随着网络的发展带来的安全隐患

1、Internet 是一个开放的、无控制机构的网络，黑客（Hacker）经常会侵入网络中的计算机系统，或窃取机密数据和盗用特权，或破坏重要数据，或使系统功能得不到充分发挥直至瘫痪。

2、Internet 的数据传输是基于 TCP/IP 通信协议进行的，这些协议缺乏使传输过程中的信息不被窃取的安全措施。

3、Internet 上的通信业务多数使用 Unix 操作系统来支持，Unix 操作系统中明显存在的安全脆弱性问题会直接影响安全服务。

4、在计算机上存储、传输和处理的电子信息，还没有像传统的邮件通信那样进行信封保护和签字盖章。信息的来源和去向是否真实，内容是否被改动，以及是否泄露等，在应用层支持的服务协议中是凭着君子协定来维系的。

5、电子邮件存在着被拆看、误投和伪造的可能性。使用电子邮件来传输重要机密信息会存在着很大的危险。

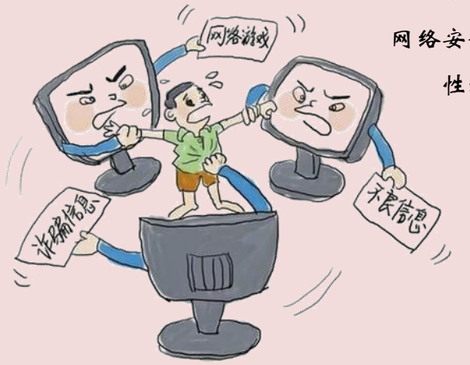
6、计算机病毒通过 Internet 的传播给上网用户带来极大的危害，病毒可以使计算机和计算机网络系统瘫痪、数据和文件丢失。在网络上传播病毒可以通过公共匿名 FTP 文件传送、也可以通过邮件和邮件的附加文件传播。

关于网络安全的小例子

美国网络间谍活动公诸于世。2013 年 6 月曾经参加美国安全局网络监控项目的斯诺登披露“棱镜事件”，美国秘密利用超级软件监控网络、电话或短信，包括谷歌、雅虎、微软、苹果、Facebook、美国在线、PalTalk、Skype、YouTube 等九大公司帮助提供漏洞参数、开放服务器等，使其轻而易举地监控有关国家机构或上百万网民的邮件、即时通话及相关数据。据称，思科参与了中国几乎所有大型网络项目的建设，涉及政府、军警、金融、海关、邮政、铁路、民航、医疗等要害部门，以及中国电信、联通等电信运营商的网络系统。

据国家互联网应急中心(CNCERT)的数据显示，中国遭受境外网络攻击的情况日趋严重。CNCERT 抽样监测发现，2013 年 1 月 1 日至 2 月 28 日，境外 6747 台木马或僵尸网络控制服务器控制了中国境内 190 万余台主机；其中位于美国的 2194 台控制服务器控制了中国境内 128.7 万台主机，无论是按照控制服务器数量还是按照控制中国主机数量排名，美国都名列第一。

我国网络遭受攻击近况。根据国家互联网应急中心 CNCERT 抽样监测结果和国家信息安全漏洞共享平台 CNVD 发布的数据，2013 年 8 月 19 日至 8 月 25 日一周境内被篡改网站数量为 5470 个；境内被植入后门的网站数量为 3203 个；针对境内网站的仿冒页面数量为 754 个。被篡改政府网站数量为 384 个；境内被植入后门的政府网站数量为 98 个；针对境内网站的仿冒页面 754 个。感染网络病毒的主机数量约为 69.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 23 万以及境内感染飞客（Conficker）蠕虫的主机约 46.4 万。新增信息安全漏洞 150 个，其中高危漏洞 50 个。



共筑网络安全 共享绿色家园

（一）保护网络安全。

网络安全是为保护商务各方网络端系统之间通信过程的安全性。保证机密性、完整性、认证性和访问控制性是网络安全的重要因素。保护网络安全的主要措施如下：

（1）全面规划网络平台的安全策略。

（2）制定网络安全的管理措施。

（3）使用防火墙。

（4）尽可能记录网络上的一切活动。

（5）注意对网络设备的物理保护。

（6）检验网络平台系统的脆弱性。

（7）建立可靠的识别和鉴别机制。

预防措施

（二）保护应用安全。

保护应用安全，主要是针对特定应用（如 Web 服务器、网络支付专用软件系统）所建立的安全防护措施，它独立于网络的任何其他安全防护措施。虽然有些防护措施可能是网络安全业务的一种替代或重叠，如 Web 浏览器和 Web 服务器在应用层上对网络支付结算信息包的加密，都通过 IP 层加密，但是许多应用还有自己的特定安全要求。

由于电子商务中的应用层对安全的要求最严格、最复杂，因此更倾向于在应用层而不是在网络层采取各种安全措施。

虽然网络层上的安全仍有其特定地位，但是人们不能完全依靠它来解决电子商务应用的安全性。应用层上的安全业务可以涉及认证、访问控制、机密性、数据完整性、不可否认性、Web 安全性、EDI 和网络支付等应用的安全性。

（三）保护系统安全。

保护系统安全，是指从整体电子商务系统或网络支付系统的角度进行安全防护，它与网络系统硬件平台、操作系统、各种应用软件等互相关联。涉及网络支付结算的系统安全包含下述一些措施：

（1）在安装的软件中，如浏览器软件、电子钱包软件、支付网关软件等，检查和确认未知的安全漏洞。

（2）技术与管理相结合，使系统具有最小穿透风险性。如通过诸多认证才允许连通，对所有接入数据必须进行审计，对系统用户进行严格安全管理。

（3）建立详细的安全审计日志，以便检测并跟踪入侵攻击等。

19 网 1 姚虹