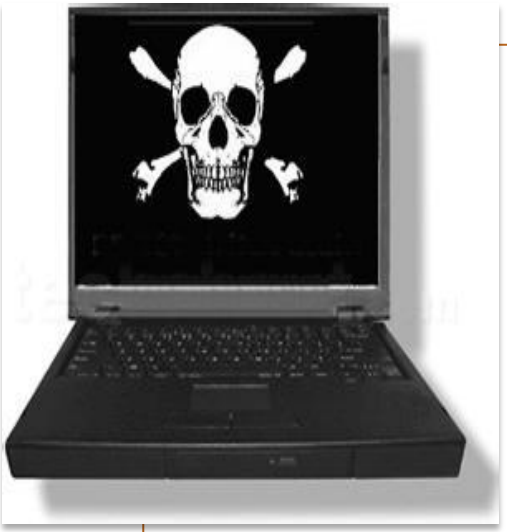
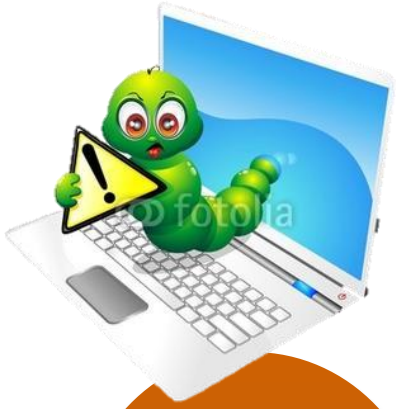
第二讲　计算机病毒的基本知识和预防

一、计算机病毒的概念



计算机病毒是指编制成单独的或者附着在其他计算机程序上，用以破坏或降低计算机功能或者毁坏数据、影响计算机使用、并能够自我复制的一组计算机指令或者程序代码。随着计算机网络的发展，计算机病毒从早期单机的感染已发展到利用计算机网络进行病毒传播，其蔓延的速度更加迅速，破坏性也更为严重。

二、计算机病毒的特征



可执行性

寄生性

传染性

破坏性

欺骗性

隐蔽性和潜伏性

衍生性

三、计算机病毒的表现形式

- 平时运行正常的计算机，
- 突然经常性无缘无故地死机；
- 运行速度明显变慢；
- 打印和通信发生异常；
- 系统文件的时间、日期、大小发生变化；
- 磁盘空间迅速减少；
- 收到陌生人发来的电子邮件；
- 在未执行读写磁盘命令的情况下，硬盘灯不断闪烁；
- 计算机无法识别硬盘；
- 操作系统无法正常启动；
- 部分文档丢失或被破坏；
- 网络瘫痪；
- U盘无法正常打开；
- 锁定主页；
- 经常性的显示“主存空间不够”的提示信息；
- 磁盘无故被格式化。

四、木马

木马

- 是一种远程控制程序，木马本身并不具备破坏性和主动传播性。它的传播机制和计算机病毒有本质的区别，但目前大多数人的观点，它也是一种计算机病毒。

木马的目的

- 通常并不是去破坏你的计算机系统，而是通过对你的计算机某个端口的监听来盗窃用户计算机中某些敏感的数据：例如用户的某个密码、口令、IP地址等，并利用远程传送 把这些数据发送到盗窃者的计算机系统中，从而实现盗窃者对用户计算机的控制。

木　马

木马　VS　病毒

- 木马不是主动传播，而是通过欺骗的手段，利用用户的误操作来实现传播
- 木马的主要目的不是破坏，而是“盗窃”
- 计算机病毒是主动攻击，而木马属于被动攻击，所以更难预防

五、计算机病毒和木马的预防

一般来说，计算机病毒和木马的预防分为两种：

管理方法上的预防

技术上的预防

- （如防病毒软件、防火墙软件等，预防计算机病毒对系统的入侵）

六、病毒的清除