

电脑安全

高手秘笈 *666* 招

Fascn 工作室 编著

西安电子科技大学出版社

2005

内 容 简 介

本书主要介绍电脑日常使用常识，电脑数据和文件损坏后的修复以及电脑安全防护的方法和技巧。

本书适合所有电脑用户使用。对于初学者，通过本书可以学到很多电脑安全的基础知识，并能对自己的电脑进行基本的防护，在遇到问题的时候能够想办法解决。对于有一定基础的电脑用户，本书可以提高其个人电脑安全技巧，从容面对数据损坏或丢失、文件损坏以及黑客病毒等状况。对于电脑高手，本书更是一本查漏补缺的宝典，可以扩大其知识面，使其从一个电脑高手晋级为一个电脑多面手！

图书在版编目（CIP）数据

电脑安全高手秘笈 666 招 / Fascn 工作室编著. —西安：西安电子科技大学出版社，2005

ISBN 7-5606-1526-0

I. 电… II. F… III. 电子计算机-安全技术 IV. TP309

中国版本图书馆 CIP 数据核字（2005）第 047111 号

策 划 李惠萍

责任编辑 阎 彬 李惠萍

出版发行 西安电子科技大学出版社(西安市太白南路 2 号)

电 话 (029)88242885 88201467 邮 编 710071

<http://www.xduph.com>

E-mail: xdupfxb@pub.xaonline.com

经 销 新华书店

印刷单位 西安文化彩印厂

版 次 2005 年 6 月第 1 版 2005 年 6 月第 1 次印刷

开 本 787 毫米×960 毫米 1/16 印张 19

字 数 423 千字

印 数 1~6 000 册

定 价 26.00 元

ISBN 7-5606-1526-0/TP·0815

XDUP 1817001-1

如有印装问题可调换

本社图书封面为激光防伪覆膜，谨防盗版。

前 言

2004年5月3日，是一个让我永远难忘的日子。就在这一天，我亲历了一场数据浩劫。一个小小的疏忽让一个古老的病毒乘虚而入，由于过度相信自己的电脑是安全的，又被黑客利用病毒留下的后门潜入电脑，于是乎就发生了一场让我窒息的惨剧：大量的数据资料被恶意毁掉，5位QQ号码、MSN号码、邮箱密码等都被窃取；尤为严重的是，黑客用我的网上支付卡购买了2000多元的东西……其实我最心疼的是多年积累的资料，还有十年的电子日记！于是我就开始手忙脚乱地自己拯救数据，恢复资料。可是由于经验不足，等到我实在黔驴技穷，带着硬盘来到一家著名的数据拯救公司的时候，工程师告诉我：“如果在发现异样的时候你没有进行任何操作，如果你第一时间就拿到这里，或许你的数据会在10分钟之内完璧归赵！”

此后，我开始潜心研究电脑安全：从病毒到木马，从黑客到恶作剧，从恶意网页到善意代码，从资料备份到数据拯救，还请教了无数专家，求助了很多高手。为了学艺，我故意拿着几个坏硬盘到数据拯救公司去花钱修复；为了能够得到样本，我特意准备了一个毫无防范的电脑等待入侵……

一年多的经验积累与资料储备，促成了本书的诞生。非常感谢李惠萍编辑给我这个机会，将这些经验之谈加以组织整理和重新规划，最后终于成书。撰写本书的目的很简单，就是希望朋友们能多一些安全意识，多一些防范意识，多一些备份技巧，多一些拯救手段，在遇到各种病毒、黑客时都能应对自如。

本书适合所有电脑用户使用。对于初学者，通过本书可以学到很多电脑安全的基础知识，并能对自己的电脑进行基本的防护，在遇到问题的时候能够想办法解决。对于有一定基础的电脑用户而言，本书可以提高其个人电脑安全技巧，从容面对数据危险、文件损坏以及黑客病毒等状况。对于电脑高手来说，本书更是一本查漏补缺的宝典，可以扩大其知识面，使其从一个电脑高手晋级为一个电脑多面手！

Fascn工作室

2005.4



第一章

本章从日常使用电脑的安全谈起，告诉大家使用时常见的危险，常见的个人隐私防护以及最基本的本机安全防护，各种数据文件的隐藏、加密经验与技巧，以及密码遗忘的紧急处理。当然，对于重要数据的清理工作，即如何将它们彻底从硬盘上删除，也是本章的重点之一。



第一节 主动防御，电脑安全从点滴做起

上网也好，写作也好，你总会在电脑上留下痕迹，这些痕迹不经意间就会泄露你的秘密。要想安全，一定要先学会主动防御。

第 1 招 清除访问过的文档和程序

单击“开始→文档”，会看到最近打开的文档的列表。有很多时候，我们希望这些内容是保密的。单击“开始→运行”，会在“运行”窗口的下拉列表框中发现我们运行过的项目。右击任务栏，选择“属性”，打开“任务栏和开始菜单属性”面板，单击“高级”标签，单击“清除”按钮，即可清除最近访问过的文档、程序、Web 站点等记录(见图 1-1)。

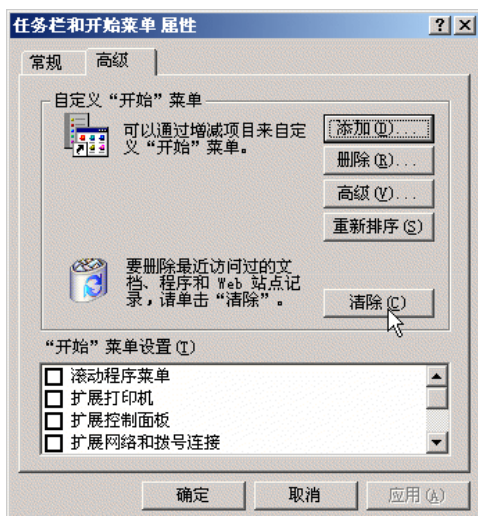


图 1-1

第 2 招 清除上网历史记录

IE 会把用户访问过的网址记录下来。在地址栏输入网址的位置单击下拉箭头按钮时，就能看到这些网址。如果不想让人看到这些网址，可以立即清除。

单击 IE 的“工具→Internet 选项”，在“常规”选项卡中单击“清除历史记录”，即可立即清除上网历史记录。同时，设置“网页保存在历史记录中的天数”为“0”，即可让 IE 不再保存访问记录。

另外，我们也可以下载并安装 Tweak UI 软件(最新版本为 2.10，下载地址为 <http://www.skycn.com/soft/2981.html>)。完成后，打开“控制面板”，再双击 Tweak UI 图标，在打开的窗口中单击“其他杂项”标签，然后选中除了“登录时清除上一次用户”外的其



他所有项目，并单击下方的“马上清除所选项目”按钮即可(见图 1-2)。

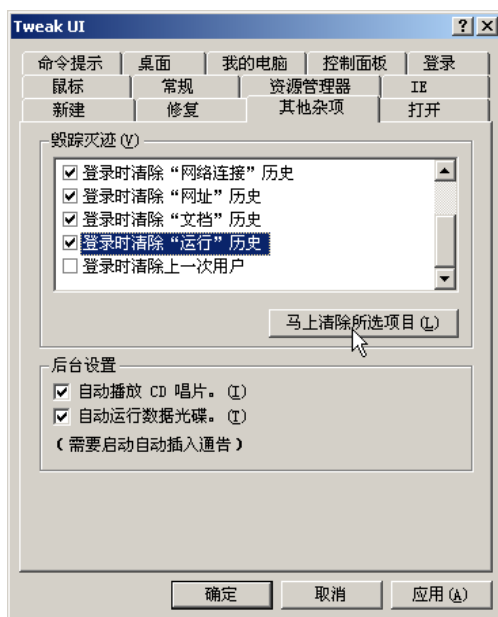


图 1-2



敬请注意

Recent 目录里面存放着更多的历史记录。打开资源管理器，定位到 <C:\Documents and Settings\用户名\Recent> 文件夹，将里面的文件删除即可。

第 3 招 清空 Windows 临时文件夹

临时文件夹下经常会有很多文件，这里面的文件也极有可能是我们不想让别人看的。这时，我们完全可以让它自动删除掉。

对于 Windows 9x/Me 系统，可以首先拷贝 <C:\Windows\Command\Deltree.exe> 文件到 C:\ 目录下，然后编辑 C:\Autoexec.bat 文件，加入以下语句即可。

```
deltree /y c:\windows\temp >nul  
md c:\windows\temp
```

对于 Windows 2000/XP 系统，可以在 C:\winnt 中新建一个文件 cls.bat，并输入以下内容：

```
c:\  
cd %temp%  
del /f/q/s *.*
```



```
rd /s /q
```

然后将其快捷方式放到“开始→程序→启动”中。这样，当 Windows 启动时，会自动删除掉临时文件。



敬请注意

`deltree` 命令的作用是删除一个文件夹及其下的所有内容，其使用与 `del` 命令无异，但在 Windows 2000/XP 中已经取消了此命令。

第 4 招 彻底删除文件

要想直接删除文件而不是把文件移入回收站，只需在删除的时候按住 **Shift** 键就行了。

我们还可以设置按下 **Del** 即直接删除，其方法是：右击回收站，勾选“删除文件时，不将文件移入回收站，而是彻底删除”。



敬请注意

一定要注意，在删除网络邻居共享文件夹、移动设备(如软盘、U 盘、USB 硬盘)中的文件时，文件不会被送入“回收站”而是直接被删除。

第 5 招 清空回收站

在删除重要文件后，一定记住还有个回收站，这里保存着被删除的文件，这些文件随时可以恢复。按 **Win+D** 键切换到桌面，打开“回收站”，选中要删除的文件，再按下 **Del** 键即可从硬盘中删除它。如果要删除整个回收站中的内容，右击“回收站”，选择“清空回收站”即可。

第 6 招 手工删除 Windows 的 Cookies 数据

Cookies 是 Web 服务器发送到电脑里的数据文件，它记录了诸如用户名、密码和关于用户兴趣取向的信息。而且，现在很多网站收到的 **Cookies** 文件中的用户名和密码都是以明文方式存放的，这样就更不安全了。因此，删除 **Cookies** 文件很有必要。

对于 Windows 9x/Me，打开<C:\Windows\Cookies>文件夹，将 **index.dat** 外的其他所有文件删除即可。

对于 Windows 2000/XP，打开<C:\Documents and Settings\用户名\Cookies>文件夹，然后删除 **index.dat** 外的所有文件即可。

第 7 招 自动清空 Cookies 的批处理

下载并安装 **xxcopy**(下载地址为 <http://act.it.sohu.com/download/show-23081.html>)，新建一个快捷方式，即在命令行输入“**xxcopy C:\Windows\Cookies*.*/s /h /y /rs /xindex.dat**”(Windows 9x/Me)或“**xxcopy "C:\Documents and settings\用户名\Cookies*.*" /s /h /y /rs /xindex.dat**”(Windows 2000/XP)，然后把其放到桌面上，这样随时双击该快捷方式即可清空



Cookies。xxcopy 需要单独安装。

第 8 招 彻底阻止 Cookies

如果你非常担心 Cookies 泄密，不如干脆禁止它！打开 IE，选择“工具→Internet 选项”，选中“隐私”选项卡，再用鼠标调节 Cookies 滑杆到最高处(见图 1-3)，表示阻止 Cookies，这样就可以一劳永逸，用不着每次进行删除操作了(但有些论坛要求打开 Cookies 功能)。

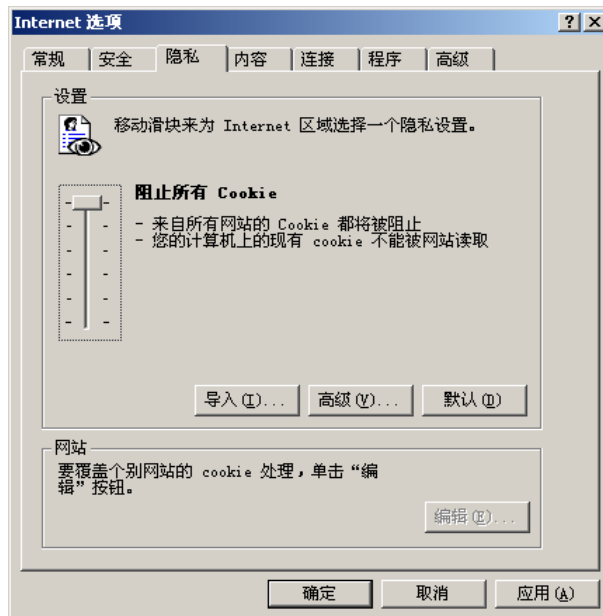


图 1-3

第 9 招 防止“自动完成”泄密

当我们在网上进入 E-mail 信箱或访问论坛时，需要输入密码，此时，IE 会提示你是否保存这些密码。如果选择“是”，那么下次访问时，IE 就能帮你自动输入密码了。这虽然方便了操作，但一旦别人使用了你的电脑，这个保存密码的功能就给我们留下了巨大的安全隐患。因此应清除此设置。

打开 IE，选择“工具→Internet 选项”命令，再单击“内容”标签，单击“自动完成”按钮，在打开的窗口中取消“Web 地址”、“表单”和“表单上的用户名和密码”复选框，这样 Windows 就不会记录这些东西了。单击“清除表单”和“清除密码”按钮可以立即清除掉先前自动完成的内容(见图 1-4)。

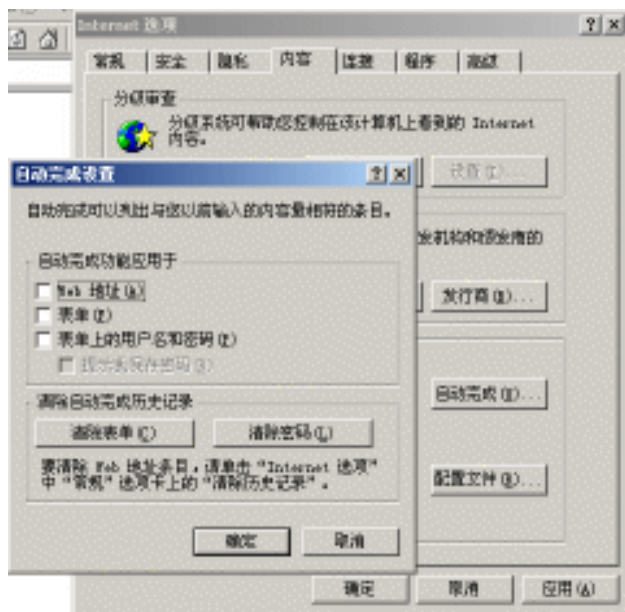


图 1-4

第 10 招 别忽视剪贴板泄密

很多用户有很多密码，并喜欢将其保存在“记事本”里面，用的时候按 **Ctrl+C** 复制出来随时使用。还有一些文字处理人员，经常会用到复制和粘贴，可是如果你没有做任何处理就离开电脑，那么别人只要按下 **Ctrl+V** 键就可以轻易看到剪贴板里面的信息。

怎么避免泄密呢？很简单，在“记事本”里面随便拷贝一个数字或字母就行了，这样最新复制的内容会覆盖原先的内容。



敬请注意

如果你使用了诸如 ClipCache Plus、Clipmate 之类的剪贴板增强工具，那么它会自动记录剪贴板中的信息，而且会保存在磁盘上，这时就必须使用这些软件中的清除功能了。

第 11 招 禁止 Word 显示最近文件列表

Word 会列出最近的几个文件的列表，单击“工具→选项”命令，切换到“常规”选项卡，清除“列出最近所用文件”复选框前的“√”标记，即可取消显示列表功能(见图 1-5)。在 Excel 和 PowerPoint 中也可以进行类似的操作。

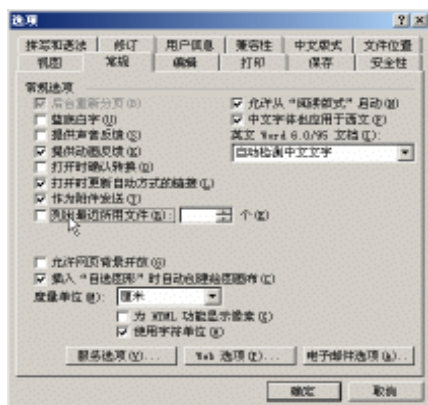


图 1-5

第 12 招 禁止 WPS 显示最近打开的文件列表

对于 WPS 2000 和 WPS Office 2002/2003, 请选择“工具→综合设置”命令, 并在打开的“综合设置”窗口中选择“系统”标签, 把“列出最近使用的文件”后面的数值设置为 0 即可。

第 13 招 保密 FlashGet 下载内容

如何不让别人看到你的 FlashGet 下载记录呢? 进入 FlashGet 安装文件夹, 如 <C:\Program Files\FlashGet>, 删除 Default.bk1、Default.bk2、Default.bk3、Default.jcd 和 Default.jcd.bak 这五个文件即可清除 FlashGet 的下载记录。

第 14 招 清除网络蚂蚁的下载记录

对于 NetAnts, 选择“文件→清除下载记录”命令可以清除下载记录, 或者将 <C:\Program Files\NetAnts\netants.job> 文件删除, 也可达到此目的。

第 15 招 防止网络黑客入侵

对个人而言, 除了病毒、误操作、恶意代码等危险外, 来自网络的黑客也会造成很大的威胁。

邮件入口是黑客入侵的主通道。现在最厉害的病毒(如“求职信”、“新欢乐时光”等)都是从这个通道入侵的。如果在这个入口能加进一道病毒过滤网, 那么电脑中毒的机率将大大减少。

网页成为病毒的入口也就是近两年的事。病毒炮制者在网页脚本中加入病毒程序, 让你在不知不觉中就已经中了它的圈套。如“爱情森林”, 听起来是多么富有诗意, 多么令人神往的地方, 可它却是病毒诱人的陷阱。

文件成为病毒的入口, 从病毒诞生之日起就开始了。由于人们在实际工作中需要频繁地使用和拷贝文件, 病毒就以此为载体, 在电脑与电脑之间传播。尤其是现代社会, 人们



为了共享资源，组建了局域网，这就使得网络更加成为病毒感染的高速公路。

注册表是恶性病毒攻击的最大目标，也是系统最薄弱的环节。注册表一旦被病毒破坏，就意味着系统的崩溃。

内存是病毒最安全的藏身之所，很多时候病毒都藏在内存里面，任你怎么用杀毒软件都不能查杀，这时候必须重启电脑，并且到 DOS 下面才能彻底查杀。

第二节 重要数据，想方设法保安全

相比泄露密码而言，数据安全更重要，尤其是重要的数据，无论如何都要确保它的绝对安全！

第 16 招 改文件名避免被关注

给文件或文件夹取名，尤其是给重要的文件夹或文件起名时，千万不要在文件名中出现过于敏感或引人注意的词，相反应取一些常见的文件名，比如 Autoexec、config、system、帮助等，这样可以避免受关注。

第 17 招 隐藏文件夹是最简单的手段

右击文件夹，单击“属性”标签，在如图 1-6 所示的窗口中勾选“隐藏”，然后单击菜单“查看→文件夹选项→查看”，在“隐藏文件和文件夹”选项卡中勾选“不显示隐藏的文件”（见图 1-7）即可隐藏文件夹。这种方法只能对付菜鸟，但是对于有一些电脑基础的人来讲，只要在“隐藏文件和文件夹”选项卡中勾选“显示所有文件和文件夹”，就可以轻松地看到所有文件。



图 1-6

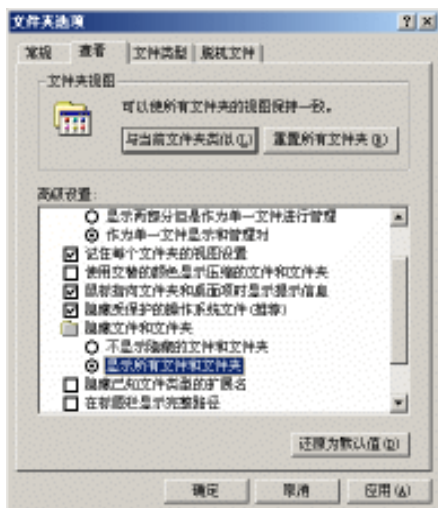


图 1-7

第 18 招 让隐藏的文件看不见

虽然将一些文件的属性设置成了“隐藏”，但如果打开资源管理器的“查看→文件夹选项→查看”，选择“显示所有文件和文件夹”，那么所隐藏的文件就会一览无余地被显示出来。通过下面的技巧可以让隐藏的文件彻底看不见。

打开注册表编辑器。找到[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\explorer\Advanced\Folder\Hidden\SHOWALL]，在右侧窗格中找到名为 CheckedValue 的 DWORD 值(如没有请添加)，将其值改为 0，然后关闭注册表编辑器。这样你的隐藏文件就彻底隐身了。如果想再显示出来，只需把 CheckedValue 的值再改为 1 即可(见图 1-8)。

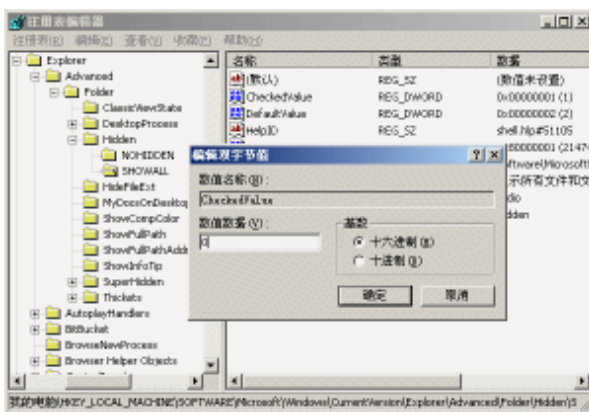


图 1-8



第 19 招 在文件管理器里藏文件

如何隐藏一些重要文件呢？可以打开文件管理器(运行 Winfile.exe)，单击“查看→按文件类型”命令。在弹出的“按文件类型”对话框中选中“显示隐含/系统文件”的复选框，然后单击“确定”按钮退出(见图 1-9)。按 F5 键刷新显示，这时在“文件管理器”左侧的目录列表里会发现多出一个名为 Recycled 的隐藏目录(它实际上就是“回收站”的文件夹)，由于在“文件管理器”里只能看到已删除的文件，其他文件则不会显示(见图 1-10)，因此我们可以把要隐藏的文件拖动到里面即可。以后不管你怎样进行“回收站”清空，都不会删除自己隐藏的文件。如果想使用文件，只需运行 Winfile.exe，打开“文件管理器”，找到 Recycled 文件夹，选中欲恢复的文件，把它移动到其他地方即可(仅适用于 Windows 98)。

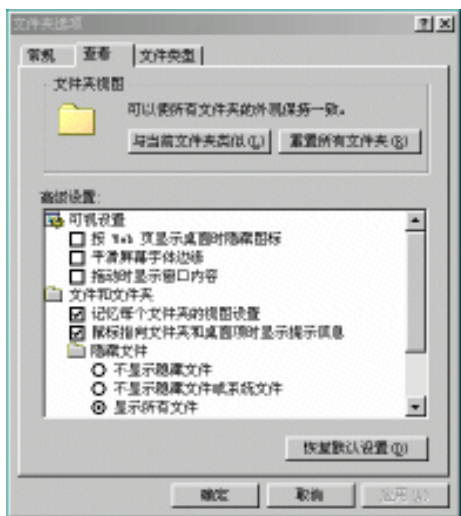


图 1-9

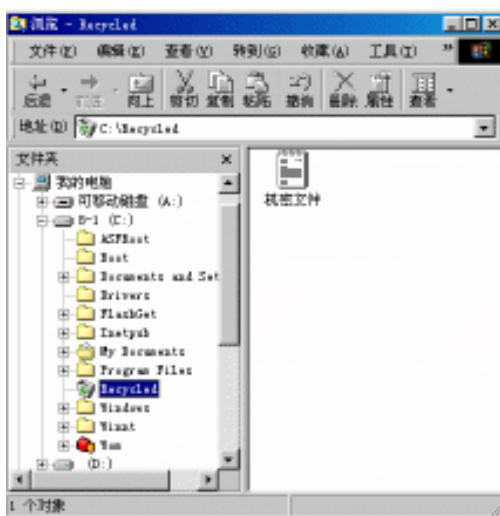


图 1-10



敬请注意

为进一步提高安全性，你可以在用“文件管理器”把文件移动到回收站后，把 Windows 文件夹下的 Winfile.exe 改成其他名字，比如 Winf.exe，这样如果有人想用“文件管理器”来窥探你的秘密，恐怕连门儿都找不到。

第 20 招 在资源管理器里藏文件

打开记事本，输入如下内容：

```
[Shell]
Command=2
IconFile=explorer.exe,1
[Taskbar]
```



```
Command=Explorer
```

然后单击“文件→另存为”，保存为“”fascn.scf” (fascn 为文件名，可以随便命名，一定要加半角引号，才能保证 scf 为扩展名)，最后保存生成的文件变成了“资源管理器”图标。双击此文件，熟悉的“资源管理器”就会被打开了。

用记事本打开此文件，在上面的内容下面输入需要保密的内容，比如手机号码、QQ 号码、E-mail 地址、各种密码等，保存后这就是一个绝对安全的私人文件了。任何人双击只会打开资源管理器，而只有我们自己知道，使用记事本或者其他文本处理软件打开才能看到里面的内容。



敬请注意

(1) 在 `IconFile=explorer.exe` 一行后可以键入 0~7 中除了 1 以外的任意一个数字，每一个数字对应一个图标。如果不喜欢这些图标，那就干脆在“`IconFile=`”后键入喜欢的图标的具体路径吧。

(2) 将“`Command=Explorer`”换成“`Command=ToggleDesktop`”，双击此文件时就是自动最小化所有程序窗口和最大化程序窗口。

第 21 招 让 Subst 帮你藏起驱动器

微软建议用户虚拟磁盘驱动器符(Subst)时采用未使用的盘符进行虚拟，但并不表示它不能虚拟已经存在的盘符，比如 A 盘、C 盘、D 盘等。利用这一点，你可以通过 `Subst` 命令虚拟 A、C 等盘符，直接覆盖这些已存在的盘符，使别人无法看到该盘的真正内容，达到隐藏真实驱动器的目的。

例如，可以先在 C 盘根目录下创建一个名为 `fascn` 的文件夹，建立完成后最好将文件夹的属性设置为“只读”和“隐藏”。然后对 C 盘根目录中的自动批处理程序 `Autoexec.bat` 进行编辑，加入以下代码：

```
C:\Windows\Command\Subst A: C:\fascn
```

这样每次系统启动后软盘的图标就变为硬盘的样子，打开看一下，其中的内容也变了，这样就轻松达到了偷梁换柱的目的，别人一般难以发现其中的奥秘！当要还原时，只需单击“开始→运行”，输入：`Subst A: /D` 即可。

第 22 招 用映射法访问隐藏的驱动器

如果自己要访问被隐藏的驱动器，可采用下面的方法将目录映射成该驱动器。在删除驱动器后，右击已经被删除的驱动器，选择“更改驱动器名和路径”，然后单击“添加”，在“添加驱动器号和路径”窗口单击“装入以下空白 NTFS 文件夹”，然后单击“浏览”，选择一个空白文件夹，最后单击“确定”即可。注意选择的文件夹必须是建立在 NTFS 文件系统上的空白文件夹，而且选择的文件夹最好不要放在明显的位置上。以后就可以通过打开该文件夹来访问被隐藏的驱动器了。



第 23 招 电脑启动软驱成空

单击“开始→运行”，输入“regedit”并回车，启动注册表编辑器，在 [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run] 下新建一个字符串值，并命名为 system(这样就不会有人敢随意修改它了，除非他不识英文)，双击它，在键值中输入以下代码(见图 1-11)：

```
subst a: d:\temp
```

退出注册表编辑器，下次启动系统时，你的软驱就变成空的了！

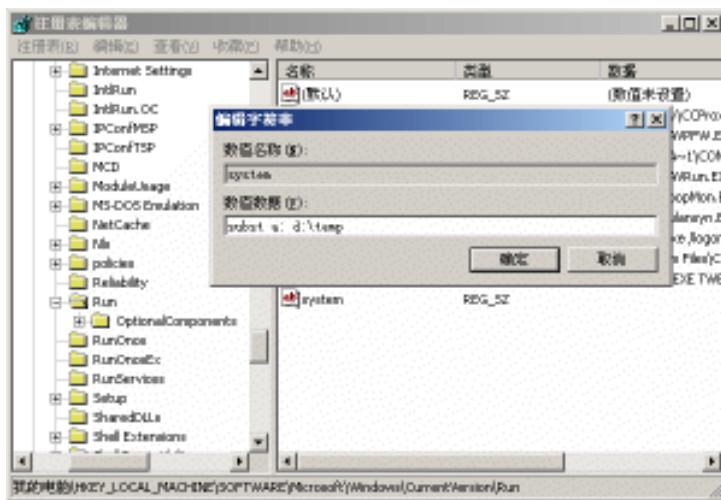


图 1-11

第 24 招 把一般文件夹图标改成系统文件图标

有时候，将文件夹变成一个系统文件，会起到很好的防护作用，起码能够减少一些“眼球”的关注。这里举例将 fascn 文件夹的图标变成 DLL 文件的图标样子。

单击“开始→运行”，输入“cmd”后回车，在命令行提示符状态下输入：`attrib +s c:\fascn`，回车即可为该文件加上系统属性。

然后打开记事本，键入如下字符串：

```
[.ShellClassInfo]
IconFile=C:\WINNT\SYSTEM32\Shell32.dll
IconIndex=72
```

将其另存为名为“Desktop.ini”（注意一定要加英文的引号）的文件并保存到 C:\fascn 文件夹中。关闭 desktop.ini 文件，然后按 F5 刷新一下文件夹，这时图标就变成 DLL 文件的图标了。



第 25 招 让文件夹图标更多样

上面是以 Windows 2000 为例的，其中：IconFile 就是图标文件，可采用 .ico、.exe、.dll 等包含有图标的文件充当，DLL 文件的图标就在 Shell32.dll 文件中，因此应输入：C:\WINNT\SYSTEM32\Shell32.dll(如果是 Windows 98 则为 C:\WINDOWS\SYSTEM\Shell32.dll)，而 Iconindex 用来指定一个图标。如果指定的 EXE 或 DLL 中包含不止一个图标，若想使用第一个图标，就写上 Iconindex=0。DLL 文件的图标为 72(Windows 98 的为 66)。在没有该行定义的情况下，默认使用第四个图标，即 Iconindex=3。

第 26 招 借系统目录警告打造系统级目录

当我们打开 Windows 文件夹时，会在左边看到提示信息，警告该文件夹里面的文件比较重要。如果你想看里面的文件，可以单击“显示文件”命令。下面我们就来自制一个系统级警告文件夹，而且还要把“显示文件”链接去掉，这样除非知道内情的人，否则想要看到里面的文件还真要费一番心思。

打开资源管理器，单击“查看→文件夹选项”菜单，设成显示全部文件；然后复制系统目录下的 Folder.htt 和 Desktop.ini 两个文件到需要隐藏的文件夹里，将文件夹属性设为“只读”；接着用记事本打开文件夹里的 Folder.htt 文件，找到并删除“显示文件”即可(见图 1-12)。这样这个文件夹就会像 Windows 系统目录一样出现一段警告语。当我们需要使用这个文件夹的时候，只要去掉“只读”属性，文件将全都呈现出来。

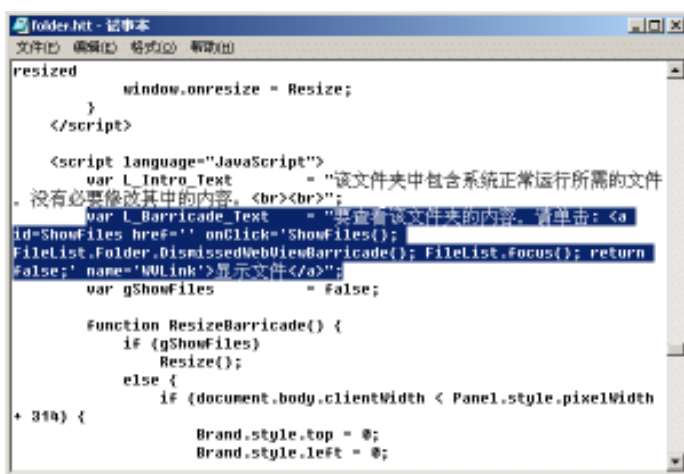


图 1-12

第 27 招 打造系统级别的隐藏文件夹

进入 DOS 命令行提示符状态，输入“attrib +s +r 文件夹名”，这样就给文件夹添加了



系统和只读属性。由于属性呈灰色(未激活状态),不能在 Windows 界面将其属性去除,因此不熟悉 DOS 命令的人根本无法修改它。要想去除系统和只读属性,就必须使用命令“attrib -s -r 文件夹名”。

第 28 招 将文件夹变成声音文件

类标识符在 Windows 中的英文缩写为 CLSID,是一个 128 位长的符号代码(16 个字节),由花括号和一些数字、字母组成,用来标识应用程序、文件、控件类型等对象,就好像文件类型的身份证一样。通过它我们可以将一些文件夹变成某些特定系统文件,比如 .wav 文件。

新建一个文件夹,把要隐藏的文件放入该文件夹中,然后将文件夹重命名为 fascn.wav.{00020C01-0000-0000-C000-000000000046}(见图 1-13),这样你会看到该文件夹的图标变成了 wav 文件的图标,名称是 fascn.wav。双击它,执行的动作不是进入文件夹,而是启动“媒体播放器”。文件夹仿佛变成了声音文件,但却提示打不开,右击则出现播放命令,别人一定会以为是受损的声音文件。要想打开它,可直接选中并右击该文件(其实是文件夹),选择“打开”即可。

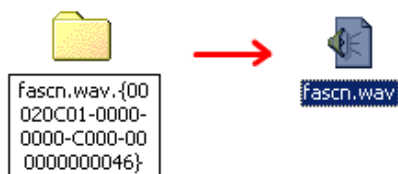


图 1-13

第 29 招 将文件夹变成网页文件

将文件夹重命名为“fascn.{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}”,就能将文件夹变成网页,双击后可用 IE 浏览器来打开。

第 30 招 将文件夹伪装为网上邻居

将要伪装的文件夹改名为“网上邻居.{208D2C60-3AEA-1069-A2D7-08002B30309D}”,确定后你就会看到文件夹变成了“网上邻居”!双击,确实实现的是网上邻居的功能!

第 31 招 将私人文件夹变为回收站

当然还可以把自己的文件夹伪装成其他系统文件夹,比如回收站。这时只需将要伪装的文件夹改名为“.{645FF040-5081-101B-9F08-00AA002F954E}”即可。

第 32 招 将文件夹变为桌面

将文件夹重命名为“桌面.{00021400-0000-0000-C000-000000000046}”,可将其变为桌面按钮。

第 33 招 将文件夹变为公文包

将文件夹重命名为“公文包.{85BBD920-42A0-1069-A2E4-08002B30309D}”,可将其