****

**西安医学院网络安全**

**知识宣传手册**

**党委宣传部 信息技术处 团委**

**2014.11.24**

**西安医学院网络安全**

**知识宣传手册**

****

**党委宣传部**

**信息技术处**

**团委**

**2014.11.24**

**目 录**

一、计算机网络安全 …………………… 1

二、网络的不安全因素……………………4

三、计算机病毒 …………………………7

四、如何使网上信息更安全?……………13

五、个人电脑使用规范 …………………19

附录： ……………………………………22

**计算机网络安全基础知识**

目前中国网民已达6.32亿，全球每天约20亿网民在使用网络。

大事件：2014年2月27日中央网络安全和信息化领导小组宣告成立，习近平主席担任组长。11月19日至21日，第一届世界互联网大会在中国浙江乌镇召开，以“互联互通、共享共治”为主题。11月24日至30日，定为首届国家网络安全宣传周，于24日在北京中华世纪坛正式启动，旨在宣传“共建网络安全，共享网络文明”。

一、**计算机网络安全**

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统可以连续可靠正常地运行，网络服务不被中断。

网络安全，是计算机信息系统安全的一个重要方面。如同打开了的潘多拉魔盒，计算机系统的互联，在大大扩展信息资源的共享空间的同时，也将其本身暴露在更多恶意攻击之下。如何保证网络信息存储、处理的安全和信息传输的安全的问题，就是我们所谓的计算机网络安全。信息安全是指防止信息财产被故意的或偶然的非法授权泄露、更改、破坏或使信息被非法系统辩识、控制；确保信息的保密性、完整性、可用性、可控性。信息安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密和鉴别七个方面。设计一个安全网络系统，必须做到既能有效地防止对网络系统的各种各样的攻击，保证系统的安全，同时又要有较高的成本效益，操作的简易性，以及对用户的透明性和界面的友好性。

 1、主要特性

　　网络安全应具有以下五个方面的特征：

　　保密性：信息不泄露给非授权用户、实体或过程，或供其利用的特性。

　　完整性：数据未经授权不能进行改变的特性。即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

　　可用性：可被授权实体访问并按需求使用的特性。即当需要时能否存取所需的信息。例如网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击；

　　可控性：对信息的传播及内容具有控制能力。

　　可审查性：出现的安全问题时提供依据与手段

　　从网络运行和管理者角度说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，对国家造成巨大损失。从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

　　随着计算机技术的迅速发展，在计算机上处理的业务也由基于单机的数学运算、文件处理，基于简单连接的内部网络的内部业务处理、办公自动化等发展到基于复杂的内部网（Intranet）、企业外部网（Extranet）、全球互联网（Internet）的企业级计算机处理系统和世界范围内的信息共享和业务处理。在系统处理能力提高的同时，系统的连接能力也在不断的提高。但在连接能力信息、流通能力提高的同时，基于网络连接的安全问题也日益突出，整体的网络安全主要表现在以下几个方面：网络的物理安全、网络拓扑结构安全、网络系统安全、应用系统安全和网络管理的安全等。

　　因此计算机安全问题，应该像每家每户的防火防盗问题一样，做到防范于未然。甚至不会想到你自己也会成为目标的时候，威胁就已经出现了，一旦发生，常常措手不及，造成极大的损失。

2、网络安全类型

　　运行系统安全，即保证信息处理和传输系统的安全。它侧重于保证系统正常运行，避免因为系统的崩溃和损坏而对系统存贮、处理和传输的信息造成破坏和损失，避免由于电磁泄漏，产生信息泄露，干扰他人，受他人干扰。

　　网络上系统信息的安全。包括用户口令鉴别，用户存取权限控制，数据存取权限、方式控制，安全审计，安全问题跟踪，计算机病毒防治，数据加密。

　　网络上信息传播安全，即信息传播后果的安全。包括信息过滤等。它侧重于防止和控制非法、有害的信息进行传播后的后果。避免公用网络上大量自由传输的信息失控。

　　网络上信息内容的安全。它侧重于保护信息的保密性、真实性和完整性。避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为。本质上是保护用户的利益和隐私。

3、网络安全特征

　　网络安全应具有以下四个方面的特征：

　　保密性：信息不泄露给非授权用户、实体或过程，或供其利用的特性。

　　完整性：数据未经授权不能进行改变的特性。即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

　　可用性：可被授权实体访问并按需求使用的特性。即当需要时能否存取所需的信息。例如网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击；

　　可控性：对信息的传播及内容具有控制能力。

**二、网络的不安全因素**

  计算机网络本身不能向用户提供安全保密功能，在网络上传输的信息、入网的计算机及其所存储的信息会被窃取、篡改和破坏，网络也会遭到攻击，其硬件、软件、线路、文件系统和信息发送或接收的确认等会被破坏，无法正常工作，甚至瘫痪；其不安全因素主要表现在5个方面：

（一）网络通信隐患。网络通信的核心是网络协议。创建这些协议的主要目的是为了实现网络互联和用户之间的可靠的通信。但在实际网络通信中存在三大安全隐患：一是结构上的缺陷。协议创建初期，对网络通信安全保密问题考虑不足，这些协议结构上或多或少地存在信息安全保密的隐患。二是漏洞。包括无意漏洞和故意留下的“后门”。前者通常是程序员编程过程中的失误造成的。后者是指协议开发者为了调试方便，在协议中留下的“后门”。协议“后门”是一种非常严重的安全隐患，通过“后门”，可绕开正常的监控防护，直接进入系统。三是配臵上的隐患。主要是不当的网络结构和配臵造成信息传输故障等。 （二）计算机病毒。计算机病毒会给计算机系统造成危害：网上传输或存在计算机系统中的信息被篡改、假信息被传播、信息完整性、可靠性和可用性遭到破坏。目前看，病毒传播的主要途径有：一是利用软盘和光盘传播；二是通过软件传播；三是通过因特网，如电子邮件传播；四是靠计算机硬件（带病毒的芯片）或通过镶嵌在计算机硬件上的无线接收器件等途径传播。 （三）黑客入侵。“黑客”的主要含义是非法入侵者。黑客攻击网络的方法主要有：IP地址欺骗、发送邮件攻击、网络文件系统攻击、网络信息服务攻击、扫描器攻击、口令攻击、嗅探攻击、病毒和破坏性攻击等。黑客通过寻找并利用网络系统的脆弱性和软件的漏洞，刺探窃取计算机口令、身份标识码或绕过计算机安全控制机制，非法进入计算机网络或数据库系统，窃取信息。现在全球每20秒钟就有一起黑客事件发生。按黑客的动机和造成的危害，目前黑客分为恶作剧、盗窃诈骗、蓄意破坏、控制占有、窃取情报等类型。其中，西方一些国家的情报部门秘密招聘黑客“高手”，编制专门的黑客程序，用于窃取别国（集团）因特网或内部网上的涉密信息和敏感信息。对此，尤须引起我们高度注意。 （四）软件隐患。许多软件在设计时，为了方便用户的使用、开发和资源共享，总是留有许多“窗口”，加上在设计时不可避免地存在许多不完善或未发现的漏洞，用户在使用过程中，如果缺乏必要的安全鉴别和防护措施，就会使攻击者利用上述漏洞侵入信息系统破坏和窃取信息。目前，不少单位使用的软件是国外产品，这给信息安全保密带来很大困难。 （五）设备隐患。主要指计算机信息系统中的硬件设备中存在的漏洞和缺陷：1、电磁泄漏发射。电磁泄漏发射是指信息系统的设备在工作时向外辐射电磁波的现象。计算机的电磁辐射主要有两种途径：一是被处理的信息会通过计算机内部产生的电磁波向空中发射，称为辐射发射。二是这种含有信息的电磁波也可以经电源线、信号线、地线等异体传送和辐射出去，称为传导发射。这些电磁辐射包含数据信息和视频信息等内容。这些辐射出去的电磁波，任何人都可借助仪器设备在一定范围内收到它，尤其是利用高灵敏度的仪器可稳定清晰地获取计算机正在处理的信息。日本的一项试验结果表明：未加屏蔽的计算机启动后，用普通电脑可以在80米内接收其显示器上的内容。据报道，国际高灵敏度专用接收设备可在1公里外接收并还原计算机的辐射信息。早在20世纪80年代，国外情报部门就把通过接收计算机电磁辐射信息作为窃密的重要手段之一。2、磁介质的剩磁效应。存储介质中的信息被删除后，有时仍会留下可读痕迹；即使已多次格式化的磁介质（盘、带）仍会有剩磁，这些残留信息可通过“超导量子干涉器件”还原出来。在大多数的操作系统中，删除文件只是删除文件名，而原文件还原封不动地保留在存储介质中，从而留下泄密隐患。3、预臵陷阱。即人为地在计算机信息系统中预设一些陷阱，干扰和破坏计算机信息系统的正常运行。预臵的陷阱一般分为硬件陷阱和软件陷阱两种。其中，硬件陷阱主要是“芯片捣鬼”，即蓄意更改集成电路芯片的内容设计和使用规程，以达到破坏计算机信息系统的目的。计算机信息系统中一个关键芯片的小小故障，就足以导致计算机以至整个信息网络停止运行。 我国不少计算机硬件、软件，以及路由器、交换机等网络设备都依赖进口，给网络的安全保密留下了隐患。发达国家利用对计算机核心技术的垄断，迫使别国依赖其现成技术，以达到控制别国计算机信息系统的目的。美国基本上掌握了网络地址资源的控制权。美国国内网事实上已成为全球因特网的骨干网。

**三、计算机病毒**

　　计算机病毒是具有自我复制能力的并具有破坏性的计算机程序（下简称"病毒"），它会影响和破坏正常程序的执行和数据的安全。它不仅侵入到所运行的计算机系统，而且还能不断地把自己的复制品传播到 其他的程序中，以此达到其破坏作用。病毒一般都具有很强的隐蔽性，所以不易被发现。计算机病毒发展到今天，已成为计算机世界里的一种恶性顽疾，是研究计算机安全保密防范时必须经常考虑和面对的一个主要问题。

　　1、病毒的特点

　　计算机病毒与生物病毒几乎具有完全相同的特征，如生物病毒的传染性、流行性、繁殖性、表现性、针对性等特征，计算机病毒都具备，所不同的是：计算机病毒不是微生物，而是一段可执行的计算机程序。

　　2、病毒的传染途径

　　传染性是计算机病毒最显著的特征，威胁也最大。如没有传染性，即使病毒的破坏性再大，也只能破坏一台计算机，而不能威胁其它计算机。 计算机病毒从一个计算机系统向其它计算机系统进行传染的主要途径是联网线路、磁盘和光盘。在单机环境下，病毒主要是通过互相交换的带毒磁盘或光盘传染的。硬盘虽然是固定式存储介质，但是硬盘是病毒的重要滋生地，许多病毒都寄生在硬盘上，一旦用寄生有病毒的硬盘启动计算机，并且对某些软盘和光盘进行读写操作，那么，病毒就会传染到软盘和光盘上，并通过这张软盘和光盘扩散开来。 对于网络来说，带病毒的服务器则是病毒的集散点，它一般通过可执行文件的传递而传播。在联网条件下，计算机病毒扩散的途径，增加了许多，它可以通过访问、文件下载、电子邮件等各种途径来传播病毒。

　 3、病毒的种类

　　在以前，人们用汇编语言来编写病毒以减小它的尺寸，到了今天很多病毒是用VB、JAVA和ActiveX 来编写的。病毒的种类有如下几种：（1）文件病毒。此类病毒会将它自己的代码附在可执行文件（EXE、COM、BAT…）上。典型的代表是"黑色星期五"。（2）引导型病毒。此类病毒在软硬磁盘的引导扇区、主引导记录或分区表中插入病毒指令。典型的代表是大麻病毒、磁盘杀手等。（3）混合型病毒。是前两种病毒的混种，并通过可执行文件在网上迅速传播。（4）宏病毒。1995年8月，Windows95发表，并迅速成为主流操作系统，原先在DOS系统下猖獗一时的各种病毒，由于不适应新系统，而渐失活力。代之而起的新型病毒，一类也是攻击可执行文件，如臭名昭著的CIH病毒，另一类就是宏病毒，它主要感染日常广泛使用的字表处理软件（如Word等）所定义的宏，从而迅速漫延。美丽莎就是这方面的"突出"代表。（5）网络病毒。网络病毒通过网站和电子邮件传播，它们隐藏在Java和ActiveX程序里面，如果用户下载了有这种病毒的程序，它们便立即开始破坏活动。由于网络传播迅速，这类病毒造成的危害更大。最近，活动十分猖獗，破坏力很大的"爱"病毒就属于这一类。

4、计算机感染病毒的主要症状

计算机感染了病毒后症状很多，其中以下25种最为常见

(1)信息系统运行速度明显减慢；

(2)平时运行正常的电脑突然经常性无缘无故地死机；

(3)文件长度发生变化；

(4)磁盘空间迅速减少；

(5)系统无法正常启动；

(6)丢失文件或文件损坏；

(7)屏幕上出现异常显示；

(8)电脑的喇叭出现异常声响；

(9)网络驱动器卷或共享目录无法调用；

(10)系统不识别硬盘；

(11)对存储系统异常访问；

(12)键盘输入异常；

(13)文件的日期、时间、属性等发生变化；

(14)文件无法正确读取、复制或打开；

(15)命令执行出现错误；

(16)虚假报警；

(17)换当前盘，有些病毒会将当前盘切换到C盘；

(18)时钟倒转，有些病毒会命令系统时间倒转，逆向计时；

(19)以前能正常运行的软件经常发生内存不足的错误甚至死机;

(20)系统异常重新启动；

(21)打印和通讯发生异常；

(22)异常要求用户输人密码；

(23)WORD或EXCEL提示执行“宏”；

(24)不应驻留内存的程序驻留内存；

(25)自动链接到一些陌生的网站。

5、病毒的危害

计算机病毒对计算机的危害形式主要有以下几种：（1） 减少存储器的可用空间；（2）使用无效的指令串与正常运行程序争夺CPU时间；（3）破坏存储器中的数据信息；（4）破坏相连网络中的各项资源；（5）构成系统死循环；（6）肆意更改、破坏各类文件和数据；（7）破坏系统I/O功能；（8）彻底毁灭软件系统。（9）用借读数据更改主板上可擦写型BIOS芯片，造成系统崩溃或主板损坏；（10）造成磁头在硬盘某些点上死读，从而破坏硬盘。计算机病毒通过这几种危害形式，给计算机造成的灾害是巨大的。这方面的事例数不胜数。

　 6、病毒的防治

　　由于病毒对微机资源造成严重的破坏，所以必须从管理和技术两方面采取有效措施，以防止病毒的入侵。在日常工作中，防止病毒感染的主要措施有：（1）首先，也是最重要的一点是选择并安装一个反病毒软件，由于新的病毒不断出现（平均每天13个），没有一台计算机能在如今高度共享、高度网络化的世界里在不装反病毒软件的情况下躲过病毒的攻击。定期对所用微机进行检查，包括所使用的软盘和硬盘，以便及时发现病毒，防患于未然。（2）减少服务器中用户写的权力。把服务器中写的权力控制在尽量少的人手中，能避免不必要的麻烦和损失。（3）防范来历不明软盘和盗版光盘。应对来历不明的软盘和盗版光盘保持高度警惕，在把它塞进驱动器前要考虑清楚，如果你不得不这样做，请先用反病毒软件对软盘进行检查，扫描盘中的每一个文件（不仅仅是可执行文件），包括压缩文件。同样，在你给别人软盘时，及时对软盘写保护，这样别人机器里的病毒就不会传到你的软盘里。（4）在阅读电子邮件的附件前进行扫描。有些邮件接收软件在用户打开一封邮件后会自动打开附件，请千万关闭这个功能。（5）下载的时候要小心。下载文件是病毒来源之一。（6）把文件存为RTF或ASCII格式。如果你想在网络服务器上与别人共享一些数据，但又不愿了解更多的病毒知识，那你最好把文件存为RTF或ASCII格式，因为这两种文件格式都能避免宏病毒的攻击。（7）合理设置硬盘分区，预留补救措施。一般C盘宜采用FAT 32格式，容量应大于1G。这时C盘万一被病毒感染，也能用KV300恢复98%以上数据，而采用FAT 16格式，C盘容量小于2G，也只能恢复5%的数据。（8）用Ghost（克隆）软件、备份硬盘，快速恢复系统。（9）及时升级杀毒软件、提高防范能力。（10）重要数据和重要文件一定要做备份。

防范计算机病毒常用的技术手段主要有：操作系统和防病毒软件的及时升级、重要信息的及时备份以及重要信息遭破坏后的恢复。

个人防范计算机病毒的主要要求：

(1)参加安全培训和讲座，提高防范意识和技能；

(2)遵守各单位结合自己情况建立的计算机病毒防治管理制度；

(3)杀毒软件由单位统一安装，不要同时安装多个后自行再安装；

(4)按要求及时升级杀毒软件、操作系统和应用软件补丁；

(5)按要求和操作规范关闭办公电脑上不用的端口，防止各种恶意程序的进入和信息外泄；

(6)在接收电子邮件时，要仔细观察，不打开来历不明的邮件；

(7)未经许可不在电脑中安装其他软件(如游戏等)；

(8)及时做好重要信息的备份工作，使用存储介质时，要确认不带病毒；

(9)确保提供共享的信息资源不带病毒；

发现感染病毒后的操作：

断开与网络的连接(拔掉网线)；

按Ctrl+Alt+Del调出任务管理器，观察并记录其中可疑的进程名；

重新启动计算机,进入系统安全模式(按F8)；

打开防病毒软件，扫描所有磁盘；

运行regedit，删除注册表启动项中的所有可疑键值；HKEY\_LOCAL\_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run(RunOnce,RunServices)
HKEY\_LOCAL\_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run

删除可疑的进程文件。

**四、如何使网上信息更安全？**

　　虽是基础知识，但对经常上网的用户还是不可缺的.

1、不轻易运行不明真相的程序

　　如果你收到一封带有附件的电子邮件，且附件是扩展名为ＥＸＥ一类的文件，这时千万不能贸然运行它，因为这个不明真相的程序，就有可能是一个系统破坏程序。攻击者常把系统破坏程序换一个名字用电子邮件发给你，并带有一些欺骗性主题，骗你说一些：“这是个好东东，你一定要试试”，“帮我测试一下程序”之类的话。你一定要警惕了！对待这些表面上很友好、跟善意的邮件附件，我们应该做的是立即删除这些来历不明的文件。

2、屏蔽小甜饼信息

　　小甜饼就是Cookie，它是Web服务器发送到电脑里的数据文件，它记录了诸如用户名、口令和关于用户兴趣取向的信息。实际上，它使你访问同一站点时感到方便，比如，不用重新输入口令。但Cookies收集到的个人信息可能会被一些喜欢搞“恶作剧”的人利用，它可能造成安全隐患，因此，我们可以在浏览器中做一些必要的设置，要求浏览器在接受Cookie之前提醒您，或者干脆拒绝它们。通常来说，Cookie会在浏览器被关闭时自动从计算机中删除，可是，有许多Cookie会一反常态，始终存储在硬盘中收集用户的相关信息，其实这些Cookie就是被设计成能够驻留在我们的计算机上的。随着时间的推移，Cookie信息可能越来越多，当然我们的心境也因此变得越来越不踏实。为了确保万无一失，对待这些已有的Cookie信息应该从硬盘中立即清除，并在浏览器中调整Cookie设置，让浏览器拒绝接受Cookie信息。屏蔽Cookie的操作步骤为：首先用鼠标单击菜单栏中的“工具”菜单项，并从下拉菜单中选择“Internet选项”；接着在选项设置框中选中“安全”标签，并单击标签中的“自定义级别”按钮；同时在打开的“安全设置”对话框中找到关于Cookie的设置，然后选择“禁用”或“提示”。

3、不同的地方用不同的口令

　　对于经常上网的用户，可能会发现在网上需要设置密码的情况有很多。有很多用户图方便记忆，不论在什么地方，都使用同一个口令，殊不知他们已不知不觉地留下了一个安全隐患。因为攻击者一般在破获到用户的一个密码后，会用这个密码去尝试用户每一个需要甬道口令的地方！想想看，别人用一个口令慢慢地盗用你的帐号上网；再去偷看与冒发你的E-mail；也许还会用你的身份去聊天室损害你的形象；还有.....，想想看那后果该有多严重呀！所以笔者强烈建议各位用户，每个不同的地方用不同的密码，一定不能不同，同时要把各个对应的密码记下来，以备日后查用。另外一点就是我们在设定密码时，不应该使用字典中可以查到的单词，也不要使用个人的生日，最好是字母、符号和数字混用，多用特殊字符，诸如%、&、#、和$,并且在允许的范围内，越长越好，以保证你的密码不易被人猜中。

4、 屏蔽ActiveX控件

　　由于ActiveX控件可以被嵌入到HTML页面中，并下载到浏览器端加以执行，因此会给浏览器端造成一定程度的安全威胁。目前已有证据表明，在客户端的浏览器中，如IE中插入某些ActiveX控件，也将直接对服务器端造成意想不到的安全威胁。同时，一些其他技术，如内嵌于IE的VB Script语言，用这种语言生成的客户端可执行的程序模块，也同 Java小程序一样，有可能给客户端带来安全性能上的漏洞。此外，还有一些新技术，如ASP(Active serv er Pages)技术，由于用户可以为ASP的输出随意增加客户脚本、ActiveX控件和动态HTML，因此在ASP脚本中同样也都存在着一定的安全隐患。所以，用户如果要保证自己在因特网上的信息绝对安全，可以屏蔽掉这些可能对计算机安全构成威胁的ActiveX控件，具体操作步骤为：首先用鼠标单击菜单栏中的“工具”菜单项，并从下拉菜单中选择“Internet选项”；接着在选项设置框中选中“安全”标签，并单击标签中的“自定义级别”按钮；同时在打开的“安全设置”对话框中找到关于ActiveX控件的设置，然后选择“禁用”或“提示”。

5、定期清除缓存、历史记录以及临时文件夹中的内容

　　我们在上网浏览信息时，浏览器会把我们在上网过程中浏览的信息保存在浏览器的相关设置中，这样下次再访问同样信息时可以很快地达到目的地，从而提高了我们的浏览效率。但是浏览器的缓存、历史记录以及临时文件夹中的内容保留了我们太多的上网的记录，这些记录一旦被那些无聊的人得到，他们就有可能从这些记录中寻找到有关个人信息的蛛丝马迹。为了确保个人信息资料的绝对安全，我们应该定期清理缓存、历史记录以及临时文件夹中的内容。清理浏览器缓存并不麻烦，具体的操作方法如下：首先用鼠标单击菜单栏中的“工具”菜单项，并从下拉菜单中选择“Internet选项”；接着在选项设置框中选中“常规”标签，并单击标签中的“删除文件”按钮来删除浏览器中的临时文件夹中的内容；然后在同样的饿对话框中单击“清除历史记录”按钮来删除浏览器中的历史记录和缓存中的内容。

6、在自己的计算机中安装防火墙

　　为自己的局域网或站点提供隔离保护，是目前普遍采用的一种安全有效的方法，这种方法不是只针对Web服务，对其他服务也同样有效。

　　防火墙是一个位于内部网络与Internet之间的计算机或网络设备中的一个功能模块，是按照一定的安全策略建立起来的硬件和软件的有机组成体，其目的是为内部网络或主机提供安全保护，控制谁可以从外部访问内部受保护的对象，谁可以从内部网络访问Internet，以及相互之间以哪种方式进行访问。所以为了保护自己的计算机系统信息，不受外来信息的破坏和威胁，我们可以在自己的计算机系统中安装防火墙软件。

7、突遇莫名其妙的故障时要及时检查系统信息

　　上网过程中，突然觉得计算机工作不对劲时，仿佛感觉有人在遥远的地方遥控你。这时，你必须及时停止手中的工作，立即按Ctrl+Alt+Del复合键来查看一下系统是否运行了什么其他的程序，一旦发现有莫名其妙的程序在运行，你马上停止它，以免对整个计算机系统有更大的威胁。但是并不是所有的程序运行时出现在程序列表中，有些程序例如Back Orifice（一种黑客的后门程序）并不显示在Ctrl+Alt+Del复合键的进程列表中，最好运行“附件”/“系统工具”/“系统信息”，然后双击“软件环境”，选择“正在运行任务”，在任务列表中寻找自己不熟悉的或者自己并没有运行的程序，一旦找到程序后应立即终止它，以防后患。

8、对机密信息实施加密保护

　　对机密信息进行加密存储和传输是传统而有效的方法，这种方法对保护机密信息的安全特别有效，能够防止搭线窃听和黑客入侵，在目前基于Web服务的一些网络安全协议中得到了广泛的应用。

　　在Web服务中的传输加密一般在应用层实现。WWW服务器在发送机密信息时，首先根据接收方的IP地址或其他标识，选取密钥对，信息进行加密运算；浏览器在接收到加密数据后，根据IP包中信息的源地址或其他标识对加密数据进行解密运算，从而得到所需的数据。在目前流行的WWW服务器和浏览器中，如微软公司的IIS服务器和浏览器IE，都可以对信息进行加解密运算，同时也留有接口，用户可以对这些加解密算法进行重载，构造自己的加解模块。此外，传输加解密也可以在IP层实现，对进出的所有信息进行加解密，以保证在网络层的信息安全。

9、加密重要的邮件

由于越来越多的人通过电子邮件进行重要的商务活动和发送机密信息，而且随着互联网的飞速发展，这类应用会更加频繁。因此保证邮件的真实性（即不被他人伪造）和不被其他人截取和偷阅也变得日趋重要。所以，对于包含敏感信息的邮件，最好利用数字标识对你写的邮件进行数字签名后再发送。所谓数字标识是指由独立的授权机构发放的证明你在Internet上身份的证件，是你在因特网上的身份证。这些发证的商业机构将发放给你这个身份证并不断效验其有效性。你首先向这些公司申请数字标识，然后就可以利用这个数字标识对你写的邮件进行数字签名。如果你获得了别人的数字标识那么你还可以跟他发送加密邮件。你通过对发送的邮件进行数字签名可以把你的数字标识发送给他人，这时他们收到的实际上是公用密钥，以后他们就可以通过这个公用密钥对发给你的邮件进行加密，你再使用私人密钥对加密邮件进行解密和阅读。在Outlook Express中可以通过数字签名来证明你的邮件的身份，即让对方确信该邮件是由你的机器发送的，它同时提供邮件加密功能使得你的邮件只有预定的接收者才能接收并阅读它们，但前提是你必须先获得对方的数字标识。数字标识的数字签名部分是你的电子身份卡，数字签名可使收件人确信邮件是您发送的，并且未被伪造或篡改。

**五、个人电脑使用规范**

1、使用计算机应形成良好习惯

(1)保持键盘、鼠标、显示器等常用设备的清洁，防止茶水等液体进入键盘、显示器等外设造成设备短路损毁；

(2)暂时离开时要锁定计算机，或使用计算机屏幕保护程序并设置口令；

(3)妥善管理计算机各种用户名(账号)与口令；

(4)使用软件前，阅读软件说明书，熟悉软件的特性及使用方式；

(5)未经许可不擅自使用他人的办公计算机；

(6)严禁擅自将外网电脑接入内网，接入内网的电脑必须确认没有病毒；

(7)重要文件按规定随时备份；

(8)禁止在计算机上使用来路不明的光盘；

(9)外出或下班时应关闭办公电脑、显示器等终端的电源。

2、正确设置用户名与口令

口令至少六个字符，切忌设置空口令和与用户名(帐号)名相同的口令。

一个好的口令首先要不易被猜出，您的名字、生日、电话号码、password、root、admin、123456，等都不是好的口令。

第二要求口令不易被破解，以现今主流家用计算机的处理能力，破解8位字符纯数字或纯字母组成的口令只需2—10分钟。所以，在能够记住的前提下，好的口令至少应该由大小写字母、数字和其他字符组成，尤其在信息安全危险度较高的场合(比如，24小时开机的计算机，直接连接广域网、城域网的服务器等)。

3、多种方式灵活设置口令

(1)开机口令(又称为CMOS口令)：在计算机主机板BI0S中设定；

(2)登录用户名(帐号)：进入操作系统所需键入的用户名和口令；高权限用户名(帐号)对整个操作系统具有控制权，甚至是整个工作组或域的控制权，是最重要的口令，须正确设置口令，妥善管理口令；

(3)屏保口令：在暂时离开时要使用计算机屏幕保护程序并设置口令；

(4)应用程序口令：大部分信息管理软件都可以设置口令功能，具有口令者才能使用；

(5)常用的文档编辑软件；

(6)电子邮件及各种网络通讯软件等等。

4、上网浏览的注意事项

(1)不要同时打开太多链接窗口；

(2)当某个网站提出要将本网站设置为主页时，要取消操作；

(3)当网页中弹出安装某个插件的对话框时，如果一时不能确认，取消安装；

(4)定期清除历史访问信息、cookies以及Internet临时文件。

(5)严禁在网络上运行任何黑客软件；若工作需要，应在独立的测试环境中试验。

5、使用电子邮件的注意事项

(1)邮件和邮件通讯录都要做好备份；

(2)发送邮件大小不超过邮箱总容量，附件大小应做适当控制，可先行压缩，或分成几个压缩包；

(3)多个文档文件作为附件发送时，最好压缩打包成一个文件发送；

(4)群发邮件时，收件人地址之间用逗号“，”或分号“；”分隔；

(5)邮件客户端程序建议弃用Outlook Express，使用Foxmail，并设置账户口令；

(6)以Web方式收取邮件，在阅读完毕时，一定要退出登录，并关闭网页；

(7)不要打开来历不明、奇怪标题或者非常有诱惑性标题的电子邮件；exe、com、pif、scr、vbs为后缀的附件，或者名字很特别的TXT文件，不要轻易打开；

(8)重要邮件在发送前应做加密处理；禁止将含工作内容的邮件通过互联网上免费邮箱发送；

(9)应该及时清理自己的个人邮箱，删除或转移邮件，以保证邮箱的可用容量；

(10)多个邮箱使用时最好做分类处理。例如，其中一个用作单位内部工作邮箱，另一个用作单位对外联络邮箱；

(11)严禁在邮件内容中透露涉及单位和个人的重要信息内容。如身份证号码、银行帐号、计算机账号及口令等；

(12)禁止任何人发送或有意接收垃圾邮件。

6、注意保护重要数据和文件

(1)重要数据和文件根据不同的需要按规定进行加密和设置访问权限；

(2)重要数据和文件应及时按规定进行备份。核心数据和文件要考虑在本地备份的基础上进行异地备份；

(3)重要数据和文件不要放在共享文件夹内，确因工作需要临时设立共享文件夹的，应设置口令，并应针对不同的用户名(帐号)设置不同的操作权限。临时共享文件夹使用结束后，应立即取消。

**附录：**

防范钓鱼网站的主要措施：

（1）通过查询网站备案信息等方式核实网站资质的真伪；（2）安装安全防护软件；（3）警惕中奖、修改网银密码的通知邮件、短信等信息。

谨防网络“中奖”陷阱：

（1）准备一份具有查毒、防毒、解毒及重要功能的软件，将有助于杜绝病毒。（2）不要轻易打开电子邮件的附件。近年来造成大规模破坏的许多病毒，都是通过电子邮件传播的。不要以为只打开熟人发送的附件就一定保险，有的病毒会自动检车受害人电脑上的通讯录并向其中的所有地址自动发送带毒文件。最妥当的作法，是先将附件保存下来，不要打开，先用查毒软件彻底检查。

使用无线WIFI发生信息泄露的原因：

（1）用户安全意识不强，轻易连接公共场所的WIFI信号源。（2）攻击者专注用户蹭网心理，设置隐蔽性很高的钓鱼WIFI站点。（3）不要将电子设备（只能终端、笔记本电脑）随意介入公开网络，处理涉及私密信息的事物。

防范网购假货的主要措施：

（1）在购物时要注意商家的信誉、评价和联系方式；（2）尽量通过网上第三方支付平台交易，切忌直接与买家私下交易；（3）在交易完成后要完整保存交易订单等信息。

防范电脑病毒的主要措施：

（1）定期查杀病毒；及时更新病毒库、更新系统补丁；（2）下载软件时尽量到官方网站或大型软件下载网站；（3）对公共磁盘空间加强权限管理，定期查杀病毒。

防范个人信息泄露的主要措施：

（1）尽量不要在可访问互联网的设备上保存或处理个人敏感信息；（2）只将个人信息转移给合法的接收者；（3）废弃的光盘、U盘、电脑灯要消磁或彻底破坏。

学生上网注意事项：

上网要注意安全，如果不加防范，网络的危害并不小，以下几方面应当引起同学们的足够重视。

（1）网上购物谨防上当。

（2）网上娱乐谨防过度。

　　（3）网上交友谨防受骗。

　　（4）对网上内容要有取舍，自动远离发布不良信息的网站。

　　（5）网上逗留谨防“毒黑”。也就是要防范病毒侵扰和黑客攻击，不要随便下载不知名网站的程序和附件。

（6）网上玩游戏容易近视，许多人都很喜爱网络，但网络游戏却让人情有独钟。



厚

德

精 博

益 学

求

精