

Email Box Overload? Guidelines and Tips by Gary J Slager

Do you receive junk email messages from people you don't know? Most email users find unsolicited commercial email, known as "spam", annoying and time consuming.

How did they get your email address? Typically, an email spammer buys a list of email addresses from a list broker, who compiles it by "harvesting" addresses from the Internet. If your email address appears in a newsgroup posting, on a website, in a chat room, or in an online service's membership directory, it may find its way onto these lists. The marketer then uses special software that can send thousands - even millions - of email messages to the addresses at the click of a mouse.

The FTC conducted a test investigation and determined that 86 percent of new undercover email addresses posted to a variety of web pages received spam. It didn't matter where the addresses were posted on the page: if the address had the "@" sign in it, it drew spam. Chat rooms are virtual magnets for harvesting software, with postings to a chat room, spam is often sent just minutes after it is posted.

Here are 15 guidelines and tips on how to reduce the amount of Spam you receive.

1. Best tip - when you do receive spam, just delete it.
2. Do not buy anything from an unsolicited email offer.
3. Never respond to the "Remove" or "Unsubscribe" offer in spam. Often these instructions on how to "remove yourself from our list" are nothing more than another tactic to get you to respond. Usually they not work. Why is this? Basically, because of what many call "rule #1": Spammers Lie. Responding to "Remove" just let's the spammer know that your mailbox does work and its contents are read. The spammer can then send you more spam, and sell your address to other spammers, allowing the spammer to make money off you even if you don't buy anything.
4. Never respond to mail chain letters, even if you apparently got the mail from someone you know. Spammers (and sometimes hackers) utilize chain mail to collect the addresses of dozens of people who know each other. These messages can gradually accumulate large numbers of addresses, and spammers only have to come across one copy to get every address of the people who handled that message.
5. Only send mail to people you know. If you are replying to a piece of mail from a friend, delete any Cc'ed addresses that you don't know from that mail when replying. Also be aware that a piece of mail may say that it is from a friend, but look at the e-mail address carefully and make sure that any reply you make will really be going to where you think it should go.
6. Select strong passwords for your Internet accounts. Never use a password that consists of the account name, any part of your name or family member name or any number that is related to any personal information that someone could determine by crosschecking public databases. Also, do not use dates for passwords that are part of public records.
7. Change your Internet account passwords at least once a year. If you have multiple accounts or multiple sites that you visit where you must enter a password, avoid using the same password at all of them.

8. Use a unique email address, containing both letters and numbers. Your choice of email address may affect the amount of spam you receive because some spammers use "dictionary attacks" to email many possible name combinations at large ISPs or email services, hoping to find a valid address. For example, JSMITH is always going to get more spam than JZ6SMITH.
9. Change your mailbox address from time to time, particularly if there is a sudden increase in spam coming to that mailbox. For businesses, changing addresses may not be practical, but for individuals it is usually not too much trouble to tell your friends that your mail address has changed.
10. Avoid displaying your email address in public. That includes newsgroup postings, chat rooms, websites or in an online service's membership directory. You may want to opt out of member directories for your online services; spammers may use them to harvest addresses.
11. If you have a web site, you can reduce spam by avoiding putting your e-mail address anywhere on any web page, because spammers use automated software to search web pages for e-mail addresses. You can conceal addresses on web pages and in other publicly visible messages from these address harvesting programs simply by not using @ in the address. Instead, use " at " as in "j6mith at myisp.net". A human who reads your web site will figure out how to send you mail if they really want to. The spammers software that scans your web site won't even realize that "j6mith at myisp.net" was a mail address. Another trick is to use a graphical image of the @ sign instead of the actual font character.
12. Consider "masking" your email address. Masking involves putting a word or phrase in your email address so that it will trick a harvesting computer program, but not a person. For example, if your email address is "johndoe@myisp.com," you could mask it as "johndoe@spamaway.myisp.com."
13. Set up disposable email addresses. Decide if you want to use two email addresses - one for personal messages and one for posting in public. Consider using a disposable email address service that creates separate email addresses that forwards to your permanent account. If one of the disposable addresses begins to receive spam, you can shut it off without affecting your permanent address.
14. Use an email filter. Check your email account to see if it provides a tool to filter out potential spam or a way to channel spam into a bulk email folder.
15. In the software you use to read mail, disable any included features like Active-X, Java, Javascript, automatic URL fetching, auto-preload and anything else that will run programs or access web sites based on instructions contained in the mail you receive. Do not use preview windows. Not only can these immediately alert the spammer that you have read the mail, these "features" of your mail program can install viruses and other undesired software on your computer.

Remember the best tip - when you do receive spam, don't even preview it - just delete it. ■