网络入侵四大主要途径对应策略保安全 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/257/2021_2022__E7_BD_91_E7_BB_9C_E5_85_A5_E4_c67_257595.htm 计算机病毒入侵主要有源代码嵌入攻击型、代码取代攻击型、系统修改型和外壳附加型四种方式，而对网络入侵来讲我个人认为主要分为主动入侵和被动入侵。 主动入侵主要是指用户主动去执行病毒以及木马程序，例如浏览存网站中植入了恶意病毒及其木马程序的网页，这些木马程序（病毒）大多是利用操作系统的漏洞，当用户访问网页时，将会主动下载该类木马程序并执行。还有就是目前比较流行的优盘病毒，通过优盘来进行传播和执行，这种类型的攻击非常隐蔽，不易察觉，当用户连接互联网时，木马（病毒）的客户端可以对感染木马（病毒）的服务端进行控制。 被动入侵主要是指由入侵者主动发动的攻击，例如扫描系统口令，利用系统存在的远程溢出漏洞进行溢出攻击，SQL注入攻击等。如果用户具有一定安全意识，被成功入侵的几率较低。 通过分析研究，对于网络计算机通过采取以下措施，将会大大降低安全风险：（1）及时更新操作系统补丁程序。系统安装完成后，不要立即连接互联网，而是安装操作系统最新的一些安全补丁程序，特别是要安装一些高危漏洞的补丁程序，很多网页就是利用这些漏洞来执行木马程序。（2）安装杀毒软件和防火墙，并及时更新病毒库。及时更新杀毒软件的病毒库可以有效的查杀病毒和木马程序。（3）谨慎下载软件。目前计算机运行的很多程序大多为盗版，无法进行来源验证，很多提供下载的程序都捆绑有木马程序，因此不要运行来历不明的程序，尽量

到大型正规网站下载软件。（4）做好系统和数据备份。系统安装完成后，一定要进行数据和操作系统的备份，最好做一个Ghost文件，便于出现问题后可以立即恢复系统或者数据。