Reducing Spam Risks

Spam is mass-distributed, unsolicited email and instant messaging advertising. Most spam promotes get-rich-quick schemes, questionable products, fraudulent offers, or pseudo-legal services. Until recently, the only problem with spam besides annoyance was that much of it cheats consumers, undermining their confidence, and harms legitimate Internet marketers that use ethical practices.

Spam is very cheap for the sender to distribute, and a substantial burden to recipients. It can also be very dangerous, since cyber criminals use spam to deliver deceptive phishing emails. The number of phishing and pharming schemes has skyrocketed. Criminals are stealing identities and hijacking systems using blended attacks that use spam to lead users to web sites compromised with Trojans, spyware, and exploit code.

Weblogs, commonly called blogs, are experiencing a steep rise in spam. This “splog” is an onslaught of junk postings that look like real user comments but instead contain advertising links to web sites.

To use your computer and the Internet safely, you need to safeguard your files, identity, and personal information and to protect the overall online experience for your and your family. Following the tips in this article will help reduce the risks associated with spam and protect you from hackers, spammers, and phishers.

How Do Spammers Get My Address?

Spammers buy lists from brokers who have harvested email addresses from newsgroups, chat rooms, web sites, social networking sites such as MySpace, blogs, and Internet directories. Even replying to a spam message—requesting removal from a distribution list—can be a trick to get you to validate your email address for them.

Spammers also run dictionary attacks that throw billions of combinations of words and numbers at an email database to find valid address combinations. Large email hosts like Hotmail and AOL are most at risk because of the sheer volume of email they handle.

How Do Spammers Avoid Detection?

Leveraging Internet connections, spammers use other peoples’ home computers to send bulk emails by the millions. They take advantage of security weaknesses to remotely install hidden software that transforms private PCs into mail or proxy servers. They route bulk email through these "spam zombies," obscuring its true origin. Spam is also routed through overseas servers to avoid detection.

How Do Phishing Schemes Work?

Phishing schemes are becoming more cunning, fooling even savvy users. Phishers send spam emails pretending to be from trusted corporations like banks, eBay, credit card companies, and utility companies. They claim that you must respond to their message by clicking on a link in the email in order to confirm a transaction, to investigate fraud on your account, or to keep your account from being cancelled. The emails can be very convincing and will include logos and seemingly authentic data. The links then lead users to spoofed phishing web sites that are rigged to steal personal data from the consumer.

Top 10 Tips for Fighting Spam

You can protect yourself from spam in email and instant messages by following these tips.

1. **Install a comprehensive PC security package** and keep it up to date. An email filter and PC spam blocking software are absolutely critical. The McAfee® SecurityCenter lets you enjoy a worry-free Internet experience by protecting your identity, by eliminating viruses, spyware, email scams, hackers and online predators, and by providing automated back up for important files. A firewall monitors PC activity and prevents Trojans from installing on your computer.

2. **Protect your email address and instant message ID**. Do not post them on newsgroups, chat rooms, web sites, blogs, social networking sites such as MySpace, or online service directories. Try setting up two email addresses, one for real use and one for newsgroups and chats. You should understand privacy policies and forms, and use opt-out options.

3. **Use great caution when opening attachments** on your PC, PDA, or wireless device. Configure your anti-virus software to automatically scan all email and instant message attachments. Make sure your email program doesn't automatically open attachments or automatically render graphics, and ensure that the preview pane is turned off. Refer to your program's safety options or preferences menu for instructions. Never open unsolicited business emails, or attachments that you're not expecting—even from people you know.

4. **Educate your kids not to fill out online surveys, or register for contests or fan clubs**. If they want to become a member of a legitimate site such as Nickelodeon or Cartoon Network, have them come to you first so you can read the site's privacy policy.

5. **Watch out for phishing scams**. Don't click on links in emails or instant messages. Instead, open a separate web browser and visit the site directly. You can also verify that an email is legitimate by calling the business directly.

6. **Use an Internet service provider (ISP) that implements strong security**, such as anti-spam and anti-phishing procedures.

7. **Do not reply to spam**. Even replying to spam to unsubscribe could set you up for more spam. Never send your credit card information, Social Security number, and other private information via email or instant message.

8. **Create a complex email address**. This makes it more difficult for hackers to auto-generate your email, or target your email for other types of attacks. Try to use letters, numbers, and other characters in a unique combination. Substitute numbers for letters when you can. A sample complex email is *Tracy3Socc3r2@samplemail.com*.

9. **Create smart and strong passwords that are difficult for hackers to crack**. Try incorporating capital letters, numbers, special characters and using more than six characters. An example of a strong password is Go1dM!n3.

10. **Never enter your personal information in a pop-up**. Sometimes a phisher will direct you to a real company's web site, but then an unauthorized pop-up created by the scammer will appear, with blanks in which to provide your personal information. If you fill it in, your information will go to the phisher. The pop-up blocker in the McAfee SecurityCenter helps prevent this type of phishing attack.

McAfee
227 Bath Road
Slough, SL1 5PP
United Kingdom
+44.1753.217.500
www.mcafee.com