

電子郵件保安

1. 濫發電郵對互聯網社群有什麼負面影響？

每當濫發電郵者發出垃圾電郵，整個互聯網社群均需付出代價，尤其以收件人和接收一方的互聯網服務供應商損失最大。有些互聯網用戶是按聯網時間繳費，所以下載無用的垃圾電郵令他們耗用額外的時間和聯網費用。

垃圾電郵浪費收件人時間，對電郵用戶造成滋擾。假如垃圾電郵的數量繼續增加，最終會令電郵作為便利溝通工具的好處大打折扣。此外，濫發電郵亦會佔用分布在互聯網上的電腦和路由器的帶寬和資源。每個無用的電郵訊息都會增加傳送和接收該訊息的電腦網絡的操作成本。濫發電郵會破壞電郵伺服器 and 佔用硬碟空間，從而擾亂網絡，並侵犯互聯網用戶的私隱。

2. 濫發電郵者如何獲得我的電郵地址？

濫發電郵者可藉掃描網上討論區及新聞組張貼的信息、從別人處盜取郵址名單、搜尋網站或網上聊天（Internet Relay Chat）網址所載的電郵地址，從而建立潛在目標名單。透過專門設計用以在不同的互聯網服務環境濫發電郵的自動套裝軟件及機器人(robots)，濫發電郵者可輕易取得這些資料。隨著帶寬的成本降低，有些濫發電郵者現採用一種稱為「字典攻擊」的技倆，發送電郵給猜測的電郵地址。此方法同樣是借助自動化軟件進行。

3. 我應否向濫發電郵者作出投訴或回覆，以期把我的電郵地址從濫發電郵名單中剔除？

切勿隨便按回覆鍵作回覆或投訴。垃圾郵件所附的回郵地址多屬虛構，如你向該址或提供該址的服務供應商回覆，有很大機會你會受濫發電郵者欺騙，把投訴送到錯誤的地方，徒然浪費時間（包括受影響的服務供應商的時間）。如要找出濫發電郵者的真正身分，可向你的互聯網服務供應商求助。

除非你確信濫發電郵的組織是可靠的，否則不要向他們發出要求他們刪除你的電郵地址的電郵。這樣的要求多數會被置諸不理，更嚴重的是這會證實你的電郵地址是真確的，從而促使濫發電郵者未來發送更多電郵給你。

4. 有沒有任何軟件在用戶的層面上能協助我阻截或篩選濫發電郵？

有，控制濫發電郵最有效的一個方法是採用稱為過濾裝置的保護軟件。雖然你不能以過濾裝置阻止別人向你濫發電郵，但卻可阻止那些信息在你的電子信箱出現，並可將該信息自動刪除。過濾裝置使你輕易阻截任何具指定地址、域名、題目或正文的電郵信息儲存到你的收件夾內。有些廣為使用的電郵軟件已內設過濾功能。一些可配合常用電郵軟件使用的獨立過濾工具可在市面找到。不過，過濾裝置有時未必能辨別垃圾電郵，又或（雖然機會很微）會把正當電郵誤認為垃圾電郵。

5. 如果我收到濫發電郵，是否有途徑讓我作出投訴？

如果你懷疑有人出售或使用地址收集清單，你應該向電訊管理局(Office of the Telecommunication Authority; OFTA)舉報。電訊管理局會進行調查，並可能會起訴賣方或用戶。如果你的電腦已經被駭客入侵，並被人利用發送濫發電郵，你也應向電訊管理局舉報。電訊管理局會整理報告，並可能把個案移交香港警方處理。

如果你懷疑寄件者違反任何發送商業電子訊息的規則，你可以向電訊管理局作出投訴。

6. 甚麼是第三者電子郵件驛遞伺服器？

第三者郵件驛遞指一個電郵伺服器從不知名寄件者接收郵件後，再把它們發送到一個或多個不屬於該電郵系統用戶的收件者。部分電郵系統在安裝時會預設啟動這個轉發功能。考慮到互聯網上電郵伺服器的龐大數量，容許郵件轉發的電郵伺服器數量仍是相當多的。

電郵濫發者可以透過一些掃描程式，簡單地從互聯網上收集第三者郵件驛遞名單。有了這些名單，電郵濫發者便可為濫發工具設定轉發郵址，向收件者隱藏身分，並把有關的沉重工作轉嫁到他們無需擔心負荷過重或當機的電郵伺服器上。

7. 香港的互聯網服務供應商怎樣應付濫發電郵問題？

幾乎所有在香港的互聯網服務供應商均在其服務協議書上訂明禁止用戶濫用其服務來濫發電郵。電郵濫發者將要面對警告，甚至預先警告暫停或終止服務。

此外，互聯網服務供應商通常會採取技術措施來對付濫發電郵問題。例如，他們的電郵

伺服器或會拒絕傳輸那些並非由寄件者撰寫的電子郵件（好像拒絕把服務訂戶所收到的電郵轉寄給第三者）；又或整理出一份電郵伺服器黑名單（即拒絕接收從黑名單上伺服器所發出的電子郵件）；又或限制那些預先繳費戶口發送電郵的數量。