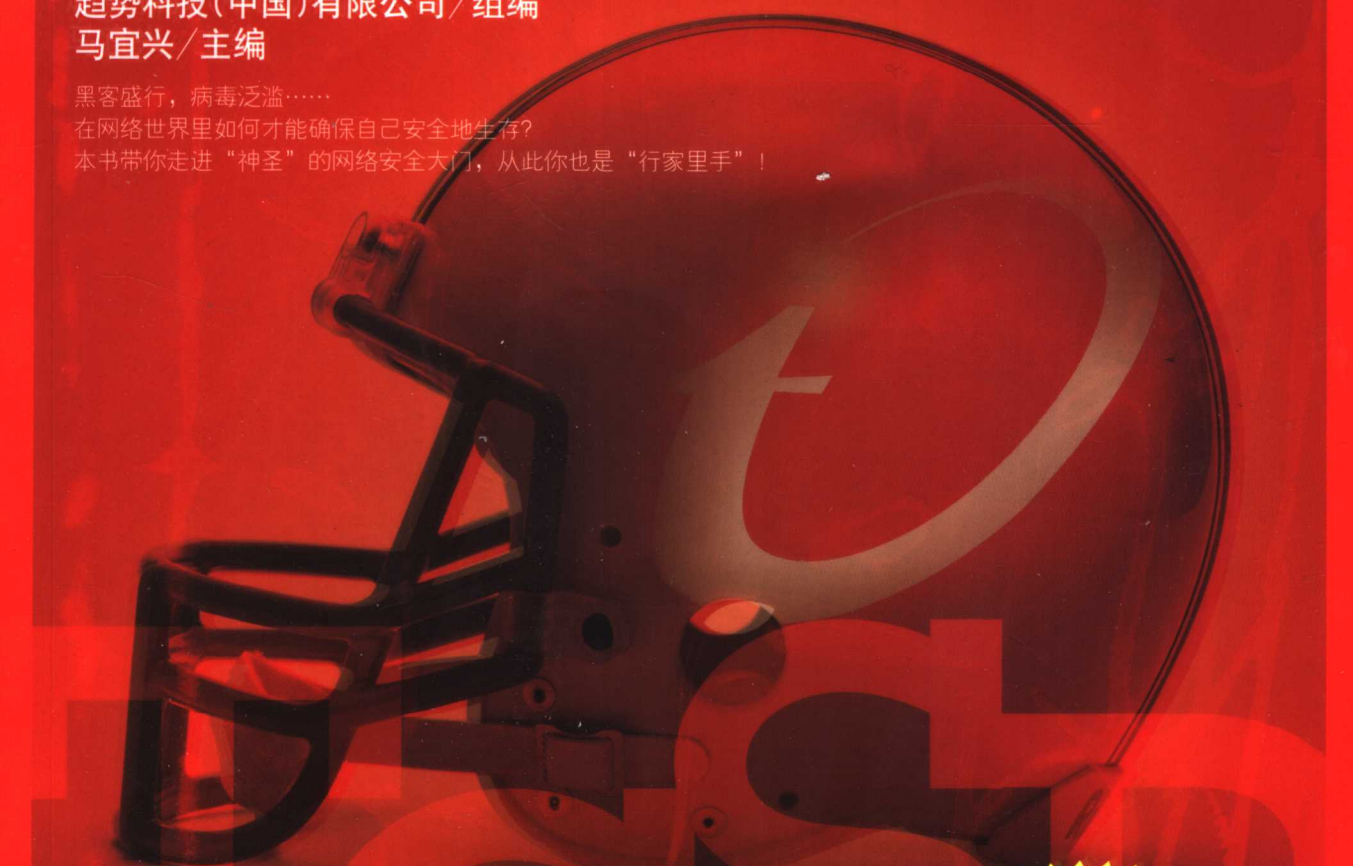
TREND MICRO™ 趋势科技认证信息安全专员(TCSP)教材

网络安全与病毒防范（第二版）

趋势科技(中国)有限公司／组编
马宜兴／主编

黑客盛行，病毒泛滥……
在网络世界里如何才能确保自己安全地生存？
本书带你走进“神圣”的网络安全大门，从此你也是“行家里手”！



随书赠送PC-Cillin2005
单机版防毒软件

上海交通大学出版社

趋势科技认证信息安全专员(TCSP)教材

网络安全与病毒防范

(第二版)

趋势科技(中国)有限公司　组编
马宜兴　主编

上海交通大学出版社

内 容 提 要

本书是 TCSE 初级认证课程的培训教材，全书共分两篇。第一篇：网络安全基础，就当前网络安全的现状进行了分析，并就常见的网络安全防范技术和产品展开了描述，同时阐述了构建企业安全网络的过程和策略，以帮助初学者轻松跨入网络安全领域的大门，对于长期从事网络安全工作的人士也将大有裨益；第二篇：病毒、恶意代码和垃圾邮件，深入阐述了病毒的相关知识，所谓知己知彼，百战不殆，通过这部分内容的学习，读者能够全面了解病毒的特征和应对方法；同时，第二篇还为用户分析了当前企业防毒技术的现状，介绍了当前防毒领域最先进的安全防护策略，以帮助用户建立最新的防毒观念。

图书在版编目(CIP)数据

网络安全与病毒防范 / 马宜兴主编 . －2 版 .—上海：上海交通大学出版社，2005
ISBN 7－313－03665－5

Ⅰ. 网… Ⅱ. 马… Ⅲ. ①计算机网络－安全技术 ②计算机病毒－防治 Ⅳ. ①TP393.08②TP309.5

中国版本图书馆 CIP 数据核字(2004)第 019245 号

网络安全与病毒防范
(第二版)
马宜兴 主编
上海交通大学出版社出版发行
(上海市番禺路 877 号 邮政编码 200030)
电话：64071208 出版人：张天蔚
上海市崇明县裕安印刷厂印刷 全国新华书店经销
开本：787mm×1092mm 1/16 印张：14.75 字数：355 千字
2004 年 4 月第 1 版 2005 年 7 月第 2 版 2005 年 7 月第 3 次印刷
印数：8 101－13 150
ISBN7－313－03665－5/TP·586 定价：31.00 元

序一

安全政策新观点

安全是个长久以来的老观念，相信没有任何一个企业或单位会认为它不重要。不管是实体上的安全、思想上的安全，或是维持企业持续经营成长的安全问题，均是企业营运的关键。

今天，从信息技术的角度来说，“网络就是计算机”已经不再是SUN公司几年前提出的商业口号，而是发生在大多数人每天生活中的现象。从前计算机提供的运算能力（computing power）的角色已经被“沟通（communication）”所取代。今天大多数买计算机的人，都是为了上网或发送电子邮件，和朋友、同事等互通信息。一台没有连上网络的计算机，似乎已经不具有太多的价值了。

随着计算机网络化的普及，网络的安全也随之上升到了一个相当重要的程度。换言之，没有好的安全管理机制，网络的发展与运用也将受到极大的影响，甚至面临不可预知的危机。对于众多的企业来说，网络已经是每天营运活动中不可或缺的一部分了。而内部网络和外部网络之间的界线，也越来越模糊。企业必须要借助网络，不断地和客户、供货商、合作伙伴等作沟通及交流。一旦网络停摆，对于企业可能造成的损失，是相当惊人的。网络的安全和其他的安全问题有时候更是无法分割的。例如，愈来愈多的罪犯，利用网络的相关技术，进行财务上的诈骗、偷盗等犯罪行为；而在“9·11”事件这样的恐怖攻击，或是网络上的全球感染攻击中，唯有能够继续运作的企业，才能持续不断地提供产品及服务给他们的客户，维持客户的忠诚度，而不让客户投向竞争者。事实上，企业的持续及稳定运作，已经成为竞争力极其重要的一环了。尤其在全球化的浪潮下，委外制造、共同开发等各种合作方兴未艾，各国企业之间往来频繁，互相依赖的程度极深。当企业在选择合作伙伴时，能不受安全事件的影响，持续及稳定运作，成为考虑的必要条件。

在这样的状况下，越来越多的企业开始思考如何更广泛地提升营运安全。从一次又一次的攻击事件中，人们渐渐地了解到，单单对攻击做出响应，是不足以有效地防止攻击的，因为响应的时间往往太晚，灾害早已发生。在几千年前，中国的黄帝内经就已经提到：“圣人不治已病治未病，不治已乱治未乱……夫病已成而后药之，乱已成而后治之，譬犹渴而穿井，斗而铸锥，不亦晚乎。”许多人都有这样的想法，因此，

有些人致力于预测未来可能发生的攻击或灾害，作为现在行动的依据，但效果并不好。在“9·11”事件之前，有谁曾经想到，恐怖分子会挟持民航机，作为攻击的工具呢？因此，“预测未来”并非真正有效。相对地，建立一套“早期预警”系统（early warning system）以防患于未然，才是比较有效的一种方法。

Gartner Group 顾问 McGee 最近在其新作 Heads Up 中提到一个相当不错的观念，认为我们无法真正预防未知的危险，只能尽力做好“预测现在（predict the present）”。作者认为出其不意的事件（surprise events），是因为未能及时察觉早期的警讯，进而做出回应。灾害的发生，常常看起来很突然，但事实上是有迹可循的。通过一套系统的方法，持续地搜集、分析、监控企业营运的各项指标，从各项细微变化中查出各种可能危害企业经营的蛛丝马迹，以达到早期预警的效果，才是防止灾害的有效方式。作者建议首先应该分析应该实时监控哪些信息，并将整个过程分为辨认（identification）以及验证（justification）两个阶段。“辨认”指的是辨认可能会导致灾害的各种相关事件，并订定指标及决定优先级。而“验证”则是指标的筛选。决定了需要分析的信息之后，时时监控这些指标的变化，并实时报告给适当的人员来做响应。作者并建议由最高管理层主导，将及时监控的系统扩展部署到整个企业中，并全面检查企业的流程，以改进企业做出回应的能力。

作者提出这些观念及做法，主要是用在灾害的早期发现以及早期防范。在网络的安全问题上，更是适合。现今的网络安全政策，通常只着重在应变响应，并未考虑到早期防范。因此，当攻击事件一再发生时，大多数的企业与机构，都无法有效地做出响应。大多数的时间及资源，就只好花在灾后的重建了。网络的普及增加了企业的便利性，但同时也增加了其脆弱性，在一个 e 化的企业中，我们相信建立严谨的监控管理机制更是当务之急，尤其是建立在体制的健全化、平时的诊断、实时且持续的监控。单纯的应变响应，恐怕完全不足以阻挡各式各样、日新月异的网络安全问题吧。

趋势科技全球副总裁
亚太区总裁
刘象雅
Raymond Liu

序二

安全认证时代的来临

随着全球数字经济一体化和信息化的来临，IT界及相关企业都面临着一个共同的问题——信息安全问题。日益泛滥的病毒和猖獗的黑客活动令大家十分头痛。与安全问题日趋突出，形势亦十分严峻形成对比的是训练有素的信息安全人才出现了严重短缺，信息安全人才的匮乏是一个不可回避的现实。据统计，76%以上的企业信息技术安全人才配备严重不足。信息安全无法得到充分有力的技术支持将使得企业陷入更大的威胁之中。

因此，在今天和未来的日子里，拥有扎实基础和丰富实战经验的安全专家和顾问人才将备受欢迎。近年来，网络安全业界的认证数量和种类上的急剧成长，其受欢迎程度大有超过网络和操作系统平台等传统认证项目的趋势，这也恰恰印证了安全人才需求在日益成长。安全认证已经成为时下一大迫切的社会需求。信息安全技术工程师在世界各国正在或即将成为一种新的职业。无论是企业、个人还是商家都期待着信息技术安全认证尤其防毒这一领域的空白能够迅速得到填补，对大量信息技术安全人才的涌现抱有深厚的期待。

趋势科技，作为网络安全软件及服务领域的全球领导者，其TCSE认证体系也受到了越来越多现代信息专业人士的青睐，为全球企业培养了大量的防毒专才。趋势对中国市场非常关注，在国内有着巨大的市场和研发投入，防病毒产品在中国市场份额也日益扩大。TCSE认证培训也在国内如火如荼地展开了，我们在国内已经拥有了ATA Learning（北京全美教育）、神州数码、上海信息化培训中心、网域科技以及众多国内知名高校等合作伙伴，迄今为止，已有超过1000名学员参加TCSE培训，为企业培养了大量的信息安全人才。

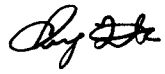
在此，我们非常高兴地迎来了本书的再版。本书注重实用，兼顾基础，较为系统

地介绍了网络安全领域的相关知识、怎样构筑安全有效的网络专业知识、最先进的病毒防范理念和技术。

与此同时，我想以我多年从事 IT 行业的经验告诉各位从事或有志从事信息安全技术工作的朋友们：信息安全的世界是永不停滞的,正如趋势科技企业文化中倡导的“change”，所以安全专家的学习需要不断的更新和不懈的努力。诚祝诸位学习愉快，共同迎接安全认证时代的来临。

趋势科技全球副总裁

郑奕立



序三

网络安全防护刻不容缓

我们正生活在一个网络时代，这是一个激动人心的时代，计算机网络技术的发展改变了人类所熟悉的生活形态与方式，电子邮件、WWW 服务、网上购物、在线娱乐等应用使得地球变得越来越小了，企业的发展也越来越依靠信息化作为助动力。但应该看到的是，随之而来的越来越多的安全隐患、网络攻击事件和病毒事件已经成为社会关注的焦点。面对日益复杂的黑客以及病毒攻击事件，架构一个全方位完整的防护体系已刻不容缓。这些工作需要专业的技术咨询服务和专业人员进行处理。于是，网络安全服务和网络安全人才成为了社会一大迫切的需求。

作为网络防毒与互联网内容安全软件及服务领域的全球领导者，趋势科技不仅以卓越的前瞻和技术革新能力提供优秀的安全产品，更注重为企业提供高品质的服务。同时，趋势科技视构筑安全的网络环境为己任，通过建立完善的教育培训体系，将怎样构筑安全有效的网络专业知识、最先进的病毒防范理念和技术提供给迫切需要的人士，帮助那些有志从事或正在从事网络安全工作的人士进一步提升网络安全知识，帮助企业培养迫切需要的网络安全人才是我们的一个重要目标。

趋势科技已经开始逐步在全国建立多家授权培训中心体系，通过与优秀的培训机构以及高等院校合作，推广趋势科技的 TCSE 认证。另外，通过已经开展并将一直持续的“病毒防范知识普及校园行活动”普及网络安全知识，为网络信息安全教育事业贡献一份力量。

趋势科技（中国）有限公司

总经理　吕理臣

2005 年 3 月

序四

时代需要网络安全人才

现今网络环境越来越复杂，网络入侵的危险性越来越大，特别是2003年的冲击波病毒，对全球众多电脑都造成了冲击，危害有目共睹。而每次病毒事件到来之所以能造成巨大的损失，都和计算机网络使用者安全意识薄弱以及安全知识匮乏有关。因此，掌握必要的病毒防范技术和网络安全知识是计算机使用者一项基本技能。企业更加关注黑客与病毒攻击带来的严重后果，在很多的企业中甚至设置了专门的网络安全相关职位，专业的网络安全职位渐已成为IT行业最热门的　职位。

目前，对专业的网络安全人才的培养已经引起了广泛的关注，很多知名的大学已经设置了信息安全专业，CIW、CISSP等非厂商中立性认证以及防火墙、入侵检测等安全厂商提供的技术认证越来越被众人所推崇。随着网络病毒的越发频繁的扰乱，反病毒技术已经向多层次、整体化发展，这就涉及如何在企业内构建完整的防毒体系问题。

作为防病毒领域领先厂商趋势科技开始逐步推广的TCSE认证培训及时地满足了广大企业的需求。通过与高等院校的合作，趋势科技直接将网络安全知识带给求知若渴的学生，以满足学子们对网络安全知识的需求，并将进一步促进网络安全知识在校园的普及。

国家“八六三计划”信息安全主题专家

上海交通大学信息安全工程学院副院长、教授

李建华

2005年3月

前　言

面对现今网络环境越来越复杂、网络入侵的危险性越来越多的现状，对于网络信息安全与防毒观念您是否一知半解？对于企业的防毒工程建置是否一筹莫展？完善的信息系统需建立在“安全”的机制上，通过信息安全专家系统的课程培训与技术认证，可以让用户在 IT 信息领域中建立“铁三角”的信息安全防护网；同时，也可以提升本身安全防护的价值。

作为防病毒及内容安全软件服务领域的全球领导者，趋势科技以卓越的前瞻和技术革新能力引导了从桌面防毒到网络服务器和网关防毒的潮流，同时也愿意将提高广大计算机网络使用者的安全意识和防范水平视作己任，趋势科技的信息安全专家认证课程就是针对这一需求开发的。

本书是 TCSE 初级认证课程的培训教材，全书共分两篇。第一篇：网络安全基础，就当前网络安全的现状进行了分析，并就常见的网络安全防范技术和产品展开了描述，同时阐述了构建企业安全网络的过程和策略，以帮助初学者轻松跨入网络安全领域的大门，对于长期从事网络安全工作的人士也将大有裨益；第二篇：病毒、恶意代码和垃圾邮件，深入阐述了病毒的相关知识，所谓知己知彼，百战不殆，通过这部分内容的学习，读者能够全面了解病毒的特征和应对方法；同时，在第二篇中，为用户分析了当前企业防毒技术的现状，给用户带来了企业防毒领域最先进的安全防护策略，帮助用户建立最新的防毒观念。

本书由趋势科技总部资深网络安全专家组成的培训团队组织开发，由几位在国内长期从事网络安全咨询和培训工作的专任培训讲师编辑成书。第二版在第一版的基础上增加了网络病毒、手机病毒等流行病毒的趋势分析。趋势科技资深病毒医生张志徐对有关病毒技术部分作了修改，增加了技术深度。全书由马宜兴任主编，陆亚灵、徐白负责整理和校稿，趋势科技中国服务事业部经理蔡昇钦对全书进行了审阅。

希望本书的出版能为广大有志从事网络安全事业或对网络安全感兴趣的人士提供一些有益的帮助。

本书的编写得到了上海交通大学出版社的大力支持，在此表示感谢！

由于时间仓促，谬误之处难免，还请广大学员和读者指正，如有疑问，你可以发送电子邮件到以下信箱：tcse@trendmicro.com.cn。

祝大家能愉快的学习并顺利的通过趋势科技信息安全专家认证。

编　者

2005 年 2 月

TCSE 认证之路

TCSE 简介

TCSE（Trend Certified Security Expert 趋势认证信息安全专家）是由趋势科技公司所推行的一项国际性信息安全专家的技术认证，取得 TCSE 证书即表示用户具备防毒专业知识、技能及对于趋势产品的了解与熟悉。趋势科技公司希望通过 TCSE 课程的训练与认证，将“如何建构有效的防毒环境”这项专业知识提供给迫切需要的现代信息专业人士。

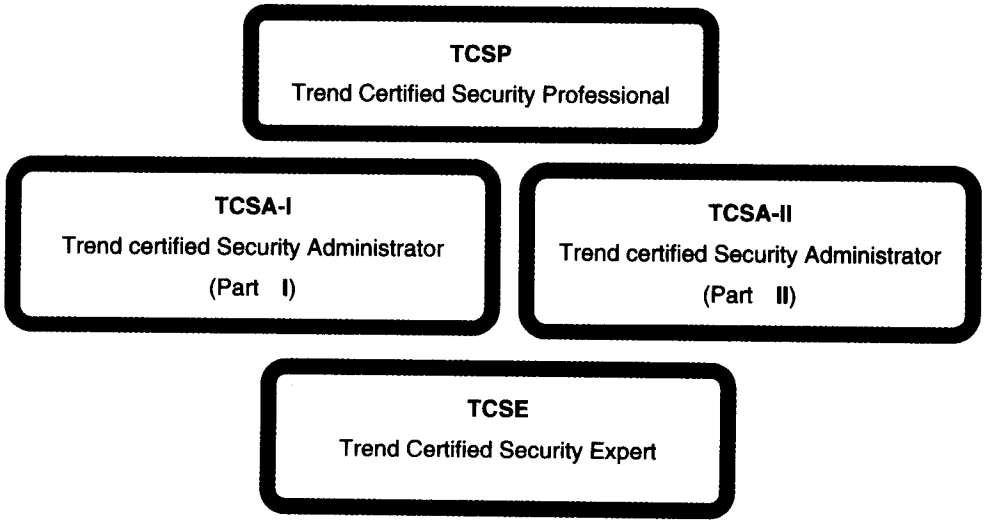
TCSE 认证之路

趋势科技认证共有 4 种认证类型，分为三个级别，每种认证都有对应的考试需要通过。进阶方法如下：

第一个级别的认证即 TCSP：TCSP (Trend Certified Security Professional)为基础认证，是获得 TCSA 认证的基本条件。

第二个级别的认证分两部分：TCSA- Ⅰ——Trend certified Security Administrator(Part Ⅰ) 和 TCSA- Ⅱ——Trend certified Security Administrator(Part Ⅱ)。

第三个级别的认证即 TCSE：获得 2 个 TCSA 认证后自动晋升为 TCSE 认证。



TCSP	趋势认证信息安全专员(Trend Certified Security Professional)
课程目的	建立网络信息安全观念，了解病毒的特性
适合对象	欲学习网络信息安全及防毒架构实务者，企业网络安全管理者或需要建置网络安全的系统维护者，具有网络架构的认知与了解
课程教材	趋势科技原版教材
课程内容	先修条件：对网络安全基础知识有兴趣的人士 * 网络安全技术基础（TNSE）：以分析计算机网络面临的安全威胁为起点，阐述常用的网络安全技术，介绍主流网络安全产品和常用网络安全策略 * 病毒防护与分析（VPA）：计算机病毒基础知识，病毒特征分析，病毒查杀技术 * 电脑病毒观念与企业防毒规划（Trend EPS）：介绍业界最先进的病毒防范理念及其实现技术

TCSA-I	趋势认证信息安全企业网络管理员(Trend Certified Security Administrator—Part I)
课程内容	* OSCE——企业工作站病毒防护知识与技能 * SPNT——企业服务器病毒防护知识与技能 * SMEX——企业群件服务器（针对 MS Exchange）病毒防护知识与技能 * SMLN——企业群件服务器（针对 IBM Lotus Notes）病毒防护知识与技能
课程教材	趋势科技原版教材

TCSA-II	趋势认证信息安全企业网络管理员(Trend Certified Security Administrator—Part II)
课程内容	* ISNT/Unix——介绍企业网关系统的安全防护， InterScan VirusWall for NT/Unix 安装及规划，提供企业防毒墙的机制 * IMSS——学习邮件网关防毒和内容过滤技术，延伸企业网络安全体系 * TMCM——介绍中央控管技术，TMCM 安装及规划，方便管理与设定所有的趋势防毒产品，病毒防范策略的实现，并可通过网络取得网络上整体的病毒分析与统计资料
课程教材	趋势科技原版教材

* 更多更新的信息可登录趋势科技的网站: http://www.trendmicro.com.cn/tcse。

如何报名？

趋势科技将在各地区建立授权培训中心，你可以到趋势科技的网站上进行查询，也可以来电咨询。

咨询电话：800-820-8876

E-mail：tcse@trendmicro.com.cn

课程综述

课程内容

本课程以分析计算机网络面临的安全威胁为起点，阐述了常用的网络安全技术，介绍了主流网络安全产品和常用网络安全策略，并着重强调内容安全（防病毒）在网络安全中的重要地位。随后，着重介绍了病毒及与病毒防护相关的知识，并就目前业界最先进的病毒防护理念展开了深入的说明。

本课程的内容分为三个部分，涉及以下几个方面：

- 计算机网络面临的安全威胁；
- 常用的计算机网络安全技术；
- 主要的网络安全产品类型；
- 企业网络安全策略；
- 病毒、恶意代码与垃圾邮件的基础知识；
- 计算机病毒的危害与防范措施；
- 病毒的发展趋势；
- 传统病毒防范技术的不足；
- 趋势科技企业防护战略。

课程目标

本课程的目标是提高学员的网络安全意识和病毒防范水平，使学员熟悉基本的网络安全理论知识和常用网络安全产品，了解部署整个网络安全的防护系统和策略的方法，尤其是病毒防护的相关策略。在此基础上，让学员充分了解病毒防范的重要性和艰巨性，了解“内部人员的不当使用”和“病毒”是整个网络系统中最难对付的两类安全问题。

主要涉及以下内容：

- 基本的网络弱点；
- 安全技术原理；
- 各类安全技术的产品及其实现方式；
- 内容安全（防病毒）的难度及在网络安全中日益重要的地位；
- 病毒防范技术和病毒防护体系的实施。

授课对象

本课程面向下列人员：

- IT 部门工作人员；
- 工程师；
- 对网络安全基础知识有兴趣的人士。

目录

第一篇　网络安全基础

第二篇 病毒、恶意代码和垃圾邮件