Web与无线
实用技术译丛

信息时代的个人安全策略

刷卡消费、ATM机取款、网上购物、在线股票交易……
你是否已经在享受信息时代带给你的这些便利了呢？
不过请注意，在进行这些活动的同时，你的个人信息
有可能会被网上的黑客所窃取。本书将告诉你如何防
范这类犯罪，保护你的信息安全。

(美) Teri Bidwell
Michael Cross
Ryan Russell
著

吴东升 杨战伟
廖 兰 贺 勇
译

科学出版社
www.sciencep.com

Web 与无线实用技术译丛

信息时代的个人安全策略

Teri Bidwell
（美） Michael Cross 著
Ryan Russel

吴东升 杨战伟
廖 兰 贺 勇 译

科学出版社

北 京

图字：01－2002－6693

内 容 简 介

本书系统地介绍了当今信息化社会中人们可能遇到的各种身份盗用问题，并给出针对这些安全隐患所应采取的措施。全书共分 8 章，分别介绍了身份盗用问题的概念及目前的状况、硬盘的保护、电子邮件的保护、上网过程中的保护、针对青少年的保护和监管以及一旦遭受损失时应该采取的措施等。

本书内容深入浅出，举例翔实，适合于各种知识层次专业和非专业人员使用。

图书在版编目（CIP）数据

信息时代的个人安全策略 / （美）比德韦尔（Bidwell，T.）等著；吴东升等译. —北京：科学出版社，2003
（Web 与无线实用技术译丛）
ISBN 7-03-011533-3

Ⅰ.信… Ⅱ.①比… ②吴… Ⅲ.电子计算机－安全技术
Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2003）第 039298 号

责任编辑：袁永康 / 责任校对：耿 耘
责任印制：吕春珉 / 封面制作：一克米工作室

科学出版社 出版
北京东黄城根北街16号
邮政编码:100717
http://www.sciencep.com
双青印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2003 年 6 月第 一 版 开本：787×1092 1/16
2003 年 6 月第一次印刷 印张：15
印数：1—4 000 字数：330 000

定价：28.00 元

（如有印装质量问题，我社负责调换〈环伟〉）

丛书序

十几年前，Internet 对平常人来说还是一个新生事物。如今，计算机网络技术飞速发展，其应用已经渗透到各行各业。网络通过信息交换来实现资源共享，不但能快速传输、集中和综合处理数据信息，而且也为我们提供了相当灵活的工作环境。网络技术已经成为经济发展的强大动力！网络正在改变人们的生活、学习和工作方式，提高人们的生活质量，推动社会的进步。要想在网络飞速发展的今天大展身手，就必须了解网络、掌握网络、应用网络！这套《**Web 与无线实用技术译丛**》正是为此而量身定做的！

从技术角度来说，这套丛书的内容涉及网络的构建、管理、安全与维护以及网络应用程序的开发，涵盖了计算机网络网络技术的各个方面，提供了全方位的网络技术教程和解决方案。从网络类型上来讲，这套丛书不仅以 Cisco 网络为例详细讲解了构建局域网技术的方方面面，而且对日益火爆的无线网络（无线局域网、无线 Internet 和蓝牙技术）作了深入的剖析。

Windows 2000 无疑是微软最为成功的一款操作系统，其网络特性也十分突出。而在网络的硬件方面，Cisco 也是一支独秀，其完整的产品结构及其产品本身的强大功能，使其成为网络设计中路由器和交换机的首选。如何将这两个领域中最优秀的产品结合起来，让这种组合发挥最大的潜能，是对网络体系结构设计师的挑战。有了《**在 Windows 2000 上构建 Cisco 网络**》，您就可以清楚地了解到何时、何种情况下应该使用何种硬件，以及该硬件如何与 Windows 2000 操作系统结合。

无线局域网（WLAN）技术的发展使人们摆脱了传统线缆的束缚，可以更方便、灵活、快捷地访问网络资源。无线局域网具有像以太网和令牌环这样的传统局域网的所有特性和优势，而且不受电缆连接的限制，实现了更大的自由和灵活性。由于便携式设备（例如笔记本电脑和 PDA）的普及，这些设备的使用者要求随处都能够使用网络，但却不需要“寻找”或“插拔”网线，这样的需求导致了对无线局域网络需求的不断增加。无线局域网适用于工矿企业、大专院校、科研院所、金融证券、商业网点，与 Internet 相连可实现数据信息的自动、高速且无地域限制的传输。《**构建 Cisco 无线局域网**》详细介绍了 Cisco 公司的基于 802.11 的产品，并且全面讲述了构建 Cisco 无线局域网的技术。虽然无线局域网的应用扩展了网络用户的自由，然而，这种同时也带来了新的挑战——网络安全性。本书详细介绍了各种形式的网络攻击以及相应的无线局域网各种级别的安全措施。当然，读者如果对网络安全尤为感兴趣，《**信息时代的个人安全策略**》当是首选。

当上网成为一种生活习惯，电子化成为一种生活方式时，我们的目光已从身边的真实世界转移到了一个虚拟的时空。从此我们的思维有了更广阔的飞翔天地，我们的交流再没有了障碍……但与此同时，以身份盗用为代表的信息化犯罪也与日俱增，对人们的信息安全构成了威胁。《**信息时代的个人安全策略**》对这个问题进行了深入的探讨，并从硬件、软件和用户自身等多个角度讨论了若干解决方案。

伴随无线技术的迅猛发展，客户端的移动设备也在快速地更新换代。作为 Web 管

理员，应该如何从容面对复杂形势愈演愈烈的场面？如何使自己的工作能真正为用户带来体贴的服务？如何使自己能够在发展空间巨大但同时竞争激烈的市场中站稳脚跟？《**无线网站管理实战**》从最基本的无线 Internet 构成，到移动设备的发展，为 Web 管理员提供了无线 Internet 方面的工具和技术，例如向现有的 Web 站点上添加无线 Internet 功能、构建新的无线应用，以及帮助管理员了解无线 Internet 解决方案的部署，并用实用而具体的示例做出详细解释及说明。

蓝牙是一种近程无线互联技术，它使笔记本电脑、移动电话和其他便携式设备及家用设备可以相互交换信息。蓝牙技术被美国《网络计算》杂志评为“十年来十大热门新技术”之一。业界人士预计，继 Internet、3G 移动通信之后，蓝牙技术热将席卷全球。这种新技术的“能量”何在？蓝牙技术能让各种电器之间密密麻麻的连线在您面前消失，蓝牙设备就像一款万能遥控器，将传统电子设备的一对一的连接变为一点对多点的连接。而且，这种连接无需复杂的软件支持。另外，蓝牙设备使用全球通行的、无需申请许可的 2.4GHz 频段，可进行实时数据和语音传输，而且有较高的传输质量（传输速率可达到 10Mbps，在支持 3 个语音频道的同时还支持高达 723.2Kbps 的数据传输速率）。2000 年，爱立信公司推出不必手拨的手机——R520 手机，这是第一次使用了蓝牙技术的手机和头戴式耳机，只要与该手机的距离保持在 10 米以内，您就能用耳机来接听和拨打电话。现在，已经有越来越多的蓝牙技术产品投放市场。《**蓝牙应用开发指南**》详细介绍了蓝牙技术以及在各种常用的操作系统上开发蓝牙应用产品的全过程，是蓝牙技术开发人员的必读书。

面对当今网络程序开发的挑战，最好有一种与语言和平台无关的开发方法，能让众多的单位和个人在使用已有硬件和应用程序的前提下享受到更多的网络服务，而且开发人员不必经过培训就可以进行更新。新出现的 XML Web 服务就可以将这样的设想变成现实，这是一种极具有潜力和应用前景的技术。《**使用 XML 开发.Net Web 服务**》意在介绍 XML Web 服务的最新知识，让读者顺利掌握开发 Web 服务的利器。

电子商务时代，企业经营的制胜关键在于强调速度和品质，如何善用信息系统提供即时管理信息以协助决策，将从订单到出货的业务流程全部自动化，是电子商务要解决的重要课题。企业的业务经营和内部管理需要各式各样不同的信息系统，通过网络提供应用软件租赁服务的应用服务提供商 ASP（Application Service Provider）便应运而生。《**应用服务提供商配置宝典**》全方位介绍了 ISP 如何成功转型为 ASP，从而使得 ISP 通过集成现有的基础结构实现向未来的技术无缝移植。

总之，技术领先、实用，结构完整、严谨，是我们引进这套书的重要依据；向读者朋友提供创作水平高、翻译质量好的热门图书，是我们的初衷；以书会友，书友互动，是我们的理念。我们热切希望广泛结识技术界、图书界以及社会各界的读者、作者和支持者，同时鞭策自己不断创新，以飨厚爱。

在丛书的出版过程中，得到了许多老师和朋友的热情帮助，不一一赘述，一并致谢！

丛书编辑组

前　言

我已经花费了多年的时间研究罪犯如何闯入计算机系统，但是第一次在本地电子存储器上看到签名采集设备时，还是以为自己得了狂想症。你知道我说的是什么，就是职员在那上面划信用卡的平垫，你用钢笔在上面签上自己的名字，不仅留下了墨水笔迹，还记录了签名的电子印记。我的好奇心很强，因此我问某位职员："我在纸片上签名之后会出现什么情况？"我推测我的签名应该发送到批准信用卡支付的金融网络，以便与原始信用申请进行比较，这种方式类似于银行使用可以保留为文件的签名卡。

该职员回答："所有的签名都存储在密室的存储器服务器上。我们（存储器）会保管所有电子签名，以防信用卡公司需要验证是否在收条上签了字。"这无疑不是我想要的答案。

然后我又问该职员："密室里的服务器锁上了吗？"我再次得到了并不想知道的答案。

"没有，它在办公室外面执行人员的后面用来存储。"

"可以访问受限的计算机吗？"我继续问。

"只有一个人知道如何操作那个系统，所以其他人都无法经常使用。"他回答。

"计算机上的数据备份了吗？"

"你知道，这是一个很好的问题。"这仍然不是我想要的答案。

实际情况是我很高兴地得知，我的签名已经发送到一个很大的信用卡公司，至少他们有一名专门的计算机安全人员来保护所有的数据。但是上面所描述的这个人却告诉我，很多人都可以轻易访问我的私人信息。

钻研了存储器所使用设备的技术背景之后，我得知签名在发送到密室的计算机之前就被加密了；因此减少了被盗窃的可能性。但是，整个事件使我很想知道：当那些不关注安全性的人们不安全地存储私人信息、使用脆弱的加密技术，并最终将其放入未经训练的操作者的手中时，有多少技术会导致出现错误？

如果你像大多数人一样的生活，那么生活中就会包括开支票或在商店使用提款卡、在加油站使用信用卡或使用 ATM 机提取现金的情况。如果你是日益增多的互联网用户中的一个，还可能在线购买一、两件东西，甚至使用网络银行或进行在线股票交易。每次进行这些事务的时候，你都必须与外界共享自己的私人信息。大多数人都不会对此再三考虑。但是你知道自己的私人信息将用作何种用途吗？你的私人信息是否安全不会失窃？

可能直到某一天发现别人盗窃了你的私人信息，并用你的身份将你的名字提交给合法的捆绑协议，如信用卡支付、申请贷款、驾驶执照或其他各种协议，这时才会关心这些问题的答案。你该怎么办？如何弥补损失？怎样防止这些情况再度发生？

《信息时代的个人安全策略》专门回答了这些问题，并教给你如何找到本书没有涉及到的问题的答案。不幸的是，随着当前新技术的快速发展，你根本无法预料某人窃取

身份时可能使用的方式。因此，我们希望本书会教给你如何以崭新的方式考虑自己的私人信息、如何认清自己或家人何时会有身份被盗的风险，以及如何分辨减少风险的机会，并在管理个人隐私的方式上有一些小的改变（不管是在线还是离线）。

像 Syngress 出版社“Hack Proofing”丛书的其他书籍一样，本书也包括多个编号列表，其中会列出你应该进行的操作，它还会提供解释，并用示例说明为什么要这么做的原因。

第 1 章将介绍身份盗用的定义、以及它是如何发生的，并将说明现在的身份盗窃是如何发展到超出预料的程度的。

第 2 章将详细介绍通过使用安全的口令、最新的防病毒软件和适当的临时文件处理来保护硬盘的各种步骤。硬盘上有很多隐藏文件，你可能意识不到这一点，但是身份盗贼却无处不在，而且知道要寻找什么。

第 3 章说明如何利用电子邮件向外界公开你的计算机上的内容。其中还包括对病毒、恶意代码、垃圾邮件和电子邮件诈骗等方面的讨论，以及保护私人信息和防止潜在计算机破坏性安全缺口的提示。

第 4 章和第 5 章将介绍什么是网络、在身份盗窃中你的网络和互联网是如何被利用的，以及如何避免方便他人进行盗窃的常见错误。在你检验各种网络和互联网连接的风险时，我们会示范一些访问其他计算机的极其简单的方式。这些示范仅用于教学，目的是向读者展示网络上可以看到的其他计算机中的信息类型。

第 6 章的主题是“孩子是否使你身处险境”。不幸的是，如果孩子在共享私人信息方面（包括他们自己的信息和父母的信息）没有受到合适的教育，就有可能在互联网上冒险。根据孩子的兴趣或对计算机的熟练程度，他们在游戏网站上下载授权的材料、用父母的雇主提供的连接访问互联网（等等）时可能会无意中违反法律。本章会强调适当教育的重要性，并提供一些建议监控孩子的在线活动。

第 7 章提供了一些建议和该问题的可能答案。本章将提供关于成为身份盗窃的受害者之后，联系执法部门、填写报告、联系信用局和重新构建财政方面的帮助提示。

最后，第 8 章将逐步提供一些实际设置用户 Internet 浏览器和个人防火墙的指示，以便进一步保护自己的计算机免于入侵或身份盗窃的危险。

与 Syngress 系列的其他图书不同，本书不是专门为高科技读者编写的。我们假定读者家里至少有一台计算机连接到互联网上（可能另一台正在运转），而且经常使用电子邮件并上网。如果你是 IT 专业人士，可能已经了解了本书中的多数技术信息；但是，可能还没有将这种知识应用到自己私人信息的保护方面。本书会帮助技术和非技术人员理解如何更好地保护私人信息，并避免成为身份盗窃的受害者。

创作队伍简介

Teri Bidwell（GCIA）是本书的作者，她是一位独立安全顾问，GIAC 认证的计算机入侵分析员，以及 SANS 学会 GGIA 咨询委员会的成员。另外，Teri 还有十多年为各种规模的公司设计和构建安全计算机体系的经验。她还教授过计算机安全和计算机入侵分析方面的许多课程，并发表过与此相关的各种文章。Teri 是《Hack Proofing Your E-Commerce Site》（Syngress 出版社，ISBN：1-928994-27-X）一书的作者之一。作为一位独立安全顾问，Teri 协助公司和个人进行评估并减少计算机网络入侵方面的风险；她的专长包括创建安全策略、建立安全管理规程以及安装防火墙和入侵检测系统等。

Michael Cross（MCSE、MCP+I、CNA、Network+）是本书的技术编辑和撰稿人，他是尼亚加拉地方警署的互联网专家和程序员，同时还是他们的网络管理员。Michael 负责执行罪犯调查中所涉及的计算机法庭检验，还鉴定和协助处理与计算机及网络相关的犯罪。他负责设计和维护警署的 Web 站点（www.nrps.com）和两种内部网（一种用于工作站，另一种在巡逻车辆上使用）。他还编写用于警署不同部门的应用软件，还负责过网络安全和管理方面的工作，并一直在这方面提供协助。Michael 是 IT 团组的成员，该团组为超过 800 个民间和官方用户提供技术支持。

在为尼亚加拉地方警署工作以前，Michael 在英国伦敦、加拿大安大略省的私立大学和技术学校担任讲师。在这期间，他受聘成为 Syngress 出版公司的作者，成为了他们写作小组的正式成员。

Ryan Russell 是本书的技术审核，他是 Syngress 出版社出版的《Hack Proofing Your Network: Internet Tradecraft》（ISBN：1-928994-15-6）和《Hack Proofing Your Network, Second Edition》（ISBN：1-928994-70-9）两本畅销书的作者之一。他是 SecurityFocus 的事故分析员，曾经是安全方面的鉴定人，还为一家大型软件厂商做过国内安全调查。Ryan 已在 IT 领域工作了 13 年多，最近 7 年他将主要精力放在了信息安全方面。他多年来积极地加入到各种安全邮件列表（如 BugTraq）中，在成为安全会议的发方言人之后，就经常成为媒体追逐的对象。Ryan 还参与编写了 Syngress 出版社另外 4 本关于网络技术方面的图书，以及关于计算机安全的 4 本图书。他有计算机科学专业的学士学位。

目　录

第 1 章　身份盗用：您是否身处险境

本章内容

- 定义身份盗用
- 了解什么是私人电子信息
- 预防盗用
- 保持私人信息的私密性

1.1　概　　述

在购物或签署合同时，传统习惯是使用图章、卡或其他身份证明。但是近年来，当商人和顾客开始使用 Internet 进行在线交易时，却在身份证明方面面临很大的挑战，因为他们必须找到和传统格式（如手写签名和照片 ID 等）一样可信的数字证明。而身份证明的传统格式在 Internet 上很难处理，所以还没有找到通用的 ID 格式可以适用于那些意欲进行在线交易的公司。

Web 站点拥有者、使用计算机追踪销售情况的商人和电子服务提供商都不得不找到自己独特的解决方案，以此来对仅使用计算机的顾客进行身份证明。许多使用电子商务的商人都离不开密码。有人使用电子身份标识，也叫做“数字证书（digital certificates）”。其中多数都要附加顾客的账户名或账号、电子邮件地址、物理地址、电话号码和其他标识信息等。

与用户有电子业务往来的公司都增加了用户标识符的数目。这些数字格式的身份证明（如密码）与传统格式（如许可证）一样需要采取安全措施进行保护。但是，它们是无形的（无法看到或触摸），因此就不能像锁上自己的财产那样使用传统方法了。而这不但会使您身处险镜，而且，计算机罪犯更易利用那些不习惯给信息上锁的人们，这就好比小偷常常算计那些对周围事物陌生的人一样。

现在，在信用卡支付条上签字时都要求使用签名采集设备，这种设备专门用来复制签名并将其存储为电子格式。您可以将自己的信用卡号码键入 Web 表格上，几天后，您的门前就会神奇地出现所要的产品。现在，很多家庭都将存储在计算机上的私人信息展示在 Internet，每周 7 天，每天 24 小时。这对于我们传统的个人身份证明的概念是一个全新的挑战，而且这些挑战给个人信息保护带来了新的职责。

公司和顾客都开始以从未要求过的方式查看个人身份证明。每晚将钱包放在安全的床头柜上，这种方法现在已经不够用了。您还需要懂得如何保护自己的数字格式的身份。

在本章，我们将研究在 Internet 世界中说明身份的身份证明的格式。开始会着重介绍如何使用切实的安全方法来保护标识个人的信息源。而本章的最后将介绍一些使用计算机和 Internet 的无形特点保护个人信息的方式。本书其余章节会继续深入探讨

这些方法。

1.2 定义身份盗用

身份盗用（identity theft）是某人冒充他人的身份以获得经济利益或其他个人利益的一种犯罪行为。受害者可能是个人，也可能是公司，而作恶者可能是一个人，也可能是多个人共同盗窃或连环诈骗。通常情况下，窃用个人或公司的身份其实是想用其进行其他犯罪活动，如信用卡欺诈、用别人的名字申请贷款等。

冒充他人以得到个人利益这个问题已经存在了若干个世纪，但是现在变得更为普遍，因为易获取的他人信息已经变得越来越多了。过去，身份盗窃的目标通常是有钱人和著名人士，但是现在，更多的普通市民成为了受害者。下面是近些年来美国政府机构进行的一些统计：

- 身份盗用是发生在普通人（如您、我）身上的一种犯罪行为；受害者的平均年龄为 41 岁。
- 据美国情报局估计，1997 年因身份盗窃造成的损失为 7.45 亿美元。从那时起，身份盗用变得更为普遍了，估计盗用受害者、金融机构和纳税人的总损失已达上亿美元。
- 身份盗用的新案件数量在增加。因为 Internet 使得信息访问更为简单，导致了这一新趋势的产生。
- 与信用差或收入低的人们相比，身份盗用对信用好或收入高的人们影响更大。
- 从 1999 年 11 月到 2001 年 6 月，提交给美国联邦贸易委员会（FTC）的身份盗用起诉达 69370 宗（www.consumer.gov/idtheft/charts/01-06c.pdf）。
- 根据 FTC 主席 Robert Muris 在 2002 年 4 月的报告中显示，向 FTC 报告身份盗用事件的电话从 2001 年的 2000 个涨到了每周 3000 个（www.technews.com）。
- 根据身份盗用资源中心（www.idtheftcenter.org/html/facts_and_statistics.htm）的报告显示，身份盗用事件使受害者平均需要白白用去 175 个小时和白白花掉 1000 美元来澄清自己的名誉。

为了更清楚地说明什么是身份盗用，下面举出了构成身份盗用的一些行为作为示例：

- 偷盗钱包不是身份盗用。但是，如果偷走钱包的盗贼使用您的驾驶执照和信用卡购物，这就变成了身份盗用。
- 丢失 ATM 卡并不构成身份盗用。但是，如果您丢失了 ATM 卡后，某人发现了它并用您的 PIN（个人身份号码）从您的银行账户里提取现金，或使用该 ATM 卡获取其他经济利益，这也是身份盗用。
- 蜂窝电话被偷也不是身份盗用，除非盗贼使用您的蜂窝电话打电话，或使用存储在蜂窝电话里的数据以某种方式冒充您的身份。

1.2.1 进行风险因素测试

读者可以做以下测试来确定自己的风险因素。如果下列情况中有一半以上都为

“真”，您在身份盗用方面就存在很大的风险。在阅读本书其余章节提出的解决方案时，请牢记这些风险因素：

- 每周至少收到一封贷款请求或预批准的信用报价。
- 总是将没有销毁的预批准信用或贷款请求扔进垃圾桶。
- 总是将没有销毁的旧的银行文件或信用文件扔进垃圾桶。
- 邮件递送到没有上锁的邮箱中。
- 用未上锁的邮箱寄发邮件。
- 在钱包中携带社会保障卡或社会保险卡。
- 社会保险号码印在健康保险卡上，而健康保险卡装在钱包里。
- 社会保险号码印在驾驶执照上。
- 社会保险号码或驾驶执照号码印在私人支票上。
- 使用信用卡在线购物。
- 使用信用卡在线购物之前，或向某 Web 站点透露私人数据（如社会保险号码）之前，很少检查该站点是否安全。
- 在透露私人信息之前很少阅读 Web 站点的保密策略。
- 您的在线银行账户、健康保险人或股票经纪人将您的社会保险号码作为账号使用。
- 银行在允许您亲自提款时不要求输入密码。
- 在线银行账户的密码写在未上锁的位置。
- ATM PIN 写在钱包上或 ATM 卡上。
- 有时在 Web 站点上共享自己的名字、地址、电子邮件地址和/或电话号码。
- 没有使用保密软件从自己的计算机上删除识别信息。
- 很少利用专门的退出信息共享的程序。
- 还没有看到去年的信用报告。
- 与 Internet 相连接的计算机存储了私人信息或财务信息，但却没有用防火墙和防病毒软件进行保护。

1.2.2　他们为什么这么做

身份盗贼冒充别人的理由可能有很多。在某种犯罪形式中，一个抓住机会的盗贼会获取受害者的多条信息，然后利用这些信息在短期内免费获取商品或服务。例如，盗贼使用您的社会保险号码、名字和地址开设信用卡账户，然后多次购物。当您收到陌生的账单时，盗贼为避免被捕已经不再使用偷来的新账户了。这种盗贼一般要偷盗一两个信用卡、一个社会保险号码或驾驶执照等用来犯罪。

身份盗用的另一种形式是长期冒充。例如，某人用您的名字开设了银行账户，然后将报告寄回自己的地址而不是您的地址。这类犯罪的另一个示例是，使用偷来的社会保险号码找到工作或获得政府救济金。使用盗贼的地址开设新账户后，该账户可以使用很长一段时间。盗贼甚至可能会成年累月地保留这种冒用身份，并努力隐藏自己的真实身份。这种罪行的受害者，可能直到下次查看自己的信用报告，由于信用差而被拒绝贷款，或者在社会保险记录中查看到错误的人事数据时才会发现。下面看一下 1999 年 7 月 13

日 FTC 提供的受害者声明（摘自美国联邦贸易委员会的消费者保护 Web 站点 www.ftc.gov）：“有人在冒用我的名字和社会保险号码开设信用卡账户。所有账户都被他使用了。直到我申请抵押时才知道发生了这样的事情。由于我的信用报告中显示出这些‘坏’账户，结果我没有申请到抵押。”

1.2.3 他们如何侥幸成功

在忙忙碌碌的生活中，多数人购物时都会使用信用卡、签写支票以及使用自动柜员机的 ATM 卡，而且使用时不会多加考虑。但是，每次处理这些财务事务的时候，您都在与他人一起共享自己的私人信息。当然，在没有被需要使用的服务拒绝的情况下，您是不会完全停止私人信息共享的。一方面需要例行共享信息，另一方面需要尽量保护不必共享的私人信息，您必须要在这两者之间找到一种平衡。

在了解如何保护私人信息之前，需要研究一下获取和偷窃私人信息的方式，因为平时您可能意识不到这些方式。要记住，本节讨论的每个条目都有可能发生，只是不一定发生在您身上。当您阅读这些内容时，根据自己的常规和习惯考虑这种情况是否适合自己。稍后，研究可以对常规和习惯进行改变的方式，以防止发生这里所描述的盗用情况。

1. 翻查废弃物

当某人翻找其他人的垃圾以获得有用信息或内容的时候，就是翻查。您的垃圾中包含了大量关于您自己的有价值的信息，除非您已采取步骤防止翻查这种情况的发生。例如，您可能丢弃了包括有价值数据的银行记录、贷款表格或旧账单。当您取得新的支票时，可能会丢弃旧支票。翻查废弃物的人则可能找回这些旧支票，并马上开始使用您的银行账户。

如果您有一张信用卡，可能还会收到预批准的信用报价的邮件。信用公司从信用局和其他来源那里购买邮件列表，再将这些报价发送给那些使用信用卡的人们。多数人都将它们作为垃圾邮件扔进了垃圾桶，甚至没有打开看一眼。但是，某个有胆量的盗贼可能会翻查您的垃圾桶，然后找到这些预批准的报价，并将它们发送出去。多数预批准的报价都可以在地址部分进行简便的改变，盗贼可以用他自己的地址填写，然后在申请表单上签上您的名字。一些预批准的报价或已有的信用卡报告里面都带有支票，您可以将它用于整理账单。如果您将支票扔进垃圾桶里，盗贼就可以找出来、签上名，然后用您的名字开始大量购物。

翻查废弃的不算犯罪，除非在该过程中有违法行为。目前法律对这方面还没有很好的陈述，除了有关禁止非法侵扰他人的财产的法律。例如，如果您的垃圾箱上有一个“不准擅自闯入”的标记，就可以证明任何人从其中取走任何票据的行为都是盗窃行为。但是，很难证明丢弃的票据有足够的价值可以看作是“被盗财产”。1988 年美国最高法院在对 California vs. Greenwood 的裁决中的规定，事实上乱翻某人的垃圾并没有侵犯隐私权，因此就更难对此做出定论了。但是您可以采取一定的行动，尽量不要把自己的东西暴露给总是喜欢乱翻的人，1.4 节将讨论这些内容。

计算机的回收站

聪明的人们可能会把纸撕成碎片，但是他们可能不会考虑计算机上的回收站。回收