# 2024年网络安全教育个人心得 网络安全教育心得体会(三篇)

来源：网络 作者：心上人间 更新时间：2024-10-16

*我们在一些事情上受到启发后，应该马上记录下来，写一篇心得体会，这样我们可以养成良好的总结方法。好的心得体会对于我们的帮助很大，所以我们要好好写一篇心得体会以下我给大家整理了一些优质的心得体会范文，希望对大家能够有所帮助。网络安全教育个人心得...*

我们在一些事情上受到启发后，应该马上记录下来，写一篇心得体会，这样我们可以养成良好的总结方法。好的心得体会对于我们的帮助很大，所以我们要好好写一篇心得体会以下我给大家整理了一些优质的心得体会范文，希望对大家能够有所帮助。

**网络安全教育个人心得 网络安全教育心得体会篇一**

他还详细的讲到了云计算和云安全：但一到云，这件事情就比较麻烦了，云的墙不知道在什么地方，你也不知道门在什么地方。所以这时候传统的内外之分就不是那么靠谱了，什么是内什么外是件说不清楚的事;也许我们现在需要找找另一种思维模式;谈云，就想跟自然界的云做对比，这种计算模式一开始起名字确实非常好。并提到云安全计划是网络时代信息安全的最新体现，它融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念，通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，传送到server端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。他的这些生动讲解使我们对“云”这个概念有了一个初步印象。更为重要的是他还使我们了解了在上网过程中保护个人信息的重要性。

听完潘总的讲座后，我想为了很好的保护自己的信息安全，应该做到以下几点：第一在自己电脑上安装能够实时更新的杀毒软件。最好是性能比较高的杀毒软件，诸如卡巴斯基、瑞星之类的，虽然这类软件会收取一定的使用费用，但考虑到我们电脑可能受到的潜在威胁，这些钱花的也是值得的。有了杀毒软件之后一定要定期进行杀毒，而且上网时一定要保证杀毒软件的开启状态，有些人在玩游戏或者使用大型软件的时候为了避免占用内存而把杀毒软件关闭，如果不能及时开启我们电脑还是可能受到威胁的。如果时间允许我认为还可以在安全模式下进行查杀处理，这样有效杀出病毒的几率会大大提高。有了杀毒软件也不能肆无忌惮的上网，最好能够上一些有一定声誉、安全性高的网站。第二在安装从网上下载下来的软件时一定要一步步看清楚各个选项。

现在很多软件为了自身盈利的需要而夹杂了流氓软件，流氓软件安装之后又是极不容易卸载的。这些流氓软件可能会修改你的浏览器主页，定期打开某一网页等等，造成了我们使用电脑时的极大不便，这些软件还会记录下我们上网偏好，随时向我们发垃圾广告。所以下载安装软件一定要慎重。第三慎用u盘、移动硬盘之类的存储设备。某些破坏性的病毒可能导致移动存储设备损坏。我们在使用u盘之类的存储设备时也要小心谨慎，打开u盘时尽量不要双击打开，这样很可能会激活存在于里面的木马，使用打开前最好能够先杀一遍毒，甚至我们可以专门去网上搜取u盘木马专杀来预防电脑再次被感染。第四尽量不要在互联网上公布个人信息。除非是万不得已，否则不要公布自己任何详细的信息，以防被不良分子利用。另外在网上不要随意公布自己的邮箱，因为邮箱是一个十分便利的切入口来搜取你的个人信息，我们在各个网站注册时一般都会被要求留下邮箱，这样在这个过程中或多或少我们都会偷漏一些个人信息，如果通过搜取邮箱的方法获得你在各个网站上公布的个人信息经过综合整理很可能是自己更多的信息被公布出来。更多的我们考虑的自身安全问题，公布照片不仅是我们信息安全得不到保护，甚至现实中我们人身安全也可能因为一张照片而受到威胁。

在互联网日益普及的今天，我想，作为一名学生，在我们学习信息安全相关知识的同时还一定要在上网时提高个人信息保护意识。

**网络安全教育个人心得 网络安全教育心得体会篇二**

在21世纪，网络已经成为人们日常生活的一部分，很多人甚至已经离不开网络。有了网络，人们足不出户便可衣食无忧。前些天刚从电视上看到关于年底网购火爆，快递公司也在“春运”的新闻。以前人们找东西得找人帮忙，现在人们找东西找网帮忙。记得有一次钥匙不知道放到了什么地方，就百度了一下“钥匙丢在那里了”，结果按照网友们提示的方案还真给找到了。

网络爆炸性地发展，网络环境也日益复杂和开放，同时各种各样的安全漏洞也暴露出来，恶意威胁和攻击日益增多，安全事件与日俱增，也让接触互联网络的每一个人都不同程度地受到了威胁。在此，我就生活中、工作中碰到看到的各种网络安全问题谈谈自己的体会：

1.有网络安全的意识很重要

谈到网络安全，让我们无奈的是很多人认为这是计算机网络专业人员的事情。其实，每个人都应该有网络安全的意识，这点对于涉密单位人员来说尤其重要。前段时间看了电视剧《密战》，其中揭露的泄密方式多数都是相关人员安全意识薄弱造成：单位要求机密的工作必须在办公室完成，就是有人私自带回家加班造成泄密;重要部门要求外人不得入内，偏有人把闲杂人员带入造成泄密;专网电脑不允许接互联网，有人

接外网打游戏造成泄密;甚至涉密人员交友不慎，与间谍谈恋爱造成泄密。虽然这只是电视剧，但对机密单位也是一种警示。看这部电视剧的时候我就在想，这应该作为安全部门的安全教育片。

不单单是涉密单位，对于个人来说，网络安全意识也特别重要。网上层出不穷的摄像头泄密事件、这“门”那“门”的都是由于个人安全意识淡薄所致。正如老师所说的“看到的不一定是真的!”。

我自己的电脑上有一些自己平时做的软件、系统，虽说没什么重要的，但那也是自己辛苦整出来的呀，所以使用电脑一直很小心，生怕有什么木马、病毒之类的，“360流量监控”的小条一直在我的“桌面”右下角，只要有上传流量肯定得去看看是什么进程在上传。

平时为别人维护系统经常会碰到杀毒软件很久不升级的情况，主人还振振有词的说自己装了杀毒软件的。在他们看来杀毒软件有了就成，剩下的就不用管了，我很多时候这样对他们说：“你养条狗还得天天喂它吃呢!”

2.设备安全—很多技术是我们想不到的

网络设备是网络运行的硬件基础，设备安全是网络完全必不可少的一个环节。

以前听说过电泄密，一直没见过，最近单位有同事拿来了两个“电力猫”(电力线以太网信号传输适配器)，一个接网线插到电源上，另一个在30米内接电源通过接口接网线链接到电脑便可上网。这让我想到，只要有人将涉密的网络线路接到电源线路便可轻易泄密，当然这块国家安全部门肯定有相关的防范措施。

在搜索引擎里搜索诸如：intitle:\"liveview/-a\_is206w\"等，可以搜到网络摄像头，在电视剧《密战》中，某涉密部门的监控系统被接入了互联网，间谍就利用监控系统窃取工作人员的屏幕信息和按键信息。在某政府机要室的复印机上安装基于移动网络的发射器，便可再用另外一台接收机上受到所有扫描的机要文件。

1985年，在法国召开的一次国际计算机安全会议上，年轻的荷兰人范〃艾克当着各国代表的面，公开了他窃取微机信息的技术。他用价值仅几百美元的器件对普通电视机进行改造，然后安装在汽车里，这样就从楼下的街道上，接收到了放臵在8层楼上的计算机电磁波的信息，并显示出计算机屏幕上显示的图像。

他的演示给与会的各国代表以巨大的震动。本人最早知道电磁泄密是在20\_\_年为部队某部门开发软件的时候听说的，在部队很多地方时安装了\_的就是为了防止电磁泄密。

硬盘数据不是删掉就不存在了，用诸如easyrecovery等恢复软件都可以恢复。看来，只有将涉密硬盘用炼钢炉化掉才能保证完全安全。

3.小心木马

最早知道木马，是自己大学期间。当时在网上看到了一款叫“大眼睛”的屏幕发送软件，很好奇就试着用了。大学的机房里的计算机只装常用软件，其他诸如qq等软件都是在服务器上存放，用的时候自己安装，学生机有保护卡重启就被恢复了，又得装。

于是就将“大眼睛”的客户端放在服务器上取个很吸引人的名字。结果很多同学的屏幕都被我们监控。有同学嘲笑说“不就是个木马嘛!”经过查询才知道有种叫“木马”的程序也是用同样的方法进行隐私窃取。后来自己还做过假的qq程序盗取别人的qq，但盗来都给了别人，谁知道现在7、8位qq号码能这么畅销。

以前电脑都防cih、蠕虫等病毒，当现在更多的是防木马病毒，主要是由于个人电脑上可以窃取诸如支付宝、qq账号、网上银行等密码。当你打开不安全的网页、别人发给你的恶意邮件时，当你安装不安全的软件时，当你使用u盘时都可能感染木马病毒。

前一段时间的“360和qq之争”，在我们的电脑里有很多不安全的的软件，都可能泄露我们的隐私。

4.网页安全

在单位，我负责几个部门的网站维护，主要是网页制作。在一开始编程的时候，根本没想到能被攻击。后来自己做的网站经常被攻击，这才知道诸如sql注入、ewebeditor漏洞等攻击手段，所以在编程时会注意到这些方面的安全。比如我的后台数据库一般都是“#”。防止数据库被下载。

记得又一次为某部门自己编写了一个留言板程序，结果发布没1天就有3000多条恶意留言，还是英文的，挺让人头疼。最后设臵了验证码、用户验证都不起作用，直到用了检测留言来源网页代码才堵住。原来人家是用工具攻击的。

5.养成良好的上网习惯

网络安全涉及到使用网络的每一个人。对个人来说，要保证自己安全上网，每个人都得养成良好的上网习惯。我想应该包含以下几点：

1)电脑要安装防火墙和杀毒软件，要及时升级，如果电脑上网则设臵为自动升级。并且养成经常性安全扫描电脑;

2)及时更新windows补丁;

3)在确保系统安全的情况下，做好ghost备份，防止碰到顽固病毒时能及时恢复系统;

4)网友用qq等发给的网站和程序，不要轻易去点击和执行;

5)不浏览不安全的网页;

6)共享文件要及时关闭共享，在单位经常会在工作组计算机中看到别人共享的东西;

7)不熟悉的邮件不浏览;

8)u盘杀毒后再去打开;

9)不在别人的计算机上登录自己的银行账号、支付宝、qq等;对于我们每个人来说，提高网络安全意识，学习网络安全知识，是网络时代对我们基本的要求。

**网络安全教育个人心得 网络安全教育心得体会篇三**

接触网站安全管理的工作有几个年头了，非常感谢最初让我接触到网站木马工作任务的陈总对我的信任，那时候虽然完全没有接触过，也没有想过自已是否能够处理，但最终还是凭自已的毅力，找到好多木马处理好了，同时也感谢客户西北在线对我的忍耐，这是我的动力。虽然这些年不是专业在做网络安全管理工作，但是时不时会接触到，并把它当做自已的责任，下面我来下谈谈做网络安全管理工作的体会。

网络管理是一个系统工程，通过几次黑客入侵，攻击的案例，更加觉得日常的检查和维护，特别是安全管理要求十分必要。下面来说具体的体会：

1、定期进行安全体检，检查日志文件是否有异常，如有陌生帐户登录，检查比对服务器文件内容，是否发现有明显木马或病毒程序的植入。

2、做好服务器数据备份，一是服务器系统备份，这样一旦发现黑客入侵，可以快速的恢复系统，二是数据库备份，必须服务器数据信息是一个网站的核心。

3、作为网络管理员，如果真的被黑客入侵了，查找和解决问题最便捷的办法是充分应用网络资源，可以到网上或论坛搜集一些相关的信息，也许能找到相应的解决办法，同时还可以分享自已经验技巧。

还有一个解决办法就是重装系统，重新更换除数据之外的所有文件，找起来太费事，这样子做清除的很彻底。

4、预防为主，问题发生了心理压力很大，所以要做好提前预防。

具体预防的方法首先需要修改管理员帐号，不用默认的administrator，其次修改远程桌面端口3389，再次修改入站规则。

本文档由站牛网zhann.net收集整理，更多优质范文文档请移步zhann.net站内查找