**如何防范木马及病毒的攻击**

**一、计算机中毒有哪些症状？**

人生病了，会有各种各样的症状，同样，电脑中毒了也会有一些中毒反应。如果你的电脑有如下症状，要赶紧用杀毒软件查个毒了。

1.经常死机；

2.文件打不开；

3.经常报告内存不够；

4.提示硬盘剩余空间不足；

5.出现大量来历不明的文件；

6.数据无端丢失；

7.系统运行速度变慢；

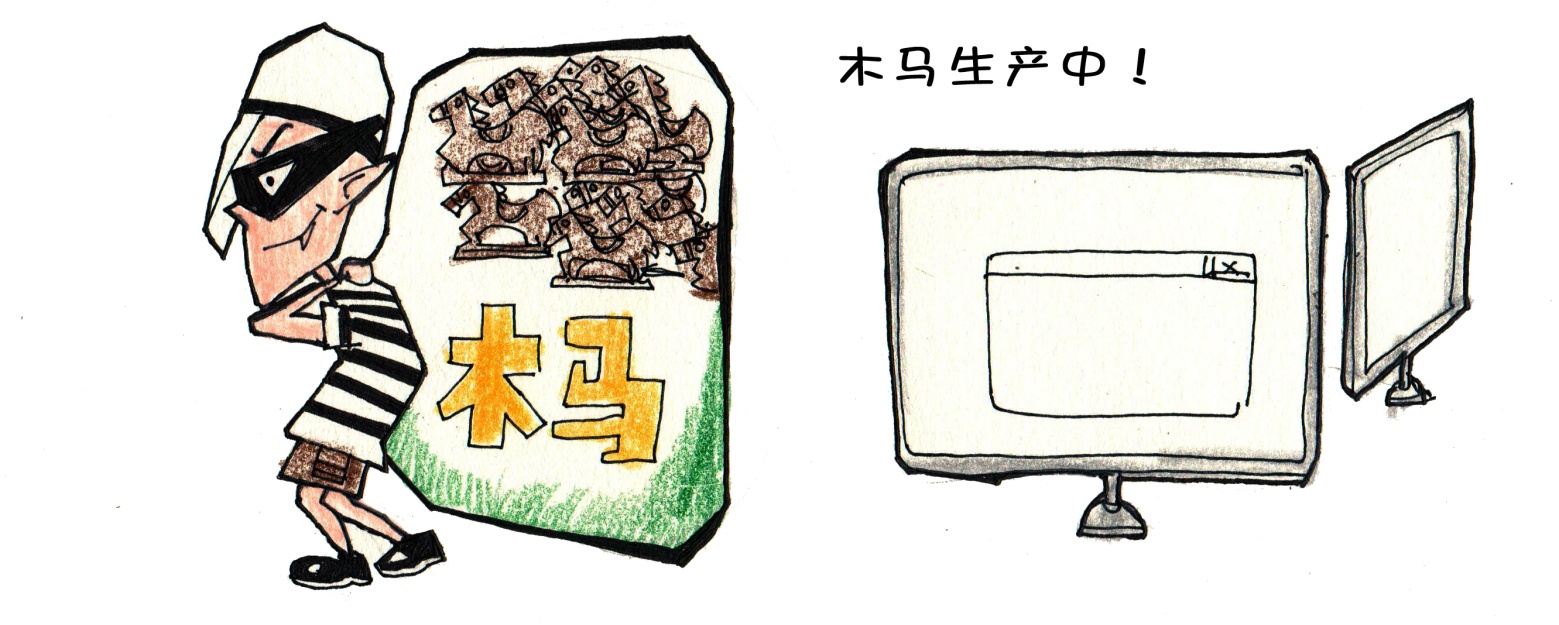
8.操作系统自动执行操作。

**二、木马病毒**

大家一定都听说过木马病毒，但木马病毒到底是什么呢？

（一）木马病毒

木马病毒是指通过特定的程序（木马程序）来控制另一台计算机。木马通常有两个可执行程序：一个是控制端，另一个是被控制端。木马这个名字来源于古希腊传说（荷马史诗中木马计的故事，Trojan一词的特洛伊木马本意是“特洛伊的”，即代指特洛伊木马，也就是木马计的故事）。“木马”程序是目前比较流行的病毒文件，与一般的病毒不同，它不会自我繁殖，也并不“刻意”地去感染其他文件，它通过将自身伪装吸引用户下载执行，向施种木马者提供打开被种主机的门户，使施种者可以任意毁坏、窃取被种者的文件，甚至远程操控被种主机。木马病毒的产生严重危害着现代网络的安全运行。



（二）木马病毒的种类

木马不是马，但是它也有不同的品种，让小笔记给大家介绍一下常见的木马变种吧。

1.网游木马

网络游戏木马通常采用记录用户键盘输入、Hook游戏进程、API函数等方法获取用户的密码和帐号。窃取到的信息一般通过发送电子邮件或向远程脚本程序提交的方式发送给木马作者。

网络游戏木马的种类和数量，在国产木马病毒中都首屈一指。流行的网络游戏无一不受网游木马的威胁。一款新游戏正式发布后，往往在一到两个星期内，就会有相应的木马程序被制作出来。大量的木马生成器和黑客网站的公开销售也是网游木马泛滥的原因之一。

2.网银木马

网银木马是针对网上交易系统编写的木马病毒，其目的是盗取用户的卡号、密码，甚至安全证书。此类木马种类数量虽然比不上网游木马，但它的危害更加直接，受害用户的损失更加惨重。

网银木马通常针对性较强，木马作者可能首先对某银行的网上交易系统进行仔细分析，然后针对安全薄弱环节编写病毒程序。2013年，安全软件电脑管家截获网银木马最新变种“弼马温”，弼马温病毒能够毫无痕迹的修改支付界面，使用户根本无法察觉。通过不良网站提供假QVOD下载地址进行广泛传播，当用户下载这一挂马播放器文件安装后就会中木马，该病毒运行后即开始监视用户网络交易，屏蔽余额支付和快捷支付，强制用户使用网银，并借机篡改订单，盗取财产。

随着中国网上交易的普及，受到外来网银木马威胁的用户也在不断增加。





3.FTP木马

FTP型木马打开被控制计算机的21号端口(FTP所使用的默认端口)，使每一个人都可以通过一个FTP客户端程序、不用密码就可直接连接到受控制端计算机，并且可以进行最高权限的上传和下载，窃取受害者的机密文件。新FTP木马还加上了密码功能，这样，只有攻击者本人才知道正确的密码，从而进入对方计算机。

（三）木马病毒的危害

希腊人凭借一只大木马攻下了特洛伊的城门，而黑客们会用木马程序攻破你满是漏洞的电脑，造成各种危害。

1、盗取我们的网游账号，威胁我们的虚拟财产的安全

木马病毒会盗取我们的网游账号，盗取帐号后，并立即将帐号中的游戏装备转移，再由木马病毒使用者出售这些盗取的游戏装备和游戏币而获利。

2、盗取我们的网银信息，威胁我们的真实财产的安全

木马采用键盘记录等方式盗取我们的网银帐号和密码并发送给黑客，直接导致经济损失。

3、利用即时通讯软件盗取我们的身份，传播木马病毒等不良信息

中了木马病毒的电脑会下载病毒作者指定的程序，具有不确定的危害性，如使电脑瘫痪等。

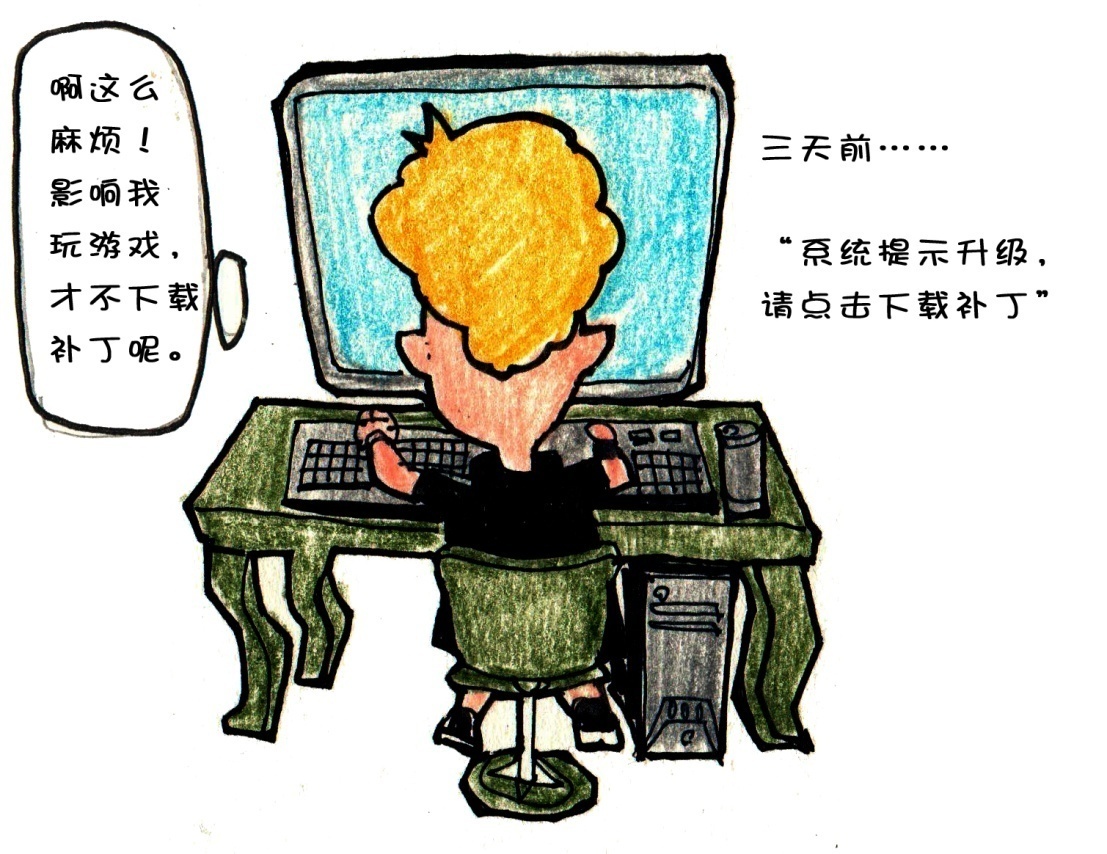
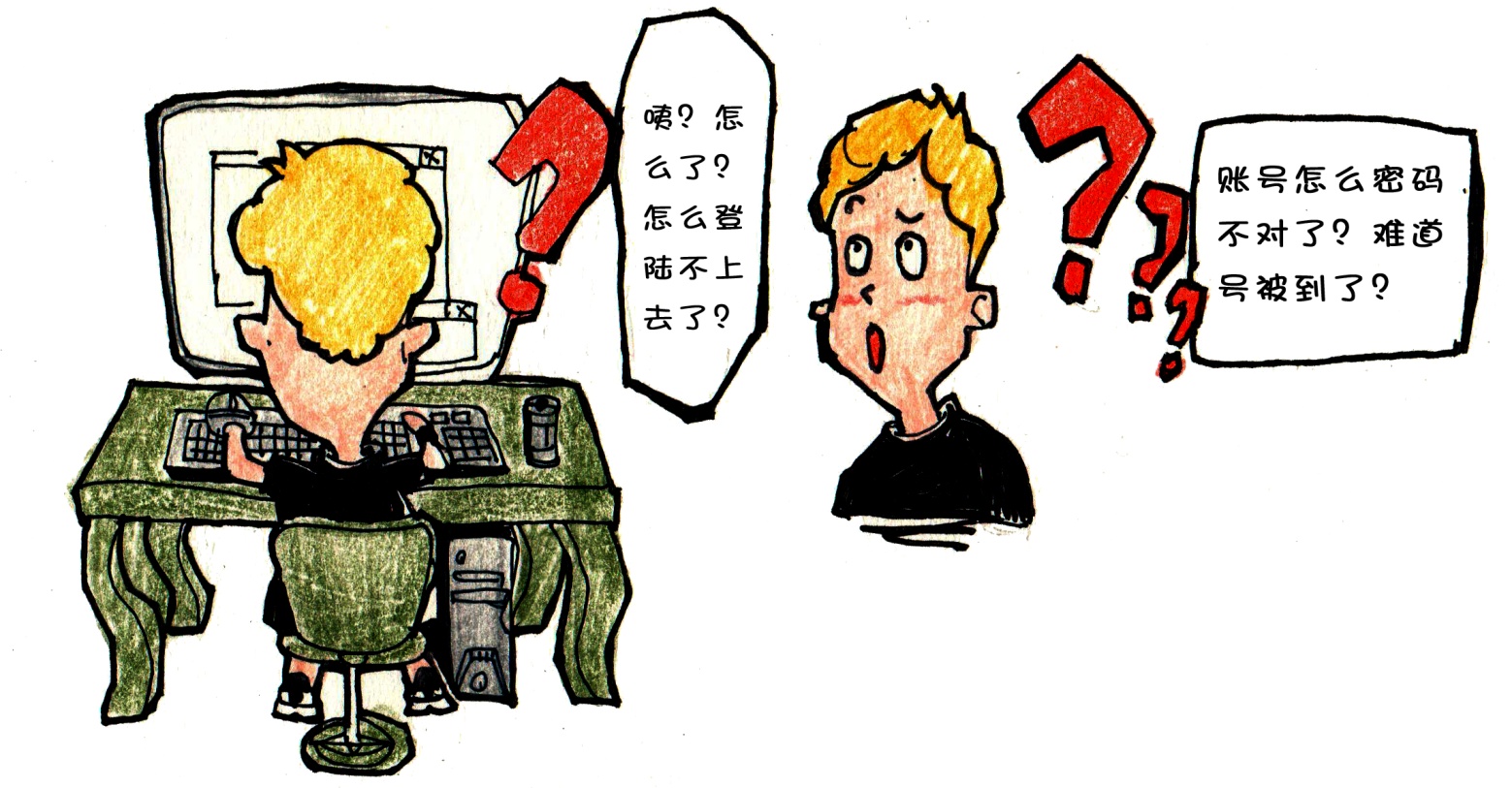


**三、如何防范木马病毒及其他病毒的攻击？**

为了不像特洛伊国人那样被希腊人的木马打败，我们需要这样做：

1.为计算机安装杀毒软件，定期扫描系统、查杀病毒；及时更新病毒库、更新系统补丁；

TIP:编写程序不是十全十美，所以软件也免不了会出现BUG，而补丁是专门用于修复这些BUG的。因为原来发布的软件存在缺陷，发现之后另外编制一个小程序使其完善，这种小程序俗称补丁。定期进行补丁升级，升级到最新的安全补丁，可以有效地防止非法入侵。



2.下载软件时尽量到官方网站或大型软件下载网站，在安装或打开来历不明的软件或文件前先杀毒；

3.不随意打开不明网页链接，尤其是不良网站的链接，陌生人通过QQ给自己传链接时，尽量不要打开；

4.使用网络通信工具时不随便接收陌生人的文件，若接收，可在工具菜单栏中“文件夹选项”中取消“隐藏已知文件类型扩展名”的功能来查看文件类型；

5.对公共磁盘空间加强权限管理，定期查杀病毒；

6.打开移动存储器前先用杀毒软件进行检查，可在移动存储器中建立名为“autorun.inf”的文件夹（可防U盘病毒启动）；

7.需要从互联网等公共网络上下载资料转入内网计算机时，用刻录光盘的方式实现转存；

8.对计算机系统的各个账号要设置口令，及时删除或禁用过期账号；

9.定期备份，以便遭到病毒严重破坏后能迅速修复。