting e-mail addresses on the company Web site (or anywhere else) as text. E-mail addresses on Web sites can be posted as graphic elements, which spammers' automatic search engines can't read. Companies that provide a feedback option on their Web sites should use a server-side script and button rather than a link to an e-mail address.
3. Use different e-mail addresses for postings on news groups. Employees who post on news groups will receive spam in return. By using another e-mail address, they avoid receiving spam at their business e-mail addresses.

4. Avoid giving out your e-mail address without knowing how it will be used or disclosed. When asked for an e-mail address, always read the fine print in privacy statements to determine if you're protected.
5. Don't buy anything advertised by spammers. The information you're asked to provide always includes your e-mail address, and providing it negates your right to privacy. If people stop buying from spammers, companies using their services to advertise on the Internet will stop when their products don't sell.
6. Use built-in filtering features of your mail server to eliminate most spam. Subscribe to a "black hole" list such as www.mail-abuse.org and filter known mail servers used by spammers. A feature called reverse DNS can filter host name records to check for valid e-mail addresses.
7. Disable the mail relay function on your e-mail servers. Spammers typically bounce their e-mail spam off e-mail servers that have the mail relay function enabled. Disabling mail relay not only makes it more difficult for spammers to be successful, but it also prevents your company's IP address or domain name from being registered with the public blacklists as a suspected source of spam.
8. Implement e-mail virus scanning. Use a virus-protection solution to prevent opening e-mail that contains a script to gather e-mail addresses from your address book. Macro viruses can scavenge your e-mail, as well as the e-mail of anyone you've sent mail to.

If all else fails, use a spam filter. These tools detect unsolicited e-mail by analyzing message content and words. Several solutions are available, ranging from an appliance called a gateway scanner to server-based software that resides in the e-mail host computer.

These spam-fighting measures will eliminate some, but not all, unwanted messages. Spammers continually use new technologies and methods and,

to avoid being stopped, even send messages using image or HTML attachments to circumvent content filters. Every time technology service providers discover these methods, they in turn devise ways to close that loophole.

Keeping current with the latest spam-fighting techniques is a full-time job, but one worth pursuing. Local solution providers can help you implement spam-fighting recommendations and stay current with the latest tools to control this problem. Contact your local IT solution provider—a one-stop resource for hardware, software, network integration, and professional services—for help with controlling spam and other business and technology issues.

Copyright Information Technology Solution Providers Alliance 2004. Reprinted with permission.



Copyright 2004 The American Institute of Architects. A version of this article was published in *AIArchitect*.

Key Terms

- Practice
- Office property
- Office equipment
- Office equipment records
- Computer software

RESOURCES

More Best Practices

The following AIA Best Practices provide additional information related to this topic

- 10.02.09 Risks with IM & Camera Phones
- 10.01.02 The Paperless Office
- 10.02.06 Watch Your Language: The Risks of Email

For More Information on This Topic

See also “Using the Internet in Practice,” by Paul Doherty, AIA, with Michael Tardif, Assoc. AIA, *The Architect’s Handbook of Professional Practice*, 13th edition, Chapter 13, page 392.



See also the 14th edition of the *Handbook*, which can be ordered from the AIA Bookstore by calling 800-242-3837 (option 4) or by email at bookstore@aia.org



Feedback

The AIA welcomes member feedback on Best Practice articles. To provide feedback on this article, please contact: bestpractices@aia.org