如何杜绝垃圾邮件的“入侵”

◎胡光能

随着互联网技术的快速发展，电子邮件应运而生。时至今日，电子邮件逐渐成为最为便捷的通信手段之一，它极大地改变了人们的交流方式，然而随之而来的垃圾邮件却像瘟疫一样蔓延，给网络安全造成了极大的威胁。

垃圾邮件的困扰

电子邮件于20世纪70年代被发明，之后随着个人电脑的兴起而得以传播。20世纪90年代，互联网浏览器的诞生进一步促进了电子邮件的发展。电子邮件不仅可以用于进行文字的交流，声音、图像等各种信息的传输同样也不在话下。

垃圾邮件，英文名为Spam，它呈现出无孔不入的特征，全球垃圾邮件甚至已超过邮件总数的50%。你也许时常会遭遇这样的尴尬：打开邮箱，里面却充斥着众多来历不明的垃圾邮件，繁琐的删除过程会极大的影响我们对有用邮件的甄选。之所以会出现这种情况，与邮件的收发特征不无关系。只要知道他人的邮箱地址，任何人都可以便捷地向他人发送电子邮件。一旦这种自由为某些人蓄意利用，电子邮箱便会成为他们制造垃圾邮件的工具，恶性的垃圾邮件甚至会包含欺诈性的信息和木马病毒，造成信息安全隐患。

向垃圾邮件全面宣战

为拦截排山倒海般的垃圾邮件，还邮箱一片净土，由邮箱用户和网络服务商发起的反垃圾邮件大战已全面展开。

邮箱是个人进行信息交流的工具，网络生活中要注意隐藏自己的邮箱地址，切忌随意在网络上发布。如确实需要，可将邮件地址嵌入在图片上，而不是纯文本的格式，这样恶意的邮件地址采集器便无法识别。

此外，垃圾邮件中往往还潜伏着窃取个人信息的木马病毒，因此千万不能随意点击垃圾邮件中的任何链接。对付这类垃圾邮件，最有效的方法就是将其删除并将发件人拉入黑名单。说到黑名单，每当系统检测到从黑名单发出的邮件时，就会自动将其移入垃圾箱。相应的，白名单就是你愿意接收邮件的邮箱地址。

除黑白名单设置，使用关键字过滤功能也是一种行之有效的方法。垃圾邮件的主题和正文中通常含有诸如“发票”“价格”“抢购”“订购热线”等关键词，而通过关键词过滤功能便能有效地将其中大部分的垃圾邮件拦截掉。

近年来，智能便捷的客户端软件逐步兴起，“贝叶斯过滤”等反垃圾邮件技术也在反垃圾邮件大战中大展身手。“贝叶斯过滤”是一种具有“自我学习”能力的智能技术，它能够根据对更多垃圾邮件的分析，不断调整对垃圾邮件的定义，从而提高对垃圾邮件的命中率。含“抵押”一词的邮件多半会被系统归类为垃圾邮件，但对金融类公司而言却极有可能是正常的业务邮件，因此对过滤器的判断进行人工干预十分必要。“贝叶斯过滤”对垃圾邮件的辨别不单可以由系统自动进行，还可以由用户自己对接收邮件进行手动操作，从而使过滤器也不断地获得自我更新，“学习”并“理解”用户对邮件的偏好，对垃圾邮件的判断更精确、更智能。设计优良的贝叶斯过滤器，可以识别99.7%以上的垃圾邮件，而且误判率极低，是目前最有效的反垃圾邮件技术。

“邮件炸弹”

在邮件使用的过程中，要慎用慎用邮箱的“自动回信”功能，一旦收发件人都同时启用此功能，便极有可能因双方均未及时查收邮件而陷入“自动回信”的恶性循环之中，导致短时间内邮箱受到几百、几千甚至上万封垃圾邮件的“突袭”，造成邮箱达到容量上限而引起使用功能异常，因超负荷而“爆炸身亡”。尽管有些邮件系统对此采用了预防措施，并且“邮件炸弹”的威力并不如想象中的大，不过一旦这个漏洞为不法分子利用，也会造成难以挽回的后果。

将垃圾邮件“绳之以法”

垃圾邮件是对能源和网络资源的极大浪费。美国是反垃圾邮件的先驱者，自20世纪90年代开始，美国便开始通过立法加强对垃圾邮件的控制。我国于2005年审议通过了《互联网电子邮件服务管理办法》，对规范互联网电子邮件服务做了具体的规定，同时也增设了互联网电子邮件举报受理中心等反垃圾邮件专设机构。

防范垃圾邮件是邮件使用者和垃圾邮件制造者双方之间的博弈过程，需要用户、邮件服务商和国家网络监管者在日常使用和技术层面上共同协作。与此同时，对垃圾邮件的治理、监管和处罚措施也必不可少。只有这样，才能让垃圾邮件无处遁形、无路可逃！