E-mail Spam

Email spam, also known as junk email, is unsolicited bulk messages sent through email. The use of spam has been growing in popularity since the early 1990s and is a problem faced by most email users. Recipients of spam often have had their email addresses obtained by spambots, which are automated programs that crawl the internet looking for email addresses. Spammers use spambots to create email distribution lists. A spammer typically sends an email to millions of email addresses, with the expectation that only a small number will respond or interact with the message.

5 Simple Ways You Can Fight Spam and Protect Yourself

Electronic mail or Email is one of the easiest and most convenient channels where we can transfer information and share data with others. However, it is also common to receive information or emails that contain malicious attachments or dubious messages. Some email service providers filter and mark such dubious emails with the word “SPAM” in the subject of the email, indicating to the recipient that the email is either a junk email or unsolicited email with dubious content sent to numerous recipients by the sender. Clicking on links in such spam email may direct the recipient to phishing web sites or sites that download malware to the victim’s computer.

- **Never give out or post your email address publicly**

You should remember that everyone can easily access the Internet. That means, spammers are also lurking on the Internet and are constantly seeking available email addresses which they will send spam emails to. Posting your email address publicly allows others to send spam emails to you, or worse, hack your account if you are using a weak password.

- **Think before you click**

There might be instances where your email service providers’ automated email filter mistakenly mark legitimate emails as spam email due to its content (e.g. the email contains a hyperlink). However, in most cases, emails marked as “SPAM” or redirected to the spam folder of your mailbox are sent by spammers. Subject of spam messages

usually include offer of cheap prescription drugs, advertisements on new medicines, and status of packages from shipping companies. Make sure that you scrutinize the content of spam emails before opening any attachments (even if it looks like an innocent text or image file) or clicking on hyperlinks. Refrain from downloading contents blocked by your email service providers in such emails too.

- **Do not reply to spam messages**

Almost all spam messages are malicious emails sent by unknown sources. These sources could be hackers who aim to hack into the computers of their victims. Never respond to spam messages because through this, the spammer will know that the email address is active and thus, it increases the chance of your email to be constantly targeted by the spammer.

- **Download spam filtering tools and anti-virus software**

Spam filtering tools and anti-virus software can help to scan the emails that you received for malware. If the emails that you received contain malware, the malicious content would be quarantined and you would be prevented from opening it. This helps to alleviate the chance of emails containing malware from infecting your computer. As such, do select spam filtering tools and anti-virus software with such features to reduce your woes of having to decipher email contents.

- **Avoid using your personal or business email address**

Do not use your personal or business email address when registering in any online contest or service such as applications, deal updates, etc. Many spammers watch these groups or emailing lists to harvest new email addresses.

References:

- https://searchsecurity.techtarget.com/definition/spam
- https://en.wikipedia.org/wiki/Email_spam
- https://www.csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/5-simple-ways-you-can-fight-spam-and-protect-yourself