电脑报 总策划
http://www.yesky.com

随时技巧丛书

个人电脑与网络安全

自己动手彻底解决你的安全隐患

DIY

徐锋
邱建辉 编著

公共机房隐私防范大全

文件加密与解密绝招

个人PC安全软、硬总动员

“Internet网络安全”技巧精解

100余款加密、解密、防黑、反黄软件

附赠金山毒霸2002、金山网镖2002电脑报试用版

随盘赠送，光盘定价：18.00元

电脑报书友会
www.itbook.com.cn

序

对于现在的个人计算机来说，其内记载的各种隐私越来越多了，怎样才能让自己的计算机不做“叛徒”是每个计算机使用者最头疼的问题。特别是那些在公司或单位以及学校，使用公用计算机的人，这一点尤为重要。

随着网络技术的发展，家庭上网的普及，Internet已走进了我们的生活。它除了给我们带来丰富的知识和广阔的资源外，也为我们带来了不少的麻烦，黑客、木马、病毒成为上网者谈之变色的话题；网络上的黄毒泛滥，避免儿童不受伤害也成为家长们的一大心病。

怎样保证自己的隐私不被计算机泄漏，怎样保证自己在上网时不被黑客、木马、病毒所困扰、怎样让自己的孩子远离黄毒的侵害呢？也许你不是一位电脑高手，不知道怎样去解决这些问题。不过，你也不用担心，《个人电脑与网络安全DIY》可以帮你轻松搞定，只需你明确自己的目的，找到你想要做的目录，按目录翻开那页书，照着上面的内容做就行了。简单、明了，我们不讲原理，不讲为什么，只告诉你怎么做才能保护你的隐私不被泄漏、怎样才能让你不受黑客、病毒、木马的侵扰、怎样让在你远离黄毒的同时，享受网上冲浪的乐趣。

请注意：本书针对的操作系统是现在主要流行的Windows 98/2000/me。

严正声明：

本书所涉及的破解、解密等内容均为在某些特殊的情况下，对用户自己的计算机采用各种破解方式，可作为加密、解密初学者研究参考之用，严禁用于非法用途。凡因本书造成的各种负面影响，本书不负担任何责任。

电脑报社

2002年3月

第一部分　公共机房安全篇

公共机房里使用私人的文件及私人密码是相当危险的，有时，在不知不觉间，这些看似无关紧要的东西，会给你带来相当大的损失。本部分将为你讲述在公共机房里使用计算机时，如何保障个人的隐私不被泄漏、保护自己的个人帐号、密码不被盗用、以及各种私人文件的加密、解密技巧。

第二部分　个人PC安全篇

相信每个拥有计算机的人都不希望自己的机器被别人改动得一塌糊涂吧，无论这次改动是有意还是无意的，给自己的机器加把锁是每个拥有机器的人所共有的想法，现在我们来了解如何设置、解除软、硬件系统的密码，怎样对病毒进行防范与清除，以及磁盘数据的备份与恢复。

第三部分　Internet 网安全篇

Internet 的普及给我们提供了新的联系方式，为人们之间的沟通提供了新的渠道，但伴随而来的安全问题又成为每个上网族的心病，这一篇将为你解决这块心病。它将讲解个人 PC 在接入 Internet 后的个人隐私安全如何保障、怎样防范黑客的骚扰、怎样避免你可爱的宝贝受到 Internet 上黄毒的侵害，以及怎样对付网络上横行肆意的病毒等。

第一章　公共机房隐私安全

随着计算机技术的发展和我国计算机教育的普及，近年来我国公共机房无论是在设备和数量上都有了很大的发展，所谓公共机房指的是一个能够共享互联网资源的小型局域网络，大则几十上百台电脑，小则十几台电脑。

公共机房可以用来学习、教学、科研，也可以用作经营赢利。我国现有的公共机房大体分为两种：一种是教育科研等机构供内部人员使用的公共机房，这类机房一般只对内部人员开发，管理较为规范；另外一种则是纯粹以商业盈利为目的的公用机房，也就是我们现在常说的网吧、网络咖啡屋等。网吧在我国的发展速度相当快，短短几年，各式各样的网吧几乎遍及大江南北。公共机房的出现为处于信息时代的现代人接触互联网络、掌握讯息提供了一个方便快捷的途径。

公共机房的优势就在于资源共享，谁都可以方便地使用公共机房内的计算机，为那些没有条件上机者提供了良好的上机环境。但是同时在公用机房内的计算机都是公用的，在安全隐私方面存在严重的隐患，特别是近年来黑客技术的不断发展和传播，一些心存不轨的使用者经常通过公用机房设备窃取他人隐私，因此在公共机房里使用私人文件及私人密码都是相当危险的。有时，在不知不觉间，这些看似无关紧要的东西，会给你带来相当大的损失。本章将为你讲述在公共机房里使用计算机时，如何保障个人的隐私不被泄漏、如何保护自己的个人账号、密码不被盗用、以及各种私人文件的加密、解密技巧。

第一节　保护自己的钥匙——账号与密码安全

1.1.1　什么是账号和密码

计算机系统都使用一定的方法来限制用户的使用对账号的存取，最常用的方法就是使用账号和密码。账号是计算机系统鉴别用户时使用的标记。密码是与此账号唯一匹配的口令。当进入一个系统时，用户必须提交一个有效的账号，并输入与这个账号相关的密码，才能登录（如图1-1-1所示）。正因为账号和密码如此重要，所以在公用机房使用账号和密码的时候尤其要注意安全问题，否则后果将不堪设想！

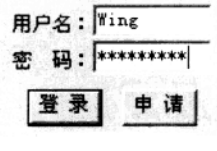

图 1-1-1

1.1.2 账号的类型

你可能会见到类似的名称，如："user IDs"，"IDs"，"logins"或一些其它的名称。许多系统在用户第一次登录时，都会提示你输入你的账号，然后会提示你输入这个账号所匹配的密码。黑客不知道你的账号而要窥视你的隐私比不知道你的密码更加困难。

账号一般都很普通。例如：用户名的一部分（如"Mike"，"Tony"等）；用户职责的简称（"admin"，"webmaster"等）；或者起得很笨拙，如使用号码（如OICQ、ICQ等）；有时账号的名称也会没有任何意义。

账号通常被分为四种：特权、系统、常用、客人。

特权账号：可以在系统中做任何事，删除账号、更改用户密码、重新配置系统等。对于一个黑客来说，获取特权是其最终目标。

系统账号通常是系统本身使用的账号，或者是具有部分特权的账号。

常用账号：一般被正常用户用来完成他们的日常工作，这是最为简单的账号。

客人账号（guest）：一般被设计成任何人都可以使用。这对那些在系统上没有正常账号的人使用系统提供了便利。最典型的例子就是匿名 FTP 。一般客人账号存取系统时都会受到限制，特别是在对外公开的系统上。

图1-1-2显示了几种账号的类型， Administrator为系统的特权账号，用于管理整个系统，系统账号Finance用于使用一些特殊软件，比如财务软件等，常用账号"Wing"主要用于一些非管理的日常操作，"Guest"则是客人账号，它可以使用系统，但权限相当低，只能进行一般的操作。

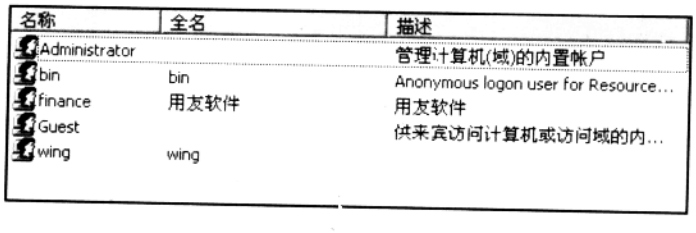

图 1-1-2

大部分的计算机在用户输入密码时，不把密码显示到屏幕上，有时不显示任何字符，有时是用星号代替，以防泄露密码。例如我们在使用OICQ的时候会发现，在"用户口令"一栏用"*"把密码隐藏了（如图1-1-3所示）。

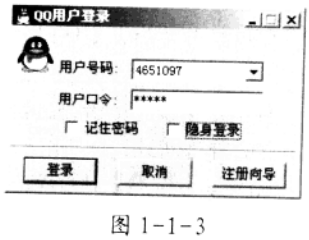

图 1-1-3

1.1.3 使用账号密码的注意事项

尽管所有系统都有一些安全措施，但是在公用机房使用账号和密码还是危机四伏，使用时要特别注意，一不小心账号和密码很容易就会被别人在无声无息间窃取。

● “记住密码”——天使？恶魔？

不适当的设置可能导致在公用机房的计算机内遗留密码，有些软件在设计时，出于为方使用户使用的考虑，一般在有需要用户认证的地方都会设计一个“记住密码”的选项（如图1-1-4所示）。这个选项一经被用户选中，用户在第一次输入正确的用户名和密码时，系统就会自动把该密码保存下来，用户下次继续使用时就不需要再次输入密码，的确是很方便。但是有部分粗心大意的用户，在公用机房上机时把该选项选上，而下机时又没有及时把密码清除掉，造成的结果就是：下一位使用该计算机的用户可以毫不费劲地得到这位用户的账号和密码。

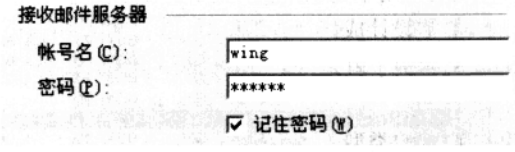

图 1-1-4

因此大家在使用“记住密码”选项的软件时要特别小心，如果你在公用机房上机，尽量避免使用该选项，如果选了该选项在下机的时候切记要把选项去掉，最好把账号设置全部删除，以保障自己账号的安全（如图1-1-5所示）。

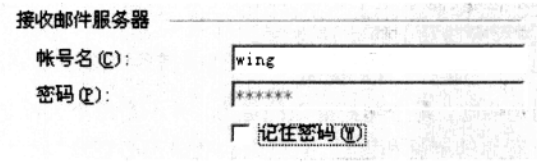

图 1-1-5

● “黑客软件”——机房谍影

不要以为黑客软件都是一些带攻击性质的软件。形象一点说，我们可以把黑客软件分成两种：一种是恐怖分子型的，这种工具极具攻击性，可以让你的系统在不知不觉中崩溃。还有一种则属于间谍型的，象好莱坞电影中充满神秘色彩的职业特工。它们不带任何攻击性，就象个超级间谍侵入到你的系统里，窃取你最机密的资料，包括个人隐私文档以及你的账户密码等等，或者在你的系统里开个后门让你防不胜防。

在机房中使用最多的莫过于一种用于记录使用者敲击键盘活动的工具，一旦机器运行了这样的程序，程序就会记录下使用者所有的键盘活动，包括用“*”号隐藏的密码（如图1-1-6所示），而且这种工具一般都在后台运行，驻留在系统的进程中，使用者很难察觉到自己的一举一动都被记录下来了（如图1-1-7所示）。

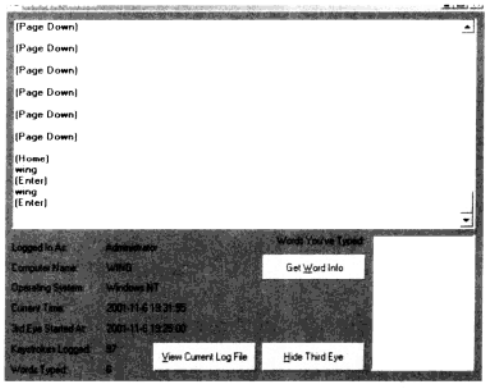

图 1-1-6

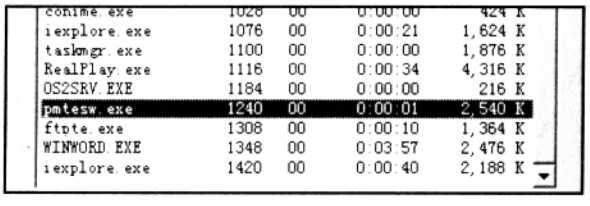

图 1-1-7

要防止自己的键盘活动被记录下来最根本的方法是在每次开机使用前，特别是在使用机要密码前先察看一下系统的进程，看看是不是有多余或可疑的进程，有些杀毒软件也能侦测到这种后台进程。如果有可疑的进程应该马上终止该进程。

● “偷窥者”——“鹰”一样的眼睛

公用机房，特别是网吧，是个龙蛇混杂的地方，并不是每个人都是正人君子。在你的周围可能会有一双眼睛正盯着你的屏幕和键盘，有些人会装成热心观众“潜伏”在你的身边，当你输入账号和密码的时候，你的账号和密码已经被记录到他们的脑海里了。为了躲开这些鹰一样的眼睛，在公用机房中使用密码和账号的时候应尽量避免把自己的屏幕和键盘暴露在别人的视线之内，输入密码时应有连贯性，不要停停敲敲，更不能在嘴里嘀咕出密码来。

● “偷天陷阱”——坑你没商量

最近在各大ICP网站特别是像联众、腾讯OICQ这样的网站正不断地在显眼的位置警告用户不要随便把自己的账号和密码告诉一些自称是网管或维护人员的陌生人。当你在纵情游戏的时候，可能会有一条莫明奇妙的信息发给你，他们会自称是网管，因为测试需要你的账号和密码；或告诉你玩游戏中了大奖需要确认你的身份，叫你说出你的账号和密码。这些人一般会给自己取一个很像网管的账号，例如Admim，WebMastee（很像Admin、webmaster吧）以迷惑用户，如果你轻信了他所说的话，把账号和密码告诉了他，不出一分钟你的密码就会被改了，从此你将痛失你的高分账号。记住：账号和密码是你网络生活的钥匙，不要轻易交给别人！

第二节　看住自己的秘密——个人隐私安全

个人隐私安全一直是个很热门的话题。个人隐私在这个信息高度发达的社会越来越受到人们的重视，保护个人隐私已经成为现代人维护自身利益的一个重要部分。在公共机房中个人隐私同样面临着严重的问题，主要的泄漏个人隐私的途径有两种：通过网络窃取个人隐私以及通过使用的计算机泄漏个人隐私。

1.2.1　“暗藏杀机”——网络世界中的隐私

网络是个极度开放的世界，公共信息可以在这里得到高度的共享。你的信息可以在短短的几秒内与大洋另一边的朋友分享。如果你是一家跨国公司的员工，你的商业信息同样可以方便快捷地传递到世界各地的分支结构。同时网络也是现代人的虚拟世界，人们可以在这里相互交流情感和信息，有了网络也就多了一种沟通的方式，电子邮件、聊天室、ICQ、IP PHONE、网络视频会议的出现让人们的沟通逐渐摆脱了电话、信件、电报的单一模式，只要你身处在信息网络世界里就可以在任何地方，任何时间，以任何方式和身处网络的朋友们交流信息。

当你在聊天室里和远方的朋友分享幸福时光的时候，别忘了这是个公共场合，你们的谈话别人也同样能看到。即使是在私人聊天室里，管理者也可以以隐身状态把你们的谈话看得一清二楚，ICQ、电子邮件和IP电话等都不是在绝对安全的环境之下。即使在美国这样的国家，公民的电子邮件、聊天记录、在网上的一举一动都在政府机构的监管之下，更何况还有成千上万的黑客工具可以轻易的监视你的言行举止，可以说，网络是个没有绝对隐私可言的地方，因此除非迫不得已最好不要在网络中谈论重要的个人隐私。

别以为不上网聊天，不发电子邮件，只作些信息查询、逛逛网上商城就不会泄漏自己的个人隐私了。当你浏览网站、填写幸运抽奖表格的时候，你的个人隐私就已经成了别人的囊中之物。

随着电子商务的发展，人们已经渐渐开始接受网上购物和网上贸易，电子商务的交易量这几年总是呈现稳步上升的趋势，越来越多的网民已经习惯在办公室或家中进行生活用品的采购，参与网络拍卖等电子商务活动，只要一根电话线、一个银行账号就可以免去出门购物的一切烦恼。

以往，我们到商店买东西从来都是一手交钱、一手交货，商店店员一般不会轻易询问我们的姓名、住址、身份证号码以及联系电话等。但是在网上交易中，这些却往往是我们需要填写的基本信息。于是人们的担心也就在所难免。由于目前互联网的安全制度还不够完善，网络安全技术还有待发展，人们的防范意识也比较弱，因此在网上窃取他人的信息简直是易如反掌，有时就好像天下掉下馅饼一样。金融机构及各大网上服务公司用以确认用户身份的密码、用户名、身份证号码、驾驶执照编号以及其他数据均可以在互联网上手到擒来。很多政府及私营机构将公众的“私人信息”存储在互联网数据库里，但这些数据库的安全性实在令人怀疑，因此给了黑客很多机会窃取这些重要信息。正是因为万维网、在线数据库、搜索引擎以及公共文档的存在，才使得电脑黑客可以在更加便利的条件下获取他人信息。网络中存在的诸多不安全因素都会成为个人隐私的杀手：

1）Cookie　这种被称为“网络小甜饼”的是一些会自动运行的小程序。网站设计师使用它们来为你提供方便而高效的服务。它可以帮你记住经常使用的一些密码，使你不必每次重新输入。要是你常在网上购物，它还可以记住你每次购物栏里的内容。但正是因为它具有这些功能，网站管理者们便可以由此进入你的私人世界。比如你总喜欢购买哪一类书籍或商品，你总喜欢看哪一类网

页内容：你的收入和消费方式；你在哪里开有电子账户……而将这些数据拼凑起来，你将如同玻璃一样“透明”，毫无隐私可言，商业公司和网络入侵者能够轻易获得你机器上的信息，当悲剧发生的时候“小甜饼”就变成“小毒药”了。

2）**电子邮件病毒** 超过85%的人使用互联网是为了收发电子邮件。著名的电子邮件病毒“爱虫”发作时，全世界有数不清的人惶恐地发现，自己存放在电脑上的所有文件已经被删得干干净净，更可恶的是有些病毒在你浑然不觉的情况下就把你硬盘中的文档发给一个你素不相识的人，也许第二天起来后你就发现你的邮箱里多了几封莫明奇妙的求爱信。

3）**认证和授权** 每当有窗口弹出，问使用者是不是使用本网站的某某认证时，绝大多数人会毫不犹豫地按下“YES”。但如果商店的售货员问：“把钱包给我，请相信我会取出合适数量的钱替您付款，您说好吗？”你一定会斩钉截铁地回答：“NO！”这两种情况其实本质上没有不同，鬼才知道那只是个认证程序还是个黑客程序。

4）**ICP** 网民们经常会遇到这样的情况：在申请邮箱、个人主页和进行网上购物之前，网站往往会要求网民们提供自己的个人资料，如姓名、性别、年龄、电话、信用卡号码、家庭住址，甚至是在金融、医疗、税收等完全属于个人隐私方面的资料。ICP让我们注册，并提供免费或者收费服务，获得巨大的注意力或经济效益，这是标准的网络经营模式之一。但并没有太多人留意到有很多经济状况不太好的ICP把用户的信息卖掉，以换取银票，更可怕的是如果你的信用卡号码就这么轻易地落到了别人手里，那也许不出一个月，一打的付账单就会把你彻底淹没。

5）**网络管理员** 管理员可以得到我们的个人资料、阅读我们的信件、获悉我们的信用卡号码，如果做些手脚的话，还能通过网络操控我们的机器。我们只能期望技术高超的他们同时也道德高尚。

随着网站的增多和覆盖范围的扩大，许多网络公司最终就会像一张巨网将网民牢牢套住。不管你去哪里漫游，你的个人信息终将会被捕捉而去。加之，在网上的信息传播要比其他任何渠道都要容易、方便得多，因此个人隐私也较容易被浏览和扩散。由此带来的麻烦，已经令你防不胜防。在一家公司做文秘工作的小陈谈到，在他所申请的几乎所有的免费邮箱甚至是付费邮箱中，经常会收到莫名其妙的电子邮件，有些甚至还是颜色不正、气味不大对头甚至带有电脑病毒的。这种遭遇，有了一定网龄的网民想必都是经常碰到的，大家也似乎已经见怪不怪了。

1.2.2 保护自己的隐私

“想想自己的隐私掌握在别人手中，被人跟踪，就如同生活在玻璃房子中”，一位网民说，“玻璃房中的生活让我恐惧”。其实对于网民来说，首先要做的是管好自己：

① 在某些网站要求你提供个人信息时一定要三思而行，对那些所谓的巨额抽奖活动更是要小心又小心；

② 不要轻易在网上用信用卡进行消费，既使是知名的大网站。如果确实要用，也要在进行交易或发送信息之前阅读网站的隐私保护政策；

③ 微软和网景公司的浏览器软件都有关于接受Cookie的设置选项，浏览器的默认设置是接受一切Cookie，你可以将它改为更安全的隐私设置，例如在IE6.0中就可以在Internet选项的隐私设置中对Cookie进行多种的安全级别的隐私设置，如图1-2-1所示。或者在浏览网页的时候采用匿名方式浏览；

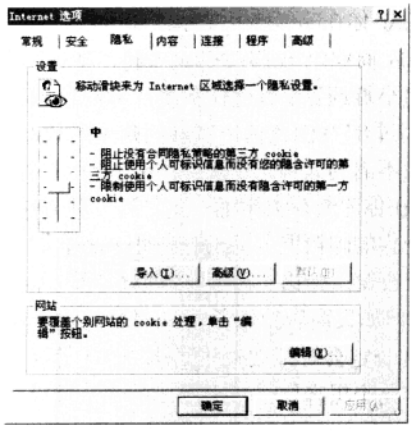

图 1-2-1

④ 不要轻易安装来历不明的软件；

⑤ 安装并定期更新你的杀毒软件；

⑥ 不要轻易把重要的电子邮件地址告诉别人。

同时业内人士提醒国内的一些网站：一方面网上用户的资料是网站的资源和财富，希望这些资源可以得到很好的利用，获得商业机会。另一方面，如果不尊重网民的意愿，滥用或泄露个人资料，就有可能导致侵犯个人隐私。明智的网站应该做保护网上隐私的表率。首届“全国十佳律师”岳成认为，很多国家都规定了对个人隐私进行保护，隐私权在我国的法律上虽然还没有很明确的概念，但可以利用名誉权、著作权、肖像权等进行起诉。所以网上隐私应该受到保护，侵犯网上隐私同样是要被起诉的。泄漏网民个人资料，并将之用于商业用途的做法，毫无疑问已成为信息时代的一种新公害。面对隐私被曝光，网民们感到了前所未有的窘迫与焦虑。保护自己的隐私不被泄露，确保行动不被追踪，已经成为网民们最普遍的期望。

第三节 “失落的世界”——公共机房中的隐私

在公共机房中打开计算机后，写文章、看图片、访网站、发邮件……，这一切操作，都可能被他人“窥视”：一个有经验的电脑高手能够毫不费力地找到你刚编辑过的报告、被你删除的邮件、你过去曾经访问过的站点、你去过的新闻组和聊天室、你下载的文件以及你的ICQ通话记录，总之，你的一切隐私都可能被别有用心的人窥探。是不是有些恐怖？想保护隐私、守住秘密并做到信息安全吗？请注意防堵日常操作中容易泄密的漏洞。

进入Windows 中的一切操作，无论是工作、学习或娱乐，自进入Windows 系统开始，都将被Windows以及它运行的服务(程序)记录在案，并保存在硬盘中，此项“功能”叫做日志(LOGO)，它原本是系统设计者为了方便用户而设置的，但也会成为泄露你所进行过的工作的漏洞。也许你在离开公用机房后，在你之后使用这台计算机的人只要在你刚用过的计算机中查找一阵，就会发现大量信息：已经被你删除的和发出的邮件、你访问过的Internet网站、搜索规则及在网页表单中输入的数据。这些“记录”可能会把你的“隐私”泄露，使你的信息安全受到威胁，这也许是你所不希望发生的。泄密的漏洞其实就在你的日常操作中：

浏览器中的历史记录

用IE浏览器浏览文件后，在History文件夹中将“自动”记录最近数天（最多可记录99天）的一切操作过程，包括去过什么网站、看过什么图片等信息。你只要点击IE浏览器上的按钮，就可以显示你最近一段时间以来用IE浏览器浏览过的网站的地址和网页内容（如图1-3-1所示）。这个文件夹相当独特，不能进行备份，但会暴露您在网上的“行踪”。不想让他人知道您的“历史记录”的话，记住删除“History”文件夹中的一切。有三种方法可以将“历史记录”删除：

图 1-3-1

1）从资源管理器中进入该文件夹并删除其中的所有文件；

2）单击“开始”→“设置”→“控制面板”→“Internet 属性”→“常规”标签，在“网页保存在历史记录中的天数”输入框中敲入“0”→“确定”；

3）每次在下机的时候，单击“开始”→“设置”→“控制面板”→“Internet 属性”→“常规”标签，直接按“清楚历史记录(H)”按钮把历史记录全部清空（如图1-3-2所示）。

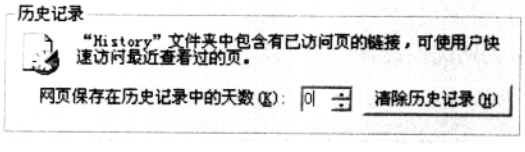

图 1-3-2

浏览器地址栏中的历史记录

下网后，按一下地址栏的下拉选单，已访问过的站点无一遗漏尽在其中（如图1-3-3）怎么办？在下网之前用鼠标右键点击桌面上的IE图标，打开属性，在“常规”栏目下点历史记录项目的“清除历史记录”。若只想清除部分记录，单击浏览器工具栏上的“历史”按钮，在右栏的地址历史记录中，用鼠标右键选中某一需要清除的地址或其下的一网页，点选“删除”。

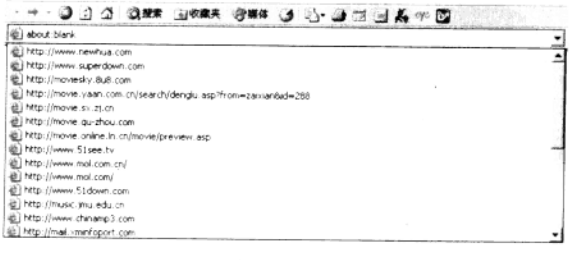

图 1-3-3

收藏夹中的收藏记录

大多数人上网时，常把喜爱的网址添加到“收藏夹”中，甚至设置为“允许脱机使用”(如图1-3-4所示)，其优点当然是便于下次快速地进行浏览，但你的爱好和兴趣就必然暴露给他人了。这些网址都保存在Favorites文件夹下，即是“收藏夹”的位置，要想清除“收藏夹”中的历史记录，只要进入它，选中目标文件，执行“删除”操作即可。

图 1-3-4

开始菜单中的文档

“开始”菜单的“文档”选单中，以快捷方式保存着您最近使用过的约15个文件包括您刚从网上下载并打开过的文件(如图1-3-5所示)。通过它，我们可以迅速地访问一段时间前编辑过的文档。但对于那些使用计算机编辑个人文件或机密文件的朋友们来说，这种设置却会向他人泄露自己的秘密。

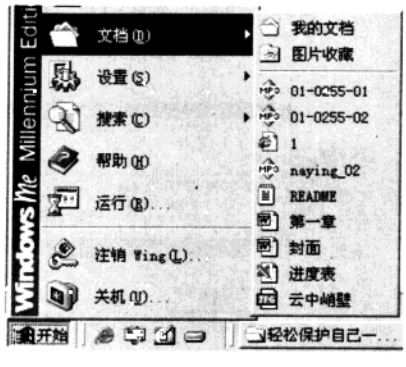

图 1-3-5

这些快捷方式可以象清除IE历史记录一样清除，单击“开始”→“设置”→“任务栏和开始选单”，点击“开始选单程序”栏目下的文档项目的“清除”按钮，就把“文档”选单中的历史记录全部清除掉(如图1-3-6所示)，若要个别清除，可以直接选中快捷方式点击右键，执行“删除”操作即可或者从资源管理器中进入“Recent”文件夹，删除需要删除的项目即可。

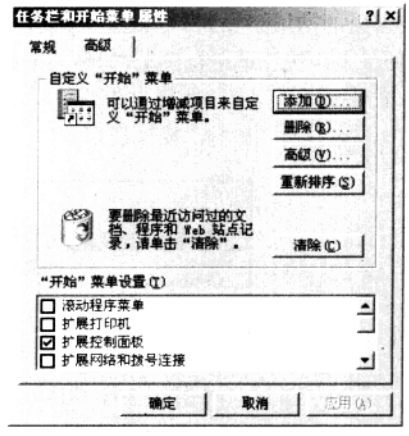

图 1-3-6

开始菜单中的运行记录

使用Windows“开始”选单中的“运行”选单项运行程序或打开文件，退出后，“运行”中运行过的程序及所打开文件的路径与名称会被记录下来，并在下次进入“运行”项时，在下拉列表框中显示出来供选用（如图1-3-7）。这些“记录”会被窥视，需要清除可以使用“运行”菜单“文档”的办法进行删除。

图 1-3-7

回收站中的文件

“回收站”是已删文件的暂时存放处。在“清空回收站”之前，存放在那里（回收站）的文件并没有真正从硬盘上删除。Windows 9x操作系统，除了在“桌面”上放置一个图标为灰色的“垃圾筒”外，在每个硬盘（分区）的根目录下建立了一个隐藏属性的文件夹——Recycled，这个“Recycled”子目录（文件夹）就是回收站实际的位置所在。窥探者可以从“回收站”中通过“还原”功能恢复被删除的文件（如图1-3-8所示）来发现您的工作内容。所以，每次结束操作，离开计算机之前，要记住“清空回收站”，或者在进行“删除”操作同时按下“Shift”键直接把文件删除而不进“回收站”，不过这样的操作不能再通过还原来恢复了。

图 1-3-8

应用程序中的各种记录

使用Word、Excel、WPS2000等软件进行工作后，会在“文件”选单中留下一些过去曾经编辑过的历史记录（如图1-3-9所示），这些软件由于设置“列出最近所用文件数”的不同，“文件”选单“记录”数也不同，但都会记录下您最新的操作。

在OFFICE家族中如果你不想让他人知道其中的某个文件的话，可按“Ctrl+Alt+ -（减号）”键，光标会变成一个粗“减号”。打开“文件”选单后，用粗“减号”单击需要删除的文档即可。也可在Word中单击“工具”选单→“选项”→“常规”标签→选择“列出最近所有文件”选项，在其后的输入框中输入“0”，最后单击“确定”按钮，这样就会把所有的文件记录清空，其它的应用程序都有类似的设定，比如RealPlayer就在“首选项”中和Word一样有类似的设置。Word 2000等Office 2000系列软件的“打开”对话框新增了一个“历史”按钮，利用它可以快速打开最近使用过的数十个文档。所以，此处也须提防。这里都是一些快捷方式，直接选中他们执行删除操作就可以。

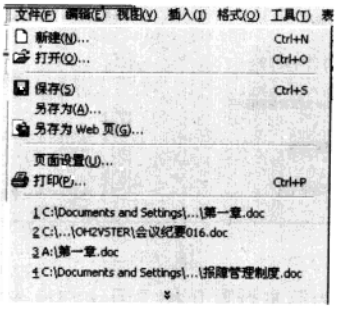

图 1-3-9

除了文件历史记录外，有些应用程序甚至把一些重要的个人信息以明码的形式保存在硬盘上。如果你下机的时候没有把这些文件删除的话，你的隐私或谈话记录就有可能被他人窃取。早期的OICQ版本若是按默认目录安装，那么，在OCIQ的安装目录下可以看到许多账号。双击进入任意一个账号，可以看到“.cfg”的文件，那是本账号的配置文件。还会有很多“.msg”文件，“.msg”文件的文件名就是您的OICQ的朋友的账号。如果有“Tempfiles.tmp”文件，通常是其他人用“语音传送”发来的声音文件，“Tempfiler.tmp”通常是本账号用户发给其他人的声音文件，可以用录音机打开播放。虽然在以后的QQ版本中对这些都进行了加密，但是多多少少都会暴露一些你的信息，至少你的账号会被记录在硬盘上。因此最根本的解决办法是在每次下机后，在QQ的安装目录里把以你QQ号码为目录名的目录整个删除是解决问题的根本办法。