# 描写网络安全个人感悟总结(10篇)

来源：网络 作者：无殇蝶舞 更新时间：2024-10-09

*描写网络安全个人感悟总结一网络爆炸性地发展，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...*

**描写网络安全个人感悟总结一**

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:\"live view/-axis 206w\"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20xx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干扰器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“#.mdb”。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)最好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。

**描写网络安全个人感悟总结二**

文章分析了上海嘉定区有线电视中心网络的安全管理所涉及的问题，并根据本身的工作实践介绍了对于网络内外的供电设备系统、计算机病毒防治、防火墙技术等问题采取的安全管理措施。

网络安全；防火墙；数据库；病毒；网络入侵者

当今许多的企业都广泛的使用信息技术，特别是网络技术的应用越来越多，而宽带接入已经成为企业内部计算机网络接入国际互联网的主要方式。而与此同时，因为计算机网络特有的开放性，企业的网络安全问题也随之而来，由于安全问题给企业造成了相当大的损失。因此，预防和检测网络设计的安全问题和来自国际互联网的网络入侵者攻击以及病毒入侵成为网络管理员一个重要课题。

在实际应用过程中，遇到了不少网络安全方面的问题。网络安全是一个十分复杂的问题，它的划分大体上可以分为内网和外网。如下表所示：

由上表可以看出，外部网的安全问题主要集中在入侵方面，主要的体现在：未授权的访问，破坏数据的完整性，拒绝服务攻击和利用网络、网页浏览和电子邮件夹带传播病毒。但是网络安全不仅要防范外部网，同时更防范内部网。因为内部网安全措施对网络安全的意义更大。据调查，在已知的网络安全事件中,约70%的攻击是来自内部网。内部网的安全问题主要体现在：物理层的安全，资源共享的访问控制策略，网内病毒侵害，合法用户非授权访问，假冒合法用户非法授权访问和数据灾难性破坏。

综合以上对于网络安全问题的初步认识，有线中心采取如下的措施：

对于外网造成的安全问题，使用防火墙技术来实现二者的隔离和访问控制。

防火墙是实现网络安全最基本、最经济、最有效的措施之一。防火墙可以对所有的访问进行严格控制（允许、禁止、报警）。

防火墙可以监视、控制和更改在内部和外部网络之间流动的网络通信；用来加强网络之间访问控制，防止外部网络用户以非法手段通过外部网络进入内部网络，访问内部网络资源，从而保护内部网络操作环境。所以，安装防火墙对于网络安全来说具有很多优点：（1）集中的网络安全；（2）可作为中心“扼制点”；（3）产生安全报警；（4）监视并记录internet的使用；（5）nat的位置；（6）www和ftp服务器的理想位置。

但防火墙不可能完全防止有些新的攻击或那些不经过防火墙的其它攻击。为此，中心选用了realsecuresystemagent和networkengine。其中，realsecuresystemagent是一种基于主机的实时入侵检测产品，一旦发现对主机的入侵，realsecure可以中断用户进程和挂起用户账号来阻止进一步入侵，同时它还会发出警报、记录事件等以及执行用户自定义动作。realsecuresystemagent还具有伪装功能，可以将服务器不开放的端口进行伪装，进一步迷惑可能的入侵者，提高系统的防护时间。re?鄄alsecurenetworkengin是基于网络的实时入侵检测产品，在网络中分析可疑的数据而不会影响数据在网络上的传输。网络入侵检测realsecurenetworkengine在检测到网络入侵后，除了可以及时切断攻击行为之外，还可以动态地调整防火墙的防护策略，使得防火墙成为一个动态的、智能的防护体系。

通过部署入侵检测系统，我们实现了以下功能：

对于www服务器，配置主页的自动恢复功能，即如果www服务器被攻破、主页被纂改，系统能够自动识别并把它恢复至事先设定的页面。

入侵检测系统与防火墙进行“互动”，即当入侵检测系统检测到网络攻击后，通知防火墙，由防火墙对攻击进行阻断。

网络物理层的稳定主要包括设备的电源保护，抗电磁干扰和防雷击。

本中心采用二路供电的措施，并且在配电箱后面接上稳压器和不间断电源。所有的网络设备都放在机箱中，所有的机箱都必须有接地的设计，在机房安装的时候必须按照接地的规定做工程；对于供电设备，也必须做好接地的工作。这样就可以防止静电对设备的破坏，保证了网内硬件的安全。

病毒程序可以通过电子邮件、使用盗版光盘等传播途径潜入内部网。网络中一旦有一台主机受病毒感染，则病毒程序就完全可能在极短的时间内迅速扩散，传播到网络上的所有主机，可能造成信息泄漏、文件丢失、机器死机等不安全因素。防病毒解决方案体系结构中用于降低或消除恶意代码；广告软件和间谍软件带来的风险的相关技术。中心使用企业网络版杀毒软件，（例如：symantecantivirus等）并控制写入服务器的客户端，网管可以随时升级并杀毒，保证写入数据的安全性，服务器的安全性，以及在客户端安装由奇虎安全卫士之类来防止广告软件和间谍软件。

应用系统的安全主要面对的是服务器的安全，对于服务器来说，安全的配置是首要的。对于本中心来说主要需要2个方面的配置：服务器的操作系统（windows20xx）的安

全配置和数据库（sqlserver20xx）的安全配置。

（1）系统升级、打操作系统补丁，尤其是iis6.0补丁。

（2）禁止默认共享。

（3）打开管理工具-本地安全策略，在本地策略-安全选项中，开启不显示上次的登录用户名。

（4）禁用tcp/ip上的netbios。

（5）停掉guest帐号，并给guest加一个异常复杂的密码。

（6）关闭不必要的端口。

（7）启用win20xx的自身带的网络防火墙，并进行端口的改变。

（8）打开审核策略，这个也非常重要，必须开启。

（1）安装完sqlserver20xx数据库上微软网站打最新的sp4补丁。

（2）使用安全的密码策略设置复杂的sa密码。

（3）在ipsec过滤拒绝掉1434端口的udp通讯，可以尽可能地隐藏你的sqlserver。

（4）使用操作系统自己的ipsec可以实现ip数据包的安全性。

除了以上的一些安全措施以外，作为网络管理员还要准备一些针对网络监控的管理工具，通过这些工具来加强对网络安全的管理。

ping、ipconfig/winipcfg、netstat：

ping，tcp/ip协议的探测工具。

ipconfig/winipcfg，查看和修改网络中的tcp/ip协议的有关配置，

netstat，利用该工具可以显示有关统计信息和当前tcp/ip网络连接的\'情况，用户或网络管理人员可以得到非常详尽的统计结果。

solarwindsengineer\'\'seditiontoolset

另外本中心还采用solarwindsengineer\'\'seditiontoolset。它的用途十分广泛，涵盖了从简单、变化的ping监控器及子网计算器（subnetcalculators）到更为复杂的性能监控器何地址管理功能。”

solarwindsengineer\'\'seditiontoolset的介绍：

solarwindsengineer’sedition是一套非常全面的网络工具库，包括了网络恢复、错误监控、性能监控和管理工具等等。除了包含professionalplusedition中所有的工具外，engineer’sedition还增加了新的switchportmapper工具，它可以在您的switch上自动执行layer2和layer3恢复。工程师版包含了solarwindsmib浏览器和网络性能监控器（networkperformancemonitor），以及其他附加网络管理工具。

snifferpro能够了解本机网络的使用情况，它使用流量显示和图表绘制功能在众多网管软件中最为强大最为灵活；它能在于混杂模式下的监听，也就是说它可以监听到来自于其他计算机发往另外计算机的数据，当然很多混杂模式下的监听是以一定的设置为基础的，只有了解了对本机流量的监听设置才能够进行高级混杂模式监听。

除了上面说的五个措施以外，还有不少其他的措施加强了安全问题的管理：

●制订相应的机房管理制度；

●制订相应的软件管理制度；

●制订严格的操作管理规程；

●制订在紧急情况下系统如何尽快恢复的应急措施，使损失减至最小；

●建立人员雇用和解聘制度，对工作调动和离职人员要及时调整相应的授权。

总之，网络安全是一个系统工程，包含多个层面，因此安全隐患是不可能完全消除的，但是通过各种有力措施，却可以将其减到最小程度。所以需在网络安全问题方面不断探索，使网络建设和应用两方面相互促进形成良性循环。

**描写网络安全个人感悟总结三**

尊敬的各位领导、同事们：

大家好，很高兴能参加这次演讲，生命是如此的精彩，生命是如此的辉煌，不过今天我演讲的内容里没有生死间的大悲恸，也没有平平仄平平的华丽辞藻，我演讲题目是：互联网，精彩而危险的世界。

网络世界呢是一个精彩的世界。qq、网络购物、网络游戏、远程办公，丰富并改变着我们的生活，但是精彩的背后蕴含着危险。大家可曾碰到过，你的qq号被盗?这个很常见吧。网银被盗?文档、照片或者其他数据不见了?正在电脑上看文档的时候，鼠标自己动了，恩，你的系统被劫持了。大家一直以来，都对黑客和病毒有一份“特殊化的感情”，认为所有的黑客都是非常厉害的，所有的病毒都是灾难性的，是吧?同大家分享2个网络安全的案例。

20xx年，中国软件开发联盟csdn，中国最大的开发者技术社区，密码泄漏，超1亿用户密码被泄，黑客在网上公开了一部分用户信息数据库，导致600余万个注册邮箱账号和与之对应的明文密码泄露。这次事件以后，又陆续曝出了多玩网、人人网、搜狗浏览器等安全事件。

唔前面的案例大家没有亲身体会，说个大家接触过的，考过职称考试的人都知道，有时候会被杂志社打电话问到要不要发表职称论文，呵呵，这个大家都有经验吧，恩，很明显你的电话信息泄露了呀，怎么泄露的呢，考职称考试要网上注册报名缴费吧?报名时电话号码是必填选项，呃，基本就是这么泄露的。当然很可能其他信息也泄露了。

下面进入正题，我的演讲的内容分为四个版块：什么叫网络安全、网络安全的重要性、网络安全的现状、如何防范网络安全、打造一个和谐网络。

首先讲一下什么是我们这里所讲的“网络安全”，网络安全呢，就是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。是个高难度的行业啊。

有人说过，“谁掌握领了信息，控制了网络，谁将拥有整个世界。”这句话不完全对啊。不过这点在股市里体现的挺好。从此可见掌握网络是何等的重要，网络安全的重要性也从中体现出来。

在大量网络应用中，安全面临着重大的挑战，事实上，资源共享和安全历来是一对矛盾。在一个开放的网络环境中，大量信息在网上流动，这为不法分子提供了攻击目标。他们利用不同的攻击手段，获得访问或修改在网中流动的敏感信息，闯入用户或政府部门的计算机系统，进行窥视、窃取、篡改数据。不受时间、地点、条件限制的网络诈骗，其“低成本和高收益”又在一定程度上刺激了犯罪的增长。

咱们宝地公司现有两套系统完成建设并已接入网络，oa系统和财务系统，财务系统的重要性自不必说，oa系统，初始密码大家修改了没有?oa系统的建设一般是企业信息化走出的第一步，伴随着使用时间的增加，oa系统日后会积累大量的公司资料，oa系统的好处是大家传输的资料都在本地服务器，而不像使用qq或者其他邮箱等工具，资料保存在对方服务器上，这样数据安全能有一定保证，特别是上市以后。所以密码大家一定要管理好哦。公司呢现在配置有防火墙一台，在一定程度上保护着公司两台服务器的安全。

下面谈一谈大环境下的网络安全现状吧

第一个，诚信问题严峻。随着互联网的发展，尤其是商务类应用的快速发展，许多不法分子纷纷将牟利黑手伸向互联网，导致近年来网络安全威胁和诚信危机事件频发。据《20xx年中国互联网网络安全报告》，20xx年，我国境内被篡改网站数量为16388个，其中政府网站有1802个，有50余个我国网站用户信息数据库在互联网上公开流传或通过地下黑色产业链进行售卖，其中已证实确为真实信息的数据近5000万条。

第二个，信息保护意识淡薄，安全意识亟待提高。这就需要网民，或者我们多多的了解网络安全基础知识，增强网上个人信息的自我保护意识。

第三个，信息网络安全服务行业的发展不够成熟，专业的服务行业都是要收费的，面向个人的网络安全防护产品优秀的较少。个人防护领域的类似于3q大战、金山毒霸全免费之类的事件一直伴随着这几年国内个人网络安全方面的发展，只能说国内个人网络安全产品还有待发展。

关于网络安全，那可以说是恶意代码肆虐，病毒数量爆炸式增长，网络安全形势那是相当的严峻。

网络安全是个问题，而且是无法根治，不容易彻底解决的问题。作为企业，随着企业信息化程度的提高，网络安全方面的投入也是要增加的，选择国内优秀的网络安全服务公司，是一般的解决办法。作为个人用户，我们手段很少，我们只有加强防范，如何做呢?首先，天上不会掉馅饼，不要贪图便宜，不要被一些“中奖陷阱”所迷惑，发来的中奖页面啊，中奖链接不要随便点开。在注册论坛、邮箱等网络工具时，不过多公开个人信息，因为填写信息就等于将信息的保密工作委托于管理方，密码设定不能过于简单，也不要用自己的生日作为密码，至不济用老婆的生日吗，呵呵。还有下载任何资料多到正规网站下，以免文件被捆包木马。网上购物时不要被“钓鱼网”所蒙骗。在自己的pc上装上杀毒软件和防火墙，及时更新安全漏洞，避免黑客入侵。

网络安全是个大课题，好吧，我的小演讲就到这里，祝大家拥有一个安全和谐的网络生活。

谢谢大家!

**描写网络安全个人感悟总结四**

亲爱的同学们：

大家好!很高兴在这里和大家一起探讨有关网络安全的演讲，说到互联网大家应该并不陌生，身为90后的我们生活在21世纪这个信息时代里，是网络让我们的生活更加丰富多彩。 网络在我们的生活中发挥着重要的作用，扮演着重要的角色，我们的衣食住行都离不开网络的联系。网络通讯让我们联系他人更加方便，使世界变成一个地球村，网上购物也方便了我们的生活。身为学生的我们上网可以及时了解实事新闻，开阔视野。真是鼠标一点，大千世界尽收眼底!

可是这样的生活我们真的放心吗?网络带给我们益处的同时就不会给我们带来弊端吗?答案是可想而知的，网络也确确实实给我们带来了很多危险，网络安全问题不容小视。大家可能碰到过，你的qq号被盗?这个很长见吧。网银被盗?文档、照片或者其它数据不见了?正在电脑上看文件的时候，你的鼠标自己动了，这个时候你的系统经被拦截了。这都是黑客和病毒所导致的。同大家分享几个网络安全的事例

“棱镜门”事件的爆发，美国国家安全局监控用户隐私;微软20xx年停止对windows xp安全更新;black hat和def con大会在拉斯维加斯召开，韩国政府等多家网站多次爆发大规模的黑客攻击，瘫痪数小时;美国银行、彭博社等金融机构重要资料遭黑客曝光;apple facebook twitter等科技巨头相继被入侵，用户数据泄露等事件。这些案例虽然离我们很遥远，但是或多或少也影响着我们的生活，给我们带来不便。

下面将网络安全这个大问题分成两个部分来分别解释。

首先要讲一下网络安全的现状：据国家互联网应急中心的数据显示，中国遭受境外网络攻击的情况日趋严重。cncert抽样检测发现境外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。

在我国国内诚信问题日益严重，电子商务的快速发展，许多不法分子纷纷吧牟利黑手伸向互联网。公民的信息保护意识淡薄，安全意识亟待提高。信息网络安全服务行业的发展不够成熟。

关于网络安全，那可以说是恶意代码肆虐，病毒数量爆炸式增长，网络安全形势是相当严峻。

面对如此严峻的形势，我们只有加强防范，要如何做呢?首先天上不会掉馅饼，不要贪图便宜，不要被一些“中奖陷阱”所迷惑，在注册论坛、邮箱等网络工具时，不过多公开个人信息。还有下载任何资料多到正规网站下载，以免文件被捆包木马。网上购物时不要被“钓鱼网”所蒙骗。在自己的pc上装上杀毒软件和防火墙，及时更新安全漏洞，避免黑客入侵。 网络是个缤纷多彩的世界，网络安全也是个重要的课题，希望大家在以后有一个安全丰富的网络生活!

**描写网络安全个人感悟总结五**

尊敬的各位领导、老师，亲爱的同学们：

大家好!今天我演讲的题目是《理性上网 成就梦想》

上网是我们都有过的经历。那么同学们，你们上网又做什么呢?回答最多的是，玩游戏和聊天;其次是看小说、看电影，也有少数同学是看新闻、查资料。

但同学们，过度沉迷网络会让一个人的品行，及身心发展丢失许多。

一、失去诚信

这几年，网络游戏风靡全国，但没有父母会鼓励孩子沉迷网络游戏。每一位做父母的都痛恨孩子沉迷于网络游戏。所以，他们不会给孩子这样一份支出款额。那么，这份钱从哪儿来?先是“省”，从口食里省，省吃俭用，挤出这份钱。继而是“骗”，骗父母，骗亲人，骗同学伙伴，甚至进行抢劫，勒索，走向犯罪的道路。这样的学生，当他们还是一个单纯的孩童时，都怀揣着诚实。可一旦沉迷于网络，就丢失了诚信，丢失了这块生命的黄金。

二、缺乏正义

网络，给了学生一个虚拟的空间，一个自我崇尚、自我膨胀的空间。在这样的空间里，传统的正义正在消失，不断升级的暴力充斥其中。而虚拟世界与现实情境的的虚幻化，也使不少青少年走上犯罪。

三、丧失志向

在少年时，每一个人都有一个意气飞扬的梦想。每一个人都知道，知识是成就梦想飞翔的翅膀。可是沉迷于网络，使那么多的孩子荒废了时光，丧失了志向。网络，会磨灭少年的梦想，也打碎了家人的希望。

四.危害健康

电脑在给我们带来方便的同时，它的危害也是非常大的。其中，辐射对身体的危害不容忽视 ，英国一项研究证实，电脑屏幕发出的低频辐射与磁场，会导致7～19种病症，包括眼部疾病、颈背痛、短暂失去记忆、暴躁及抑郁等。

此外，网络的一些其他危害也不容小视。通过网络买卖个人信息、诈骗、侵犯隐私、散布谣言甚至人身攻击，不仅危害了国家信息安全，影响社会安定，也为公众带来巨大困扰。如果不从立法角度保护个人信息安全，一些网络谣言、网络犯罪便会无孔不入地给人们带来许多不利影响，导致个人信息的泄露，跟商业推销、经济诈骗、造谣生事、人身攻击搅和在一起，后果有多严重不言自明。

青少年，处于人生的黄金时代，美丽的大自然向我们招手，科学的高峰需要我们去攀登，含辛茹苦的父母期望我们健康成长，祖国的未来需要我们去铸造辉煌„„我们该做的实在太多了!一方小小屏幕，岂能涵盖我们生活的全部?

最后，让我们一起做到《全国青少年网络文明公约》:

要善于网上学习 不浏览不良信息 要诚实友好交流 不侮辱欺诈他人 要增强自护意识 不随意约会网友 要维护网络安全 不破坏网络秩序 要有益身心健康 不沉溺虚拟时空

同学们，俗话说：“玩物丧志”。我希望我们每一个同学都能能对网络有清醒的认识，在头脑中建起一道安全的“防火墙”!理性上网，努力学习，成就我们的梦想，成就父母，老师的希望。

**描写网络安全个人感悟总结六**

亲爱的同学们：

大家好!很高兴在这里和大家一起探讨有关网络安全的演讲，说到互联网大家应该并不陌生，身为90后的我们生活在21世纪这个信息时代里，是网络让我们的生活更加丰富多彩。 网络在我们的生活中发挥着重要的作用，扮演着重要的角色，我们的衣食住行都离不开网络的联系。网络通讯让我们联系他人更加方便，使世界变成一个地球村，网上购物也方便了我们的生活。身为学生的我们上网可以及时了解实事新闻，开阔视野。真是鼠标一点，大千世界尽收眼底!

可是这样的生活我们真的放心吗?网络带给我们益处的同时就不会给我们带来弊端吗?答案是可想而知的，网络也确确实实给我们带来了很多危险，网络安全问题不容小视。大家可能碰到过，你的qq号被盗?这个很长见吧。网银被盗?文档、照片或者其它数据不见了?正在电脑上看文件的时候，你的鼠标自己动了，这个时候你的系统经被拦截了。这都是黑客和病毒所导致的。同大家分享几个网络安全的事例

“棱镜门”事件的爆发，美国国家安全局监控用户隐私;微软20xx年停止对windows xp安全更新;black hat和def con大会在拉斯维加斯召开，韩国政府等多家网站多次爆发大规模的黑客攻击，瘫痪数小时;美国银行、彭博社等金融机构重要资料遭黑客曝光;apple facebook twitter等科技巨头相继被入侵，用户数据泄露等事件。这些案例虽然离我们很遥远，但是或多或少也影响着我们的生活，给我们带来不便。

下面将网络安全这个大问题分成两个部分来分别解释。

首先要讲一下网络安全的现状：据国家互联网应急中心的数据显示，中国遭受境外网络攻击的情况日趋严重。cncert抽样检测发现境外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。

在我国国内诚信问题日益严重，电子商务的快速发展，许多不法分子纷纷吧牟利黑手伸向互联网。公民的信息保护意识淡薄，安全意识亟待提高。信息网络安全服务行业的发展不够成熟。

关于网络安全，那可以说是恶意代码肆虐，病毒数量爆炸式增长，网络安全形势是相当严峻。

面对如此严峻的形势，我们只有加强防范，要如何做呢?首先天上不会掉馅饼，不要贪图便宜，不要被一些“中奖陷阱”所迷惑，在注册论坛、邮箱等网络工具时，不过多公开个人信息。还有下载任何资料多到正规网站下载，以免文件被捆包木马。网上购物时不要被“钓鱼网”所蒙骗。在自己的pc上装上杀毒软件和防火墙，及时更新安全漏洞，避免黑客入侵。 网络是个缤纷多彩的世界，网络安全也是个重要的课题，希望大家在以后有一个安全丰富的网络生活!

**描写网络安全个人感悟总结七**

尊敬的各位领导、同事们：

大家好，很高兴能参加这次演讲，生命是如此的精彩，生命是如此的辉煌，不过今天我演讲的内容里没有生死间的大悲恸，也没有平平仄平平的华丽辞藻，我演讲题目是：互联网，精彩而危险的世界。

网络世界呢是一个精彩的世界。qq、网络购物、网络游戏、远程办公，丰富并改变着我们的生活，但是精彩的背后蕴含着危险。大家可曾碰到过，你的qq号被盗?这个很常见吧。网银被盗?文档、照片或者其他数据不见了?正在电脑上看文档的时候，鼠标自己动了，恩，你的系统被劫持了。大家一直以来，都对黑客和病毒有一份“特殊化的感情”，认为所有的黑客都是非常厉害的，所有的病毒都是灾难性的，是吧?同大家分享2个网络安全的案例。

20xx年，中国软件开发联盟csdn，中国最大的开发者技术社区，密码泄漏，超1亿用户密码被泄，黑客在网上公开了一部分用户信息数据库，导致600余万个注册邮箱账号和与之对应的明文密码泄露。这次事件以后，又陆续曝出了多玩网、人人网、搜狗浏览器等安全事件。

唔前面的案例大家没有亲身体会，说个大家接触过的，考过职称考试的人都知道，有时候会被杂志社打电话问到要不要发表职称论文，呵呵，这个大家都有经验吧，恩，很明显你的电话信息泄露了呀，怎么泄露的呢，考职称考试要网上注册报名缴费吧?报名时电话号码是必填选项，呃，基本就是这么泄露的。当然很可能其他信息也泄露了。

下面进入正题，我的演讲的内容分为四个版块：什么叫网络安全、网络安全的重要性、网络安全的现状、如何防范网络安全、打造一个和谐网络。

首先讲一下什么是我们这里所讲的“网络安全”，网络安全呢，就是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。是个高难度的行业啊。

有人说过，“谁掌握领了信息，控制了网络，谁将拥有整个世界。”这句话不完全对啊。不过这点在股市里体现的挺好。从此可见掌握网络是何等的重要，网络安全的重要性也从中体现出来。

在大量网络应用中，安全面临着重大的挑战，事实上，资源共享和安全历来是一对矛盾。在一个开放的网络环境中，大量信息在网上流动，这为不法分子提供了攻击目标。他们利用不同的攻击手段，获得访问或修改在网中流动的敏感信息，闯入用户或政府部门的计算机系统，进行窥视、窃取、篡改数据。不受时间、地点、条件限制的网络诈骗，其“低成本和高收益”又在一定程度上刺激了犯罪的增长。

咱们宝地公司现有两套系统完成建设并已接入网络，oa系统和财务系统，财务系统的重要性自不必说，oa系统，初始密码大家修改了没有?oa系统的建设一般是企业信息化走出的第一步，伴随着使用时间的增加，oa系统日后会积累大量的公司资料，oa系统的好处是大家传输的资料都在本地服务器，而不像使用qq或者其他邮箱等工具，资料保存在对方服务器上，这样数据安全能有一定保证，特别是上市以后。所以密码大家一定要管理好哦。公司呢现在配置有防火墙一台，在一定程度上保护着公司两台服务器的安全。

下面谈一谈大环境下的网络安全现状吧

第一个，诚信问题严峻。随着互联网的发展，尤其是商务类应用的快速发展，许多不法分子纷纷将牟利黑手伸向互联网，导致近年来网络安全威胁和诚信危机事件频发。据《20xx年中国互联网网络安全报告》，20xx年，我国境内被篡改网站数量为16388个，其中政府网站有1802个，有50余个我国网站用户信息数据库在互联网上公开流传或通过地下黑色产业链进行售卖，其中已证实确为真实信息的数据近5000万条。

第二个，信息保护意识淡薄，安全意识亟待提高。这就需要网民，或者我们多多的了解网络安全基础知识，增强网上个人信息的自我保护意识。

第三个，信息网络安全服务行业的发展不够成熟，专业的服务行业都是要收费的，面向个人的网络安全防护产品优秀的较少。个人防护领域的类似于3q大战、金山毒霸全免费之类的事件一直伴随着这几年国内个人网络安全方面的发展，只能说国内个人网络安全产品还有待发展。

关于网络安全，那可以说是恶意代码肆虐，病毒数量爆炸式增长，网络安全形势那是相当的严峻。

网络安全是个问题，而且是无法根治，不容易彻底解决的问题。作为企业，随着企业信息化程度的提高，网络安全方面的投入也是要增加的，选择国内优秀的网络安全服务公司，是一般的解决办法。作为个人用户，我们手段很少，我们只有加强防范，如何做呢?首先，天上不会掉馅饼，不要贪图便宜，不要被一些“中奖陷阱”所迷惑，发来的中奖页面啊，中奖链接不要随便点开。在注册论坛、邮箱等网络工具时，不过多公开个人信息，因为填写信息就等于将信息的保密工作委托于管理方，密码设定不能过于简单，也不要用自己的生日作为密码，至不济用老婆的生日吗，呵呵。还有下载任何资料多到正规网站下，以免文件被捆包木马。网上购物时不要被“钓鱼网”所蒙骗。在自己的pc上装上杀毒软件和防火墙，及时更新安全漏洞，避免黑客入侵。

网络安全是个大课题，好吧，我的小演讲就到这里，祝大家拥有一个安全和谐的网络生活。

谢谢大家!

**描写网络安全个人感悟总结八**

尊敬的各位领导、老师，亲爱的同学们：

大家好!今天我演讲的题目是《理性上网 成就梦想》

上网是我们都有过的经历。那么同学们，你们上网又做什么呢?回答最多的是，玩游戏和聊天;其次是看小说、看电影，也有少数同学是看新闻、查资料。

但同学们，过度沉迷网络会让一个人的品行，及身心发展丢失许多。

一、失去诚信

这几年，网络游戏风靡全国，但没有父母会鼓励孩子沉迷网络游戏。每一位做父母的都痛恨孩子沉迷于网络游戏。所以，他们不会给孩子这样一份支出款额。那么，这份钱从哪儿来?先是“省”，从口食里省，省吃俭用，挤出这份钱。继而是“骗”，骗父母，骗亲人，骗同学伙伴，甚至进行抢劫，勒索，走向犯罪的道路。这样的学生，当他们还是一个单纯的孩童时，都怀揣着诚实。可一旦沉迷于网络，就丢失了诚信，丢失了这块生命的黄金。

二、缺乏正义

网络，给了学生一个虚拟的空间，一个自我崇尚、自我膨胀的空间。在这样的空间里，传统的正义正在消失，不断升级的暴力充斥其中。而虚拟世界与现实情境的的虚幻化，也使不少青少年走上犯罪。

三、丧失志向

在少年时，每一个人都有一个意气飞扬的梦想。每一个人都知道，知识是成就梦想飞翔的翅膀。可是沉迷于网络，使那么多的孩子荒废了时光，丧失了志向。网络，会磨灭少年的梦想，也打碎了家人的希望。

四.危害健康

电脑在给我们带来方便的同时，它的危害也是非常大的。其中，辐射对身体的危害不容忽视 ，英国一项研究证实，电脑屏幕发出的低频辐射与磁场，会导致7～19种病症，包括眼部疾病、颈背痛、短暂失去记忆、暴躁及抑郁等。

此外，网络的一些其他危害也不容小视。通过网络买卖个人信息、诈骗、侵犯隐私、散布谣言甚至人身攻击，不仅危害了国家信息安全，影响社会安定，也为公众带来巨大困扰。如果不从立法角度保护个人信息安全，一些网络谣言、网络犯罪便会无孔不入地给人们带来许多不利影响，导致个人信息的泄露，跟商业推销、经济诈骗、造谣生事、人身攻击搅和在一起，后果有多严重不言自明。

青少年，处于人生的黄金时代，美丽的大自然向我们招手，科学的高峰需要我们去攀登，含辛茹苦的父母期望我们健康成长，祖国的未来需要我们去铸造辉煌……我们该做的实在太多了!一方小小屏幕，岂能涵盖我们生活的全部?

最后，让我们一起做到《全国青少年网络文明公约》:

要善于网上学习 不浏览不良信息 要诚实友好交流 不侮辱欺诈他人

要增强自护意识 不随意约会网友 要维护网络安全 不破坏网络秩序

要有益身心健康 不沉溺虚拟时空

同学们，俗话说：“玩物丧志”。我希望我们每一个同学都能能对网络有清醒的认识，在头脑中建起一道安全的“防火墙”!理性上网，努力学习，成就我们的梦想，成就父母，老师的希望。

**描写网络安全个人感悟总结九**

我局对网络信息安全系统工作一直十分重视，成立了专门的领导组，建立健全了网络安全保密责任制和有关规章制度，由局信息中心统一管理，各科室负责各自的网络信息安全工作。严格落实有关网络信息安全保密方面的各项规定，采取了多种措施防范安全保密有关事件的发生，总体上看，我局网络信息安全保密工作做得比较扎实，效果也比较好，近年来未发现失泄密问题。

一、计算机涉密信息管理情况

今年以来，我局加强组织领导，强化宣传教育，落实工作责任，加强日常监督检查，将涉密计算机管理抓在手上。对于计算机磁介质(软盘、u盘、移动硬盘等)的管理，采取专人保管、涉密文件单独存放，严禁携带存在涉密内容的磁介质到上网的计算机上加工、贮存、传递处理文件，形成了良好的安全保密环境。对涉密计算机(含笔记本电脑)实行了与国际互联网及其他公共信息网物理隔离，并按照有关规定落实了保密措施，到目前为止，未发生一起计算机失密、泄密事故;其他非涉密计算机(含笔记本电脑)及网络使用，也严格按照局计算机保密信息系统管理办法落实了有关措施，确保了机关信息安全。

二、计算机和网络安全情况

一是网络安全方面。我局配备了防病毒软件、网络隔离卡，采用了强口令密码、数据库存储备份、移动存储设备管理、数据加密等安全防护措施，明确了网络安全责任，强化了网络安全工作。

二是信息系统安全方面实行领导审查签字制度。凡上传网站的信息，须经有关领导审查签字后方可上传;二是开展经常性安全检查，主要对sql注入攻击、跨站脚本攻击、弱口令、操作系统补丁安装、应用程序补丁安装、防病毒软件安装与升级、木马病毒检测、端口开放情况、系统管理权限开放情况、访问权限开放情况、网页篡改情况等进行监管，认真做好系统安全日记。

三是日常管理方面切实抓好外网、网站和应用软件“五层管理”，确保“涉密计算机不上网，上网计算机不涉密”，严格按照保密要求处理光盘、硬盘、u盘、移动硬盘等管理、维修和销毁工作。重点抓好“三大安全”排查：一是硬件安全，包括防雷、防火、防盗和电源连接等;二是网络安全，包括网络结构、安全日志管理、密码管理、ip管理、互联网行为管理等;三是应用安全，包括网站、邮件系统、资源库管理、软件管理等。

三、硬件设备使用合理，软件设置规范，设备运行状况良好。

我局每台终端机都安装了防病毒软件，系统相关设备的应用一直采取规范化管理，硬件设备的使用符合国家相关产品质量安全规定，单位硬件的运行环境符合要求，打印机配件、色带架等基本使用设备原装产品;防雷地线正常，对于有问题的防雷插座已进行更换，防雷设备运行基本稳定，没有出现雷击事故;ups运转正常。网站系统安全有效，暂未出现任何安全隐患。

四、通讯设备运转正常

我局网络系统的组成结构及其配置合理，并符合有关的安全规定;网络使用的各种硬件设备、软件和网络接口也是通过安全检验、鉴定合格后才投入使用的，自安装以来运转基本正常。

五、严格管理、规范设备维护

我局对电脑及其设备实行“谁使用、谁管理、谁负责”的管理制度。在管理方面我们一是坚持“制度管人”。二是强化信息安全教育、提高员工计算机技能。同时在局开展网络安全知识宣传，使全体人员意识到了，计算机安全保护是“三防一保”工作的有机组成部分。而且在新形势下，计算机犯罪还将成为安全保卫工作的重要内容。在设备维护方面，专门设置了网络设备故障登记簿、计算机维护及维修表对于设备故障和维护情况属实登记，并及时处理。对外来维护人员，要求有相关人员陪同，并对其身份和处理情况进行登记，规范设备的维护和管理。

六、网站安全及

我局对网站安全方面有相关要求，一是使用专属权限密码锁登陆后台;二是上传文件提前进行病素检测;三是网站分模块分权限进行维护，定期进后台清理垃圾文件;四是网站更新专人负责。

七、安全制度制定落实情况

为确保计算机网络安全、实行了网络专管员制度、计算机安全保密制度、网站安全管理制度、网络信息安全突发事件应急预案等以有效提高管理员的工作效率。同时我局结合自身情况制定计算机系统安全自查工作制度，做到四个确保：一是系统管理员于每周五定期检查中心计算机系统，确保无隐患问题;二是制作安全检查工作记录，确保工作落实;三是实行领导定期询问制度，由系统管理员汇报计算机使用情况，确保情况随时掌握;四是定期组织全局人员学习有关网络知识，提高计算机使用水平，确保预防。

八、安全教育

为保证我局网络安全有效地运行，减少病毒侵入，我局就网络安全及系统安全的有关知识进行了培训。期间，大家对实际工作中遇到的计算机方面的有关问题进行了详细的咨询，并得到了满意的答复。

九、自查存在的问题及整改意见

我们在管理过程中发现了一些管理方面存在的薄弱环节，今后我们还要在以下几个方面进行改进。

(一)对于线路不整齐、暴露的，立即对线路进行限期整改，并做好防鼠、防火安全工作。

(二)加强设备维护，及时更换和维护好故障设备。

(三)自查中发现个别人员计算机安全意识不强。在以后的工作中，我们将继续加强计算机安全意识教育和防范技能训练，让员工充分认识到计算机案件的严重性。人防与技防结合，确实做好单位的网络安全工作。

**描写网络安全个人感悟总结十**

历城六中学校网站于20xx年9月重新改版上线，自新网站运行以来，我校对网络信息安全系统工作一直十分重视，成立了专门的领导组，建立健全了网络安全保密责任制和有关规章制度，由学校谢主任统一管理，各科室负责各自的网络信息安全工作。严格落实有关网络信息安全保密方面的各项规定，采取了多种措施防范安全保密有关事件的发生，总体上看，我校网络信息安全保密工作做得扎实有效。

一、计算机和网络安全情况

一是网络安全方面。我校配备了防病毒软件、，采用了强口令密码、数据库存储备份、移动存储设备管理、数据加密等安全防护措施，明确了网络安全责任，强化了网络安全工作。

二是信息系统安全方面实行领导审查签字制度。凡上传网站的信息，须经有关领导审查签字后方可上传;二是开展经常性安全检查，聘请网站制作公司的技术人员，主要对sql注入攻击、跨站脚本攻击、弱口令、操作系统补丁安装、应用程序补丁安装、防病毒软件安装与升级、木马病毒检测、端口开放情况、系统管理权限开放情况、访问权限开放情况、网页篡改情况等进行监管，认真做好系统安全日记。

三是日常管理方面切实抓好外网、网站和应用软件“五层管理”，确保“涉密计算机不上网，上网计算机不涉密”，严格按照保密要求处理光盘、硬盘、u盘、移动硬盘等管理、维修和销毁工作。重点抓好“三大安全”排查：一是硬件安全，包括防雷、防火、防盗和电源连接等;二是网络安全，包括网络结构、安全日志管理、密码管理、ip管理、互联网行为管理等;三是应用安全，包括网站、邮件系统、资源库管理、软件管理等。

二、学校硬件设备运转正常。

我校每台终端机都安装了防病毒软件，系统相关设备的应用一直采取规范化管理，硬件设备的使用符合国家相关产品质量安全规定，单位硬件的运行环境符合要求，打印机配件、色带架等基本使用设备原装产品;防雷地线正常，对于有问题的防雷插座已进行更换，防雷设备运行基本稳定，没有出现雷击事故;ups运转正常。网站系统安全有效，暂未出现任何安全隐患。

三、严格管理、规范设备维护

我校对电脑及其设备实行“谁使用、谁管理、谁负责”的管理制度。在管理方面我们一是坚持“制度管人”。二是强化信息安全教育、提高员工计算机技能。同时在学校开展网络安全知识宣传，使全体人员意识到了，计算机安全保护是“三防一保”工作的有机组成部分。而且在新形势下，计算机犯罪还将成为安全保卫工作的重要内容。在设备维护方面，专门设置了网络设备故障登记簿、计算机维护及维修表对于设备故障和维护情况属实登记，并及时处理。对外来维护人员，要求有相关人员陪同，并对其身份和处理情况进行登记，规范设备的维护和管理。

四、网站安全及维护

我校对网站安全方面有相关要求，一是使用专属权限密码锁登陆后台;二是上传文件提前进行病素检测;三是网站分模块分权限进行维护，定期进后台清理垃圾文件;四是网站更新专人负责。

五、安全教育

为保证我校网络安全有效地运行，减少病毒侵入，我校就网络安全及系统安全的有关知识进行了培训。期间，大家对实际工作中遇到的计算机方面的有关问题进行了详细的咨询，并得到了满意的答复。

六、自查存在的问题及整改意见

我们在管理过程中发现了一些管理方面存在的薄弱环节，今后我们还要在以下几个方面进行改进。

(一) 网站的安全防护设备还存在不足，只有路由器附带的防火墙，没有硬件版防火墙设备，存在安全隐患。

(二)加强设备维护，及时更换和维护好故障设备。

(三)自查中发现个别人员计算机安全意识不强。在以后的工作中，我们将继续加强计算机安全意识教育和防范技能训练，让员工充分认识到计算机案件的严重性。人防与技防结合，确实做好单位的网络安全工作。

本DOCX文档由 www.zciku.com/中词库网 生成，海量范文文档任你选，，为你的工作锦上添花,祝你一臂之力！