Spam Email I

Spam refers to the sending of bulk electronic messages through public networks, regardless of whether the recipients have given any consent to receive the messages or even after the recipients have requested not to receive such messages. The messages can be in form of email, fax, SMS or MMS etc. As spam covers a wide scope, here we would only introduce "Spam Emails" which is most related to computer.

"Spam Email" is about the sending of bulk electronic mails to promote products and services or to spread malicious code such as computer virus. Spammers hope that recipients will be interested in the products or messages in the emails, and reply to the emails.

How To Identify Spam Email?

If an email has one or more of the following characteristics, it will probably be a spam email:

● Information about the sender or organisation is not clearly and accurately listed in the email.

● Subject of commercial email is unclear or misleading.

● Neither unsubscribe option nor unsubscribe facility statement are provided in the email.

● Contents of the email are the same as or similar to those of other emails received.

How Do Spammers Collect Email Addresses?

Many organisations publish business email addresses on their websites. This will facilitate spammers to collect these email addresses for the spam email list. These organisations are at a risk of being attacked by spam.

Spammers generally make use of specific software to scan messages from online forums or newsgroups to harvest email address list, and to search for email addresses on websites in order to create a spam mailing list.

Potential Threats

A large quantity of spam emails do not only annoy the recipients, but also waste bandwidth of networks and hard disk capacity, resulting in substantial money and time required to handle them.

Spam emails are also channels of spreading malicious code or computer virus. If the spam email contains an attachment that is infected by malicious code or computer virus, recipient's computer may also be infected after the spam email or the attachment is opened. The recipient's email account will then be controlled by the spammer. The malicious code may send spam emails containing virus-infected attachments to the email addresses in the address book at the affected computer to spread out the computer virus.

To learn more about information security, please visit the InfoSec website at: http://www.infosec.gov.hk