

Email Security

1. What are the negative impacts of spam email on the Internet Community?

Every time someone sends out a spam email, the entire Internet community bears the cost, not just the recipients and the ISPs at the receiving end. Some Internet users are charged according to connection time, and spam email forces people to spend extra time online, costing them for downloading unwanted spam messages.

Spam is of course disruptive for email users, wasting their time, and ultimately making email less convenient and useful as the amount of spam continues to grow. Spam email ties up bandwidth and resources on computers and routers all over the Internet. Every unwanted email message adds to the total cost of operating the networks of computers that form the paths of delivery to recipients. Spam email can disrupt a network by crashing mail servers and filling up hard drives. It also constitutes an invasion of the online privacy of Internet users.

2. How do spammers obtain my email address?

Spammers seek out potential lists of targets by scanning online forums, newsgroup postings, stealing mailing lists from other sites or users, or searching websites and Internet Relay Chat sites for email addresses. The gathering such information is facilitated by automated software packages or robots, designed for spam searching across different Internet service environments. As bandwidth costs get cheaper, some spammers are using a tactic called the "dictionary attack", by which emails are sent to guessed email addresses drawn from words in the dictionary. Again, this can also be done with automated software.

3. Should I complain or reply to a spammer in order to get my email address removed from a spam email list?

Do not reply or complain by simply clicking the reply button. Most likely, the reply address is forged. If you reply to that email address, or to the ISP that provides the spammer's email address, you are more than likely being tricked by the spammer into

wasting your time (and the victim ISP's time) by complaining to the wrong party. Seek help from your ISP if you want to find out the real person sending you spam emails.

Unless you are confident that the organisation sending out the spam email is trustworthy, do not send any unsubscribe request. It is more than likely that such a request will be either ignored or worse, used as a confirmation that your email address is valid and operational, exposing you to yet more spam in the future.

4. Is there any software that can help me to block or screen out spam emails on the user side?

Yes. One of the most effective ways to control spam emails is to use protective software known as filters. While you cannot stop people from sending spam emails to you with anti-spam filters, you can stop the messages from showing up in your inbox and have them deleted automatically. Filters allow you to easily block any email messages carrying specified addresses, domains, subjects, or text from entering your inbox. Some popular email programmes already offer spam-filtering features. A number of separate filtering tools that work with popular email packages are also available on the market. However, filters may sometimes fail to identify spam emails, or (less likely) classify legitimate emails as spam messages.

5. Is there a way for me to lodge a complaint if I receive spam emails?

If you suspect that someone is selling or using harvested address lists, you should report it to the Office of the Telecommunications Authority (OFTA). OFTA will investigate and may prosecute the seller or user. If your computer has been hacked and exploited by someone sending out spam emails, you should also report the incident to OFTA. OFTA will collate reports and may transfer the case to the Hong Kong Police where applicable.

If you suspect that the sender is contravening any rules for sending commercial electronic messages, again you may report this to OFTA.

6. What is a third party relay email server?

A third party mail relay is an email server receiving email from an unknown sender and then sending it on to one or more recipients that are not users of that email system. Some email systems enable this relay feature by default after installation. Taking into account the large number of mail servers that exist on the Internet, this is still a considerable number of servers that allow mail relay.

Spammers are able to simply collect lists of third party mail relays on the Internet using automated scanning programs. Once they have some lists, spammers can configure their spamming tool with the relay's address, so it obscures their identity from recipients and places the burden of the work on an email server that is not their own, so they don't worry about overloading or crashing it.

7. How do the Internet Service Providers (ISPs) in Hong Kong react on the issue of email spamming?

Almost all ISPs operating in Hong Kong have included in their service agreements provisions to prohibit users from abusing their services for the purpose of email spamming. Spammers face warnings or even suspension or termination of services with forewarnings if they persist.

Furthermore, many ISPs commonly adopt a number of technical measures to combat the spamming problem. For example, their email servers may refuse to transmit emails not composed by the sender (such as rejecting to forward an email received by the subscriber to the third party); or they may maintain a blacklist of known bad email servers (i.e. they reject to receive and forward emails sent from blacklisted servers); or they may limit the quantity of emails sent from prepaid accounts.