第5章　信息安全

小澜：费了半天劲，终于让计算机连上互联网，可以畅游网络啦！

王老师：不能高兴得这么早，现在你的电脑还是不安全的。

小澜：不安全？为什么呀！

王老师：看过《黑客帝国》这个电影么？

小澜：看过，但是没看明白，真是不好意思。

王老师：在网络的世界里有很多威胁，诸如“病毒”“黑客”等时刻都会侵入你的计算机，如果此时你又在网上购物，那么你的账户就是非常危险的。

小澜：对呀对呀！我经常听说某人的账户被盗用之类的。那要怎么预防呢？

王老师：安装杀毒软件和防火墙是必需的，除此之外，每天还要进行必要的维护哦。本章就会给大家介绍相关的知识。

5.1　信息安全概述

信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名、信息认证、数据加密等）所组成的安全系统，其中任何一个安全漏洞便可以威胁全局安全。

狭义的信息安全是指信息网络的硬件、软件以及系统中的数据受到保护，不被偶然的或者恶意的原因所破坏、更改和泄露，系统能够连续可靠地正常运行，信息服务不中断。

信息安全的目标是保证信息的机密性、完整性和可用性。为保障信息安全，要求有信息源认证、访问控制，不能有非法软件驻留，不能有非法操作。

5.1.1　计算机病毒

1. 什么是计算机病毒

《中华人民共和国计算机信息系统安全保护条例》中指出：计算机病毒（Computer Virus）是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。

2. 计算机病毒的特征

计算机病毒具有寄生性、传染性、潜伏性、隐蔽性、破坏性和可触发性的特征。

（1）寄生性。计算机病毒寄生在其他程序之中，当执行这个程序时，病毒就能够起到破坏作用，而在未启动这个程序之前，它是不易被人发觉的。

（2）传染性。传染性是病毒的基本特征。只要一台计算机染毒，如不及时处理，那么病毒就会在这台电脑上迅速扩散，计算机病毒可通过各种可能的渠道，如软盘、硬盘、移动硬盘、计算机网络去传染其他的计算机。是否具有传染性是判别一个程序是否为计算机病毒的最重要条件。

（3）潜伏性。一个编制精巧的计算机病毒程序，进入系统之后一般不会马上发作，此种病毒可以静静地躲在磁盘或磁带里几天，甚至几年，一旦时机成熟，得到运行机会，就会四处繁殖、扩散，产生危害。

（4）隐蔽性。计算机病毒具有很强的隐蔽性，有的可以通过病毒软件检查出来，有的根本就查不出来，有的时隐时现、变化无常，这类病毒处理起来通常很困难。

（5）破坏性。计算机中毒后，可能会导致正常的程序无法运行，计算机内的文件、资源等受到不同程度的破坏。

（6）可触发性。病毒具有预定的触发条件，这些条件可能是时间、日期、文件类型或某些特定数据等。有些病毒像定时炸弹一样，让它什么时间发作是预先设计好的。比如黑色星期五病毒，不到预定时间一点儿都觉察不出来，等到条件具备的时候一下子就爆炸开来，对系统进行破坏。

3. 病毒的类型

（1）引导区病毒。这类病毒隐藏在硬盘或软盘的引导区，当计算机从感染了病毒的磁盘启动，病毒就开始发作。一旦病毒被拷贝到计算机的内存中，马上就会感染其他磁盘的引导区，或通过网络传播到其他计算机上。

目前传播最为广泛的引导区病毒是 WYX，这个病毒传播的唯一途径就是使用带有该病毒的启动盘（包含可启动的光盘）启动计算机。如果只是读取感染有引导区病毒的磁盘或者光盘上的文件是不会被感染的。如果计算机已经感染该病毒，并且病毒驻留了内存，则插入的 U 盘如果没有写保护的话很容易被感染。

（2）文件型病毒。文件型病毒主要感染可执行文件，常常通过对它们的编码加密或其他技术隐藏自己。文件型病毒劫夺用来启动主程序的可执行命令，用做它自身的运行命令。同时还经常将控制权还给主程序，伪装计算机系统正常。一旦运行感染了该病毒的程序文件，病毒便被激发，执行大量操作，进行自我复制。

由于文件型病毒是通过文件进行传播的，所以当使用来历不明的文件时，先用最新升级过的杀毒软件进行检查，确认没有文件型病毒之后方可使用，切忌双击打开或复制。

（3）宏病毒。宏病毒是一种寄存在文档或模板的宏中的计算机病毒。一旦打开含有宏的文档，宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在 Normal 模板中。从此以后，所有自动保存的文档都会“感染”上这种宏病毒，而且如果其他用户打开了感染宏病毒的文档，宏病毒又会转移到其他用户的计算机上。

Word 宏病毒的破坏性体现在两个方面：

● 对 Word 运行的破坏：不能正常打印；封闭或改变文件存储路径；将文件改名；乱复制文件；封闭有关菜单；文件无法正常编辑。如 Taiwan No.1 Macro 病毒每月 13 日发作，所有编写工作无法进行。

● 对系统的破坏：Word Basic 语言能够调用系统命令，造成破坏。

（4）脚本病毒。依赖特殊的脚本语言（如 VBScript、JavaScript 等）起作用，同时需要软件或应用环境能够正确识别和翻译这种脚本语言中嵌套的命令。脚本病毒与宏病毒有些类似，但脚本病毒可以在多个产品环境中进行。脚本语言比宏语言更具有开放终端的趋势，使病毒制造者对感染脚本病毒的计算机可以有更多的控制力。

（5）蠕虫病毒。网络蠕虫是利用网络进行复制和传播的计算机病毒。有些网络蠕虫拦截 E-mail 系统向世界各地发送自己的复制品；有些则出现在高速下载站点中传播自身。它的传播速度相当惊人，成千上万的计算机感染病毒造成众多的邮件服务器先后崩溃，给人们带来难以弥补的损失。

曾经肆虐网络的“熊猫烧香”病毒，是一种经过多次变种的蠕虫病毒。病毒会删除扩展名为 .GHO 的文件，使用户无法使用 Ghost 软件恢复操作系统。“熊猫烧香”感染系统的 .exe、.com、.f 、.src、.html、.asp 文件，添加病毒网址，导致用户一打开这些网页文件，浏览器就会自动连接到指定的病毒网址中下载病毒，在硬盘各个分区下生成文件 autorun.inf 和 setup.exe 文件。该病毒可以通过 U 盘和移动硬盘等方式进行传播，并且利用 Windows 系统的自动播放功能来运行，搜索硬盘中的 .exe 可执行文件并感染，感染后的文件图标变成“熊猫烧香”图案，如图 5-1 所示。

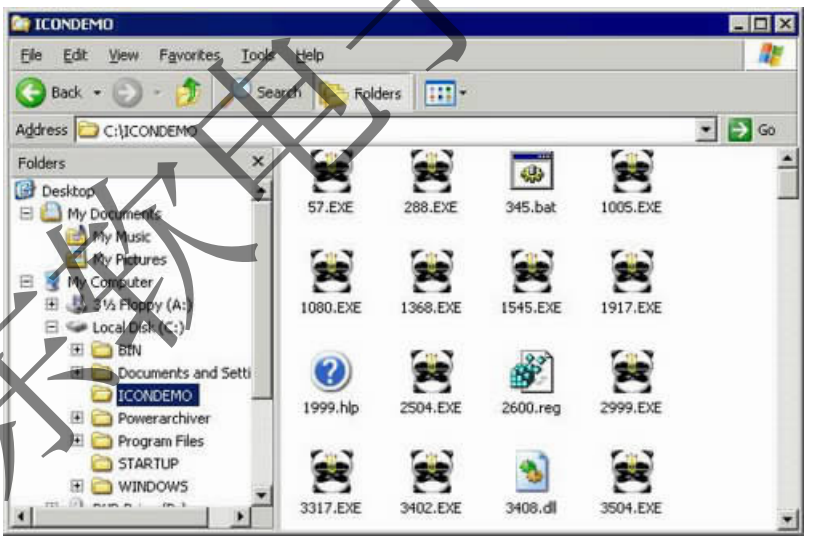

图 5-1　“熊猫烧香”病毒

5.1.2　黑客与网络安全

1. 黑客是指哪些人

“黑客”最早源自英文 hacker，早期在美国的电脑界是带有褒义的。“黑客”一词，原指热心于计算机技术、水平高超的电脑专家，尤其是程序设计人员。黑客所做的不是恶意破坏，他们是一群纵横于网络上的技术人员，热衷于科技探索、计算机科学研究。在黑客圈中，

hacker 一词无疑是带有正面意义的，例如 system hacker 熟悉操作系统的设计与维护；password hacker 精于找出使用者的密码。一些黑客攻击网站仅是炫耀其所掌握的技术，如图 5-2 所示，一个名为 rEmOtEr 的黑客成功地攻击了微软英国网站，并将网页替换成挥舞着沙特国旗的少年的图片。但是到了今天，“黑客”一词已被用于泛指利用系统安全漏洞对网络进行攻击破坏或窃取资料的人。对这些人的正确英文叫法是 Cracker，有人翻译成“骇客”。

图 5-2　被攻击的微软英国网站

2. 黑客如何入侵他人的计算机系统

黑客的入侵行为主要是对系统资源的非授权使用，常见的入侵手段有账号攻击、网络监听、木马入侵、漏洞入侵。

（1）账号攻击。有的计算机系统没有为登录账号设置口令，这会进入门户大开的危险境地。还有一些系统开放了 FTP 和 Guest 等缺省账户，却没设置口令，这会被黑客轻易进入，甚至弱口令也会被黑客破解。

（2）网络监听。网络监听是局域网中的一种黑客技术，在这种模式下，主机可以接收到本网段在同一条物理通道上传输的所有信息。此时，如果两台主机进行通信的信息没有加密，只要使用某些网络监听工具，就可以轻而易举地截取包括口令和账号在内的信息资料。虽然该方法获得的信息具有一定的局限性，但监听者往往能够获得其所在局域网的所有用户账号及口令。

（3）木马入侵。什么是木马？木马不属于病毒，病毒是用来对电脑中的各种软硬件进行破坏的程序。而木马是隐藏在电脑中进行特定工作或依照黑客的操作来进行某些工作的程序。它是一个客户端/服务器结构的程序，运行在黑客的电脑上的是客户端，运行在目标电脑上的是服务端。当目标电脑连上互联网后，客户端会发给服务端信息，然后听候黑客指令，执行黑客指令。

①个人电脑被植入木马程序的方式有几种？

- 黑客入侵后植入木马，如利用 NetBIOS 入侵后植入；
- 利用系统或软件（IE、Outlook Express）的漏洞植入；
- 电子邮件附带的木马程序，或 QQ 聊天含木马的链接文件被接收者运行而植入；
- 网站上放一些伪装后的木马程序，被不知情者下载并运行后便可成功植入木马。

②木马程序植入后，黑客可以进行哪些动作？

- 复制各类文件或电子邮件（可能包含商业秘密、个人隐私）、删除文件、查看文件；
- 转向入侵，利用被黑的电脑来进入其他电脑或服务器进行各种黑客行为；
- 监控被入侵的电脑屏幕画面、键盘操作来获取各类密码；
- 远程遥控，操作对方的 Windows 系统、程序、键盘。

预防方法：及时给系统打补丁、不随意打开来历不明的邮件、不随意下载和运行不明软件、打开杀毒软件的实时监控功能等。

（4）漏洞入侵。漏洞是系统中的安全缺陷。漏洞可以导致入侵者获取信息并导致非法访问 Windows、Office、IE、IIS 等产品中都存在漏洞。

黑客可以利用这些漏洞入侵系统，不同的漏洞产生的原因差别很大，黑客可利用专门的工具进行入侵。常见的有 Unicode 漏洞入侵、SQL 注入入侵等。

预防方法：及时升级系统，给系统打补丁。补丁是漏洞的修补程序，一般某种漏洞被发现并公布后，系统厂商会及时修补该程序，发布相应的补丁包修复程序。

5.2 案例 1：杀毒软件的安装与使用

小澜：老师，必须安装杀毒软件吗？

王老师：如果不安装杀毒软件，就等于上战场没有佩带武器装备，你说是否必要？

小澜：那杀毒软件这么多种，该安装哪一种呢？

王老师：根据个人业务的需要可以考虑不同的杀毒软件产品，今天咱们先安装一种比较常见的免费产品吧！

5.2.1 “360 杀毒”软件的安装

“360 杀毒”软件是 360 安全中心出品的一款免费的云安全杀毒软件。360 杀毒具有查杀率高、资源占用少、升级迅速等优点。同时，360 杀毒可以与其他杀毒软件共存，是一个理想杀毒备选方案。360 杀毒是一款一次性通过 VB100 认证的国产杀毒软件。

360 杀毒整合了四大领先防杀引擎，包括国际知名的 BitDefender 病毒查杀、云查杀、主动防御、360QVM 人工智能等四个引擎，不但查杀能力出色，而且能第一时间防御新出现的病毒木马。此外，360 杀毒轻巧快速不卡机，误杀率远远低于其他杀毒软件。

下面给大家具体介绍一下“360 杀毒”软件的安装方法，具体步骤如下。

步骤 1：登录 360 安全中心网站 http：//www.360.cn/即可下载最新版本的 360 杀毒安装程序，如图 5-3 所示。

图 5-3　360 安全中心网站

步骤 2：下载“360 杀毒”安装程序，如图 5-4 所示，可以选择“运行”，在线安装 360 安全卫士，也可以选择“保存”，先下载到本地再运行安装程序。

图 5-4　下载“360 杀毒”

步骤 3：下载完成后，运行下载的安装程序，单击【下一步】。

步骤 4：请阅读许可协议，并单击【我接受】，然后单击【下一步】，如果单击【取消】将退出安装。

步骤 5：可以选择将 360 杀毒安装到哪个目录下，建议按照默认设置即可。也可以单击【浏览】按钮选择安装目录，然后单击【下一步】。

步骤 6：你会看见一个窗口，输入你想在开始菜单显示的程序组名称，然后单击【安装】，安装程序会开始复制文件。

步骤 7：文件复制完成后，会显示安装完成窗口，单击【完成】，360 杀毒就已经成功地安装到计算机上了。安装完成后，可以看到桌面上出现“360 杀毒”软件图标，如图 5-5 所示。每次开机，“360 杀毒”软件将自动启动运行。

图 5-5　“360 杀毒”软件图标

360 杀毒具有以下独有功能：

(1) 快速扫描：在很短的时间内把用户所有的信息都进行一次检查。

（2）实时防护：分基本防护、中度防护、严格防护。通过这三个等级的保护，足以抵御外界侵害。

（3）产品升级：免费升级到最新的版本，以及时补充病毒库的数据。

5.2.2　启动杀毒扫描程序

360 杀毒具有“智巧模式”和“专业模式”双模式切换功能，如图 5-6、图 5-7 所示。其中，默认开启的“智巧模式”对系统资源影响极低，适合游戏玩家以及对电脑速度特别敏感的用户；“专业模式”则可以由用户对杀毒引擎和防护选项进行个性化设置。

图 5-6　360 杀毒智巧模式

图 5-7　360 杀毒专业模式

在“专业模式”下单击【快速扫描】按钮，即进入病毒查杀状态，快速扫描系统盘区、内存、注册表、文件系统、局域网共享文件夹等病毒敏感区域，如图 5-8 所示。

图 5-8　360 杀毒正在扫描病毒

扫描完毕，360 杀毒对感染型病毒会自动清除，清除失败时会删除或交由用户处理。

5.2.3　开启实时防护功能

选择“专业模式”主界面的“实时防护”选项卡，进入“实时防护”界面，如图 5-9 所示。

图 5-9　“实时防护”功能界面

实时防护必须开启才能真正保护电脑，默认为开启状态。单击“专业模式”界面右上角的【设置】按钮，可以打开设置功能面板，如图 5-10 所示。拖动“防护级别设置”的滑块设置保护电脑的级别，级别越高，越能保护电脑，但对系统的速度有一定的影响，如果电脑配置较高，可以选择“严格防护”级别，系统默认是“中度防护”级别。

图 5-10　实时防护设置

实时防护能够对以下 7 种对象进行监控：

（1）文件系统防护：通过实时监控硬盘的读写，实时、主动、准确、快速、极低系统资源占用地防护文件系统；

（2）注册表防护：防止恶意威胁跟随 Windows 自动启动，防护恶意篡改浏览器设置的威胁；

（3）网络防护：实时检测网络连接；

（4）进程防护：实时检测进程，自动防护威胁；

（5）内存防护：通过实时监控剪贴板的改变，实时防护内存系统；

（6）系统防护：当插入 U 盘/光盘时，防护自动运行型威胁，当有新的 Windows 服务/驱动添加时，自动防护可能存在的威胁；

（7）启发式防御：在没有病毒样本的情况下，对病毒进行全面而有效的全面防护，防御未知威胁。

5.2.4　产品升级

杀毒软件需要经常进行升级才能查杀最新的病毒和各种恶意程序。如果升级不及时，杀毒软件将无法查杀最新病毒、抵御最新的威胁。

360 杀毒的病毒库是在线自动更新的，我们可以不用理会，也可以单击主界面的【产品升级】，然后单击【检查更新】进行病毒库升级，如图 5-11 所示。

图 5-11　360 杀毒产品升级

5.3　案例 2：防火墙的安装与使用

小澜：安装防火墙有什么好处？

王老师：安装防火墙的好处在于一旦系统要执行程序，防火墙会提示你有文件注入注册

表或者要连接互联网，你可以手动选择是否执行操作，不熟悉的操作，你拒绝执行后，病毒和木马就无法感染系统。

小澜：噢，防火墙这么厉害，那我们赶快安装吧！

5.3.1　安装 360 安全卫士

360 安全卫士拥有查杀木马、清理插件、修复漏洞、电脑体检等多种功能，并独创了“木马防火墙”功能，依靠抢先侦测和云端鉴别，可全面、智能地拦截各类木马，保护用户的账号、隐私等重要信息。目前木马威胁之大已远超病毒，360 安全卫士运用云安全技术，在拦截和查杀木马的效果、速度以及专业性上表现出色，能有效防止个人数据和隐私被木马窃取。

360 安全卫士的安装步骤如下：

步骤 1：登录 360 安全中心网站 http：//www.360.cn/即可下载最新版本的 360 安全卫士安装程序，如图 5-12 所示。

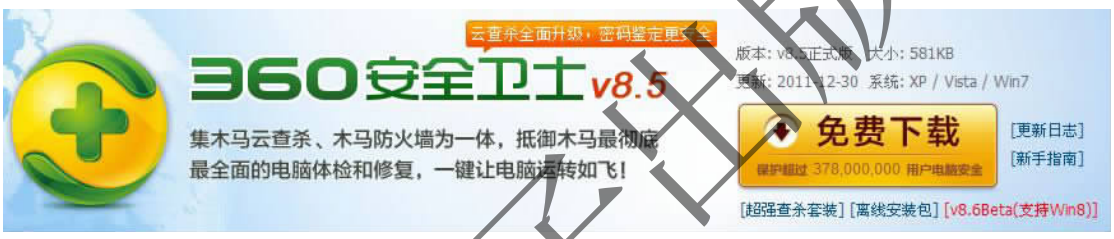

图 5-12　360 安全中心网站

步骤 2：下载“360 安全卫士”安装程序，如图 5-13 所示，可以选择“运行”，在线安装 360 安全卫士，也可以选择“保存”，先下载到本地再运行安装程序。

图 5-13　下载 360 安全卫士

步骤 3：下载完成后，运行下载的安装程序，单击【下一步】。

步骤 4：请阅读许可协议，并单击【我接受】，然后单击下一步，如果单击【取消】将退出安装。

步骤 5：可以选择将 360 安全卫士安装到哪个目录下，建议按照默认设置即可；也可以单击【浏览】按钮选择安装目录，然后单击【下一步】。

步骤 6：你会看见一个窗口，输入你想在开始菜单显示的程序组名称，然后单击【安装】，安装程序会开始复制文件。

步骤 7：文件复制完成后，会显示安装完成窗口。请单击【完成】，360 安全卫士就已经成功地安装到计算机上了。安装完成后，可以看到桌面上出现 360 安全卫士的软件图标，如图 5-14 所示。每次开机，360 安全卫士自动启动运行。

图 5-14　360 安全卫士软件图标

小提示：在程序访问网络或者程序安装写入注册表时，防火墙就会询问你这个程序的安全性，如果是熟悉的程序，可以勾选“一直允许”的选项；如果是不熟悉的程序，尽管杀毒软件没有报错，也不应该勾选“一直允许”或勾选“相同操作一直允许”的选项。对于那些突发性的操作，你不想打开但也没确定要一直禁止可以多选两次禁止，虽然麻烦点，但安全得以保障。有些人对于每次打开程序都会触发防火墙的询问操作，不堪其扰，干脆勾选了“允许所有程序访问网络”，这就埋下了隐患，被恶意插件、木马、病毒成功袭击在所难免。

5.3.2　无线防蹭网

1. 什么是蹭网

“蹭网”主要是指在私人家庭无线网络未加密的情况下，未经主人同意，主动盗用他人无线带宽的一种行为。通过网上热销的无线“蹭网卡”设备（图 5-15），甚至可以暴力破解私人无线路由器密码，强行使用他人无线网络。

2. 被蹭网会有哪些后果

很多人可能会认为，蹭网不就是自己家的无线网络被别人用一下吗？千万不要轻视被蹭网的危害。一旦你的私人网络被不怀好意的人盯上，就要承受以下两大风险：

图 5-15　无线“蹭网卡”

（1）网速被拖慢。由于上网带宽是固定的（例如 2M 带宽），被蹭网后必然会分流一部分带宽，如果蹭网的设备进行文件下载、观看在线视频等操作，自己的网速可能会变得很慢。

（2）面临安全隐私危机。蹭网成功后，蹭网的电脑就成为局域网中的网上邻居，若他们再使用一些黑客工具，就很容易直接入侵到本机，从而可轻松盗取你上网中的所有私人信息和数据，恶劣后果可想而知。

3. 如何检测和防范“无线小偷”

下载安装 360 安全卫士最新版本，在主窗口右侧找到并打开“流量防火墙”，选择【防蹭网】选项卡，直接单击【立即启用】按钮，它会自动检测所有无线连接到路由器或是无线宽带猫中的设备。如果列表中出现了“未知设备”，就需要提防了；如果该设备不是自己的电脑、手机，那极有可能就是蹭网的“小偷”，如图 5-16 所示。

图 5-16　“防蹭网”监测到疑似蹭网设备

如果确定被蹭网，也不用过度担心，只要单击【修改密码】按钮，360 流量防火墙会给出详细的修改密码方法，如图 5-17 所示。

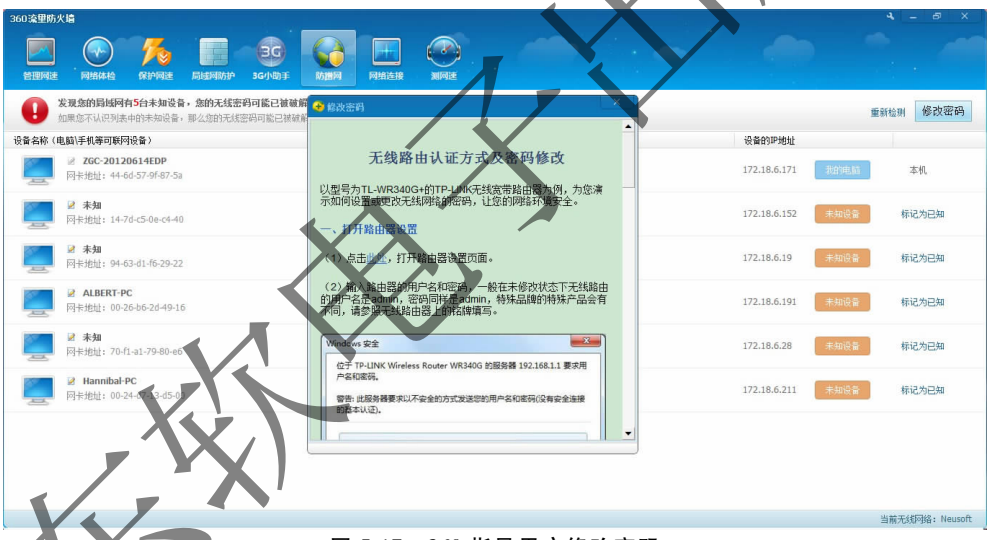

图 5-17　360 指导用户修改密码

据了解，大部分无线设备的设置页面默认密码都是“admin”，但也有部分品牌产品的账号及密码是其他字符，可以参考设备说明书或是直接以设备品牌及型号进行搜索。

小提示：使用无线路由器或是无线宽带猫上网的情况下，一定要为无线信号加密，而且尽量设置复杂的密码，防止别人破解。此外，配合 360 流量防火墙的防蹭网功能，实时监控蹭网行为，不仅可以保护自己的网速，还可以避免黑客攻击等问题。

5.3.3　系统防黑加固

虽然我们已经安装了杀毒软件，但如果电脑存在容易被黑客利用的“软肋”，就会出现经常中毒、电脑被黑客遥控等情况。针对黑客常用的一些攻击手段，360 安全卫士特别推出了

“系统防黑加固”功能，可以阻断黑客入侵通道，提升电脑的“防黑”能力。

360“系统防黑加固”使用方法非常简单：打开360安全卫士的【功能大全】→【电脑优化】，可立即找到“系统防黑加固”的图标，360安全卫士8.5版“系统防黑加固”图标位置如图5-18所示。初次使用需要几秒的安装过程，之后点一下就能立刻使用。

图5-18　“系统防黑加固”图标

打开“系统防黑加固”的操作界面，从中可以看到系统检测项目的当前状况和加固建议。该功能对检测项目的当前状况进行评分和检测，评出当前的电脑防御黑客能力。对于薄弱项目，即容易被黑客攻陷的项目，在界面的右面直接单击便可针对每一项做加固处理，或者直接单击右下角的【立即处理】按钮即可，如图5-19所示。对普通电脑来说，一般在一分钟内就能完成防黑加固的完整操作。

图5-19　360“系统防黑加固”操作界面

“系统防黑加固”继承了 360 安全产品一贯简单、方便的设计风格。对于当前的系统防范黑客能力，系统防黑加固按照“弱、中、强”的评定标准，有红色警示、蓝色提醒和绿色安全的三色设计标识。看盾牌右边的介绍就能了解当前的系统状况，如图 5-20 所示。

图 5-20　“系统防黑加固”对电脑防御黑客入侵能力的评定

此外，360 安全卫士还有 QVM 人工智能引擎、隔离沙箱等强劲功能，并在云查杀、系统修复等方面做了更新和升级，让用户获得更佳的安全防护。

说明：除了 360 安全产品之外，还有很多款流行的杀毒软件，如瑞星、趋势、卡巴斯基、MCAFEE、SYMANTEC、江民科技、PANDA、金山等。

5.4　预防互联网诈骗

随着网络功能越来越强大，因上网发生的诈骗案件呈上升态势。在学习网络安全知识的同时，也要加强防范意识，提高警惕，识别网络骗子的伎俩，保护自身财产的安全。

1. 网络诈骗有哪些常见的手段

目前，网络诈骗的常见手段有以下 5 种。

(1) 钓鱼网站。常见的“钓鱼”手段是用电子邮件做“鱼饵”。电子邮件会看起来像来自一家合法公司，它试图诱惑用户把账号和相关密码给他们。电子邮件可能解释说，公司记录需要更新，或者正在修改一个安全程序，要求用户确认账户，以便继续使用；或者在电子邮件中包含一个表格，供收件人填写自己的姓名、账号、密码或者 PIN 号。

然而，当用户查看 HTML（电子邮件内的程序代码）时，就可以看到网站地址是伪造的，点击链接实际上会把你带到另外一个位置。非法网站只是暂时开放，设计得跟真银行网站一模一样，从而诱惑你输入登录信息和密码。一旦他们获得信息，就会试图从用户的账户中汇钱出去，或者收取费用。

“钓鱼”式诈骗方法可以直接概况为以下 4 个方面：

- 群发邮件“善意”提醒，诱使网民上网操作；
- 境外注册域名，逃避网络监管；
- 高仿真网站制作，欺骗网民透露账号密码；

- 连贯转账操作，迅速转移网银款项。

专家提醒：在网络上查找信息时，应该特别小心由不规范的字母数字组成的 CN 类网址，最好禁止浏览器运行 JavaScript 和 ActiveX 代码，不要登录一些不太了解的网站。

（2）电子商务。网上购物是目前十分流行的消费方式，其中也隐藏着不法分子的诈骗陷阱。骗子通常在知名电子商务网站发布虚假信息，以“超低价”吸引消费者，而后在交易过程中以“免税”“走私货”“慈善义卖”等名义，要求消费者预先支付货款到对方的账户。一旦受骗者把款付给对方，就再也找不到骗子的踪影。

骗子还可能在网上交谈的过程中提供虚假链接，以付款等名义通过网络发送网址链接给对方。消费者以为是正常的银行网页，从而输入自己的网银信息，结果被骗子诈取了账号和密码。

（3）木马。不法分子在发送的电子邮件或网站中，隐藏“木马”程序，感染计算机。当进行网上交易时，“木马”程序即以键盘记录方式获取账号和密码。所以，建议大家在网上进行比较隐私的操作，如输入密码等应使用“软键盘”功能。

（4）口令。不法分子利用部分用户贪图方便、在网上银行设置“弱口令”的漏洞，从网上搜寻到银行储户卡卡号，进而登录该银行网上银行网站，破解“弱口令”。

（5）QQ。不法分子首先与受害者亲朋好友进行 QQ 视频联系，截取对方的视频，发送含有木马的文件或者电子邮件窃取对方密码，进而伪装成受害者的亲朋好友在 QQ 上与受害者进行聊天，以“出事”“急用”“合伙做生意”为借口骗取受害者钱财。

2. 应该采取哪些防范措施

针对这些网络诈骗的常用手段，建议大家加强法律意识，了解法律法规，不让不法分子有机可乘。为了安全享受网络带来的便捷生活，应该牢记以下行为守则：

（1）杀毒软件不可少，个人防火墙不可替代；

（2）不随意浏览黑客网站、色情网站，警惕“钓鱼网站”；

（3）设置密码并使密码设置尽可能复杂；

（4）只在必要时共享文件夹；

（5）不下载来路不明的软件及程序，不打开来历不明的邮件及附件；

（6）定期备份重要数据；

（7）不要相信“一夜暴富”“超低价”等诱惑性网络宣传。

5.5 下一代网络安全——云安全

“云安全”是“云计算”技术的重要分支，已经在反病毒领域中获得了广泛应用。云安全通过网络的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，推送到服务端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。整个互联网变成了一个超级大的杀毒软件，这就是云安全计划的宏伟目标，如图 5-21 所示。

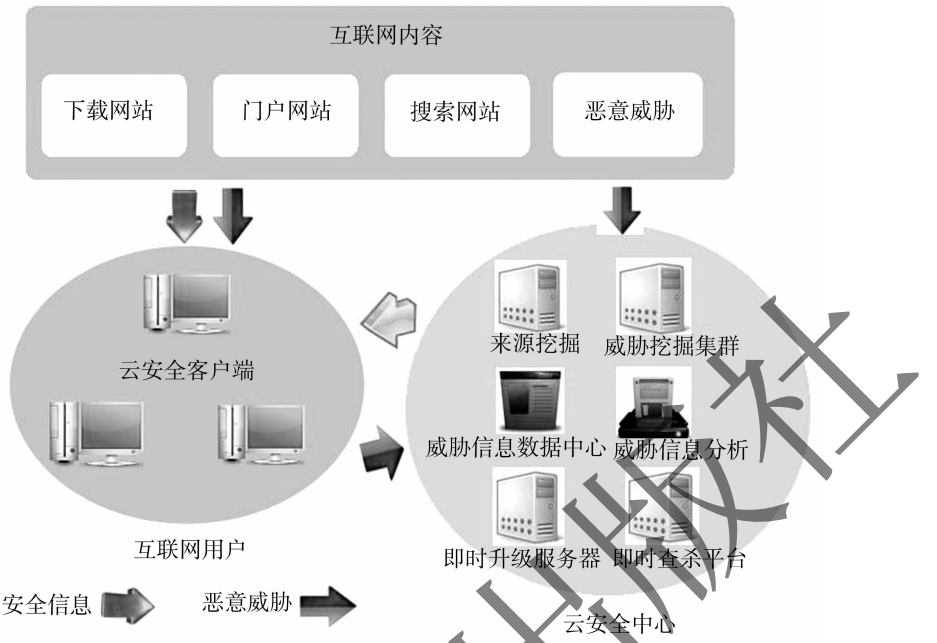

图 5-21　云安全示意图

未来杀毒软件将无法有效地处理日益增多的恶意程序，来自互联网的主要威胁正在由电脑病毒转向恶意程序及木马，在这样的情况下，特征库判别法显然已经过时。应用云安全技术后，识别和查杀病毒不再仅仅依靠本地硬盘中的病毒库，而是依靠庞大的网络服务，实时进行采集、分析以及处理。整个互联网就是一个巨大的“杀毒软件”，参与者越多，每个参与者就越安全，整个互联网也会更安全。

5.6　应用练习

一、填空题

1. 信息安全的目标是保证信息的机密性、_____和可用性。

2. 计算机病毒（Computer Virus）是影响计算机使用并且能够_____的一组计算机指令或者程序代码。

3. 计算机病毒具有寄生性、传染性、潜伏性、隐蔽性、_____和_____的特征。

4. 计算机病毒之所以称为病毒是因为其具有_____的本质特征。

5. 计算机病毒的传播途径包括通过优盘、软盘、硬盘、光盘以及_____等。

6. 引导区病毒隐藏在硬盘或软盘的_____。

二、判断题

1. 有些计算机病毒可以破坏硬件。（　　）

2. 计算机病毒是一种微生物感染的结果。（　　）

3. 杀毒软件可以完全杀掉所有的病毒。（　　）

4. 网络安全不仅需要保护主机中的软件，也需要保护硬件。（ ）

5. 只要安装了杀毒软件和防火墙，就能防止网络诈骗。（ ）

6. 是否具有寄生性是判别一个程序是否为计算机病毒的最重要条件。（ ）

7. 只要读取感染有引导区病毒的磁盘或者光盘上的文件，就会被病毒感染。（ ）

三、简答题

1. 信息安全的目标是什么？

2. 什么是计算机病毒？简述计算机病毒的特征。

3. 列举 5 种类型的计算机病毒。

4. 什么是网络黑客？黑客攻击有哪些常用方法？

5. 在日常计算机系统使用过程中，如何即时监控和防范计算机病毒？

四、上机操作题

1. 安装杀毒软件，查看病毒库是否需要更新，扫描计算机系统病毒。

2. 安装防火墙，观察它对其他程序运行的拦截情况。

3. 到百度上搜索计算机病毒与黑客及其防治等相关知识，并整理成 Word 文档，以附件的形式发送到任课教师的邮箱里。

4. 查询当前流行的 3 款杀毒软件。

5. 试使用 360 安全卫士清理插件，给浏览器和系统瘦身。

第 2 篇

Office 办公软件篇