网络安全

NETWORK SECURITY

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

如何预防

1.安装杀毒软件和个人防火墙，并及时升级。

2. 把个人防火墙设置好安全等级，防止未知程序向外传送数据。

3. 可以考虑使用安全性比较好的浏览器和电子邮件客户端工具。

4. 如果使用 IE 浏览器，应该安装卡卡安全助手，防止恶意网站在自己电脑上安装不明软件和浏览器插件，以免被木马趁机侵入。

5. 不要执行任何来历不明的软件

6. 不要随意打开邮件附件。现在绝大部分木马病毒都是通过邮件来传递的，而且有的还会连环扩散，因此对邮件附件的运行尤其需要注意。

网络安全相关条例

19 网 1 李新杰

第一，我国《刑法》第二百八十六条有规定，违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

第二，我国《关于加强网络信息保护的决定》第一条有规定，不得窃取或以非法手段获取公民个人电子信息。

第三，我国《关于维护互联网安全的决定》第一条有规定，为了保障互联网的运行安全，对有下列行为之一，构成犯罪的，依照刑法有关规定追究刑事责任：1、侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统；2、故意制作、传播计算机病毒等破坏性程序，攻击计算机系统及通信网络，致使计算机系统及通信网络遭受损害；3、违反国家规定，擅自中断计算机网络或者通信服务，造成计算机网络或者通信系统不能正常运行。

综上所述，有关网络病毒的规定以及处罚，分别是《刑法》、《关于加强网络信息保护的决定》以及《关于维护互联网安全的决定》等。