

技术安全手册

黑社会手段抢夺地盘

然而3721在圆自己的美梦时却毁掉了众多网民的基本的使用权。众多不知情的网民在无意下载3721插件后却一直在被3721的梦想所左右。3721的插件也已经开始在90%的中文上网用户打开电脑开始上网时被监控。

有懂技术的网民在论坛上发表言论时写道：这两天某些网站不是很顺利，开始我以为是网络的问题，可是其它网站上的去很正常，因此我排除了网络原因。排除了病毒原因之后，我反编译了其电脑里唯一和浏览器相关的程序——3721网络实名插件。当看到3721程序代码的时候，他说：“当时吓出了一身冷汗。原来这个程序有个后门，所有的人都不知道存在的这个后门。而3721的其他程序就通过这个后门进进出出。在这个程序中我发现了一段代码，这就是屏蔽那些网站的代码，在这个代码后面，有着一长串我们熟悉的网站，有的屏蔽是生效的，有的屏蔽还没有启用。这段代码就像一个机器人一样，在这段代码后边，如果加上<http://www.sina.com.cn> 那么新浪网将被屏蔽而无法访问。

3721为了保住他的网络实名业务，不得不保

资料点安全及运转

小型资料点的采购小经验 及推荐的硬件配置	50
制作资料 and 购买耗材的经验交流	58
对最近制作资料的一点经验 ——小型家庭资料点（图）	60
做资料工作必备的几个电脑工具软件	68
希望资料点的同修注意手机安全	70
电话监听现状分析	71
谈大陆国安对电信通讯系统的监控	77
移动通信的基本知识	80
无线上网（专门用于笔记本） 与手机上网那个更安全	84
手机的屏蔽	85
关于手机通信安全及对 《手机的屏蔽》一文的反馈意见	88

目 录

计算机安全及维护

Windows 2000 和 Windows XP安全 (一)	01
Windows 2000 和 Windows XP 安全 (二)	19
Windows 2000 和 Windows XP 安全 (三)	28
使用 Windows 任务管理器的方法	32
Windows XP默认设置需注意8个安全问题	33
“启动电脑” 密码设置	39
清除Acrobat Reader的	
最近打开文件的名称	41
关于清理电脑敏感信息的一点补充	42
清理使用花园软件上网	
在Zonealarm上的痕迹	47
删除和禁止NERO刻录软件	
文件下拉菜单历史记录的方法	49

网络安全

网上计算机安全问题分析	91
明慧网页投稿增加对传送附件的支持	94
明慧网网络突破工具支持表	96
计算机反黑客安全设置的建议	97
上网必须注意的几个安全问题	100
诺顿杀毒病毒库更新方法	103
对“2004年9月6日注意清除网络	
防火墙中的历史信息”一文的补充	104
使用网际快车和无界浏览	
下载明慧每天文章方法	107
关于使用网际快车	
和影音传送带的安全问题	109
3721有哪些严重危害?	111

希望这本小册子对你有所帮助，同时注意保护这些信息，不要让邪恶掌握我们做事的方式和方法。

住他插件的推广量，而3721用这种手段，在威胁并强迫着许多网站为他弹插件。而许多网站却敢怒不敢言。

3721就像中国互联网的黑社会，他知道你电脑里的所有信息，他占据着本属于网民的中国互联网，把他划为属于自己的地盘，牢牢控制，即便是SINA、SOHU、NETEASE、QQ这样的门户大腕，慑于3721的淫威，在3721面前也是敢怒不敢言。

用三条计谋堂而皇之的赚钱，大大方方的管理中国互联网。原本互联网所倡导的平等、自由、公开的原则，在3721的公司利益面前荡然无存。

3721的功能：

俘获浏览器的请求强制在3721自己的服务器上解析请求并存档。

你装了3721不管用多安全的破网工具等于没有用，一切都在它的眼皮底下。

3721的几个dll插入了系统的explorer进程，这更恐怖，它想对你的系统做什么就能做什么。用控制面板的「新增 / 移除程序」来移除3721不可靠吗？它像一个癞蛤蟆一样粘你的机器上了，普通方法是删不净的。

胜防的在各种网站上弹出骚扰对话框，强迫安装。有程序员表示：“不管软件写的怎样，有一点是肯定的，开发者和策略制订者缺乏起码的职业道德。现在所谓2000万用户，有多少是自愿安装的呢？又有多少是踩中地雷的呢。”

因此，3721接下来就好像故意要同程序员做一些对抗的工作。为了防止卸载删除，软件中采用各种技术手段。有程序员说：“现在3721的插件越做越霸道。不止是修改注册表，而是一直在你的系统里运行，并把自己伪装起来，我曾经把cmin*.dll删除后，用WinHex查还有，是改名运行的！而且如果用SoftICE 调程序，3721的DLL总会捣乱！”3721在煞费苦心的加入各种技巧，有的技巧与木马病毒的原理一模一样，所有3721的软件在你的计算机上都开着后门，而这个后门，正是3721走进你计算机深处的通途，3721在偷窥你的时候，你，却并不知情。

用程序员群体的眼光看，用软件开发的某些技巧来强奸用户的意志，这对3721是自辱，对中国互联网是侮辱！更有程序员还在个人网站中标注：“如果你是3721的支持者，不要安装本程序，本人不欢迎并拒绝其支持者使用本程序！”

学会上网之后，原本以为到达了一个更加便利的世界，然而，这个自由便利的世界却早被3721统治。3721从1998年成立至今一直在利用微软的浏览器做着自己的梦，试图打造中国的网络标准。用了5年时间，3721通过各种渠道、利用各种手段，让他的网络实名插件遍布90%的中文上网用户。3721插件，表面上是中文上网工具，实际上，背后利用简单的病毒原理控制着网民的电脑，玩弄着中国互联网和对技术不甚了解的7000万网民。在中国，没有政府的支持，哪一个公司敢如此坐大？

用简单的技术愚弄着中国网民

这样一个打着“简单上网”旗号的3721，在程序员眼里，甚至成为了“垃圾”的代名词。

首先，程序员对3721的技术一直没有持肯定态度。最初，3721的软件是客户端的形式，主要通过和网站合作进行免费发放，但这种方式容易被用户拒绝或者删除。不久，3721采用了微软公开的ActiveX技术标准，将客户端转变为了浏览器插件。应该说，许多软件均采用ActiveX技术开发，例如Flash动画播放插件、Microsoft Media Player插件等，这种方式也无可厚非，但3721在推行这种方式时，并没有尊重用户的意愿，而是防不

计算机安全及维护

Windows 2000 和 Windows xp 安全 (一)

【明慧网2004年10月22日】

Windows 2000 和 Windows xp 安全 (一)

在五年多的反迫害和证实法的过程中，海内外同修通过互联网突破邪恶的封锁：揭露邪恶迫害的真象，向世人送去大法的福音。事实表明，互联网给我们带来了极大的便利。

从目前的现状来看，我们对突破邪恶对网络的封锁、保证信息的安全方面做了很多工作，确实起到了否定邪恶的作用。但是，我们对计算机在互联网上的安全问题，好象重视不够；从明慧网上经常还听到资料点被破坏的消息，是不是有技术方面原因，也没有认真总结，找出不足。

因为互联网在设计当初安全问题就考虑不

服务器告诉你你所打入的网址真实（IP）地址是什么，等于告诉别人你想上的网，而域名劫持就是在中国通往国际域名服务器的出口网关处实施的）。28日文章作者采用的这种方式，目前在中国大陆许多地方由于相应的域名解析被封锁应该不能用（7月15日所提的问题应该就是这个情况），能用的应属个别现象，也有可能是圈套。

如果发现“屏幕右上角的进程框一直显示“0”，不能下载”等情况应马上停止该下载任务，否则软件还会持续发送域名解析服务请求。

解决的方法是：

1. 如果网页链接不自带代理方式，需为网际快车和影音传送带等设置代理并“选用”代理，需要说明的是网际快车和影音传送带等一些下载软件并不理会IE所设置的代理，需要在软件本身设置；软件代理只设置不行，还必须“选用”才行（代理服务设置请参考网上专有文章）。网际快车在选用代理服务器时不要勾选“多代理...”。影音传送带设置代理服务器后，每次下载的任务都要在“其它设置”选项中选择一次代理服务器（单一设置-代理名）。

需要说明的是，网际快车不支持SSL加密代

关注。

以我个人为例（为了说明问题），我在迫害的开始，写的一些揭露邪恶的文章，我是一边送给明慧网，一边给单位头头，单位没有说什么。但是同修有很多事向邪恶说了（他们还认为他们修得好），有的还是很大的事，结果把我弄得很被动。就在邪恶的劳教所，还发生这样的事，后来我真的有点受不了了。在我被迫害期间，我妻子，大法弟子，也遇到同样问题，因为她计算机技术不够，想问题变通差一点，结果数次被抄家，损失不少计算机设备。

通过这样的事情，我是想说明，我们大家配合好很重要，如果有常人心不去，被邪恶利用，就会给证实法造成很大损失。

（2）被迫害的第二个原因，就是技术上没有使用好。尽管从明慧网上看，因上网而产生的迫害事例比较小，但与实际有很大出入。一方面是因为不用说的原因，同修不愿把这样的事登在明慧网；另一个原因是在同修被迫害中上网是一个方面原因，大家也不愿把这样的事说出来让邪恶知道。事实上因为上网和资料而被迫害的同修还是比较多的。

周，连接到互联网的计算机本身就有个安全问题。我们资料点同修计算机技术通常了解不多，如果对一些软件使用不当，就会产生严重的安全问题，而这些问题表面上是看不见。

我从1999年的425以后，就开始通过互联网联系大法网站，在这个过程中经历了各种各样的事情。最开始，我通过自己的商务电子邮箱给明慧发信，好在自己在师父的呵护下及时清醒，没有造成后果。实际上那时邪恶就一直在监控我们电子邮箱。

当初自己在技术上帮助过的上网同修，很多受到了严重迫害。在自己被严重迫害中遇到的同修，很多也跟上网和资料有关。**产生迫害的原因，主要有以下方面：**

(1) 同修配合不好，还不是一般的不好，而是非常的不好，在常人的观点上看都是很不好。在求圆满的自私观念带动下，活动也想参加，资料也要，并且还说我要怎么样维护大法，可是一到关键的时刻，就把别人说了，把同修弄得很被动。还有同修之间由于显示心被邪恶利用（确实是被邪恶利用，只是没有邪悟严重），传谁谁是资料来源，而这些信息被特务收集，使在资料点工作同修被邪恶

(3) 同修对法理解不够，可以说这是根本原因。也许有同修说，有了根本原因就不用找其它原因，我认为不行，因为对法理解不是你想做就能做到的，有一个过程，那么在这个过程中，就需要我们采用必要的常人手段来解决问题。

在后来的一些证实法的工作中，我看到了大家对计算机安全重视不够的问题，提了出来，希望计算机专家研究一下，同时也怕自己把问题搞错了，给大家带来损失。通过一段时间的软件编写工作，自己在计算机方面的知识有了提高，根据师父的教导，大法弟子是一个整体，那里有问题要互相补上，所以我根据 Microsoft Press 2002 年出版的 Microsoft Windows Security Inside Out for Windows XP and Windows 2000（有中文翻译本）一书讲述的 Windows 安全问题，再结合我们证实法的需要，边读边写一些技术问题文章，希望对同修有所帮助。因为我也是边读边写，可能还有一些实验，所以一下出不了，我尽量快一点。

今天，我们首先来看一下，在我们证实法的过程中，连接到互联网的资料点计算机，**有那些安全问题**（这些问题对海外同修也是同样重要的）：

(1) 物理攻击

理，现在的代理基本都是SSL加密的，所以推荐使用影音传送带。

2. 如果网页链接自带代理则不必设置代理，直接下载即可。

区分网页链接是否自带代理的方法：打开需要的网页后，在要下载的连接上点一下鼠标右键，选择“复制快捷方式”，然后打开一个文本编辑器（如记事本、word等），在空白处点鼠标右键，选择“粘贴”如果前面显示“http://127.0.0.1:xxxx/...”的字样则是自带代理。

3721有哪些严重危害？

金山毒霸是不是和3721合作了呀，我上星期六装金山毒霸2003，装完了突然发现IE栏里多出来一条“上网助手”，我当时脑袋就大了……难道这就是传说中的3721上网助手？打开一看，果然……晕……整天喊着防备3721，也修改了注册表对付3721，谁知道它从这里冒出来了……然后……我们发现我们论坛下边的快捷跳转不能用了，要去别的主页，先要点‘天地无忧’，然后再点要去的主页，痛苦，然后……痛苦的重装系统，我绝对不允许别人随便在我的电脑里乱装东西。

定”→“另存到(A):”栏右侧按钮另行指定存放地址后，“文件分成”选1，“开始”选“手动”→“确定”即可。

使用最新的无界浏览（ultraSurf）6.2或6.0上网（可以不必用代理）当锁头图标出现后，双击网际快车里“正在下载”列表中的某日文章地址下载。如果中途停止且长时间不见继续下载，可以右键点地址选择“暂停”，然后再“开始”，如果始终不能继续下载，可以右键点地址选择“将网址复制到剪贴板”，右键点地址选择“删除”，点“任务”→“新建下载任务”，地址会自动复制到“网址(U):”栏，“另存到(A):”栏指定存放地址后“确定”→选择“重新下载”即可。

关于使用网际快车和影音传送带的 安全问题

【明慧网2004年8月1日】04年7月27日技术交流《关于网际快车下载的问题》文章中直接在“URL”的对话框里打入网址的方式有安全隐患。使用网际快车（flashget）和影音传送带（Net Transport），直接在“URL”的对话框里打入网址，会在国际域名服务器解析该域名（即要求域名

单的给出如下解决办法。这里选择的断点续传下载工具是网际快车。

打开网际快车→“工具”→“选项”→“代理服务器”→“添加”→随便命名比如“无界”，点选“HTTP (Get)”→“服务器”栏添入127.0.0.1“端口”栏添入9666→“确定”→在选项面板里勾选“无界”的前两个选框→“确定”即可。明慧每天文章单日地址是http://www.minghui.org/mh/articles/2004/9/19/2004-9-19-t.zip年月日一看便知，把某日的地址在网际快车→“任务”→“新建下载任务”→“网址(U):”栏里添入，点击“另存到(A):”栏右侧按钮另行指定存放地址后，“文件分成”选1，“开始”选“手动”→“确定”即可。如果想批量把一个月甚至几个月的地址一次性列入下载任务，而每天只需选中一个文件下载的话，批量地址如下（以2004年10月为例）http://www.minghui.org/mh/articles/2004/10/(*)/2004-10-(*)-t.zip（注意里面的括号必须是英文半角的括号）把该地址在网际快车→“任务”→“添加成批任务”→“URL:”栏里添入，“从(F):”前勾选，1到31（因为10月是大月31天），“通配符长度(L):”为1→“确

所谓物理攻击，就是你的计算机放在家里，邪恶到你家里来偷看了里面内容，还装上了后门软件，在你不知道的情况下，把你计算机中文件通过互连网发送到了邪恶那里。

也许同修说，我家门关得很紧，或我在台湾，邪恶来不了，我们不用关心这个问题。这样说，只是对了一半，还有一半不对，就是我们自己“引狼入室”会造成这样的问题。因为没有警惕注意，可能后果更严重。讲到这里，我想说明一个问题，我们通过一些渠道了解到，中国的一些信息公司后台，是国安。是国安出钱找人出面搞的公司，目地为国安收集老百姓的黑材料。××党是搞黑社会起家的（它自己叫地下工作，什么地下工作，见不得人呀，偷偷摸摸干。我看这样干的人死了要下地狱的，干这样的工作在为下地狱做准备，所以叫地下工作吧），这一项是它们的内行，很多老百姓被××党的宣传所迷惑，是不清楚邪恶背后的手段的。

也就是说，如果××软件是邪恶搞的，它里面有后门，我们不知道用了，就会中后门的毒。因为我们不知道，设置防火墙时没有限制这样的软件，所以防火墙也没有办法保护。比如，以前大家说过的QQ、3721就有这样的问题，从国内网上提供

用过的破网软件。找到这个记录后，点击鼠标右键盘，选择“Remove”，然后再点击“确定”，就可以删除这条记录了。

2、在zonealarm的program control的components也有相应的上网记录，清除的办法跟1相同，这里不在多写了。

3、以前同修在相关文章中提过，这里再强调一下，在zonealarm的Alerts&Logs（警告和日志）中有Event Logging（事件日志）和Program Logging（程序日志）两个地方，安装的时候默认是打开的，c:\winnt\internet\目录中有ZA的日志记录，都是Zalog开头的，如果有的话，请注意清除，清除完成后，在Alerts&Logs（警告和日志）中把Event Logging（事件日志）和Program Logging（程序日志）两个地方的选项中都选择“off”（关闭），这样就把za的日志记录功能给关了。保险起见，经常到c:\winnt\internet\去看看有没有什么需要删除的日志记录文件。这里强调一下，删除日志文件最好使用清道夫软件，先把这些日志文件删除到“回收站”里面，最后运行一下清道夫就可以安全删除了。

以上只是我对防火墙使用的一点粗浅认识，由于非计算机专业人员，不知道用norton和za的删除

更加认真。

（2）网络邻居

从“开始|控制面板|系统|计算机名”中，我们可以看到标识计算机的有一个项目叫“工作组”的内容，默然情况下是WORKGROUP，当我们计算机连接到网络上后，如果工作组名相同，我们就可以通过“网上邻居”查到其他计算机，如果其他计算机设置了文件共享（安装时Windows会自动设置一些，支持共享的协议是NETBIOS，NETBIOS是Microsoft开发的网络通信协议），我们就可以看到共享的内容。

在我们上网时，网络服务器就和上网计算机成了“网络邻居”，如果使用不当，邪恶就能看到我们计算机上的信息，解决办法就是在上网的“连接”属性中去掉NETBIOS协议。

我们对随e行上网进行了测试（拨1001），发现拨号连网后，被指派了一个公有IP地址，二个拨号计算机之间，可以互通TCP、UDP网络信息交往包。

（3）病毒

病毒会使计算机工作不正常，我们通过Symantec（赛门铁克）软件能很好解决这个问题，只

的情况来看，QQ肯定有后门。还有国产的杀毒软件，在我们不用它时，它们不也跳出来了，把自由门报成病毒吗？那个流光不也被后门看光了吗？肯定有鬼。

所以，我建议，在不了解真相情况下，为了对自己负责，也是对大法负责，不要使用国产软件。如果必须使用，也不能让它们连通互连网。对于确实要使用的，也应当在实验室里对特定版本测试没有安全问题后，在我们自己网站上公布，然后再使用。国外同修也应该注意这个问题，特别台湾同修，通过互联网讲真相，很好，但要注意安全问题，您连网的计算机中不能有重要信息。

国内资料点同修，可以用一台专用电脑上网，只装一个 Windows，杀毒软件，防火墙，机器可以配置低一点。个人资料点，尽量不用国产软件或让国产软件联网。如果家人要用，我们向他们讲清邪恶迫害真相，用软件做的手脚，我想家人明白后，也是同意的。

想一想，我们用计算机干点什么，信息被后门发到了邪恶那里，那多不好呀。因为我们证实法的事情很严肃，所以我们对于我们证实法中采用的一些方法，也一定要严肃对待，起码比做科学研究要

日志的功能所删除的日志是普通的删除还是象清道夫那样的擦除，估计可能是前者，因此我认为删除日志的最好办法是把日志文件找到，用清道夫来擦除。但是，我一直没有找到norton防火墙存放上网日志的文件位置及名称，请有经验的同修指教。

其实技术只是常人中的手段，我们只是加以利用，最重要的还是我们正念正行，用强大的正念清醒、理智的对待这些问题，

使用网际快车和无界浏览下载明慧 每天文章方法

【明慧网2004年9月20日】（这里需要格外指出的是，当使用过无界浏览并关闭后，再上其它普通网站有时会出现上不去的情况，那是由于无界浏览修改了浏览器的代理服务器地址，可以在浏览器的“工具”→“Internet 选项”→“连接”→“设置”中“代理服务器”的“对此连接使用代理服务器”前的勾去掉然后“确定”→“确定”即可。还有一种情况就是再拨号上网拨不上去，此时可以把拨号密码再输入一次即可。）

看了明慧网2004年9月19日资料汇编里的咨询文章“如何用影音传送带下载明慧每天文章”，简

是我们应当用正版软件，经常更新病毒库。

（4）外部入侵和木马

我们在突破网络时采用的高级手段，如SSSO，意思是说，我们可以通过 IPC 扫描，找到一个机器，然后下上一个代理跳板，就可以安全上网了。这是这个事情的正面，当反过来时，如果我们不注意，被别人扫描了一下，下上了后门，那就可能带来损失。

所以根据计算机专家建议，我们在计算机的用户组管理中（控制面板|计算机管理|系统工具|本地用户和组|用户），把 Administrator 用户名字改一下，密码加长一点为好。

木马，是病毒，也是后门，国内软件查木马根本不行。这个东西破坏力大。

我们可以装上防火墙来保护计算机，使邪恶入侵不了，使邪恶下不了木马，经常重装系统，在连网的计算机中不放重要信息，有些东西用完马上清除，比如上网文章等。ZONE 防火墙免费，很不错，Symantec 防火墙是中文的。

但是一个严重的问题是，我们资料点同修电脑知识不多（一方面是懂网络人本来不多，再一个问题是有这方面能力同修受到了严重迫害，有的邪

底清除这些上网痕迹，可以单击选中这个破网软件的记录，然后点击“删除”按钮，然后一路按确定，这样就把这条记录删除了。等下次再次使用破网软件的时候，norton防火墙会再次询问你是否放行这个软件，再次表示同意就可以了。

2、norton AntiVirus 中的活动日志：

安装norton防火墙的时候一般都同时安装了norton AntiVirus，在norton AntiVirus 中找到活动日志的图标，点击右侧的“查看报告”按钮，打开日志查看器，在左边可以看到许多分类内容，我是一个个的都看一遍，只要有内容的统统删除。实践证明，并没有影响以后的使用。

zonealarm需要手工清除的地方：

1、在zonealarm的program control的program 中有所有上网软件的相关记录，开始的时候，我把所有的程序名称全部选中删除，结果后来再上网出了许多问题，后来实践中发现，只把有关破网软件的记录一一清除，就可以来，清除办法：用鼠标点击Programs下面的程序名称，在下面Entry Detail 的框里面就会显示出有关这个程序的许多信息，在File name中会显示出这个程序文件的位置（路径）和文件名称，通过这里可以判断哪个是曾经使

的了。我装过N次了，杀新病毒比在线升级还提前几天。

更新后的机器要全面查一下毒，除非你很自信。这样你的机器就百毒不侵了！

对“2004年9月6日注意清除网络防火墙中的历史信息”一文的补充

【明慧网2004年10月10日】我使用过norton和ZA两种防火墙，在实践中发现，这两种防火墙都存在使用后手动清理上网信息的问题，先整理如下：

norton防火墙需要手工清除的地方：

1、个人防火墙：

打开个人防火墙的“配置”选项，点击“程序”选项卡，在“手动程序控制”的列表中可以看到涉及访问网络的程序名称，把鼠标指向应用程序的名称（不要点击），过1秒钟，就在鼠标指针右下方显示出这个程序所在的位置（就是路径）和文件名，通过这个提示，可以很容易的判断哪些是我们使用过的破网软件，另外需要注意的就是，虽然在应用程序里面显示的是破网软件修改过后的新名字，但是这个程序对应的图标仍然是破网软件本身的图标，熟悉的一眼就可以看出来。因此，为了彻

悟，现在还没有回来。说到这里，我想说一句，我们有好些同修是因为同修没有配合好被迫害，被迫害同修确实有执著，但是如果你不说他，他可能会提高就没有这个问题了。在被迫害中，他们做了一个修炼人不该做的事，确实很不应该。但是我们外面同修事后不是从法理上帮助这些人，而是骂，骂得很难听，两口子在家里还大打出手，我不知道这些人法怎么学的，师父在《建议》都说了，那个旧势力对迫害过不去的人还说是想要什么重新加大所谓魔难过关。可是我们地区有不少同修，自己对象被迫害回来后，不能很好处理，不是打就是骂，最后自己又被所谓转化了的对象弄到了邪恶的转化班）。所以，对防火墙使用，还需要大家通过明慧网多指点。

(5) 隐私的入侵

这个主要是我们访问了被邪恶利用的网站，当我们上这样的网站时，它们就通过 Cookie（甜饼）来偷取信息，它们还可以通过控件在你的电脑里装东西，有些是偷偷地干的。比如那个 3721 就是这样的坏。

所以，我们上网要注意一些，就是中国那个所谓的门户 WWW.SINA.COM (WWW.SINA.COM.CN)，一

许远程用户登录到系统并且使用命令行运行控制台程序。)都给禁用。

3、用户名和密码。

许多使用windows2000和windowsXp的同修，为了方便起见，用系统管理员身份登录，没有给系统管理员设置密码。这样做是很不安全的，因为系统管理员具有随心所欲权限。在这种情况下，邪恶一旦入侵你的电脑，就可轻易而举获得系统管理员权限，可以给你安装、运行木马，窃取你的资料。所以一定要设置系统管理员口令。设置时千万千万不要用你的电话号码、身份证号码、生日、地址、区号、年龄作为密码。这是弱智密码，很容易被别有用心的人猜出。你可以用你喜欢的一句话或一首歌拼音第一个字母或英语作为密码。兼用大小写，再在后面加上几个数字，就更好了。

4、IE浏览器安全设置。

打开Internet Explorer浏览器，选择“工具”→internet选项→安全→自定义级别。在此把“Axtivex控件和插件”的各种选项全部禁用。然后再把“Microsoft VM”中的“Java权限”设为禁用。点击两次“确定”。再次点击“隐私”，把滑块拉到最高。这样设置后，可能国内有些网站不能

上我开着电脑没关，第二天上班时发现我的ZoneAlarm防火墙被自动关闭掉，以前从来未发生过这种事情，这件事情引起了我的警觉；之后我又发现我机器上的下载工具被多次莫名其妙打开去一个国内网站下载一串MPEG文件；之后的第二天早上我才开机的时候，就有一个陌生的程序试图穿透我的防火墙去访问互联网，这个程序被别人放在了我的“C:\windows”目录下，我仔细查了一下这个程序，发现根本不是正规的商用程序。

从以上的现象，我基本上可以断定是邪恶对我的电脑实施的黑客行为，并且可以准确的说，是它们在我电脑中植入了木马程序，其破坏力比病毒强，并且有针对性，请同修们引起高度重视。

根据我的经验，我认为：其实病毒不是危害性最大的，最大的是黑客程序或木马程序，这些程序是专门干坏事的，并且有针对性，它往往是在机器上搜索敏感信息然后发送走，甚至操控你的电脑或者是故意使你的电脑工作不正常。

有些同修在自己的机器上安装了一些杀毒，查杀木马的软件，还有防火墙软件，使机器安装的软件环境过于复杂，出现问题时往往陷入操作这些软件的细节上，电脑问题可能没有彻底解决，还浪费

不小心就给你装东西。

(6) 密码

密码要长，要大小写字母、数字、特殊符号一起采用，比如大于20位。

(7) 远程协助

Windows 的远程协助，就是说，当你对计算机用不好时，网络上的其他计算机用户，就可以通过他的电脑，来帮助你设置好计算机。

大家想一想，如果邪恶通过“远程协助”控制了你的计算机，会怎样，我们不能让这样的事发生。所以大家应当把“远程协助”关掉。

以上只是个人观点，大法弟子证实法正念正行为主，但是我们不能让邪恶干成它们想干的。

一些关于电脑安全的有效措施(一)

读了明慧网2004年10月10日《请上网的同修小心木马》和2004年10月16日《北京地区上网同修请注意》的两篇文章后，有些感想。结合我前几天电脑被干扰的情况，写这篇关于电脑安全的技术文章给同修们参考。

我的电脑前几天发生了这样的情况：有一天晚

下载东西，不能登陆邮箱，但是明慧、海外邮箱可正常打开。以上措施有不当之处，敬请慈悲斧正。

诺顿杀毒病毒库更新方法

【明慧网2004年11月11日】很多不了解电脑的同修都是别人帮忙装的机器。病毒库很久没有更新，很多同修不知道也不会更新。病毒库不更新，杀毒软件效果将大打折扣。其实除了利用网络在线更新外。不能上网的也照样可以更新。诺顿病毒库更新其实很简单。

下载或向别人要个最新病毒库，直接安装就自动更新，和安装一个小软件没有区别。

诺顿最新病毒库安全下载地方：

<http://www.symantec.com/avcenter/download/pages/US-N95.html>

下载那个如20041104-018-i32.exe 文件就行，最新文件日期可能有变化，但i32不会变，大概5M。

安装完后看看诺顿病毒库时间是否变成最新的？执行一次LiveUpdate，不要管什么错误提示等，继续“下一步”，不用重新启动机器，你就会看到你的病毒库在LiveUpdate提示日期已经是最新

了很多宝贵的时间。我不是说这些软件不好，也不是说没有必要安装它们，我是想我们很多的同修承担着重大的救度众生的工作，加上他们很多都不是专门搞计算机这个行业的，不能在这方面太多浪费时间，但是又必须把电脑的安全做好。为解决这方面的问题，我提出了如下的做法：

一. 制作安全有效的Ghost映像文件

步骤1. 把机器上的自己的东西备份好，然后把电脑的硬盘格式化掉，至少要把C：盘格式化掉，建议格式成NTFS，这种文件系统能够具有安全性；

步骤2. 在电脑的C：盘上安装操作系统，建议安装Windows2000/XP/2003，建议尽量不装Windows98或者Windows Me；

步骤3. 安装最新版本的ZoneAlarm或者Symantec公司的防火墙软件（在安装操作系统前把防火墙软件准备好），并且设置好合适的安全选项；

步骤4. 在线更新操作系统，也就是执行Windows Update，这样更新完成后操作系统就打了微软最新的操作系统补丁，其实我们关心的主要是系统安全补丁。（需要说明的是：这种方法不绝对严密的地方在于在下载安装补丁过程中可能受到来自网上的

→我的连接→tcp/ip协议→属性→高级→wins→禁用netbois上的。

(2)、运行“优化大师”（可在国内各大中型网站下载），选择左下方的“系统性能优化”，再选择“系统安全优化”，选择“禁止向windows2000(xp)建立空连接”和“禁止系统自动起用服务器共享”（使它们前面的方框里出现对号），再点击右上方的“扫描”，让优化大师扫描，它会提示“你的系统存在445端口漏洞点击确定修复”，按照提示点击确定。最后点击“优化”，推出优化大师，重新启动电脑。

2、必须停止的服务。

一些不必要的服务不但造成资源浪费，还给别有用心的人攻击你的电脑留有空子。取消不必要服务的方法：单击“开始”→设置→控制面板→管理工具→服务→双击“ClipBook”（支持“剪贴簿查看器”，以便可以从远程剪贴簿查阅剪贴页面。）→单击“启动类型”右边的小三角→选择“已禁用”→单击“应用”。再双击“Remote Registry Service”（允许远程修改注册表）→选择“已禁用”。然后把“Server”（提供RPC支持、文件、打印以及命名管道共享。）、“Telnet”（允

机上。

9: 学会正确配置和使用网络防火墙。

这点非常重要，希望上网的同修用点时间认真学一下。我们要注意安全，通过学法我理解到这是大法对我们的要求。

上网必须注意的几个安全问题

【明慧网2004年12月22日】谈到上网的安全问题，最主要的还是正念强。在正念正行的前提下，还要注意常人方面的安全措施，不给邪恶留下任何漏洞。下面我从技术方面谈一下上网必须注意的几个安全问题。我在给同修安装、修理电脑时，发现不少同修对以下几重要的安全问题，没有引起注意，从而使电脑存在重大安全隐患。

1、允许建立空连接和硬盘共享的问题。

允许建立空连接和硬盘共享是windows操作系统（win98,win2000,winxp）中默认的。正常安装上windows它就存在，它是骇客和一些别有用心的人攻击你的电脑、给你的电脑安装木马最最常用的方法之一！！我们要做的就是防止建立空连接防止硬盘共享。步骤如下：

(1) 右键点击桌面上的“网络邻居|”→属性

攻击，当然这里在事先已经安装了最新版本的ZoneAlarm或者Symentec公司的防火墙软件，即便在下载安装补丁过程中受到来自网上的攻击，由于有了防火墙的阻拦，还是把电脑的受攻击程度降到了最低了，所以这种在线安装操作系统补丁的方法还是值得采取的，一般也不会有什么问题。)最好的打补丁的方法是预先将最新的各种补丁下载准备好，然后在这个步骤中完成打操作系统补丁；

步骤5. 在电脑的C：盘上安装各种用得着的软件(建议不要把各种常用软件安装到C：盘以外的其它硬盘分区，这样即使电脑被攻击或中毒也都会集中在C：盘，一般可能不会波及到其它盘上，这样管理起来也方便)；

步骤6. 调整优化电脑中的各种常用软件，例如：完成各种软件的注册，使之不会过期；配置好软件的各种常用选项；尤其是防火墙软件和杀毒软件需要配置好，并且保证是最新的病毒库(这些常用软件尽量不要采用国产的，因为国内的流行软件大多都可能与臭名狼藉的“3721”这类“附体”捆绑在一起)

步骤7. 用各种查杀病毒的软件，查杀木马的软件，以及各种检查系统漏洞的工具在电脑的C：上

1: 禁用“共享资源”

(1) 在网络连接中去掉“Microsoft 网络文件和打印机共享”组件；

(2) 在网络连接中去掉“NetBEUI (NetBIOS) 协议”

(3) 去掉 TCP/IP 中的 NetBIOS 协议功能。

2: 禁用“IPC\$”

IPC 是 Windows 用来建立二台计算机进程之间通信的一种通道，也叫“命名管道”。但它成了黑客攻击的主要对象。黑客用IP地址、用户名、密码就可通过 IPC\$ 进入你的计算机，甚至只要 IP 地址就可以连通，特别是 Windows 内置 Administrator 帐户没有密码时，计算机一点安全性也没有。

通过【计算机管理】|【服务】关闭 Server 服务，禁用 IPC\$。

通过【计算机管理】|【会话】可以查看是否有 IPC\$ 入侵并确定入侵者的 IP。

3: 安全设置计算机的帐户和密码

(1) 改变内置 Administrator 帐户的名字；

(2) 关掉 Guest 等不用的帐户

(2) 所有帐户名和帐户密码要坚固，这一点对上网计算机非常重要。

处：

1. 能够使出问题的电脑系统以最快的速度恢复到制作“Ghost映像文件”以前的最优状态，一般情况5GB的C：盘映像可在15分钟之内就能完成恢复，这样成倍的为同修们节约了时间；

2. 制作好的“Ghost映像文件”可以供多台机器共享，特别是多个资料点的多台电脑，只要用一份“Ghost映像文件”就可以快速安装或者恢复好多台电脑，节约的同样是时间，保证的同样是安全和效率，不同配置的机器可能用同一个“Ghost映像文件”会有点不正常，一般安装好后做一点小的调整就好了；

■ “Ghost映像文件”的有效使用：

1. 一旦发现电脑系统有不正常现象，立即从“Ghost映像文件”把系统恢复到制作“Ghost映像文件”以前的最优状态，特别是资料点上网的电脑尤其需要这样做；建议的做法如下：

从移动硬盘把“Ghost映像文件”拷贝到C：盘以外的一个大的分区，然后用启动盘启动系统再用“Ghost”软件执行恢复，这种做法是把“Ghost映像文件”的所有内容覆盖到原来的C：盘上，其上

运行以期望发现问题和漏洞，然后及时解决掉，这个步骤可以根据自己的条件而行（推荐同时也采用德国的“TuneUp Utilities 2004”，最新的“清道夫”在这个步骤中实施一遍）；

步骤8. 从软盘或者光盘启动机器，把电脑的C：盘这个分区用“Ghost”这个软件（关于“Ghost”这个软件的使用请参阅有关资料）做成“Ghost映像文件”；注意：用哪个版本的“Ghost”软件制作的“Ghost映像文件”就用哪个版本的“Ghost”软件去恢复，否则可能会有恢复不正常的情况出现；做成的“Ghost映像文件”可以放在电脑的其它分区上，以便随时用来恢复系统，建议把做成的“Ghost映像文件”拷贝到移动硬盘上保存，以免遭破坏；

注意：千万不要在做成的“Ghost映像文件”存有敏感信息。

二. Ghost映像文件的使用和维护

制作好的“Ghost映像文件”是电脑能够安全高效工作的根本保证，必须对它进行有效的使用、管理和维护。

■ “Ghost映像文件”对电脑系统有如下的好

以前的内容将被全部覆盖掉；如果要保证最高的安全性，最好在把“Ghost映像文件”作恢复之前用把C：盘彻底擦除掉然后再格式化它，最后拿“Ghost映像文件”来作恢复，这样不管以哪种方式附在C：盘上的任何有害的程序或代码都会被全部干掉，高版本的“Partition Magic”可以安全彻底擦除掉一个磁盘分区，建议使用。

2. 建议资料点的电脑，特别是用来上网的电脑一般一个星期用“Ghost映像文件”恢复一次电脑的C：盘，这样做的好处在于：

始终能保持电脑是安全和高效而优化的。举个例子：邪恶可能在你的电脑中植入了干坏事的木马或程序，你可能还未意识到，但你的电脑已经在邪恶的掌控之中了，但是它们一般会反复在你机器上搜索信息，“证据”充分或者信息掌握全面之后才会采取行动，但是如果你的电脑尽可能周期短的进行着恢复，这样就会反复不断清除着这些干坏事的木马或程序；当然周期性的进行着恢复还会周期性的清除着你电脑中的残余敏感信息，一般这些各种软件留下的残余敏感信息基本都在C：盘上。

■ “Ghost映像文件”的维护和优化：

从我了解的情况来看，我们对计算机帐户名和帐户密码设置根本不重视，内置Administrator帐户密码简单，自己使用的帐户设置很简单如IBM、DELL等，还没有密码，这样的计算机有严重的安全隐患。

4: 禁用“Telnet”

通过【计算机管理】|【服务】禁用 Telnet 服务。不过如果黑客通过 IPC\$ 联入了你的计算机，你禁用了他也可以打开。

5: SQL Server 2000 安全设置

如果计算机因工作需要装了 SQL Server 2000 服务器，则千万别忘记对 SQL Server 2000 服务器的 Sa 帐户设置密码。黑客很容易从 Sa 帐户入侵后再控制你的计算机。

6: 如果不是工作需要，不要安装 Windows 的 IIS, IIS 的漏洞有上千种，最容易产生安全问题。

7: 关闭“远程协助”、“远程桌面”。

8: 对 Windows 每日更新。

对盗版的 Windows XP 无法安装 SP2包。从我使用的情况来看，Microsoft 加大了盗版打击力度，但正版的并没有完全限制只能装在一个计算

无界浏览器 Ultrasurf	v6.4
无界漫游 Ultrascape	v3.6
花园网（海外主页： http://127.0.0.1:8567/dm/uggc/jjj.tneqraargjbexf.pbz/ ）	
花园透明代理 Garden G2	v1.12
花园软件 Garden	v3.34

计算机反黑客安全设置的建议

【明慧网2004年12月4日】我以往对计算机安全不太关心，到后来有所关心，直到最近我看了一些黑客攻防实践，我简直不敢相信，如果我们没有安全设置我们的计算机，我们计算机上的信息对别人是完全开放的！！！

通过网络防火墙能提高系统安全性，考虑到可能对网络防火墙会错误使用，所以建议对计算机要进行反黑客攻击安全设置：

明慧网网络突破工具支持表

更新时间：2005年1月27日

网络突破工具	版本
动态网（海外主页： http://127.0.0.1:8567/dm/uggcf/jjj.qbatgnvjnat.pbz/ ， http://127.0.0.1:8567/dm/uggcf/qvg-vap.hf/ ）	
直接访问网 址	http://127.0.0.1:8567/dm/uggcf/qj1.BaGurArg.Nf/ http://127.0.0.1:8567/dm/uggcf/qj1.OlVagre.arg/ http://127.0.0.1:8567/dm/uggcf/qj1.ee.ah/
自由门Freegate	5.32替换版
动网通 Dynapass	v1.5
无界（海外主页： http://127.0.0.1:8567/dm/uggc/jhwvr.arg/ ， http://127.0.0.1:8567/dm/uggc/hygenernpu.pbz/ ）	
直接访问网 址	http://127.0.0.1:8567/dm/uggcf/pn.ab-vc.pn/ ； http://127.0.0.1:8567/dm/uggcf/jy.qnzafreire.pbz/

第 96 页

1. 一般来说一个完善的“Ghost映像文件”是已经被精心优化，配置，监测好了的操作系统和相关软件的一个包，但是我们不得不面对这样的现实，操作系统的漏洞不断被查出来，新的安全系统补丁包会不断推出，防火墙技术手段会不断更新，杀毒软件病毒库不断更新，我们使用的各做软件也会不断的更新和更换以及添加；还有邪恶采用的破坏手段也在不断的加强，所以我们的“Ghost映像文件”包也得不断的精心维护，不断优化，配置，监测，使我们的电脑随时保持安全和高效。其实微软的这些操作系统到现在已经变得庞大和复杂，在加上安装在系统上的各种软件，并且它们还要在一起协同运作，其内部的复杂性已经很大了，一个小小的差错就可能使系统或者某个软件运行不起来，况且还有干坏事的病毒和邪恶的各种破坏，我想这些可能都是大家经常碰到的痛苦事情了。

现在要想在微软的操作系统上安装很多各种协同工作的软件，并且又想让它们稳定、安全、高效的运作，没有一个完善而有效的“Ghost映像文件”包我们是很难达到上述目地的。这也是我多年来使用微软操作系统的经验了。

这样就使得不断维持一个完善、优化、稳定、

第 17 页

SPX等，那么防火墙对这些协议防护怎样？需要专门试验一下。计算机如果在一个域中（也就是局域网中），还要考虑域管理员的非法查看。

（4）信息安全。注意用清道夫和加密盘，不再说了；上网注意安全也不再说了，可以看以前的文章。

明慧网页投稿增加 对传送附件的支持

【明慧网2004年9月20日】由于网络突破工具的新发展，明慧的网页投稿增加了对传送附件的支持。请读者参见下述使用说明。

1、网页投稿必须使用无界浏览、自由之门等网络突破工具访问。截至2004年9月18日，我们的测试证明以下工具能够支持网页投稿：

无界浏览6.2 (<https://www.ultrareach.net>)

无界公司的直接访问网址

自由之门5.2 (<https://www.dongtaiwang.net>)

自由网的直接访问网址

花园网G2和3.3版

2、关于发送附件：

附件最大体积为1MB

第 94 页

Windows 2000 和 Windows XP

安全（二）

【明慧网2004年10月29日】

一：计算机日常维护清单

（1）安装所有的 Windows 安全补丁

因为 Windows 系统存在漏洞，可能成为邪恶攻击点，所以我们需要从Microsoft 那里经常下载补丁，补住漏洞。

由于 Windows 正在中国搞“正版软件”活动，要减少对盗版软件提供支持，所以建议我们资料点上网电脑的 Windows 使用正版的。退一步讲我们也不知道那盗版软件的来路。

再说一个问题，由于××党破坏中国人的传统美德，黑白颠倒迫害法轮功，更采用流氓手段让全国老百姓出卖良心去与××党同流合污保持一至，使全国一遍混乱，所以我们买 Windows 还要能识别正假，请参考：WWW.Microsoft.com/china 识别正假内容。

请经常安装补丁。

第 19 页

安全、高效的“Ghost映像文件”包变得重要而又有价值。我觉得这样做还是值得的，它带给我们的是安全（让邪恶无漏可钻）、时间的节约（节约了很多我们用于安装和维护电脑系统的时间）和资源的共享（同样的一份“Ghost映像文件”包可被多个资料点共享，而这份“Ghost映像文件”包一般只需一个人维护就行了）。

2. 关于“Ghost映像文件”包的维护方法：

1.) 把“Ghost映像文件”包恢复到一台电脑上；

2.) 在恢复出来的这台电脑上升级里边已安装的各种软件版本，添加其它好软件，更新病毒库，更新防火墙软件，更新操作系统补丁等；

3.) 然后重新查杀病毒和各种有害程序，测试、调整、优化、配置整个系统；

4.) 再用前边提到的方法把电脑的C：盘做成新的“Ghost映像文件”包。

以上内容是关于操作系统以及配套软件的安全措施，这些措施我一直在使用和完善，我得到的感受就是系统软件环境高效，安全，稳定，节省时间。希望这篇文章对同修们有帮助，不足之处还望大家指出。

如果要发送超过1MB的文件，请分次传送，并在标题中注明，例如关于同一个文章要发送三个附件，第一次发送在标题上写：1/3；第二次写：2/3；第三次写：3/3。

如果有超过3MB的单个的大文件，请用winrar压缩并分块。winrar是和winzip类似的工具。中文免费试用版本可在

<http://127.0.0.1:8567/dm/uggc/jjj.eneyno.pbz/download.htm>

下载。不同于winzip的是，winrar允许将文件分成多个小块。

3、注意事项：

对于重要消息，例如迫害真象案例、技术错误报告等，请一定填写回信信箱，以便我们和您联系，核实、索取更多信息。为保证安全请尽量使用海外信箱。

死亡案例需要反复核实，因此请大陆学员填写回信信箱或用海外信箱投稿传递死亡案例。

明慧技术组

(2) 正确安装设置使用防火墙

请查阅电子书：[ZoneAlarm Pro v4.5.538.1 中文图解电子说明书](#)（2004年08月23日）如果使用Symantec 防火墙，请参考使用说明，一定要每日更新。

(3) 正确安装设置使用反毒软件

请参考 Symantec（诺顿）反毒软件使用说明，一定要每日更新。

(4) 采用移动盘或加密盘保存数据，如果是比较大资料点，请不要在上网电脑里保存我们的资料。

(5) 不安装有问题的软件

请查阅：Windows 2000 和 Windows XP 安全（一）。

(6) 采用“清道夫”安全清理遗留信息

请参考“清道夫”自带使用说明。

还可以：

(7) 在线检查计算机安全情况

可以到：www.symantec.com.cn在线检查。
www.microsoft.com/technet/tools/mbsahome.asp下载微软基线安全分析器分析。

软件不到200圆，包括一年的病毒库更新。一年之后要继续购买病毒库更新，每年费用不到100圆，我认为还是可以买得起的。

要注意一点，如果买的是诺顿网络安全特警，会有文件保护功能，你从回收站删除的文件，诺顿网络安全特警又给你保护起来了，还可以恢复。我们只要除掉该功能就可以了。诺顿网络安全特警捆绑了诺顿防病毒和诺顿防火墙，好处是中文界面。如果懂英文，或可用“东方快车”翻成中文，可以在http://www.zonelabs.com/store/content/company/products/znalm/freeDownload.jsp?lid=zadb_zadown下载免费的Zonealarm防火墙。但防毒软件还是要买诺顿防病毒的。

(3) 防止网络攻击。计算机连接到网络上后，要防止外部计算机的攻击，还要防止侵入病毒把自己计算机上内容发送出去，这就要用到防火墙。

诺顿(Norton)防火墙可以信任，但也需要进行入侵规则更新。不过一般防火墙规则很少更新。或者也可如上所述下载Zonealarm防火墙。

在这里需要说明的是，计算机连网后，靠一些网络协议进行通信，如TCP/IP、NETBEUI、IPX/

计算机操作系统，比如预装Windows XP家庭版（预装的叫OEM版）800圆（单独买要1400圆）。最好叫一个懂电脑的去，保证能正常注册。现在中国社会被江××烂鬼带动已经没有什么能放心的了。

需要注意的是拨号上网更新可能困难，所以在卖电脑的地方用宽带网先更新。然后要设置成每天自动更新。

(2) 防止病毒感染。对这个问题，我看到大家用国产的杀毒软件多，我个人建议还是不用为好，首先国产杀毒软件没有很高的信任度，君不见中国政府机关都不用国产的，除了××党宣传欺骗老百姓外，它们自己也是不相信自己的，重要的地方还是用的诺顿；其次我们也不清楚这样的东西是不是已经被邪恶所利用。

防止病毒感染另一个问题是，没有进行病毒库更新。大家好象把防止病毒感染软件一旦装上就万事大吉了，事实根本不是这样，防止病毒感染软件装上后如果不进行病毒库更新，就象没有装一样。

要进行病毒库更新，当然要用正版软件。好在symantec已经在中国设立了分公司（见www.symantec.com.cn），诺顿（Norton）杀毒中文版

二、关于电话监听

安全局有一套系统和中国移动或中国联通的移动交换机直接相连，可以监听网络上所有手机的通话内容，固定网络也是如此，它们是通过把它们想要监听的号码挂到这套系统上，来实现监听的，所以我们使用明号（自己在常人社会公开的号码）手机打电话时一定要小心。最好是都使用匿名号码（不拿身份证到号贩子手里买）联系，用一段时间一起换一批，千万不要明号和匿名号码混用，因为明号是公开的，很容易从这个号码的通话记录上查出与其联系的其它号码，更不可明号对明号打，那样一下子就能查出来与其联系的同修，而如果我们都使用匿名号码，它们就无从查起。有条件的可以配两部手机，没有条件的用一部手机换卡使用也可以，问题不是很大，但打电话前一定要确认好了是上的哪个号码，千万别忘了换卡就打电话，两个卡分别是移动的和联通的会更好识别一些。

上诉是纯粹从技术角度谈的，我们是修炼人，有正念制止邪恶的能力，一切的安全手段都只是辅助的，大法弟子正念正行，才是关键。“弟子正念足 师有回天力”（《洪吟（二）》·师徒恩）。

(8) 查看系统事件

从【开始】|【控制面板】|【管理工具】|【计算机管理】|【系统工具】|【事件查看器】|【系统】，了解系统工作情况。

对于在资料点工作的同修，请你一定阅读致海外学员：电脑的基本安全设置和使用（2003年10月8日更新）（2003年7月3日文章）

对于负责技术的同修，请你一定要阅读：

电子书：网络新手突破封锁安全上网手册
2003年05月31日

中共网络封锁技术漫谈之四：突破封锁软件概览（图） 2003年12月11日

中共网络封锁技术漫谈之三：国家级别的域名劫持（图） 2003年12月10日

中共网络封锁技术漫谈之二：国家级别的关键字过滤 2003年12月09日

中共网络封锁技术漫谈之一：国家入口网关的IP封锁 2003年12月08日

突破网络软件请及时参考突破网络软件公告。

二：计算机安全设置

(1) 删除或关闭不使用的帐户

【计算机管理】|【系统工具】|【共享文件】|【共享】检查共享情况，关掉共享。对于上网端口，通过“属性”去掉不必要的协议，如：NetBIOS协议。

(3) 正确设置 IE

IE 的问题主要有三个：

1：“缓冲区溢出”攻击，由特长的 ULR 造成内部缓冲区溢出，然后通过特别字串攻击你的计算机，Windows XP SP2 包已经解决该问题。

2：通过 Cookie 偷信息，可以通过 IE 或防火墙 禁用 Cookie。

3：通过 Axtivex 控件、JAVA、脚本（VBScript, Jscript）下后门、病毒，并起用后门监控你的计算机，起用病毒破坏你的计算机。

解决办法通过 IE 里的【Internet 选项】|【安全】或【高级】选项内容，禁用 Axtivex 控件，签名的 Axtivex 控件可能也不安全，也不用。在工作中，我们不去浏览邪恶的网站。或干脆使用更安全的浏览器，例如Mozilla（可在http://mozilla.org/下载）

请查阅：关于网络安全的若干问题（之一）

从【开始】|【控制面板】|【管理工具】|【计算机管理】|【系统工具】|【本地用户和组】|【用户】中，大家可以看到 Windows 里所有的帐户。

有几个帐户需要说明一下：

Administrator 帐户，是安装 Windows 时默认帐户，对计算机具有最高控制权，也是黑客经常攻击的帐户。安全专家建议更改该帐户名，并采用坚固密码。自己使用计算机时也尽量少用该帐户。

Guest 帐户，是安装 Windows 时默认帐户，请关掉。

HelpAssistant 帐户，是安装 Windows 时默认“远程协助”帐户，请关掉。

SUPPORT_××××××××帐户，是安装 Windows 时默认“计算机生产厂商在线支持和服务”帐户，请关掉。

如果还有其他不用帐户，请关掉。

对于海外同修的计算机，对帐户管理要复杂一些，我们就不多讨论了。

(2) 检查网络共享

从【开始】|【控制面板】|【管理工具】|

网络安全

网上计算机安全问题分析

【明慧网2004年5月10日】计算机一旦连接到网上后，首先就要考虑计算机的安全问题。这方面的文章在明慧网上有很多，但总感到是非专业的作品，有些问题没有完全讲清楚。因为现在上网的人数在逐渐增加，对这个问题大家也都很关心，所以，尽管我也是非专业人士，我感到还是有必要把自己看到的问题提出来，希望计算机方面的专家对这个问题认真研究下，给大家一个比较放心的答案。

计算机连接到网上后，我们需要考虑以下安全问题：计算机操作系统的安全、防止病毒感染、防止网络攻击、信息安全。

(1) 计算机操作系统的安全是大家都不太注意的问题，中国大陆的人又养成了不用正版计算机操作系统的习惯，所以大家好象都不太关心这个问题了。

事实上，采用正版计算机操作系统是十分必要的，通过每周定期更新(Windows Update)，可以补上Windows的漏洞，能有效防止网络攻击。

大家在买计算机的时候，要求预装正版的计

2000年08月01日

三：病毒、蠕虫、特洛伊木马

1：病毒、蠕虫、特洛伊木马形式及破坏

(1) 病毒：是一段程序代码，通常附加在别的文件(程序)上，当病毒在计算机中运行时，有的会破坏计算机，使计算机运行不稳定。

(2) 蠕虫：是一种独特的程序，可以把自身从一台计算机复制到另一台计算机，破坏作用与病毒差不多。

(3) 特洛伊木马：是一种程序，当你的计算机中特洛伊木马后，别人就可以通过网络上另一台计算机操控你的计算机，可以干任何它们想干的事情，它们操作你的计算机就象你自己操作自己的计算机一样，还可以记录键盘操作。

(4) 病毒、蠕虫、特洛伊木马复合体：三种因素都有。

2：病毒、蠕虫、特洛伊木马传播方式

(1) 电子邮件附件；

(2) Web 的攻击：ActiveX 控件、JAVA、脚本(VBScript, Jscript)

(3) MSN Messenger、Windows Messenger、

内容发送到“短信中心”(手机设置了哪个短信中心号码就使用哪个短信中心，一般一个省有几个，不是每个市都有)，短信中心再根据你发送的号码，在网络中查找这个号码，并把短信内容转发给它，当接受短信的手机关机或不在服务区时，短信内容会存储在短信中心，当这个手机开机或有网络时，再发给它。但在短信中心存储的时间是有限的，一般为48小时或72小时，即两天或三天，如果，接受短信的手机在两天或三天内不开机，就会发送失败，有的手机有信息发送成功与否的提示，有的手机没有。所以，在手机里设置“信息有效期”是不起作用的。另外，我们发送的短信内容，无论发出去与否，都会在短信中心存储一段时间，但具体多长时间，我目前还不清楚。

再者，我在使用中国联通G网手机发送短消息的时候发现，当短信内容里含有大法里的关键词汇如“法轮大法”、“发正念”等，信息会发送失败，可能是在他们的短信中心里有短信内容过滤装置，使用中国移动的手机时没有发现这个现象，解决这个问题一个简单办法是，在一个名词的几个字间加空格，例如把“发正念”敲成“发 正念”，它就识别不出来了。

出進行发送，发送时间必须控制在几秒或几十秒的之间，发送后立即将手机放入钢丝网中，余下的操作再去慢慢完成。

实践证明，将与常人讲真象和同修之间互相联系结合起来，使常人和同修的手机号码混在一起不易被公安查出，因为每天都要讲真象，手机有机会接收同修发来的短信。同修之间最好只见其号，不见其人。屏蔽后的手机只能对经过屏蔽的手机，绝对不可与没有屏蔽的手机联系，切记！否则会将对方置于危险之中，联系语言尽量用暗语。

关于手机通信安全及对

《手机的屏蔽》一文的反馈意见

【明慧网2004年6月3日】我把了解的一些关于手机通信方面的情况写出来，供同修们参考。

一、关于手机短信

在5月27日《手机的屏蔽》一文中提到在将手机里的“信息有效期”定为一周，其实是不起作用的。我介绍一下手机短信的原理：手机对手机的短信称为“点对点”短信，原理是通过电信运营商“中国移动”或“中国联通”的“短信中心”存储再转发实现的。具体说来就是，一个手机先把短信

的信号交换，在这个过程中产生电磁频谱，公安很容易利用侦察监视技术发现、识别，监视和跟踪，并且能对目标进行定位。

手机在关机状态时，有两种情况，一是使用者关闭手机，持有特殊仪器的人可遥控打开手机的话筒；另一种是在手机制造过程中就在芯片中植入接收和发送功能，这种手机虽然没有开机或不是待机状态，但只要有电池，手机上的接收装置就能将接收到的信息发送到中继站然后传递到处理系统实行跟踪定位。

所以最好的办法就是对手机进行屏蔽，即用铜丝网包裹手机，截断手机内外电磁信号的联系，同时再结合利用无声的语言——短信，就会将危险降到最低。

具体办法是：除发送信息的几秒或几十秒的瞬间外，手机的操作或存放都要在铜丝网中进行。铜丝网是一种密度象布一样的铜织丝网，丝网商店有卖，规格160—200目，买回后根据手机的大小裁制成象小手帕一样的方块。为防止脱丝，要将边窝住，然后上下左右将手机对角包严，并用皮筋扎好，一来避免弄脏，二来不易暴露，使用时隔着铜丝网打开手机开关，当信号显示为零时才能进行工

AOL Messenger、Yahoo! Messenger。

3: 识别病毒、蠕虫、特洛伊木马一般方法

(1) 异常磁盘访问：特洛伊木马要发送你计算机中内容，必定要访问磁盘；

(2) 异常网络流量：特洛伊木马要发送你计算机中内容，必定通过网络；

(3) 程序文件大小变化；

(4) 【Windows任务管理器】|【进程】可以查看进程，右键点击进程，通过属性来了解进程情况，可以查到正在运行的特洛伊木马。（注：有关“Windows任务管理器”的常识请参考P32的说明使用“Windows任务管理器”）

4: 通过反毒软件查杀病毒、蠕虫、特洛伊木马

通过诺顿杀毒软件，能够查杀病毒、蠕虫、特洛伊木马。

需要说明的是，如果邪恶有专门破坏我们资料点的木马，那么反毒软件就查不到这样的木马（反毒软件病毒库没有该木马特征）；如果我们用了有后门（后门的作用跟木马一样，只不过它伪装后表面变成了合法的）的软件，反毒软件也是查不

且2001年有同修在明慧网就提出过“网际快车”有后门，所以我们还是应当认真解剖一下“网际快车”或找个国外的替代品。

我们建议大的资料点应该有专人负责维护计算机的技术工作；对于在资料点工作的同修应该作必要的技术和安全方面的培训；我们大陆所有有能力的大法弟子都加入到资料点的工作上来，整体清除邪恶的迫害（我们有局部地区清除网络迫害经验，在那里10多岁的小弟子都会上明慧网）；最好上网跟做资料分开；我们还是应该多学点有用的知识。

我们在资料点的同修多学法，加强正念，我们真有什么还不知道的问题，我们慈悲伟大的师父会告诉我们的。

明慧网相关文章：

[请上网的同修小心木马](#) 2004年10月10日

[PGP加密软件的安装和使用说明](#) 2004年08月06

日

[近期海外电子邮件受病毒攻击的一些情况](#)

2004年06月25日

出来的，并且连防火墙也控制不了。

5: 其它的防护措施

①我们采用防火墙可以使邪恶的木马进不来，发不出去东西；

②正确设置 ZoneAlarm Pro 的邮件附件阻止功能，减少感染机会；

③不随便下载文件、邮件附件、不看国内被邪恶利用网站，减少感染机会；可以采用证书或 PGP 加密保护我们自己的邮件；

④计算机不留东西，（不输入文件，）邪恶就什么也得不到；

⑤精心维护自己计算机，保持强健性；

⑥经常重装或“Ghost”备份硬盘，清除邪恶的木马；

⑦不用 UC、QQ 等怀疑有问题的软件；

⑧打开 ZoneAlarm Pro 的事件日志，可以看到木马的行踪；

⑨不上网就关闭计算机或断线；

⑩. 使用更安全的浏览器，例如 Mozilla（可在 <http://mozilla.org/> 下载）。

需要特别说明，由于下载软件必须要用，并

作。

为了便于用铜丝网包裹手机，购买手机时，尽量选用体形小巧、天线内置、没有翻盖的直板型手机，充电器要选择能将电池取出，在机外充电的座式充电器。为了不暴露，将手机进入“情景模式”选择无声，为了保证对方能够收到信息，进入“信息设置”，将“自定义设置”里的信息有效期定为一周；为了清楚对方的接收情况进入“信息设置”将“共用设置”里的发送情况报告选择“开”，在发送信息后，如果信息报告显示“已发送”表示对方已收到；如果显示“发送暂缓”表示对方已关机，短信息将会保存在短信中心，等到对方一开机就会收到，如果显示“发送失败”表示对方的手机号已取消或没有接收短信的功能。在讲真象中我们需要多角度、多方位、反复的讲，当确认对方的手机号已取消就应及时在电话本中划掉，以避免不必要的浪费。

无论是利用手机短信讲真象，还是同修之间互相联系都要选择无人安静的地方，首先打开手机，选择已准备好的短信内容，确认对方的手机号码，（短信内容和手机号码都要提前存入手机中），然后静心发正念排除干扰。然后将手机从铜丝网中取

Windows 2000 和 Windows XP 安全（三）

【明慧网2004年10月30日】

四 网络攻击

1: 什么是网络攻击

所谓网络攻击，是指国际互联网上的恶意计算机通过国际互联网对你的（或其它正常的）计算机正常工作进行干扰破坏或非法侵入到你的（或其它的）计算机。

邪恶已经利用了网络攻击来迫害“法轮功”，例如我到××省的一个资料点帮助同修安装计算机，通过 Symantec 的网络特警检测到了对上网计算机的密集攻击，通过网络特警反向分析，发现这些攻击都来自该省的中国网通公司。不久，明慧网就报道了该地区上网同修受到国安严重迫害。

2: 保护计算机的对策

(1)：邪恶之所以能够攻击进入你的计算机，安装后门窃取信息，是因为你的计算机 Windows 或 应用程序有漏洞。如果我们经常打好补

大概范围，对于主动定位（即商业服务中的定位，用户主动要求知道自己的位置），GPS方式一般在半径40米范围内，网络方式在半径百米的范围内；而被动定位普遍都是网络方式，被动定位是用户不知道自己被定位，这种定位方式更不准确，精度在百米以上。至于大法弟子被通过定位被跟踪、查找到，那是配合多种手段达到的，单用手机定位是不可能被找到的，特别是资料点，有机会再单独整理成图文介绍。

还有一点，手机上网费用较高，可以使用邮件索取下载方式，获取明慧上的所有资料，也很安全，做这个之前把GOODARTICLE的使用说明熟悉透，并把文件列表F1、F2文件得到熟悉它的命名规律，可以非常有效的取得任意文件。

手机的屏蔽

【明慧网2004年5月27日】实践证明，手机在通话状态下就是一部窃听器，有的同修可能会想：那我就发短信不通话，虽然这也是个办法，但仍会危险重重，因为无论是待机还是关机，手机都会被跟踪和定位。

在待机状态下，手机会与通信网络保持不间断

无线上网（专门用于笔记本） 与手机上网那个更安全

求教：无线上网（专门用于笔记本）与手机上网哪个更安全。无线上网省内漫游100元包月。手机上网费用高。我们不知选择哪一种，恳请有这方面经验的同修协助解决。合十

答：无线上网（专门用于笔记本）与手机上网哪个更安全。这有很多因素，前提是都不得使用记录身份资料的卡，至于那个手机也必须是不曾被注意过的（IMEI可以更改更好），在这种情况下，两者安全度差不多。普遍说来，在上述情况下，手机的方式比无线上网卡安全些，因为手机卡和手机IMEI可以经常更换，而无线上网卡则还没见到有更改IMEI的（它内部也有特定的识别码），尤其是目前国产的上网卡，很难得知会做什么手脚。

但也不绝对，比如你要看所在地区的普遍无线上网的方式，和你上网浏览的网站和你的上网地点等，无线上网也能被地理定位，定位方式与手机定位方式基本相同，可参阅明慧这方面的介绍。

目前所有的定位方法都不是精确，只是一个

丁，就能防止被邪恶侵入。

（2）安装防火墙

防火墙（软件防火墙 或 防火墙设备）是拒绝网络攻击的利器。对于来自网络的主动连接，防火墙都拒绝回答（除非你许可）；对于从你计算机的发出流量，防火墙也要按你的要求筛选；不过要利用好防火墙需要较多的计算机、网络知识。

Windows XP自带一防火墙，该防火墙没有流出流量筛选功能。Windows XP 的 SP2 让 Windows 的内核防火墙先于 Windows 加载到内存，提高了 Windows 启动阶段的安全性。

有些防火墙也有漏洞，需要经常更新。

3: 网络攻击的其它途径

（1）通过电子邮件附件，向你的计算机下后门（木马）；

（2）通过 Web 页面，向你的计算机下后门（木马）；

（3）通过免费的软件。

对策我们已经讨论了。

4: 关于防火墙欺骗

由于你的防火墙配置规则对正常软件是放行

系，这就是通常说的漫游。

三：移动通讯是数字式的

移动台由无线接收、无线发射和控制电路（含计算机）组成。移动台与基站进行通讯的目的地，是为了通过基站与移动业务交换中心建立联系，从而完成所需要的通讯任务。

当移动台打开后，它的无线接收电路就一直是工作的，只有需要向基站发送消息时无线发射电路才工作。

移动业务交换中心（实际上就是很多高性能计算机）纪录着移动台当前的状况。移动业务交换中心通过移动台所在的基站以“AT”命令形式由基站到移动台的下行频率传送命令到移动台，而移动台与中心也是以“AT”命令形式由移动台到基站的上行频率告诉中心移动台要求任务。

四：使用移动通讯注意问题

因为移动台移动时需要与不同基站建立联系，并且在移动业务交换中心的计算机里纪录着移动台的所有信息。所以一旦移动台被跟踪，那么移动台所到之处就暴露无疑；并且，依靠基站组成的移动网还可以精确定位。其次，移动台通讯时要把

不管是特洛伊木马、后门还是“幽灵”软件，它们都要加载到计算机内存中去，我们可以在 Windows 的【运行】命令行输入 MSconfig 命令，打开【系统配置实用程序】中的【启动】【服务】中查到它们，也可以在【任务管理器】的【进程】中查到。不过这确实有点太专业。

六 安全网络设置

在【网络连接】（XP系统）或【网络和拨号连接】（2000系统）中找到你用于上网的“网络连接”，右击连接图标在【属性】中，去掉不用的协议：NetBIOS、IPX/SPX；

由【网络连接】（XP系统）或【网络和拨号连接】（2000系统）的【高级】菜单命令进入【高级设置】，找到上网连接，去掉【Microsoft 网络的文件和打印机共享】下的协议，包括 TCP/IP 协议（也就是说不能用 TCP/IP 协议共享文件了）；这样你的计算机就不用担心被其它计算机共享文件了。

的，所以有些后门软件就冒充正常软件，这样防火墙就糊涂地放跑了邪恶。尽管通过对正常软件防火墙利用加密签名来识别，但后门采用附加在正常软件上还是能骗过防火墙。

5: 确定入侵者

ZoneAlarm Pro 的日志里记录了邪恶的入侵者。Symantec 的网络特警能在线统计提示和反向跟踪。

6: 清除迫害

根据中国有关法律，从互联网侵入私人计算机是违法犯罪，所以我们可以采用法律手段严惩恶人。我们正告为江流氓集团卖命的网络人员，赶快停止迫害，挽回损失，否责等待你们的是严惩。

从明慧网的报道来看，我们有的计算机应该是中了后门（木马），希望同修能分析一下原因，公布出来，揭露邪恶。

五、“幽灵”软件

在国外，有一些“合法”的“幽灵”软件，专门用来收集你的击键、电子邮件、屏幕信息，发到指定网站。我们还不清楚中国的网吧监控是不是采用这样的“幽灵”软件。

用户的语音信号通过模数转换后变成数字信号再送出去，邪恶要偷听录音更方便，只要移动业务交换中心的计算机适当设计一下就可以。第三，通过一定的“AT”命令，邪恶就可以把移动台变成一个远端的窃听器。

那么我们除了正念正行外，还应当从技术上注意什么呢：

（一）我们的联系人不要带着手机（特别是被邪恶注意的手机）到处跑资料点；

（二）大的资料点可以用一专用手机联系，手机放在资料点，其他相关人员通过公话与资料点联系，注意说话方式，不要带手机去资料点，带手机也应当把电池拿掉。

（三）检查手机是否异常发送。邪恶可以把移动台变成一个远端的窃听器，但手机要开启无线发射电路才能把信息发送出去，检查手机是否异常发送的方法：把手机放在打开着的收音机或录音机旁边、或把手机放在电脑旁边，正常打一个对话，它们都有反应，然后观察手机如果没有来电、来短信，它们又有相同反应，则手机可能就被邪恶远端窃听了。

使用 Windows 任务管理器的方法

要执行某些任务，可能需要以 Administrators 组成员身份登录。

Windows 任务管理器提供了有关计算机性能的信息，并显示了计算机上所运行的程序和进程的详细信息。如果您连接到网络，也可以查看网络状态并迅速了解网络是如何工作的。根据您的工作环境，以及您是否与其他用户共享您的计算机，您还可以查看关于这些用户的其他信息。使用 Windows 任务管理器，您还可以结束程序或进程、启动程序以及查看计算机性能的动态显示。

打开 Windows 任务管理器。

注意

要打开 Windows 任务管理器，请用右键单击任务栏上的空白处，然后单击“任务管理器”。

有关使用 Windows 任务管理器的信息，请单击 Windows 任务管理器中的“帮助”菜单。

详细信息，请单击“相关主题”。

在一个基站内可能有多个移动台需要同时与基站通讯，那么基站又是怎样来区分移动台呢？实际它们是这样工作的：把25MHz的带宽以200KHz的频率带宽分成124个小区间，称为信道，这样不同的移动台就可以在不同的信道上与基站通信了。比如移动台A到基站在信道11（890MHz+200*10KHz—915MHz+200*11KHz）上通讯，移动台B到基站就可以在信道21（890MHz+200*20KHz—915MHz+200*21KHz）上通讯。

DCS1800网，移动台到基站的上行频率是1710MHz—1785MHz，基站到移动台的下行频率是1805MHz—1880MHz。

CDMA网，移动台到基站的上行频率是825MHz—839MHz，基站到移动台的下行频率是870MHz—884MHz。但是，CDMA是不分信道的，而是采用不同的编码方式。

二：移动通讯通过基站组网

我们大家可能注意到，在不同的地理位置上有不同的基站，移动通信正是通过这些基站组成了移动通信网络，当移动台移动时，随着移动台移动到不同的地理位置，移动台需要与不同的基站建立联

希望大陆同修对通讯安全的问题给予充分的重视，不是怕不怕的问题，我们要为大法负责，为其他同修的安全考虑，在讲清真象中清醒、理智，正念正行，做好大法弟子应该做好的三件事，救度更多的众生。

移动通信的基本知识

【明慧网2004年5月4日】中国的移动通信网，有G网（GSM900）、D网（DCS1800）、C网（CDMA）三大网。GSM900网和DCS1800网又称全球通双频系统。

移动通信系统由移动台（如手机）、基站（通常大家见到的铁塔）和移动业务交换中心组成。移动台和基站通过无线电波直接通讯，基站和移动业务交换中心通过光纤直接通讯。

一：移动台和基站之间通讯是通过无线电波实现的

GSM900网，移动台到基站的上行频率是890MHz—915MHz，共25MHz频率带宽；基站到移动台的下行频率是935MHz—960MHz，也是共25MHz频率带宽。

电话监控方面的产品很多，最初，那就是直接在电信局的用户线上搭线，从而监听通话者的通话内容，这样的产品很多，但都容易被用户察觉。

从2001年开始，一种新型的电话监控产品被国安和公安特务大量采用了，这种监控方式已将监控功能直接伸向了交换机内部，而不是用户的电话线，从而使被监听的人根本无法察觉到。这种监控方式同时可监控的用户数量非常大，它的功能就是提取被监听者的通话号码，通话时间和通话内容，一方面可以在用户通话的时候就进行监听。另一方面，将所有通话内容录音保存，随时监听，用户提起电话后，所拨的所有号码都被记录，哪怕拨错号码或对方没有接听，都可以知道；别人打给该用户的电话也能监控到。另外，通过该电话收发的传真的内容也能被看到。

但是，虽然如此，在国安开始正式使用该产品时还是心虚的，因为它是不正当的行为，他们偷偷摸摸干，害怕被人知道。因为你作为是电信局的合法客户，你的通话内容被泄露，那电信局是要负责的，所以当刚开始时阻力非常大，人大几次开会表决都未通过，结果最后被以罗干为首的恶人强行

Windows XP默认设置 需注意8个安全问题

【明慧网2005年2月1日】

Windows系列操作系统一直以易用著称，力图让本来复杂的任务通过简单的操作即可完成。但是有的时候，易用性和安全是相互冲突的；同时，由于网络的广泛使用，每一台上网的PC实际上就是一个Internet的节点，所以安全是大家必须关注的问题。XP作为Windows最新的版本，当然也是最容易使用的操作系统；另一方面，为了提高易用性而采用的许多默认设置却带来了安全风险。

一、简单文件共享。

为了让网络上的用户只需点击几下鼠标就可以实现文件共享，XP加入了一种称为“简单文件共享”的功能，但同时也打开了许多NetBIOS漏洞。关闭简单文件共享功能的步骤是：打开“我的电脑”，选择菜单“工具”→“文件夹选项”，点击“查看”，在“高级设置”中取消“使用简单文件共享（推荐）”。

户”，在右边窗格中，双击Guest帐户，选中“帐户已停用”。WinXP Home不允许停用Guest帐户，但允许为Guest帐户设置密码：先在命令行环境中执行Net user guest password命令，然后进入“控制面板”、“用户设置”，设置Guest帐户的密码。

四、Administrator帐户。

黑客入侵的常用手段之一就是试图获得Administrator帐户的密码。每一台计算机至少需要一个帐户拥有Administrator（管理员）权限，但不一定非用“Administrator”这个名称不可。所以，无论在XP Home还是Pro中，最好创建另一个拥有全部权限的帐户，然后停用Administrator帐户。另外，在WinXP Home中，修改一下默认的所有者帐户名称。最后，不要忘记为所有帐户设置足够复杂的密码。

五、交换文件。

即使你的操作完全正常，Windows也会泄漏重要的机密数据（包括密码）。也许你永远不会想到要看一下这些泄漏机密的文件，但黑客肯定会。你

二、FAT32。

凡是新买的机器，许多硬盘驱动器都被格式化成为FAT32。要想提高安全性，可以把FAT32文件系统转换成NTFS。NTFS允许更全面、细粒度地控制文件和文件夹的权限，进而还可以使用加密文件系统（EFS, Encrypting File System），从文件分区这一层次保证数据不被窃取。在“我的电脑”中用右键点击驱动器并选择“属性”，可以查看驱动器当前的文件系统。如果要把文件系统转换成NTFS，先备份一下重要的文件，选择菜单“开始”→“运行”，输入cmd，点击“确定”。然后，在命令窗口中，执行convert x: /fs:ntfs（其中x是驱动器的盘符）。注：使用这个命令要注意，转换成NTFS后不能再转成FAT32。

三、Guest帐户。

Guest帐户即所谓的来宾帐户，它可以访问计算机，但受到限制。不幸的是，Guest也为黑客入侵打开了方便之门。如果不需要用到Guest帐户，最好禁用它。在Win XP Pro中，打开“控制面板”→“管理工具”，点击“计算机管理”。在左边列表中找到“本地用户和组”并点击其中的“用

通过。罗干为此曾专门给吴基传写亲笔信，希望信产部下发文件，要求各地电信部门配合安装此类产品。

现在，在地市级以上城市都已安装了此产品，而且现在它要监控哪个号码，直接在国安或公安的监控中心就可进行，连电信局都无法知道。所有身份公开的大法学员可能都是他们监控的对象，另外国际长途电话也是监控的重点。因此我们必须注意通信的安全。

（二）怎样通信才是安全？

那么我们的电话通信应采取什么样的方式才是安全呢？个人建议所有学员之间的联络最好不要用个人电话，而用公用电话。

具体做法可以这样：老张想和小李联系，老张可用IC卡电话拨打小李的电话，如果小李是固定电话，老张可在电话上告诉小李自己所用的IC卡电话的号码，然后小李再去用公用电话回复该电话即可；如果小李是手机，则直接挂断电话，去公用电话亭回电话，这样做，双方的通话内容就不会被监听，一方的电话也不会泄漏，只要双方事先约定好，基本上很安全。不要怕麻烦，很多人就是时间一长怕麻烦而直接通话导致出现问题的。

首先要做的是，要求机器在关机的时候清除系统的页面文件（交换文件）。点击Windows的“开始”菜单，选择“运行”，执行Regedit. 在注册表中找到 HKEY_local_machine \ system \ currentcontrolset \ control \ sessionmanager \ memory management, 然后创建或修改 ClearPageFileAtShutdown, 把这个DWORD值设置为1。

六、转储文件。

系统在遇到严重问题时，会把内存中的数据保存到转储文件。转储文件的作用是帮助人们分析系统遇到的问题，但对一般用户来说没有用；另一方面，就象交换文件一样，转储文件可能泄漏许多敏感数据。禁止Windows创建转储文件的步骤如下：打开“控制面板”→“系统”，找到“高级”，然后点击“启动和故障恢复”下面的“设置”按钮，将“写入调试信息”这一栏设置成“（无）”。类似于转储文件，Dr. Watson也会在应用程序出错时保存调试信息。禁用Dr. Watson的步骤是：在注册表中找到 HKEY_local_machine \ software \ Microsoft \ WindowsNT \ CurrentVersion

智；那些不理智，总是向别人表现正念，而不考虑那些闭着修的同修，会被邪恶利用，从人间的任何一面上都能钻进来破坏，我深深的体会到没有师父的保护，哪能那么顺利的做那些事啊。

对于通讯上的安全问题，很早就想写个全面一点的，总没有写，今天凑这个机会写一点。

谈大陆国安对电信通讯系统的监控

【明慧网2005年2月9日】近日，看到一份某城市公安局的文件，发现公安采用电信监控的手段迫害大法和大法弟子。今提请广大同修注意通信安全的重要性。另外，我本人对这方面的情况比较了解，包括技术细节。几年来我也一直思考破解之法，但都没有合适的方法，想与同专业领域或通信专业方面的同修一起探讨。

明慧网一直请大家注意安全。但是，从现在的情况来看，这方面大家重视的还是不够，以至于因为这方面的漏洞给大法带来很多不必要的损失。今天，我想再次从通俗的角度来谈谈电话监控，让大家对其有个初步的认识，从而采用一定的方法避免这个问题。

（一）电话如何被监控的？

派出所没有这个能力，一般的警察不知道这些手段。

使用这种方式排查，一般只有省厅级的国安才能调用这么多的人力、物力资源，这也是对大型资料点的破坏、侦查手段之一，特别是那些跨地区的、大的资料点，在很大的地理范围上出现一样的真象资料，这些真象资料会层层上报，最后集中到省一级，国安厅往往会花大量的时间侦查，而不是立即破坏，破坏也是交给当地具体做；如果通讯方式上不注意，这样就会被连锁破坏，一个资料点，往往会牵扯出很多同修、很多有联系的资料点。往往有些新大法弟子、没有被“登记”过的弟子也被发现了，也有这个原因。前几个月，有个省的大型资料点被破坏，根据报道的内容来看，与通讯方式的不当使用有很大关系。

在人间上，没有绝对的安全，其实越是高科技的东西，越容易被控制，越不安全；但是也不是说，我们从此再也不相来往了，正念正行，堂堂正正，理智、智慧的做我们应该做的。有些在散发资料上被认为正念强的同修，特别是散发来自大资料点的资料，千万不要有欢喜心、显示心，一定要明白，你的正念来自于大法、来自于师父，一定要理

用，只是关于敏感的话题，就不再这个上联系了，但一般的还是要通过它，否则的话，也会从另一方面引起怀疑，再建立另外的安全的通讯环境，比如说就你三个人，除了显现在社会上的通讯不变之外，在内部，可以各人配置一个手机，手机功能越简单越好，原来的旧、二手机较好，因目前新的手机在安全上谁都不敢保证预留了什么。使用那种不记身份的没有月租费的手机卡，这种卡通话费虽然贵些，但总体上非常划算和安全。同时这个手机、号码只有你们自己知道，号码、平时联系时段等不要经过通讯等第三方告诉对方，而是当面告诉、约定（通过EMAIL以PGP等加密方式告诉对方除外）。

以后这些号码只在内部之间通讯，哪怕是陌生的号码也不用这个号码回话，也不要用它打给陌生的电话，还要注意一个问题，就是人要必须见面的时候，手机在汇聚之前要关机，手机“不见面”，也就是这些“号码”联系者从来都“不在一起”，通话内容避免敏感语词，比如“切磋交流、邪恶”等等，而且用过一段时间后约定同时更换（手机卡），这可以最大限度保证即时通讯上的安全；但是却也同时有一个最大的弊端，就是一旦有

\AeDebug，把Auto值改成“0”。然后在Windows资源管理器中打开Documents and Settings\All Users\Shared Documents\DrWatson，删除User.dmp和Drwtsn32.log这两个文件。

七、多余的服务。

为了方便用户，WinXP默认启动了许多不一定要用到的服务，同时也打开了入侵系统的后门。如果你不用这些服务，最好关闭它们：NetMeeting Remote Desktop Sharing, Remote Desktop Help Session Manager, Remote Registry, Routing and Remote Access, SSDP Discovery Service, telnet, Universal Plug and Play Device Host。打开“控制面板”→“管理工具”→“服务”，可以看到有关这些服务的说明和运行状态。要关闭一个服务，只需右键点击服务名称并选择“属性”菜单，在“常规”选项卡中把“启动类型”改成“手动”，再点击“停止”按钮。

八、防范IPC漏洞。

IPC是共享“命名管道”的资源，它对于程序间的通讯很重要。在远程管理计算机和查看计算机

“启动电脑”密码设置

在组建资料点时，大多都是租赁房屋。而有的地区警察专门针对租赁房屋者的电脑进行“盘查”，以此来破坏资料点。写出此文，希望大陆大法弟子在运用此“加密设置”后，使警察在短时间内不能启动大法弟子的电脑成为可能。（当然正念强，是遏制警察行恶的因素，也是大陆资料点大法弟子时刻应具备的状态）

目地：“在按下主机箱上的‘电源启动’按钮时无响应，只有在键盘上输入了正确密码后，才能启动电脑。（注意：主板必须具备“键盘开机功能”。）

主板跳线设定：

打开主机箱，在键盘接口周围，找到一个3针的跳线，它的默认值是将“跳线帽”插在第2针和第3针上（§||），关闭了“键盘开机功能”。要打开此功能只要将“跳线帽”插入第1针和第2针上即可（||§）。（此设置适应于磐英EP-3S2A5，其它主板大同小异，可参考说明书操作）

CMOS设置（Award）：

一、在启动电脑时，按下“Delete”键，进入

的共享资源时使用。利用IPC可以与目标主机建立一个空的连接（无需用户名与密码），而利用这个空的连接，还可以得到目标主机上的用户列表。一些别有用心者可能会利用IPC，查找我们的用户列表，并使用一些字典工具，对我们的主机进行攻击。防范方法：

1、禁止建立空连接

我们首先运行regedit，在注册表中找到如下组 建 [HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Control \ LSA] 把 RestrictAnonymous = DWORD 的键值改为：00000001。

2、禁止管理共享

同样也是找到如下组键 [HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ LanmanServer\Parameters]把AutoShareServer = DWORD的键值改为：00000000。

“CMOS”设置。

二、进入“Integrated Peripherals”项，选择“Power ON Function”，用翻页键将这项设置为“Password”。

三、再在“KB POWER ON PASSWORD”一项中按回车键，屏幕显示“Enter Password”时，输入密码（1—5位），屏幕显示“Confirm password”，再一次输入密码确认即可。

例子：比如用户设置的密码为“fghj”，以后只要在键盘上输入“fghj”，电脑即可启动。而没有密码，在主机箱上按“启动”按钮是没有用的。

小技巧：在键盘上随意输入字符，只要输入的字符中包含“fghj”，电脑就可启动，需要注意的一点就是，输入字符时速度要适中。

提示：如果忘记密码了，打开主机箱清除主板的COMS即可解除密码（一般在主板的电池附近有一个3针跳线，正常默认模式下“跳线帽”插在1和2针上（|| §），现在将其插在2和3针上（§ ||），几秒钟后再插回1和2针，便可清除COMS）。把主板上的电池取下来一段时间也可达到同样作用。

一个暴露，这个通讯范围就全部暴露了，因为在交换机上存有很长时期内的所有号码的所有互相之间打入打出的详细记录，比如号码A，能够查出所有打给A的所有号码，通话时间，也能查出所有A打出的其它号码；这些与A联系过的号码集里的所有的号码，又可以象A一样的方式被排查，哪怕是在数百万的号码里，这个排查也就十几分钟就确定了，对固定电话也是这样，而且固定电话的所有通讯记录保留时间都在一年以上，电话局向外部说只保留3个月，有的说只保留6个月，那是欺骗老百姓的，最低都在一年以上，而且对特定的号码可以保留终生（即一个号码的开通始到这个号码的废弃止），即在数百万的号码里给出任一个号码，要确定这个号码的联系范围（通讯圈、联系圈）就十多分钟的时间；举例来说：有个号码321×××××，程控机房里存储着一年的（假定他设定的时限是一年，这是最低的）记录集，这些记录中有它打出的，也别人打给它的，日期、时间、通话时长都有，当然这里还有误打入的、也会有它打错号的，也有偶然有联系打过一、两次的，那么可以统计、找出经常与它联系的，这几乎就是321×××××的朋友圈、亲戚圈、社会来往圈。地、县级公安局、一般

人；720之后，特别在99年10月份之后，这个监听普遍到县以下。

这个消息如果你是从国安那里得知的、或者是他们故意有意无意告诉你的，很可能是他们故意想间隔我们，让我们彼此孤立，要正念正行；特别到了最后。

因为我们之间的通话，有很多使用率较高的语词，这个估计已经被他们整理过，数字化了，这就为把特定语词识别变得容易和现实了，因此可以把大量的电话进行缓存监控，这是他们利用发现新大法弟子、新联络方式、新资料点的手段之一。

主要是如何避免损失，如果是资料点，它的联络环境已经安全建立，那么还是正念正行的保持着你们那里和谐的工作。

这里针对一种普遍的情况来说明，如果你的联络环境已经公开了，就是社会上已经知道了你的固定电话、手机等，你的联络范围（社会上的和同修之间）也基本上是确定的了，那么就可以建立一个安全、稳妥的联系方式和方法。

常识上讲，不论被定位也好、电话被监控也好，必须知道你的电话（号码），这是前提。那么已经公开的方式，不要废弃，还是和原来一样使

备，并已开始安装。另外，国安部门已将所有大法弟子的电话纳入监听范围，特别是能上网的更是监视的主要对象。但由于工作量太大，目前主要方式是不定期的监听、分析上网记录。希望懂这方面技术的同修提供相关的解决方法。

答：这个问题比较大，三言两语说不全面，特别对于电话监听方面大部分人很难理解，这里只简要的说明，主要如何避免损失等。

电话监听也就是电话监控，现在的电话监听并不是说有个人在机房里或者某个地方，实时的在那等着听你的通话，而是对所有的通话被数字录音，并记录所有联系过的电话号码、时间、次数、时长等辅助信息；但对于他们认为特别重要的人、在他们认为特别重要的日子里会实时的有人在那等着，被监听你不会有任何感觉、不会有任何异样。监听者也不需在电话局的机房里（但机房也可以监听），一般电话局机房人员也不知道哪些被监听，但在99年之前他们知道，之后他们不知道（采用了新的技术、新策略）。

其实大法弟子们的电话在大陆很早就普遍被监听，这个普遍还不是现在、近期开始的，720之前主要是各市级以上辅导员和他们认为的重要联系

希望资料点的同修注意手机安全

[编者注：希望有类似情况的地区大家都注意这方面的情况，更冷静、清醒、智慧的证实大法，更多的救度众生。]

近日来沈阳的邪恶之徒，对其已经掌握的一些资料点进行长期跟踪，以获得更多的信息。跟踪的手段包括：

一、化装成社会上各行业的人员，跟踪来往资料点的同修，观察同修在做什么、住在什么地方、都与谁接触。再根据掌握的情况，去跟踪与这个同修有一定接触的修炼人，看他们再和谁去接触、在做什么。就是这样不断的往下发展。

二、通过他们所掌握的手机号码，来监听大法弟子的交往信息，从通话中了解和他有密切交往的人的名字、这个人的大概情况、他们互相接触在做什么、说什么话（这其中包括我们自己认为的很隐晦的说法，以为恶人听不明白，其实那些恶人都有这方面经验，不一定非得是敏感的词组）。如有“可疑”，就会接着监听这个手机号码，看这个号码还和哪些号码联系、都说了什么，如有他们所需要的东西，就继续监听和跟踪所涉及到的号码。从

清除Acrobat Reader的最近打开文件的名称

【明慧网2005年1月10日】

方法1:

在Acrobat Reader软件窗口，菜单栏的第二项，点击“编辑”菜单的最下方一项“首选项”，



理。5.01以上的版本新增了清除Cookies的功能，以后不必用手动清理Cookies文件了。可在网上下载，在www.zdnet.com上用Clean Disk Security为关键字进行搜索，注意尽量在外国网站上下载。

使用这个软件要注意的是——一定要选中“Gutmann (35 passes)”（在这个软件的主界面的下半部份，以前明慧发表过类似文章，在此再强调一下），因为只有这一选项才能达到最大的安全度，它将在硬盘上写35遍乱码，被删除的数据完全不能恢复。

点击主界面的“Config”按钮，出现这个软件的配置对话框，将位于下半部份的Maintain a log of activity (in CLNDISKLOG.TXT) 选项前的对号去掉，这样就能禁止这个软件的使用记录，没人能知道你在什么时间使用过它和你使用它的频率。

同时，选中Erase traces of names of deleted files in the FAT whenever deleting files (slower)选项前的复选框，这样在清除文件时连同文件名一起清除掉了。当然，文件名尽量不要用敏感文字。

很多防火墙对于你访问过的网址有历史记

弹出首项的对话框，点左边框中倒数第2项，“一般”，最后点确定即可。

这样每次只在历史记录中存在一个文件。每次在关闭敏感文件后，我们只要随便打开一个普通pdf文件，再关闭就行了。这样就把敏感记录去掉了。

adobe reader在安装目录里有一个普通的pdf文件。

目录如上页图中所示，可在桌面创建该文件的快捷方式，关闭敏感文件后，双击该快捷方式就行了。

方法2:

使用软件PC清道夫。

敏感信息的清除见明慧“关于清理电脑敏感信息的一点补充”。

关于清理电脑敏感信息的一点补充

文/踏网无痕

【明慧网2002年3月11日】关于敏感信息的清理，明慧已刊登过很多好的文章，本文在以前的基础上再作一点补充。

使用Clean Disk Security软件进行安全清

监听的手机通话记录中，恶人会判断出这个人的真实姓名、与其使用的一个或几个不同的化名，也可判断出使用这个号码的人居住的大概位置。

希望所有资料点的大法弟子和与资料点有接触的弟子提高警惕，最近出入时注意一下周围有没有可疑的情况，不要再被恶人跟踪了几个月而浑然不知；使用手机的同修也可以测试一下自己的手机是否被监控和远端窃听了。平时最好经常把手机放到打开的收音机或录音机旁边，随时进行观测，或把手机放在电脑旁边，正常打电话或发短信，它们都有反应，如果手机没有来电、来短信，它们又有相同反应，这时就要注意了，手机可能就被恶人远端窃听了。

带手机的大法弟子去资料点时或和同修接触的时候，不管手机有无被监控，都最好把手机电池卸下来，不要忽视安全问题。也希望大法弟子全面破除旧势力的安排，多学法、多发正念，彻底清除另外空间的黑手，正念正行。

电话监听现状分析

【明慧网2005年2月1日】问：近期，北京电信部门已购进一批专门监测北京地区大法弟子上网的设

录，如果你使用防火墙，清理时一定要不要忘了将防火墙记录的你所访问过的网址删除。

windows文件夹中有几个记录历史的文件夹（以前已有文章论述），在此要说一下recent文件夹。recent文件夹是隐藏的，要看到它需进行以下操作：双击“我的电脑”图标，在上面的工具栏内依次选择“查看”——“文件夹选项”——“查看”找到“高级设置”框内“隐藏文件”部份，将“显示所有文件”选中，并按“确定”退出，进入c:\windows目录即可看到recent文件夹。

还有一个recent文件夹是记录使用word软件编辑、阅读文件的历史记录，该文件夹所在路径为：C:\WINDOWS\Application Data\Microsoft\Office\Recent。

用Clean Disk Security只能删除上述第一个recent文件夹所记录的内容，第二个recent需要用系统机械师等软件才能清理，当然也可手动清理。以上提到的两个recent文件夹，可通过修改注册表的方法关掉其记录历史的功能（打开系统注册表的方法：单击“开始”——“运行”在出现的对话框内填入“regedit”按“确定”打开

○杀毒软件

必备工具。每天和网络打交道，病毒是常见的，安装一到两个杀毒软件，定期下载最新病毒定义，对保持干净的电脑环境有重要作用。尽量使用国外的杀毒软件。

○磁盘清理软件

必备工具。每次用完电脑，运行一下磁盘清理工具，可以把所有的运行痕迹删除，意义重大。“清道夫”是极优秀的软件，有同修介绍过，可以在一些相关网站下载。

○硬盘加密软件

必备工具。可供选择的软件有很多，大家可以寻找一款试一试，一款好的加密软件和“清道夫”配合起来使用可以使我们的重要内容隐藏得很好。

以上是本人的一点体会，具体很多同修的电脑有不同用处，一些刻录软件和媒体播放软件等等，在这里就不多述了。上述很多软件都可以在互联网上找到。

不足之处，望同修慈悲指正。

做资料工作必备的 几个电脑工具软件

【明慧网2002年11月28日】目前做资料工作的大法弟子有很多不是专业学计算机的，对电脑出的一些问题并不是很了解，因此有时会带来工作中的不便，有时甚至带来惨痛的教训，因此本人就我的经验写出此文，希望起到抛砖引玉的作用，启发更多同修写出自己的好的经验。

○文字编辑软件

WORD软件是我们最常用的，目前WORD2000就可以满足我们的工作要求了，其他如WPS、CCED等也可以使用。

○压缩软件

WINZIP是必备工具，解开订阅的每日压缩文件，发送加密的电子邮件都需要它，WINRAR有时也用得上。

○阅读软件

Acrobat Reader 软件，最适合打印的软件，目前很多大法资料都用这种格式。

注册表。），方法是：先打开注册表，按这个路径依次打开文件夹：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer。单击Explorer文件夹，在右面的窗口内，单击右键，选“新建”——“DWORD值”，然后右键单击新建的键值，选“修改”，将键值名设为“NoRecentDocsHistory”（只有字母，没有引号），将键值设为“1”（也没有引号）。按“确定”后退出注册表，以上提到的两个recent文件夹就不会再记录历史了。推荐这样做，可达到一劳永逸。

若使用word软件，文本编辑完成后，可采用下述方法清除word文档所附带的个人信息（包括用户名，计算机名等）：在打开的文档中依次选中：“工具”——“选项”——“安全性”。在安全性页面中，找到隐私选项，将此项下的第一行“保存时从此文件中删除个人信息”前面的复选框选中即可。本方法参照wordXP写出，word其他版本的设置方法与此大同小异。

Winzip和realplayer用过后会在注册表中留下历史记录，用系统机械师可以清除掉，而Acrobat Reader的历史记录系统机械师就无能为力

3、swf文件转mpg的经验：

用小软件Imperator FLA

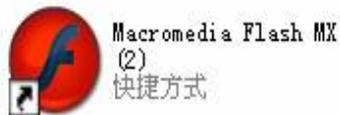


或 SWFDecompiler.exe
把FLASH影片转换成后缀为.flc的文件



（Imperator FLA不行就用SWFDecompiler.exe，

再用软件Macromedia Flash MX（30多MB大小）把.flc的文件转换成AVI文件（打开



Macromedia Flash MX，然后点击文件\导出影片，选AVI），然后用软件MainConcept MPEG Encoder把AVI文件转换成MPG文件。

4、用绘声绘影（7.0 或8.0版）切割合并合成MPG等文件的经验

此图的左下角添加多个MPG文件，注意按合成的先后顺序添加，然后打开右上角的分享就可以保

清理使用花园软件上网在 Zonealarm上的痕迹

【明慧网2004年12月23日】实践中，我发现使用花园软件上网会在Zonealarm（我使用的是Zonealarm4.5）上留下特定痕迹，以往的技术文章只是总体的介绍了如何清除Zonealarm痕迹，好像并没有单独针对花园软件，所以将其写出。第三步是本文论述重点，考虑到需要清除所有痕迹才安全，我写出了整个清理过程，供大家参考。

每次上网完成后，双击任务栏右下角Zonealarm图标进入Zonealarm程序界面：

1、点击界面左侧Program control（程序控制），在界面的右上角靠近Help的位置点击Program（程序）标签，这里显示了所有你曾经打开的程序列表，在其中找到花园软件，右键单击它将弹出一个对话框，选择其中的Remove（删除）；接下来点击Components标签，这时又显示出一个列表，在其中找到gbho.dll和GBHO.DLL两个文件（这是使用Garden所必须的配置文件，Garden运行时自动产生的）以相同方法删除。如果是使用G2上网，这里出现的配置文件将是G2NS.DLL，也要删除。

了。可以手动在注册表中清除，以5.0版为例，路径如下：HKEY_CURRENT_USER \ Software \ Adobe \ Acrobat Reader \ 5.0 \ AVGeneral \ cRecent Files \ 下的所有键值全部删除，软件显示记录的位置变灰了，以后再使用也不会有历史记录了，所以这个操作做一次就可以了。使用一段时间后未发现这样做对软件的性能有什么不良影响。

还有重要的一点提醒大家：需要清理注册表的工作尽可能在关机之前做好，因为再次开机时，windows会自动备份系统注册表，即使重开机后你彻底清理了注册表，在注册表的备份中还是会有历史记录。除非你删掉它的备份，否则无法根本清除。如在关机前做好清理，再开机时，系统注册表的备份中就不会有敏感信息了。

以上只是从常人的角度谈论安全，大法弟子遇到问题除了从心性上找以外还要多发正念。除了每周日全世界大法弟子固定的发正念时间外，希望各地区定好本地区定时发正念的时间，以清理本地区迫害大法弟子的邪恶。本文有不妥之处请广大功友及时指正，让我们作为一个整体做得更好！

注：这是早期的文章，使用清道夫后可以解决上述大部分问题，也可以解决下两篇文章的问题。

存为合成的MPG版了。



当然绘声绘影一旦入门以后，就可以随意的编辑录像了。

三、上网

宽带越来越普及，请使用WIN-XP系统，经常到微软升级补丁，然后再做一个ghost备份。基本就可以了。动态网与快车组合的网速极佳。

2、点击界面左侧Alerts&Logs（警报和登录），在界面右上角点击Log Viewer标签，这时列表显示了程序的登录时间、类型、名称、目地IP、数据进出方向等，在界面上方有View only the last () alerts, 指显示警告信息的个数，具体个数可以自己设定，实际上没有多大用处，最为有效安全的方法是点击界面下方中间位置的Clear list（删除列表）按钮，再点击“OK”即可。

3、点击界面左侧Privacy（秘密），再点击右上角的Site list标签，这时显示了你所有登陆的网站的列表，如果你刚上完明慧网就会发现有“www.minghui.org”的字样，可以采用右键单击再选择Remove（删除）将所有网站列表清空就行了。（这些网站列表是花园软件和其他破网软件的一个很大不同，使用其他破网软件一般不会出现这个列表）接下来点击右上角Cache cleaner标签，再点击clean now（立即清除）按钮，这是清理高速缓存中的信息。

此外，要删除所有的Zonealarm信息，还要到系统文件夹Windows中Internet logs文件夹中将所有以ZA开头的log文件和txt文件删除。

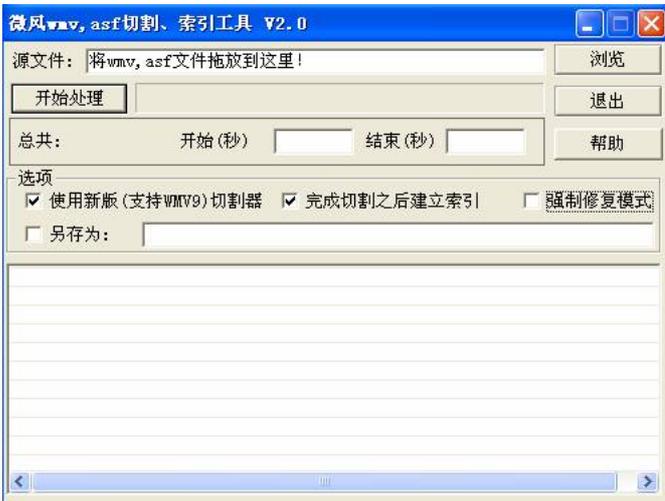
（4MB多）解码器的情况下，在WIN98下能用，在WIN-XP下不能使用，但是安装了软件RM to AVI MPEG WMV VCD SVCD DVD Converter（9M左右）的情况下，软件MainConcept MPEG Encoder就能使用了。



下，只有声音没有图像，此问题如何解决？

1、切割asf和wma的一款小软件：

WMV切割修复器，此软件才400多KB，操作简单快捷。下图是软件的使用界面。



2、rm、asf转mpg的经验：

软件MainConcept MPEG Encoder转换速度是目前最快的软件，此软件在安装RealoneED.exe

在15—20元之间，此种碳粉适用于大多数惠普和佳能机型，能够打印1000至1500张左右A4纸。如果能让打印机干一会儿歇一会，硒鼓和机器的寿命都会大大延长。同修们不看好的佳能1120，我现在已经打印了近40000页了，工作的还很好，早期用坏了两个硒鼓（400元左右），现在用的这个硒鼓（很长时间没换过了）和鼓棒（寿命在5000张到10000张以上，50元左右）寿命都大大延长。

佳能3200速度每分钟18页，下进纸，word两版A4纸骑马钉打印，印刷的却是A5型，不知什么原因？所以用佳能3200打印一整本书时，很不方便，解决办法是，先放一张纸打印，打印正常，然后放入多张。打印pdf版没问题，word四版A4打印也正常。

一台电脑托四台打印机（可以花几十元买一个usb1.0转usb2.0的电路板插在电脑主板上），可以托任意四种型号打印机（包括喷墨机）。

另外一个usb口，可以安装多个打印程序，一台机器休息或者送维修，换一台已经安装好程序的打印机，还可以继续。

如果是两台激光打印机，可以分别为一台上进纸，一台下进纸，用下进纸打印奇数页，用上进

删除和禁止NERO刻录软件文件 下拉菜单历史记录的方法

【明慧网2004年8月8日】

删除nero程序中的刻录信息

我用nero5.5刻录光盘，发现c:\Program Files\Ahead\nero\Nero History .txt 文件中详细的记录着刻录信息，所以我们在每制作一批光盘后就应该将其中的有关信息删除。方法是打开此记事本，选中要删除的记录，点鼠标右键选删除即可。或将Nero程序卸载再将c:\program Files\Nero删除即可，需要时再重新安装。

删除和禁止NERO刻录软件文件下拉菜单历史记录的方法

方法是开始→运行→Regedit→在注册表中找到HKEY_CURRENT_USER\Software\Ahead\Nero - Burning Rom\Recent File List

把类似“File1=C:\\001.nrv”这样的记录全删除。之后在Recent File List项的右键菜单中选“权限”，把每个用户的权限的完全控制和读取改成“拒绝”，确定即可。这样文件菜单上的历史记录就没有了，以后也不会再记录了。

处以2500元购得一台HP3015激光一体机，而其他同修通过其他渠道购买则花了2680元。另外要注意，代理商通常要比批发商讲信誉。对批发商的价格和信誉要了解，要货比三家，一旦发现其价格太高，要及时更换批发商。如我从科技市场收集了几个比较大的批发商的名片，通过向其他批发商询价，得知原来发光盘的那个批发商的光盘价格太高，及时停止了从其处发货。这样实际上全部设备和耗材只需要有六七个代理商和可靠的批发商即可。例如省城某纸业公司经销彩喷纸、像纸、塑封机、塑封膜、卡片纸、不干胶纸、切纸机等，可一次性采购很多种设备和耗材。

查代理商或批发商的方法：1.从科技市场收集代理商或批发商的名片。一般要找铺面大的批发商，其销量大价格也会低。2.如有手头有所需商品，包装上有厂家的联系电话，可直接打电话询问其山东的代理商。3.可从网上用google搜索，如搜索：“索尼刻录机 山东总代理”可以查到索尼刻录机其山东省代理商的相关信息。有时会查不到，但可以从厂家网站上查得。如欲采购麦普的打印机墨水，可以通过google搜索，登陆麦普公司的网站，从中可查得其销售部门的电话，然后打长途询

资料点安全及运转

小型资料点的采购小经验 及推荐的硬件配置

【明慧网2005年2月13日】我担任本地一小型资料点的设备及耗材的采购工作近一年来，一直比较顺利，未出现大的纰漏。现在介绍一下我的一点经验和做法。基本的采购流程是：1. 查询代理商或批发商的联系电话。2. 电话联系洽谈发货。3. 通过银行给对方汇款。4. 从快运公司提货并付运费。具体环节及注意事项简介如下：

一、不要就近在本县或科技市场采购，要找省（或地级市）级的总代理或省一级的批发商采购。我所处的地方是离省城较远的一个小县城。县级小经销商经过层层加价，一般价格要高得多，而且经常就近采购，安全性也成问题。总代理商或批发商的商品质量有保证，价格较低，讲信誉，一般不会漫天要价。我曾有过在科技市场购买打印机墨水被奸商以超出实际价格一两倍猛宰的教训。亚泰塑封机从批发商处以160元价格可购买，而本地至少要价二三百元。2004年下半年从代理商

问其山东的代理商即可。有时网站上也登有各地代理商的联系电话。

二、不要以个人名义采购，要以经销商的名义采购。这样代理商或批发商为争取固定的经销商，通常给经销商的按批发价，而卖给个人按零售价。不要担心自己的购买的数量少，因为现在小经销商，特别是电脑耗材经销商为避免降价风险和减少资本投入，通常都是按需进货。即使是购买一个墨盒、一包彩喷纸也可以经销商的名义发货。可以随便起个某某电脑公司或某某办公用品公司的名称，不要和本地的名称有冲突，给自己起个普通的假名，如李强、张勇等，用一个专用的手机（为安全起见不要用作和同修联系及日常公开使用），固定下来作为与代理商或批发商联系用，也用此手机作为从快运公司提货的联系电话。

三、电话联系好数量价格后，通过快运公司发货，节省时间和成本。可与代理商或批发商谈妥后，要求其告知其开户行的户名和帐号，报给对方自己所在县的地点和姓名、联系电话，汇给对方价款，对方查收后即可通过快运公司发货。一般次日即可收到。汇款实际就是以帐号的开户人的名义填写存款凭条异地存款，手续简便。汇款最好

纸打印偶数页，好处是，下进纸打印机可以减少纸槽的推拉次数，有连页，只要把多余的空白连页拿出来，不影响打印偶数页。用上进纸打印偶数页比下进纸的好处大家自然就知道了。

请有经验的同修发现上进纸的合适激光打印机型，给以介绍。最好是市场上没有淘汰的机型。

3、一体机

一体机是不用连接电脑的，所以没有电脑知识也可以上，2000到3000元的机型越来越多，而且速度也变得更快，我知道佳能3110和佳能3200激光打印机一样，硒鼓和耗材都是一样的。请使用的同修进一步介绍。

二、刻录

一台电脑除了可以带多台打印机以外，还可以安装两台刻录机，和两块硬盘。现在一台sony52速刻录机才250元左右。一张刻录盘才8毛到1元左右，只是市场上盘的质量参差不齐，让有经验的同修指点一下，事半功倍。

关于各种视频音频格式的转换，有几个小经验和同修分享一下：

asf文件在如果系统没有在微软升级的情况

要。

佳能喷墨机堵头的墨水有：信靠牌的彩色墨水，上海维尔的彩色墨水，原色牌墨水。

黑色墨水能用的有东北的锦龙牌（原来的锦江牌），麦普牌，但是此两种牌子在不过滤的情况下都有堵头的记录，锦龙牌的彩色还可以。

墨水选好过后，一定注意不要经常换品牌了，尤其是黑色，黑色一出问题，只能换喷头，彩色坏了，黑色还能打印文字啊！

我个人已经用过几种型号的佳能喷墨机，优点多多。不过现在随着正法进程的推进，资料的需求量还在长，激光打印机从目前来看，应该是有电脑的家庭资料点的首选。

2、激光打印机

从1200元至1800元，可选机型很多（首选惠普和佳能机型），对于我们来说速度很重要。最近我体会，下进纸的机型对于新手来讲很困难，尤其是骑马钉打印时，一旦连纸或错页，很难处理。新手最好选一款上进纸的机型，一旦出错，可以把纸用手拿出来。

120克或更重一些的碳粉（5L—6L粉），一只

华大学光盘国家工程研究中心监制），质量鉴定为一级，数据保存时间可长达10年，质优价廉。每张¥1.2左右。

讲真象的钱是宇宙未来的神为在救度众生的同时解体一切邪恶、邪恶因素及其因素的因素而聚集的威德，负责采购的同修一定要精打细算，节约出的每一点每一滴都可以更多的救度众生和解体邪恶。

对最近制作资料的一点经验 ——小型家庭资料点（图）

【明慧网2005年1月29日】

一、印刷

1、喷墨机

佳能喷墨打印机1000元左右的机型，在灌墨水和堵头的问题上，用久了是要用很大的精力的。佳能喷墨机的打印黑白文字的速度和其它品牌相比是非常快的。

有一位同修用I550型，新换完喷头过后，用全能牌黑色墨水（不加纯净水和或酒精），已经打印了10000张左右，还没有堵过头。选好墨水很重

组装拷贝机（可从专业经营刻录机的代理商处组装，推荐组装LG的一拖多拷贝机，刻录性能稳定，应组装带有硬盘的，这样可以存储需要经常刻录的光盘的映像）。

希望笔者的这些小经验能对同修采购制作真象资料的设备和耗材有所帮助，不当之处，敬请同修批评指正。

制作资料和购买耗材的经验交流

【明慧网2005年1月5日】

1. 市场：

建议中国大陆的同修注意观察本地耗材市场中大多数顾客的性别、年龄和装扮，以作形象参考，智慧、理智。

尤其是经常购买耗材的同修，一定注意不要贪图一时的方便老在同一家耗材市场购物。最好每次换不同的市场购物，并且最好不在卖场楼层的柜台购物，而到耗材市场较高楼层的销售公司购物最好。这样更利于安全和方便：不用穿梭于各柜台，所需各种耗材都可在一处购齐（即使一些耗材这家销售公司没有，它同样可以去别家同行内部拿货提供给我们）。建议每次都换不同的柜台或销售公司

要求对方提供农村信用社的帐号，一是不收汇费，二是不要求提供汇款人的个人信息，而其他银行收费不说，还要求提供汇款人身份证甚至开户人的身份证号等。快运费非常便宜，从省城到本地发一个放电脑主机大小的箱子运费约四五元，而直接去省城科技市场购买费用至少要四五十元，而且花费一整天时间。从快运公司提货发来货后，快运公司打联系电话通知提货人，一般去提货时说明提某某人的货和联系电话，签名付运费后即可提货。正规的快运公司有时会要求提供提货人的身份证或留下身份证号，这时可以说：“老板不在，老板通知我来提货，没带身份证”或“身份证正在换证”或“身份证正用于办理贷款”等等。如要求留下身份证号，可随便根据身份证的编码规律随便写一个，对方并不会留意。快运公司不会不让提货。笔者经常以假名提货，从未遇到提不出货的情况。卖方、快运公司对发货记录会存档，以真名联系发货、提货不安全。

四、讲究还价技巧。一般网站上公布的价格因更新慢等原因，要比实际售价高。我以前曾吃过亏：从网上查到48倍速的三星康宝刻录机价格是750元，从本地小电脑经销商处得知其售价也是750

喷纸，高光像纸用鑫王子、天威等，墨水及连续供墨系统用麦普、天威等，碳粉用天威、AB、麦普等，硒鼓鼓芯用AB的。打印机及速印一体机用纸也可从印刷物资公司购买质量较好的成领的双胶纸，一领是500张纸，要求其切成所需的A4或B5大小，质量比复印纸稍差，但打印时带纸较少，也不影响使用，价格比购买成箱的品牌复印纸便宜。使用光盘用量较多，注意不要贪图便宜而购买最便宜的“三无”光盘，这样的光盘通常质量难以保证，刻录出来的光盘有时会放不出，或有噪音，或有马赛克现象。通常应选购广东一带正规大厂家出产的有注册商标的光盘（最好内环部有喷码的），即可满足制作真象和讲法的需要，现在省城上千张购买价格约0.82-0.85元一张。少量制作讲法光盘也可选购优百特、明基、清华同方、大自然等名牌，但一般价格较贵，价格要贵出前者近一倍。至于塑封机、塑封膜、切纸机、切卡机、卡片纸、不干胶纸等技术含量较低的东西可不必太讲究，一般产品即可满足使用要求。注意大件设备有保修期最好索要发票或收据。如卖方开具发票则含税，价格要高一些，索要普通收据能证明经销单位和购买日期就能解决保修问题了。正规代理商对所售商品均有存档

元，就从本地购买了。但过后去省城科技市场一问，价格只有590元。即使是代理商给销售商的价格也有水分，应适当砍价。如初次交易可称：“我是某某电脑公司的，请给我个实在价。以后我需要什么固定下来从你那儿发货。”以后再交易可以称：“你看我也是搞经营的，也是你们的老客户，请给我个最低价。”通常对方自动会如光盘上千张购买对方要价0.85元/张，可还价为0.80。打印机要价950元，可还价为900元。塑封机要价165元，可还价160元。如我购买epson830u打印机的整套原装墨盒时，代理商出价220元，我以自己是电脑公司的名义，要求对方便宜一点，对方自动降价为210元。我出价200元，对方说给电脑公司的最低价就是205元，最后以205元成交。还价要有分寸，原则上不能还得太低，因为代理商或批发商比较讲究信誉，其出价水分不会太大，如果很冒失的还价很多，会给对方一个自己并不是业内人士的感觉，对方会怀疑你的身份。

五、注意所采购的商品的品牌和质量。采购的大件设备和电脑耗材毋庸置疑名牌产品是首选，具体可请教有经验的同修或参照明慧网交流文章。如打印纸可用旗舰版、高峰牌、威尔牌等，彩

购物：市场价格是通的，这家愿意卖的价格别家同样有的赚，都买得到。

大量购买耗材（尤其是纸张、光盘等较重的耗材），最好由男同修负责。

在学好法、炼好功、发好正念的基础上，最大限度的符合常人形式，智慧、理智，也是对自己、对同修、对大法负责。

2. 塑封膜（画像膜）和塑封机：

推荐使用宜兴市王者画像膜7个丝A4的100张一包¥23左右。塑封机A4塑料外壳的每台¥95左右，但不适于长期频繁使用；推荐使用北京意高科技A3的IC0—310塑封机（金属外壳），电机使用寿命5至6年，出膜平整度好，不易卷膜，外壳不发烫。

3. PP袋（光碟袋）：100张一包¥5。

4. 一次性可记录光盘（700MB 80MIN 2X 52X CD-R disk）：

真象光盘建议用数码多（cyberstore），市场销量巨大，兼容性优良，刻出的真象光盘几乎可在所有影碟机型上读出播放。每张¥0.85左右，600张一箱¥510。

母盘和重要的资料盘建议用龙马（LONGMA 清

记录，对售给经销商的商品即使无发票、收据，只要有保存的汇款收据、从快运公司提货的单据，向对方说明购买时间、购买单位，对方查实后也会予以保修。

六、有条件的可通过阿里巴巴网上即时交易系统从网上与厂家交易。该系统双方可直接在网上对话商谈。笔者曾试图通过该网上即时交易系统从南方生产光盘的厂家联系批发光盘。直接从厂家批发，价格会更便宜，但一般要求交易数量较大。现从省城发光盘一二千张价格约0.80元多，如从厂家直接批发一二十万张，可能会0.60元多。但因占用资金较大，且无与厂家交易的经验、对远程快运环节不熟悉，一直未能做成。建议有经商背景的同修尝试通过此方式发货，会节省很多资金。但如果是维持小型资料点正常运行，用量较小，则无必要通过此方法采购。

另外需要强调的是，做好这项工作并不难，前提是要学好法，发好正念，师父自然会安排你得到许多想要得到的信息。例如我组装光盘拷贝机时，通过发正念，非常顺利的在省城科技市场找到一家专业经营刻录机代理商，比在其他地方通过小经销商辗转组装便宜了几百元。

笔者推荐的万元小资料点的硬件配置及参考价格是：1. IBM P2 笔记本电脑+CDMA无线上网卡（2500元+2200元）能满足上网、下载、与明慧网联络、排版、打印、刻录光盘的基本需要。2. 旅之星30G移动硬盘+256M闪盘（780元+220元）3. epson 830u打印机（800元）+麦普连续供墨系统（180元+500ml墨水六瓶270元）该款打印机能满足打印照片、制作真象图片和护身符卡片的需要，配合连续供墨系统后非常经济实用。4. 三星4100激光一体机或HP3015激光一体机（2100元或2500元）具备黑白激光打印和脱机复印的功能，加粉换鼓芯比较方便。尤其推荐三星4100一体机，体积较小，性能稳定。而以前同修推荐的小型复印机价格与此基本相同，但速度太慢（一分钟3-4页），且功能单一，个人认为没必要购买。5. 优百特或建兴外置刻录机（1000元）6. 亚泰塑封机160元7. 申广手动切纸机270元8. 亚泰切卡机60元

上述配置的优点是功能齐全，性价比高。家庭资料点可根据需要选用上述设备，如使用台式机可直接安装二三百元的TEAC（帝亚克）、LG、索尼等刻录机。如果大量制作真象资料和真象光盘，则应配制能自动制版的速印一体机（如迅普牌的）和