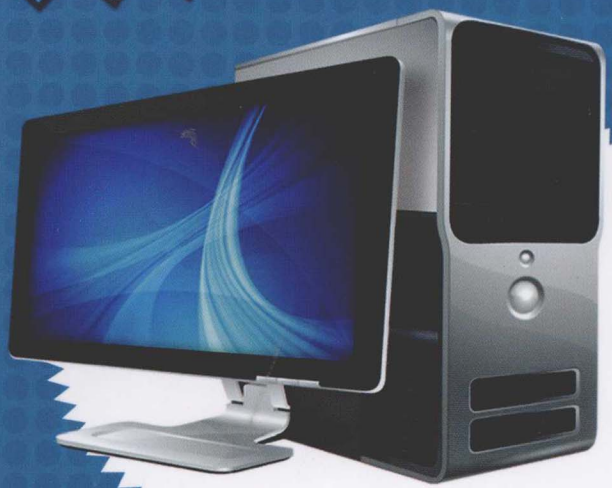
COMPUTER

自己动手

打造电脑安全防线

陈昌涛 刘小伟 向丹波 编著

DIY 解决一切



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

自己动手打造电脑安全防线

陈昌涛　刘小伟　向丹波　编著

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

目前，电脑信息系统安全已经涉及千家万户，任何电脑都需要打造一道道严密的安全防线，才能确保用户的重要信息、个人资料和秘密文件的安全，个人电脑安全防护技能也因此成为普通电脑用户也必须要掌握的一项基本技能。为了使读者较全面、系统地学会电脑信息的安全防护知识，掌握自己动手打造电脑安全防线的技能，本书针对非专业电脑人士的需求，从零开始，系统全面地讲解了电脑安全防护基础、操作系统的安全设置、电脑病毒查杀、恶意软件清除、黑客防范、木马查杀、防火墙的配置与应用、硬盘数据的安全防护等内容，还简要介绍了家庭无线局域网的安全配置手段。全书内容翔实、通俗易懂，并且实例丰富、可操作性强、图文并茂、阅读轻松，是广大个人电脑用户提高安全防范意识，掌握信息安全防护技术的首选读物，也可作为电脑短训班的培训教材。

图书在版编目(CIP)数据

自己动手打造电脑安全防线 / 陈昌涛，刘小伟，向丹波编著.—北京：电子工业出版社，2009.2
ISBN 978-7-121-08012-8

I. 自… II.①陈…②刘…③向… III.电子计算机－安全技术 IV.TP309

中国版本图书馆 CIP 数据核字（2008）第 203173 号

责任编辑：易　昆
印　　刷：北京天竺颖华印刷厂
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
　　北京市海淀区翠微东里甲 2 号　邮编：100036
开　　本：787×1092　1/16　印张：22.75　字数：570 千字
印　　次：2009 年 2 月第 1 次印刷
定　　价：41.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

目前，人们的学习、工作和生活越来越离不开电脑和网络系统。然而，大多数电脑（特别是家用电脑）都存在严重的安全隐患，轻者系统运行速度变慢、死机频繁，严重时甚至出现系统瘫痪、重要信息被窃等事故。近年来，随着 Internet 的普及，长期在线的电脑也越来越多，系统中毒、网站被黑、网上银行密码被盗、商业信息泄密、QQ 号码被盗、个人数据被窃等事件更是层出不穷，给电脑用户造成了巨大的损失。因此，任何电脑用户都应该提高防范意识、采取必要的安全手段，才能在信息社会中处于不败之地。

电脑信息安全是一个系统工程，现有的安全防护技术也不尽完善。对于普通电脑来说，只需了解必要的电脑安全防护知识，掌握个人电脑的基本安全设置措施，学会使用最新杀毒软件查杀电脑病毒，掌握必要的黑客和木马防范技能，熟悉防火墙的安装和配置方法，就能初步打造一道电脑安全防线。此外，还必须重视硬盘数据信息的安全，如果使用无线网络，也要进行必要的安全配置。

本书面向普通电脑用户，结合大量实例全面介绍了电脑信息安全的基本知识和实用的电脑信息安全防护手段，循序渐进地指导读者学习以下内容：

1．电脑安全初步知识：主要包括认识电脑系统的安全隐患、树立必要的信息安全意识、检测电脑的安全性能、立体安全防御体系的组成等内容。

2．个人电脑的基本安全手段：主要包括 Windows 安全选项设置、Windows 系统漏洞修补、重要数据的备份、密码设置技巧、 加密文件/文件夹、销毁数据、清除使用痕迹等内容。

3．应对电脑病毒：主要包括电脑病毒的基本常识、杀毒软件的设置与应用技巧、通过网络在线查杀病毒和使用专杀工具查杀病毒等方面的内容。

4．清除恶意软件：主要包括恶意软件的基本常识、恶意软件防范、使用清除工具清除恶意软件等内容。

5．黑客防范基础：主要包括黑客的基本常识、黑客的攻击类型与入侵方式、黑客的攻击过程、防黑的基本措施等内容。

6．查杀木马：主要包括木马的基本常识、使用网络在线查杀木马、使用木马查杀工具查杀木马等内容。

7．打造安全防火墙：主要包括防火墙的基础知识、Windows 防火墙的配置与应用、个人防火墙软件的配置与应用、ARP 防火墙的基本应用等内容。

8．硬盘数据信息的安全：主要包括硬盘数据的安全威胁、硬盘的日常维护、硬盘安全技术、硬盘故障处理和应用硬盘维护工具等内容。

9．小型无线局域网的安全：主要包括无线局域网的安全威胁、无线网络的安全技术、无线网络的安全对策和无线接入点（AP）的安全配置等内容。

本书由陈昌涛、刘小伟、向丹波执笔编写。此外，李丽霞、余强、郭军、刘飞、刘晓萍、

张源远等也参加了本书的实例制作、校对、排版等工作，在此表示感谢。由于编写时间仓促，编者水平有限，书中疏漏和不妥之处在所难免，欢迎广大读者和同行批评指正。

目 录

第 1 章　你的电脑安全吗

自电脑问世以来，安全问题一直就是一个难题。近年来，随着 Internet 的普及，长期在线的电脑越来越多，系统中毒、网站被黑、网上银行密码被盗、商业信息泄密、QQ 号码被盗、个人数据被窃等事件更屡见不鲜，只有提高防范意识、采取必要的安全手段，才能在信息社会中处于不败之地。

电脑系统的安全隐患究竟有哪些？网络在给人们带来广阔空间的同时，又对信息造成哪些安全威胁？应该树立什么样的信息安全意识？如何检查自己的电脑是否安全？如何打造电脑安全防线？在本章的学习过程中，我们将不断地解决这些疑问，使我们能充分意识到信息安全的重要意义，了解电脑系统面临的各种威胁，并能初步掌握保障电脑安全的一般常识。

1.1　电脑系统的安全隐患

电脑作为一种通用的现代信息工具早已深入千家万户，学习、工作和生活越来越依赖于电脑及网络系统。然而，不少电脑都存在一定的安全隐患，特别是连接在互联网上的个人电脑，安全问题更加突出。出现安全故障后，轻者系统运行速度变慢、死机频繁，严重的常常出现系统瘫痪、重要信息被窃。为了正视普遍性的电脑安全问题，本节先简要分析个人电脑系统的主要安全隐患。

1.1.1　电脑系统的安全隐患

由于电脑技术本身存在安全弱点、系统安全性差、缺乏安全防护手段等原因，电脑信息系统总的来说是比较脆弱的。防护电脑安全就是采取各种措施，保障电脑及网络的硬件、软件和信息不受自然或人为有害因素的威胁与危害。

电脑信息系统的安全威胁和攻击主要来自于系统故障、人为操作不当、环境影响及自然灾害、电脑病毒、有害信息、黑客攻击、垃圾邮件与间谍软件等方面。

1. 系统故障

由于各种原因，无论是硬件还是软件，都有可能出现各种故障，造成系统运行速度变慢、电脑部件功能丧失或系统瘫痪等现象，甚至酿成硬盘数据损坏或丢失等信息安全事故。

2. 不当操作

电脑故障很大程度上是由于使用人员操作不当造成的，重要文件损坏和很多泄密事件也是由操作不当所引起的。不少企业和个人都存在计算机安全意识淡薄和系统安全认识模糊的情况，没有对电脑采取必要的日常维护和安全防护手段。比如，没有安装杀毒软件、杀毒软件过期、没有开启防火墙、密码设置过于简单，操作失误，等等，这样很容易造成密码泄露、感染

木马或蠕虫病毒、网站被黑、系统不稳定、丢失重要数据、电脑或网络系统瘫痪等后果。

3. 环境影响及自然灾害

电脑系统比较容易受到自然灾害和工作环境的影响。很多电脑并没有完善的防震、防火、防水、避雷、防电磁泄露或干扰的措施，抵御自然灾害和意外事故的能力较差。软硬件也缺乏必要的维护，各种因环境影响而造成电脑重要信息被毁的事故时有发生。

4. 电脑病毒

电脑病毒是一种人为编制或者在电脑程序中插入的、破坏电脑功能或者毁坏数据、影响电脑使用，并能自我复制的一组电脑指令或者程序代码。感染病毒后，电脑及电脑网络系统可能会出现系统瘫痪，数据和文件丢失等严重事故。电脑病毒的传播途径很多，特别是随着 Internet 的普及，上网电脑更是时刻都容易受到各种网络病毒的威胁。

5. 黑客的威胁和攻击

一般将采用非法手段避开网络的存取控制而进入电脑系统的人称为黑客（Hacker）。由于 Internet 是一个开放的、无控制机构的网络，黑客往往会肆无忌惮地非法侵入电脑或网络系统，窃听、获取、攻击用户的敏感和重要信息，修改和破坏信息网络的正常使用状态，造成数据丢失或系统瘫痪，给单位或个人造成损失。比如，一些计算机犯罪分子利用窃取口令等手段非法侵入计算机信息系统，传播有害信息，恶意破坏计算机系统，实施贪污、盗窃、诈骗和金融犯罪等活动。

6. 垃圾邮件

垃圾邮件泛指未经请求而发送的电子邮件，如收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件；隐藏发件人身份、地址、标题等信息的电子邮件；含有虚假的信息源、发件人、路由等信息的电子邮件；含有病毒、恶意代码、色情、反动等不良信息或有害信息的邮件等。一些人常利用电子邮件地址的“公开性”和系统的“可广播性”，把各种电子邮件强行发送到他人的邮箱，迫使他人接收垃圾邮件。

7. 间谍软件

间谍软件（Spyware）是能够在使用者不知情的情况下，在用户电脑上安装后门程序的软件。用户的隐私数据和重要信息会被那些后门程序捕获，甚至这些 “后门程序”还能使黑客远程操纵用户的电脑。与电脑病毒不同，间谍软件的主要目的不在于对系统造成破坏，而是窃取系统或用户的信息。

8. 有害信息

有害信息泛指电脑及网络系统中，以电脑程序、图像、文字、声音等形式表示的，含有以下内容之一的信息：

- 煽动抗拒、破坏宪法和法律、行政法规实施的信息。
- 煽动颠覆国家政权，推翻社会主义制度的信息。
- 煽动分裂国家、破坏国家统一的信息。
- 煽动民族仇恨、民族歧视，破坏民族团结的信息。
- 捏造或者歪曲事实，散布谣言，扰乱社会秩序的信息。
- 宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的信息。
- 公然侮辱他人或者捏造事实诽谤他人的信息。
- 损害国家机关信誉的信息。

◆ 其他违反宪法和法律、行政法规的信息。

有害信息大多是通过 Internet 来传播的，上网用户应特别加强对有害信息的防范。

1.1.2　网络应用的安全风险

自从 Internet 流行以来，电脑病毒、黑客和恶意程序等安全问题就始终困扰着人们。网络是一个复杂的系统，无论是网络硬件开发、协议设计，还是网络应用软件开发，都是非常复杂的工程，也导致了网络存在许多不完善之处，从而形成各种安全风险。

从网络应用的角度来看，网络系统的主要安全风险表现在网页浏览、网络下载、即时通信、网络游戏、网上支付/交易平台、电子邮件等方面。

1. WWW 浏览器的安全风险

IE 等浏览器是使用最频繁的网络工具之一。目前，主流的浏览器都存在一定的漏洞，是黑客的主要攻击目标。黑客利用浏览器漏洞进行攻击的主要形式有。

◆ **网页挂马**：黑客在网站中植入木马和病毒，使用户访问网页后就会中毒。由于这种攻击形式可以快速地批量入侵大量电脑，快速地窃取用户资料，是黑客首选的入侵手段。

◆ **“钓鱼”诈骗**：黑客利用浏览器的漏洞，在网页中插入恶意代码或者使浏览器显示错误的网址。有些黑客还向用户直接发送邮件或者 QQ 消息，让用户点击虚假的银行、购物等钓鱼网站，骗取用户的账号、密码等重要信息。

◆ **ARP 攻击**：ARP 地址解析协议是一种常用的网络协议，每台安装上 TCP/IP 协议的电脑里都会有一个 ARP 缓存表，如果该缓存表被修改，就会出现网络无法连通或访问的网页被劫持等现象。黑客利用 ARP 协议存在的缺陷，侵入某台电脑之后发送 ARP 欺骗攻击数据包，造成局域网内所有用户在访问网络时，收到的都是带病毒的网页。

2. 网络下载的安全风险

在迅雷、网际快车、BT、电驴（eMule）和其他 P2P 下载方式广泛流行的同时，这些下载方式也成为黑客传播病毒的重要手段。由于 P2P 软件本身的特点，即使带毒的源文件被删除，其他用户还能从未删除病毒的电脑中下载到。因此，黑客将 P2P 软件作为传播途径时，不用攻击网站、不用其他代价，就能把病毒散播出去。网络下载软件的安全风险主要有：

◆ 对于迅雷和网际快车，黑客可能将病毒和热门软件、热门电影捆绑在一起，使用户下载后被感染。

◆ BT 一般用来下载网络电影和大型软件，黑客如果在 BT 种子站植入木马，用户浏览后就会中毒。

◆ 电驴的搜索功能比较强，如果用热门搜索词当做病毒文件的名字，则有很大可能搜索到并下载病毒，用户下载后就会中毒。

3. 即时通信软件的安全风险

QQ 等即时通信软件是上网用户主要使用的工具，在高使用率的同时，各种即时通信软件也成为病毒重要的传播途径。QQ 的主要安全风险有：

◆ 黑客通过 QQ 自动发送带毒网址，使用户浏览这些网站后中毒或发送钓鱼网站的网址，以骗取用户的银行账号等信息。

- ◆ QQ 自身可能出现漏洞，可能使操作系统的安全性降低，让黑客轻易入侵。
- ◆ 黑客可能通过病毒等手段截取 QQ 聊天的信息，造成用户信息泄露。
- ◆ 黑客通过“QQ 尾巴”等病毒，传送病毒文件、广告消息等。“QQ 尾巴”侵入后，就会自动向 QQ 好友发送垃圾消息。
- ◆ QQ 密码也是黑客窃取的重要对象。目前，黑客往往编写专门的 QQ 木马，通过进程注入、键盘钩子、读取内存等手段窃取 QQ 密码。

4. 网络游戏的安全风险

网络游戏的安全风险主要是黑客使用恶意软件或者电脑系统操作监听软件，偷取用户的游戏账号，然后出卖玩家的虚拟财产和其他物品。

5. 网上支付/交易平台的安全风险

近年来，网络银行、网上交易、股票交易的病毒数量一直呈上升趋势。网上支付/交易平台的安全风险主要表现在以下方面：

- ◆ 普通用户缺乏基本的安全意识，未安装或未及时升级杀毒防黑软件。
- ◆ 用户密码的安全性能低。
- ◆ 用户未严格按规程操作。
- ◆ 钓鱼网站恶意欺骗用户。

6. 电子邮箱的安全风险

电子邮件已经成为黑客传播病毒最为重要的渠道之一，使用电子邮箱的安全风险主要表现在以下方面：

- ◆ 一些邮件包含了病毒代码，一旦打开邮件，电脑就会中毒。
- ◆ 黑客通过电子邮件发送钓鱼网站、带毒网站等，用户点击电子邮件中的不良网址后，就可能中毒或被骗取银行账号、信用卡账号等信息。
- ◆ 黑客通过病毒或其他手段截取电子邮件的内容，造成用户信息被窃取。
- ◆ 电子邮件也存在着被拆看、误投和伪造的可能，这对用电子邮件传输重要机密信息的用户来说，存在很大的危险。

1.1.3 个人电脑常见的入侵形式

任何电脑都不可能绝对安全，只能尽最大努力使电脑远离隐患。对于个人上网用户，常常遇到的入侵形式主要有以下几种。

1. 密码被盗

使用电脑时，常常要用到很多密码，如邮箱密码、QQ 密码、网上银行密码、网络游戏密码、文件加密密码等，随着各种木马病毒、钓鱼网站的盛行，各类密码失窃事件层出不穷。上网用户必须提高密码保护意识和相关知识，通过各种手段确保密码信息的安全。

2. 木马攻击

木马是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。电脑一旦中上木马，黑客就可以任意在电脑上上传或下载文件，偷窥用户的隐私文件，盗取用户的重要信息。

3. 恶意 JavaScript 程序攻击

JavaScript 是一种基于对象和事件驱动的脚本语言，主要用于与 HTML 超文本置标语言、Java 脚本语言一起在一个 Web 页面中链接多个对象，从而实现 Web 与客户的交互。但是，一

些不法人员在网页中植入了恶意的JavaScript程序，只要浏览这些网页，就可能被恶意JavaScript程序攻击。

4. QQ被攻击

QQ是国内最流行的即时通信工具。在使用QQ进行通信时，所传送的信息包中包含了本机的网络信息，如用户的IP地址、地域位置、端口号等信息就有可能泄露给黑客，从而造成系统被攻击或重要信息泄密。

5. 病毒感染

电脑病毒的危害越来越大，而随着互联网的普及，各种新型的恶意病毒更是防不胜防。如果个人电脑不慎感染病毒，轻者会使系统运行速度变慢、数据受损，严重时还可能会造成系统崩溃。

6. 黑客恶意攻击

近年来，个人电脑也成为黑客恶意攻击的主要目标之一。黑客常常使用木马入侵、ipc$共享入侵、IIS漏洞入侵、网页恶意代码入侵等手段攻击个人电脑。遭到攻击后，系统往往会被他人远程控制，使得重要资料被窃取或篡改。

你在使用电脑的过程中曾经遇到过哪些安全威胁？上网时是否曾经遭遇过不法人员入侵？

1.2　提升信息安全意识

大量事实表明，个人电脑遭受病毒破坏、木马攻击、恶意程序骚扰、黑客恶意侵犯等侵害，常常是由于用户缺乏安全意识，不具备必要的信息安全知识所造成的。只要有电脑应用、有网络存在，计算机犯罪就不可避免，安全问题就不容忽视。

1.2.1　安全操作意识

用户因误操作造成设备损坏、数据丢失、信息泄密的现象时有发生，由于噪音和电磁辐射，导致网络信噪比下降，误码率增加，信息的安全性、完整性和可用性受到威胁的现象也屡见不鲜。要减少或避免误操作，必须养成良好的操作习惯，树立安全意识，从小事做起，从现在做起。下面简要介绍一些安全操作注意事项：

- 电脑必须使用3芯带接地保护的接地电源插头和插座，以确保电脑硬件，特别是保存用户数据的硬盘安全工作。
- 要严格按照规定的方法连接电脑外设，各插接件有锁定螺丝时要注意拧紧，开机时应先接通显示器的电源，然后再打开主机电源开关。
- 在没有切断主机电源的情况下，绝对不要插拔非热插拔设备或电脑板卡。
- 移动电脑时要轻拿轻放，不要在开机状态下移动电脑。关机以后不要马上搬动电脑，要等硬盘等部件完全停止工作后再移动。
- 要避免频繁开关机，否则会缩短电脑寿命。关机以后，应至少等待30秒再开机。
- 不要随便删除硬盘上不了解的文件，否则很容易使电脑运行异常甚至瘫痪。
- 要注重日常维护，比如在系统非正常退出或意外断电后，应尽快进行硬盘扫描，及时

修复错误。因为在这种情况下，硬盘的某些簇链接会丢失，给系统造成潜在危险，如不及时修复，会导致某些程序紊乱，某些数据丢失。

- 电脑工作的环境温度不能过高。由于电脑芯片和许多部件对温度非常敏感，环境温度过高、通风冷却条件差时，可能使元器件内部温度超标而发生老化。高温还会导致软磁盘的物理变化，致使磁盘损坏而损坏磁头。
- 相对湿度过低时容易产生静电，对电脑造成干扰。相对湿度过高，会使电脑内部焊点和插座焊点的接触电阻增大。对电脑来说，湿度最好在30%～80%之间。
- 要注意防尘。灰尘对电脑的损害较大。如磁盘和磁头上的灰尘太多时，轻则造成读、写错误，重则造成划盘。因此，机房内要定期除尘，同时要尽量减少人员的流动。
- 各种扩展卡、外存储器插座、芯片插座、电缆的插脚等都很容易因化学作用而锈蚀。需要通过定期清洁来解决锈蚀问题，通过清洁使接头及插脚保持干净，减少接触不良的机会。
- 电脑存储器和其他部件对电磁干扰相当敏感，严重的电磁干扰会使电脑无法正常操作。可以使用滤波来屏蔽、限制电磁干扰的来源，也可以改良布线方式、改良元件设计等。当然，摆放电脑的位置应远离强电磁场、超声波等辐射源，以避免干扰电脑的正常运行。
- 静电放电时，在电路中会造成电压脉冲，这可能使工作中的电脑程序出现偶发性的随机错误。因此，要注意静电的影响。
- 高品质的电力供应是电脑系统能否稳定操作的最重要因素。当电脑遇到了电源故障时，无论是电压过低或电压过高都可能对电脑造成相当严重的冲击，使得元件性能劣化而加快损坏的速度。特别是电压波动可能使磁盘驱动器工作不稳而引起读、写错误，甚至数据遭到破坏。

1.2.2 病毒防范意识

电脑病毒层出不穷，甚至愈演愈烈，且传播方式多样化，又具有一定的隐蔽性。对此，应把握“预防为主，防治结合”的原则。要防范病毒，首先应提高对电脑病毒的防范意识，了解电脑病毒防治的基本常识，建立长效的应急和预防机制。

1. 电脑中毒的主要症状

使用电脑时，要注意有没有奇怪的现象，如速度变慢、出现奇怪的文件、文件变大、内存减少等。如果出现这些现象，除了软硬件故障和系统配置问题，便是感染病毒了。中毒电脑的主要症状很多，凡是电脑工作不正常都有可能与病毒有关，常见的症状有：

- 电脑启动或运行的速度比平常慢，程序载入时间比平常长。有些病毒能控制程序或系统的启动程序，当系统刚开始启动或是一个应用程序被载入时，这些病毒将执行它们的动作，因此会花更多时间来载入程序。
- 系统自动执行某些操作，这一般是由于病毒在后台执行了非法操作。
- 屏幕出现特殊的错误信息或突然黑屏，系统出现异常的声音、音乐。
- 没有存取磁盘时，磁盘指示灯也在闪烁。
- 系统内存容量忽然大量减少，增加大量来路不明的常驻程序。有些病毒会消耗可观的内存容量，曾经执行过的程序，再次执行时，突然提示没有足够的内存可以利用，很

可能是病毒已经感染了文件。

- 磁盘可利用的空间突然减少，这表明病毒可能开始自我繁殖了。
- 某些文件（如可执行程序等）的容量突然变大。
- 硬盘的坏簇或坏轨增加。有些病毒会将某些磁区标注为坏簇或坏轨，而将自己隐藏其中，使杀毒软件无法检查病毒的存在。
- 文件奇怪消失、文件的内容被加上一些奇怪的资料或者出现大量来历不明的文件。文件名、扩展名、日期、属性被更改或者文件无法打开。
- 系统发生莫名其妙的死机，或者突然重新启动或无法启动。
- 程序不能运行，或者数据和程序丢失。
- 键盘或鼠标无端被死锁。正常的外设使用异常，如打印出现问题、键盘输入的字符与屏幕显示不一致等。
- 异常要求用户输入口令。

2. 病毒防范措施

对于普通电脑用户，病毒防范应从以下几个方面入手：

- 必须认识到，不可能有绝对安全的电脑系统，应时刻保持思想上的警惕，提高自身防范意识。
- 定期备份重要的用户数据。用户数据一般是指日常工作中由用户自己创作或收集来的数据文件，比如手工输入的文章、制作的图形图像、报表等，这类数据至少每周要备份一次。这样，即使遇到病毒袭击而导致系统瘫痪，也还有备份可用。
- 不要使用盗版和来历不明的软件，不要打开来历不明的移动存储器中的文件。
- 必须在系统中安装具有隐私保护等功能的优秀正版杀毒软件，开启实时监控功能，并将杀毒软件设置成自动或者定时升级。
- 正确使用杀毒软件，养成常用杀毒软件来检查硬盘、外来文件和每一张外来盘的良好习惯。
- 上网时，尽量不要访问没有安全保障的网站。QQ聊天时，不要随便打开陌生人发来的链接，不要随便接受陌生人传过来的文件或程序，不要在互联网上随意下载软件。
- 不轻易打开来历不明的邮件附件，要通过合理设置抵御垃圾邮件。
- 订阅防病毒软件生产商网站提供的电子邮件病毒通知服务，随时关注反病毒公司的最新病毒信息。
- 对于局域网内的电脑，尽量不要开放共享文件夹。如果实在要开放，要为共享文件设置密码，并在不需要共享时立即关闭共享。
- 随时注意电脑系统的各种异常现象，一旦发现异常，应立即用杀毒软件仔细检查，并将可疑文件提交专业反病毒公司进行确认。
- 保持良好的操作习惯，设置开机密码。使用屏幕保护和密码，在离开电脑时将电脑锁定。
- 开启防火墙。
- 上网时，尽量不去访问不熟悉的网站或论坛。
- 不要下载、安装、运行来历不明的插件。
- 及时安装操作系统补丁。

- 建议在进行电子商务活动或进行网上交易前，采用杀毒软件来查杀病毒。网上交易过程中要特别留意网页的变化，比如IE地址栏的详细信息、网页链接、一些可疑的进程等，并关注这些网页地址URL的变化情况。
- 尽量不要让别人随意使用自己的电脑，至少不要在自己的电脑上使用未经检查的移动存储器。

1.2.3 防黑防木马意识

黑客威胁着上网用户的安全，黑客入侵尽管防不胜防，但普通用户还是可以通过以下方面来尽量减少黑客入侵的可能：

- 定时使用扫描程序扫描系统漏洞，并安装上补丁，减少黑客入侵成功的机率。
- 关闭可疑的端口。一般木马都是通过漏洞在系统上打开端口留下后门，以便上传木马文件和执行代码，在把漏洞修补上的同时，需要对端口进行检查，把可疑的端口关闭。
- 避免让他人使用保存有重要信息的电脑，要为电脑设置个人密码。在电脑上安装杀毒软件，并关闭所有远程功能，开启系统防火墙，必要时安装上第三方防火墙和木马防范工具，如“天网防火墙”等。
- 及时备份重要数据信息。
- 使用加密机制传输数据，对于个人信用卡、密码等重要数据，在客户端与服务器之间传送时，应该经过加密处理再进行发送，以防止黑客监听、截获。
- 不要使用网页中的“记住密码”功能。
- 应该养成良好的使用习惯，不要随便开启来历不明并载有附件的电子邮件，不要点击可疑邮件内的超级链接，不要进入可疑网站。
- 不要在网上随便透露个人资料（如身份证号码、地址、银行账号、信用卡号码、用户名称及密码），除非确认使用的是可靠及信誉良好的网站。
- 在提供个人资料给网站前，应先查阅网站的保密条款及安全防护措施声明。定期更改上网密码，定期查看交易记录。
- 不要将存有重要信息的电脑用做文件共享等类型的服务器。
- 各类密码要有较高的强度，必须易记但难被猜中，切勿使用简单数字排列、出生日期、电话号码、家人的名字或常用的名字。不要向任何人透露密码，或把密码记录下来。
- 登录网上银行或交易网站时，必须严格核对登录网址，避免使用搜索引擎等第三方途径进行登录。
- 要避免在公用电脑上使用网上银行进行交易。

1.2.4 数据保护意识

电脑最宝贵的资源不是硬件，也不是安装在其中的各种软件，而是用户千辛万苦创建和保存在其中的重要数据。这些数据一旦丢失或受到破坏，多年工作的心血就可能化为乌有，因此任何电脑用户都应该牢固树立数据保护意识。基本的保护意识有：

- 定期备份重要数据。
- 加密重要文件和文件夹。
- 在硬盘读取数据时不能断电。

- 开机状态下，不要搬动机箱。
- 电脑必须放置在良好的工作环境下。
- 电脑出现故障时要注意避免进行盲目维修，免得扩大故障。
- 慎重对待各种危险命令和工具软件。
- 安装最新版杀毒软件，并定期升级。
- 硬盘出现异响时不要开机，要立即交由专业人员处理。
- 废弃的硬盘、U盘等外存储器应进行数据销毁处理，不能简单删除或格式化。

①你是否具备良好的信息安全意识？
②你还缺乏哪些必要的防护意识？
③你通常使用了哪些手段来维护电脑系统？
④你是如何检查和清除病毒的？
⑤你是如何防范黑客和木马病毒的？
⑥你是如何保护重要数据的？

1.3 检测电脑的安全性能

面对日益猖獗的病毒、木马和恶意软件，谁也不能确保自己的电脑一定安然无恙。如何了解自己的电脑是否安全呢？最简单有效的方法莫过于对电脑进行全方位的“安检”了。电脑安全性能的检测主要是通过相关软件来实现的，本节将介绍离线安检和在线安检的一般方法。

1.3.1 离线检测系统安全性能

使用优秀的系统安全测试工具，可以对电脑系统的端口进行扫描、对网络系统及操作系统的薄弱环节进行检测、对应用程序或数据库进行扫描，也可以对系统漏洞进行检查和修补，还可以清除各种恶意软件。下面简要介绍两款免费工具软件的安全检测功能和具体用法。

1. 用“金山清理专家”检测系统安全性

“金山清理专家”是一款用于对电脑系统进行全方位检查和维护，并提供修复建议和方法的网络安全工具，它提供了强大的恶意软件查杀、漏洞修补和在线系统诊断的功能。

（1）从“金山安全中心”网站（http://www.duba.net/）下载并安装免费工具软件“金山清理专家”。

“金山毒霸2008杀毒套装”中也集成了“金山清理专家”。

（2）选择【开始】|【所有程序】|【金山毒霸 2008 杀毒套装】|【金山清理专家】命令，启动“金山清理专家”，在主界面中单击【为系统打分】按钮，如图1-1所示。

（3）单击【为系统打分】按钮后，“金山清理专家”将自动扫描当前电脑的各个模块，包括恶意软件、漏洞、杀毒软件的状态、可疑文件、未知文件、BHO 和启动项等模块，全面检测并综合评估电脑系统的健康指数，如图1-2所示。

（4）扫描完成后，将评估出当前电脑的健康指数，并提示扫描发现的重大安全问题和其