Tips for Ending Email Spam

#1: Insulate and protect yourself

Your first line of defense against spam is to treat your school or other primary email address like your social security number. Only give it out to your students, staff or parents. Never give it out online while filling out surveys, buying a product or service, or corresponding with family and friends. The more widely your address is known, the more likely it will be picked up by a marketing company and sold to companies who engage in spamming.

If you need to fill out online surveys or shop online, create a second personal email account with an Internet service provider or via a free email service like Yahoo! Mail or Hotmail. That way, your most essential emailbox should remain relatively clear of spam, while your secondary address will bear the brunt of the unwanted messages.

#2: Do nothing.

You check your email and, ugh, in comes another unwanted message. What can you do about it? How about nothing.

That's right -- nothing. Every time you receive a message you didn't expect to receive, you could delete it immediately. After all, tapping the delete key takes less than a second. If every single user took this step, the theory goes that the entire bulk email business would collapse in on itself. No response means that a campaign to sell a product or service using unsolicited bulk emails has failed.

However, in the real world, marketers know that even a one percent response rate is both expected and sufficient to label an online sales campaign a success. There's a good chance that a few dozen users will respond to any given campaign, helping to keep the spammers in business and the unwanted emails flowing.

#3: Reply to the "sender."

After you fight down an urge to simply delete a spam message, what else can you do?

Many users open the message and hit reply to send the spammer a piece of their mind. They rant and rave, asking to be removed immediately under penalty of future hostile responses or worse.

Again, this tactic is likely to fail. Spammers can easily forge the sender information on an email message. Many emails come from false addresses like user222@yahoo.com, user222@hotmail.com or user222@aol.com. When users click reply and try to send a response, their message is usually returned to them a few minutes later with a "user unknown" message. Their ranting is in vain.

#4: Follow the unsubscribe directions.

Most commercial spam messages contain some kind of unsubscribe information at the very bottom. Scroll down until you see this information. Normally you need to click an "unsubscribe" or "remove" link, which connects you to a Web page with additional information on how to opt out of future mailings.

Type your email address into the box on this page and click the submit or remove button. Many times a reply instantly appears, promising that you'll be removed in a week or so and that you may receive additional messages in the meantime.

Many of these unsubscribe commands actually work, while others may be illegal email address-collection tools. In reality, there's no way to be 100% sure that your unsubscribe command will be processed, or if instead you've unwittingly given a spammer your address for future campaigns.

#5: Set up filters and use anti-spam software.

Thankfully, there are two concrete steps you can take to kill spam.

First, many email programs offer bulk email folders or special rules that watch for incoming spam and kill it automatically.

Second, several software developers have risen to the challenge of helping users like you kill spam. Many of these tools will check your email and filter out spam before it has a chance to get into your emailbox. If spam slips through, you can update the software to identify future mailings and delete them.

In reality, once your email address has been added to several spammer's email lists, purchasing one of these special software tools may be your only successful weapon against stopping these messages from getting onto your computer.

#6: Track down the perpetrators.

If you have some time on your hands and enjoy a challenge, you can attempt to find the true source of each spam message you receive.

Read the email header, find the original email server that sent the message and how to register an effective complaint to the owner of the server (usually abuse@servername) that's been hijacked to send you spam so future mailings can be blocked.