

Seven Spam Prevention Tips for Small Business

When business owners are asked what their top technology-related concerns are, invariably, a discussion on security comes up. The concern used to be more about how to use computers than the safety of using them, but the fact is that today there are hosts of people “out there” on the Internet who mean you no good and are a threat to small businesses that rely on technology. People like hackers, spammers, virus-writers and even trusted resources like your own employees can create problems that cost you time and money.

Spam is one of the more insidious time wasters for your business. If you are not convinced, download *The Hidden Cost of Spam* at www.theuptimegroup.com/downloads.php. You may be shocked at how much you are spending on spam without even being aware of it.

If your e-mail address receives upwards of 100 spam messages per day, you are not alone. Current estimates by people in the spam prevention business say that 75 percent of e-mails in circulation are spam. If changing your e-mail address is not an option for you, it is probably time to invest in some anti-spam software, either through your ISP or for your server if you host your own e-mail. There are also things you can do to try to keep the problem from getting worse or prevent it if you are starting from scratch.

- 1) Create a generic e-mail address such as info1@yourdomain.com or sales1@yourdomain.com. You and your employees should use this address exclusively for all e-commerce purchases and when registering for third-party services. Also, use this address when posting to discussion lists, news groups, message boards and when displaying e-mail addresses to the public, such as on a Web site. If the address starts getting too much spam, simply replace it with something else.
- 2) Do not give your e-mail address away unless you are comfortable that the recipient is a trusted party. If it is an optional request from a third party, leave it blank. If required, use your generic address or a free e-mail account such as Yahoo! or Hotmail.
- 3) Do not unsubscribe from spam that you receive unless you know the company. One trick spammers use is to use unsubscribe requests to verify the e-mail address is active. When you unsubscribe, they know your address is active, making it more valuable, increasing the likelihood of receiving more spam.
- 4) Do not rely on AOL or free e-mail addresses for business purposes. Many companies that provide these services make money by selling e-mail addresses and subscriber information to spammers, advertisers and other third party marketing organizations.
- 5) Do not reply to or forward long chain letters that you receive via email. While very laborious, some spammers use these letters to collect legitimate addresses because most of the addresses in chain letters are active – perfect spam targets.
- 6) Do not sign up for any service that claims to be a “Do Not Spam List,” similar to the FCC’s “Do Not Call List.” Many of these services are fraudulent and may in fact lead to your e-mail address being added to more spam lists.
- 7) If you need to put a “real” e-mail address on your Web site, have your Web developer use obfuscation techniques when publishing your e-mail address on Web pages so that spammers cannot use automated programs to crawl the Web in search of e-mail addresses. Therefore it is a good idea to use HTML tricks that are transparent to your Web site visitors, but may fool the automated programs.