# 202\_年信息安全的心得体会(汇总12篇)

来源：网络 作者：枫叶飘零 更新时间：2024-11-23

*每个人都有自己独特的心得体会，它们可以是对成功的总结，也可以是对失败的反思，更可以是对人生的思考和感悟。那么心得体会怎么写才恰当呢？下面是小编帮大家整理的心得体会范文大全，供大家参考借鉴，希望可以帮助到有需要的朋友。信息安全的心得体会篇一随...*

每个人都有自己独特的心得体会，它们可以是对成功的总结，也可以是对失败的反思，更可以是对人生的思考和感悟。那么心得体会怎么写才恰当呢？下面是小编帮大家整理的心得体会范文大全，供大家参考借鉴，希望可以帮助到有需要的朋友。

**信息安全的心得体会篇一**

随着现代化信息技术的飞速发展，越来越多的人使用互联网来处理各种事务，也越来越多的信息存储在网络中，网络安全问题也随之愈发严重。违法分子利用网络弥补了实体犯罪的不足，造成损失巨大，令人心痛。我也曾因为网络安全问题带来的经济损失而痛苦不堪。为了更好地保护自己的信息安全，我有了以下一些值得分享的思路和经验。

第一段：注意网络信息收集的隐私问题。

在互联网中，我们的每一个动作都有可能被其他人追踪，他们可能利用我们的信息来进行非法活动。为了规避这些问题，我们可以在浏览器中设置隐私模式来避免个人信息泄露，同时不要随意发布自己的隐私信息。除此之外，还可以安装一些网络安全软件来提高自身的安全防护能力。

第二段：坚持使用强密码。

强密码对于保护个人隐私来说非常重要，但是很多人在设置密码的时候往往强烈的提示来自“你的密码过于简单”，但是他们还是选择了极容易被破解的密码。建议每一个人必须制定一个安全的密码策略，每个强密码需包含大小写字母、数字、特殊字符，并尽量使用不同的密码来应对不同的账号和信息存储。

第三段：保持软件升级和补丁更新。

随着技术的不停迭代，在软件的使用过程中就不可避免的会出现各种各样的漏洞和问题，信息窃取等攻击也常常发生这一点比较突出。因此及时安装软件、插件及补丁更新可以规避一些问题的出现，减少安全漏洞的风险。尤其是对于需要输入和存储个人敏感信息的软件或者网站，一定要时刻保持警惕。

第四段：防范网络诈骗。

第二，要养成爱查看此类信息来源检查方式，特别是要查看messages平台发布的相关信息，细心和耐心是我们能够杜绝这类诈骗行为的关键。

第五段：加强教育宣传和网络安全意识。

保护网络安全要从根源开始，对孩子、青少年和普通民众进行网络安全教育、宣传和培训至关重要。我们可以通过各种形式，如广告、博客、微博等多种平台来进行现代化快速专业的社会教育和预防。（1181字）。

总结：以上体会经验来自个人的一些惨痛经历，同时总结本身的建议，每一个因为网络安全问题而蒙受损失的人，都可以从现在开始重新规划一个在网络上更加安全和舒适的生活方式。最后的最后，我们必须保持警醒，让自己成为最好的网络安全教育者和保障者。

**信息安全的心得体会篇二**

本学期我选修了信息安全导论这门课，自从第一堂课，我的观念得到了彻底的改观。首先，老师不是生搬硬套，或者只会读ppt的reader，而是一位真正在传授自己知识的学者，并且老师语言生动幽默，给了人很大的激励去继续听下去。其次，在课堂解到了保护自己信息安全的重要性，而且知道了不良分子窃取信息的诸多荫蔽方法，不禁让人有些后怕，以前从来没有注意到过这类事情，尽管也没有什么特别有价值的文献资料之类的东西，但是对自己的隐私还是十分看重的。此外，看到老师提出的关于期末考试成绩优秀有奖品的事实也十分吸引人，2年选修课还从来没有遇到过这种事情，自小的争胜心告诉我，我一定要好好学习这门课，期末得到那个最好的公仔。

信息安全顾名思义，是指所掌握的信息不被他人窃取的安全属性。由于现代社会科技高速发展，信息的数量以指数级别增加，而科技的进步也催生出很大窃取信息的技术方法，给我们信息安全带来了极大的威胁，不光说我们的个人隐私我发得到合理的保障，甚至一些商业机密乃至也都收到了潜在盗窃者的威胁。因此，如何防范信息的窃取正确的有效的保护自己信息隐私的安全性，如何处理信息被盗所造成的损失，如何亡羊补牢都是亟待解决的问题。信息安全概论这门课正是给我们提供了这样一个学习交流的台，给了我们应对新时期信息安全问题一条出路。

现在的上网环境可谓是“布满荆棘”，正如老师上课时举的例子所说，一项实验，不开杀毒软件的电脑“裸奔”上网，2小时之内就会陷入崩溃，足见上网环境的，这中间可能是因为访问某个网站时给自己电脑中木马、修改了注册表、沾染了病毒，还可能是因为从某个网站上下载的应用软件中自带了木马、病毒，在你不知不觉中已经使电脑陷入了危险，这些病毒有一部分会占用你的资源，破坏你的系统，属于完全是没事找抽型的破坏性病毒，但是另外一些病毒和大部分木马却是居心不良，有些可以你键盘的动作，也就是说你在键盘上的.输入会及时的别人所，同时也有的会强迫打开你的摄像头（前提是你有摄像头并且安装了驱动）来偷窥你所有的动作，我们经常会在一些视频网站或者上看到这样的报道，一对夫妻在房内被另一个城市的无耻网友通过安装木马自动打开摄像头偷拍并被敲诈勒索的事件，这就是这类木马做的坏事。还有的木马会通过你的电脑再次传播，比如老师上课所讲的植入木马成为电脑，进而攻击其它电脑，还有就是我们最常见的qq“尾巴”，首先在qq的对话框中给你说什么我在上看到了一段视频（这类视频前面一般加一些吸引人的定语，如我跳舞的视频，美女视频等等）然后建议你也去看一下，我敢说凡是头一次遇到这种情况的qq使用者80%都会去点开这个网站，于是不点不要紧，点了之后你也会中木马并肆意传播，我就是受害者之一，所以对它更是深恶痛绝（不是抵不住，每个人心里都有好奇心，所以就点开了）。

**信息安全的心得体会篇三**

作为当代信息时代的一员，我们每个人都离不开互联网的使用。而与此同时，也会面临着各种各样的网络安全问题，例如：病毒、恶意软件、黑客攻击等等，这些问题都给我们的信息安全带来了很大的威胁。在长期的网络使用中，我积累了一些关于信息网安全的心得体会，希望能与大家分享。

第一段：自身防范意识的培养。

信息安全的第一道防线是自身防范意识的培养。在长期的网络使用中，我会尽可能避免上陌生、不可信的网站，不轻易下载未知来源的软件。保证电脑、手机等设备的安全设置，进行定期的病毒检查和系统升级。同时还要加强密码管理，使用强密码以及不同网站使用不同密码，不轻易将密码透露给他人，防范盗号。这些都是我们个人信息安全的保证，也是前提。

第二段：对网络攻击的了解。

随着网络攻击技术的不断进步，我们也要时刻关注网络安全威胁的的动态，了解通过哪些方式对网络进行攻击。例如：钓鱼邮件、网络欺诈、拦截数据等等，对于这些我们需要时刻保持警惕。遇到可疑的邮件、信息，切勿轻易打开链接。正确处理和举报非法信息，维护自己权益的同时也起到了社会的维护作用。

第三段：保密意识的加强。

在网络使用中，我们也会受到来自我们身边人的威胁。有些人盗用他人的个人信息或账户进行恶意行为，所以保密意识也需要加强。在网上尽量减少透露自己的敏感信息，比如银行卡账号、个人的联系方式，并需要在网络使用中保持隐私，避免丢失重要资料或者受到别人的利用。

第四段：软件、系统的更新。

随着功能不断的丰富，软件安全问题也越来越多，所以软件系统的更新也是信息安全的关键。不断更新软件、系统，及时修补各种漏洞和安全问题，保证软件和系统的运行安全性。

第五段：注意社会风险。

网络安全不仅是个人安全，也是整个社会的安全，我们还需要注意哪些在网络上可能会存在风险的事物。比如：钓鱼诈骗、非法贩卖信息等等，我们需要辨别、制止这个类别的违法行为，不仅保护自己，还要通过自身的力量和社会力量共同维护网络安全。

总之，信息安全至关重要，懂得如何保护自己才能更好地利用互联网。这正如一句话所说：“网络是一把双刃剑，使用得当，你会得到便捷；使用不当，你会自食其果。”希望我们通过不断地关注安全问题、不断强化自身的保护意识，建立更加安全的网络环境。

**信息安全的心得体会篇四**

《条例》明确，重点行业和领域重要网络设施、信息系统属于关键信息基础设施，国家对关键信息基础设施实行重点保护，采取措施，监测、防御、处置来源于境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治违法犯罪活动。

“关键信息基础设施涉及公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益。”中国电子信息产业发展研究院网络安全所所长刘权对《经济参考报》记者表示，随着信息化的快速普及和发展，关键信息基础设施作为事关国家安全和社会稳定的重要战略资源的地位日益凸显，为国家机构、各行业正常运转提供必需的支撑和服务，加强对关键信息基础设施的保护是社会持续运转的重要保障。

《条例》明确了监督管理体制，规定在国家网信部门统筹协调下，国务院公安部门负责指导监督关键信息基础设施安全保护工作。国务院电信主管部门和其他有关部门依照《条例》和有关法律、行政法规的规定，在各自职责范围内负责关键信息基础设施安全保护和监督管理工作。

《条例》明确运营者责任义务，对关键信息基础设施运营者落实网络安全责任、建立健全网络安全保护制度、设置专门安全管理机构、开展安全监测和风险评估、报告网络安全事件或网络安全威胁、规范网络产品和服务采购活动等作了规定。

刘权表示，《条例》对运营者的要求更为明确和具体，便于运营者贯彻落实；同时运营者的安全责任也更加清晰，并确定到具体担责人，督促运营者主要负责人真正推动《条例》执行。下一步运营者需要落实主体责任，建立网络安全保障体系。高度重视安全保护工作，合规做好系统建设相关工作。同时根据要求，做好定期开展网络安全检测和风险评估工作。

奇安信集团安全专家杨波也对《经济参考报》记者表示，下一步运营者需加大对关键信息基础设施安全保护的保障力度。一是保障相关资金落实，加强网络安全建设资金的集约化管理与使用，平衡分配网络安全建设投资。二是壮大网络安全队伍，完善关键信息基础设施防护网络安全组织体系，健全网络安全从业资质要求和持证上岗制度。三是强化面向效果的安全考核，建立安全评价指标体系和安全项目监控评价指标体系，通过数据为安全管理工作提供依据，为安全能力建设提供决策支持。四是加强网络安全意识教育。树立科学正确的网络安全观，常态化开展全员网络安全意识教育培训。

**信息安全的心得体会篇五**

以来，就网络安全和信息化工作发表了系列重要讲话，深刻回答了网络安全工作的一系列重大理论和现实问题，为网络安全工作指明了前进方向。

今年4月19日，在网络安全和信息化工作座谈会上，站在全球信息和网络空间竞争的战略高度，深刻剖析了当前网络安全和信息化工作面临的新形势，系统阐述了更好推进网络强国建设需要的六大问题。讲话围绕践行“十三五”发展新理念、谋求网络空间战略主动、维护网络安全、建设良好网络生态、完善信息社会治理等领域，提出了许多富有创建的新思想新论断。全面学习贯彻最新讲话精神，做好新形势下网络安全工作，需要把握好一个目标和两对关系。

(一)围绕“一个目标”

在网信小组第一次会议上明确提出我们的战略目标就是要建设网络强国。网络安全是事关和国家发展、事关广大人民群众工作生活的重大战略问题。在“4.19”讲话中，回顾到：“我国曾经是世界上的经济强国，后来在欧洲发生工业、世界发生深刻变革的时期，丧失了与世界同进步的历史机遇，逐渐落到了被动挨打的境地。”这提醒我们顺应大势，把握历史机遇的极端重要性，落后就要挨打，弱国没有话语权，凝心聚力实现“两个一百年”奋斗目标是民族的最高利益和根本利益。当前新一轮科技和产业变革蓄势待发，全球竞争格局发生深刻调整，带给民族新的历史机遇，我们必须毫不动摇的把握机遇，将建设网络强国与“两个一百年”奋斗目标同步推进，实现“网络基础设施基本普及、自主创新能力显著增强、信息经济全面发展、网络安全保障有力”，达到“技术先进、产业发达、攻防兼备、制网权尽在掌握、网络安全坚不可摧”。

(二)把握“两对关系”

首先是衡好信息化发展和网络安全的关系。我国信息化发展已经进入“促发展”与“保安全”并重的阶段，适应阶段特征，把握客观实际，处理好发展与安全的关系尤为关键。指出“安全是发展的前提，发展是安全的保障，安全和发展要同步推进。”一方面，要认识到信息化发展“不进则退、慢进亦退”，发展中的问题要通过发展解决，不发展才是最大的不安全，在各国都着力抢占网络空间制高点的时期，信息化发展慢人一步，就会导致我国在信息时代的再次落后。另一方面，也要认识网络安全基石不牢固，信息化发展越快，存在的隐患也越大。网络安全是底线、红线，网络安全出了问题，核心网络和关键数据遭遇入侵和泄露，其他方面做得再好也失去了意义。

第二是处理好对外开放和产业自主的关系。掌握网络空间“制网权”，实现由“跟跑者”向“领跑者”转变，既要坚持开放竞争，又要走自主创新的道路，两者并不矛盾。明确指出：“自主创新首先是技术自主，要分清哪些技术可以站在别人肩膀上搞好引进消化吸收再创新，做好安全可控就行;哪些技术必须自主创新、自立自强”。因此，在保障安全的基本前提下，既要充分引进先进技术提升产业发展水，也要给国产技术和设备充分的尝试空间，构建起内部外部“双轮驱动”，相互切磋、相得益彰的良性循环。

当前，我国正处于全面建成小康社会的决胜阶段，经济大调整、大转型成为时代主旋律，同时，全球新一轮信息技术产业变革蓬勃兴起，关键技术交叉融合、群体跃进，与我国加快转变经济发展方式形成历史汇。在这一背景下，网络空间与现实世界从逐步交叉走向全面融合，网络空间的行为特点、思维方式及模式等向现实社会渗透，网络安全态势呈现新特点、新趋势。一方面，境内络攻击活动日趋频繁，网络攻击的来源越来越多样化，网络攻击的手法更加复杂隐蔽，攻击类型也从短时间、突发性攻击向高级别、持续性攻击转变，网络攻击和安全防御在信息层面、层面的不对称现象都十分突出。另一方面，新技术新业务带来的网络安全问题逐渐凸显。云计算、大数据、物联网、网络功能虚拟化等快速发展，带动信息系统软硬件架构的全新变革，在软件、硬件、协议等多方面引入未知的威胁隐患;规模化数据采集、网络和用户数据向云端不断集中、大规模跨境服务，导致数据和用户隐私安全威胁不断涌现。新形势下，坚持多措并举、重点突破、全面推进，加快建成完善有力的网络安全保障体系，维护国家网络安全，意义重大，任务艰巨。

(一)积极推进网络安全顶层设计和法制化建设。

古语有言，“先谋后事者昌，先事后谋者亡”。面对网络安全这一重大问题，要充分发挥战略的牵引和带动作用，完善建设和立法保障。一是积极参与制定《国家网络空间安全战略》等顶层设计工作，公开阐释我国网络空间的基本主张、重大立场。二是建立健全网络安全相关法律法规体系，积极推动出台《网络安全法》、《关键信息基础设施安全保护办法》等，加快推进用户信息安全保护、跨境数据流动分类监管等立法。三是适应云计算、物联网、大数据、下一代互联网等新技术新业务发展要求，加快推进相关网络安全管理的研究与制定。

(二)加快完善网络和数据安全保障体系。

一是强化关键信息基础设施保护。将关键信息基础设施保护提升到国家战略高度，明确关键信息基础设施保护的原则、目标和措施，探索建立关键信息基础设施清单，健全分级保护、动态调整的关键信息基础设施网络安全防护体系，强化风险管理，在关键领域大力推进自主创新、安全可控的.软硬件应用。二是加强网络数据和用户信息保护。完善网络数据资产保护，加强网络数据全生命周期的安全保护，明确企业数据采集、传输、存储、使用、共享等各环节的主体责任和具体要求，督促企业落实用户个人信息防窃密、防篡改等安全防护措施;督促落实数据资产分类分级保护要求，建立健全数据操作审计机制和数据安全评估认证体系。三是构建全局性、整体化的态势感知体系，变被动应对为主动防御。建设完善的网络防御能力体系，积极开展网络空间大数据挖掘和分析，提升对国家级、有网络攻击威胁的发现、预警和防御能力。加强网络安全突发事件预警能力建设，强化应急预案演练，提升应急状态下的网络安全事件应对以及协同处置能力。

(三)做大做强自主可控的信息技术产业。

强调，“我们要掌握我国互联网发展主动权、保障互联网安全、，就必须突破核心技术这个难题”。突破核心技术，要坚定不移地实施创新驱动发展战略，提升信息通信关键技术、产品的自主研发和产业化能力。一是夯实信息产业基础。落实好《国家集成电路产业发展推进纲要》，做好引导产业发展、和公共服务，着力解决自主产业发展面临的突出问题。大力关键基础网络设备的研发和应用，重点高端服务器、路由器等核心网络设备产业发展，提升安全性和可靠性。二是顺应大众创业、万众创新趋势，加强网络安全产业引导，以采购为引导，推动形成安全产品与服务均衡理念，统筹优化安全产品和服务市场格局;引导建设区域性安全产业基地，促进产业集聚发展，推动加快安全技术和企业孵化速度。三是壮大企业，构建全产业链协同发展格局。加快发展和形成一批掌握关键核心技术、创新能力突出、国际竞争力强的跨国大公司，促进中小企业向“专、精、特、新”方向发展，与大企业共同构建合理分工体系，加强企业间的良性互动和协同发展，推动形成密切合作的研发体系，壮大企业集群，形成产业集聚优势。

(四)强化网络安全人才队伍建设。

网络空间的竞争，归根结底是人才竞争。保障网络安全和，没有一支优秀的人才队伍，没有人才创造力迸发、活力涌流，是难以成功的。一是创新网络安全人才培养方式。积极推进网络空间安全学科建设，深化网络安全领域产教结合，依托高校、科研机构、企业的智力资源和研究台，建立一批联合培训基地，加快跨学科、跨领域的人才培养。二是用好用活网络安全人才。人尽其才百事兴，只有把广大网络安全人才的积极性充分调动起来，创新成果才会源源不断涌现。要探索建立适应网络安全事业发展特点的人事、薪酬，把优秀人才凝聚到技术部门、研究部门、管理部门中来。建立灵活的人才激励机制，让作出贡献的人才有成就感、获得感，让更多优秀人才能够脱颖而出、一展身手。三是推进国际人才交流合作。在人才选拔上要有全球视野，加大高精尖人才引进力度，改进人才引进相关配套，吸引更多的领才、紧缺人才在我国从事网络安全相关教学科研活动，构建具有全球竞争力的人才体系。

**信息安全的心得体会篇六**

随着互联网的普及和信息化程度的不断提高，信息安全问题也越来越成为人们关注的焦点。我作为一名信息技术从业人员，也深深地体会到了信息安全的重要性。在这里，我将分享我的一些心得体会。

第一段：了解信息安全的基本知识。

信息安全是一个广泛的概念，它包括了很多方面。首先，我们需要了解信息安全的基本知识，例如各种攻击方式、漏洞及其修补方法、加密技术和安全策略等等。只有了解了这些基本知识，才能更好地保护信息安全。

信息安全对于个人和组织来说都是至关重要的。个人往往需要保护自己的身份信息、财务信息和隐私信息等，而组织则需要保护自己的商业机密、专利、客户信息等。信息泄露或遭受攻击都会给个人和组织带来严重的后果，例如财务损失、信誉损失、法律责任等。

信息安全不是一次性的事情，而是需要长期的管理和维护。信息安全管理包括制定安全策略和规范、用户培训和意识提高、安全审计和漏洞管理等。这些管理工作需要全面、系统地考虑，才能更好地保障信息安全。

第四段：个人信息保护。

作为个人，我们也需要关注自己的信息安全。我们需要妥善保管自己的身份证件、银行卡和其他重要文档，避免输入个人信息时被网络钓鱼等手段诈骗。此外，我们还需要定期更换密码、使用安全软件和防火墙等措施来防范外部攻击。

信息安全问题与我们的工作和生活密切相关，未来的社会也将更加信息化。我们需要时刻保持警惕，加强信息安全意识，利用最先进的技术和方法保障信息安全。只有这样，我们才能更好地适应未来的发展。

总结：

随着技术的飞速发展和互联网的不断普及，信息安全已经成为人们生活中不可忽视的重要问题。作为信息技术从业人员，我们需要时刻关注信息安全问题，加强信息安全意识，掌握信息安全的基本知识和技能，及时采取措施进行防御和修复。只有这样，我们才能更好地保护信息安全，让我们的生活更加安全和便捷。

**信息安全的心得体会篇七**

十八大以来，习近平总书记就网络安全和信息化工作发表了系列重要讲话，深刻回答了网络安全工作的一系列重大理论和现实问题，为网络安全工作指明了前进方向。

今年4月19日，习近平总书记在网络安全和信息化工作座谈会上，站在全球信息革命和网络空间竞争的战略高度，深刻剖析了当前网络安全和信息化工作面临的新形势，系统阐述了更好推进网络强国建设需要高度重视的六大问题。讲话围绕践行“十三五”发展新理念、谋求网络空间战略主动、维护网络安全、建设良好网络生态、完善信息社会治理等领域，提出了许多富有创建的新思想新论断。全面学习贯彻习近平总书记最新讲话精神，做好新形势下网络安全工作，需要把握好一个目标和两对关系。

(一)围绕“一个目标”

习近平总书记在中央网信小组第一次会议上明确提出我们的战略目标就是要建设网络强国。网络安全是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题。在“4.19”讲话中，习近平总书记回顾到：“我国曾经是世界上的经济强国，后来在欧洲发生工业革命、世界发生深刻变革的时期，丧失了与世界同进步的历史机遇，逐渐落到了被动挨打的境地。”这提醒我们顺应大势，把握历史机遇的极端重要性，落后就要挨打，弱国没有话语权，凝心聚力实现“两个一百年”奋斗目标是中华民族的最高利益和根本利益。当前新一轮科技革命和产业变革蓄势待发，全球竞争格局发生深刻调整，带给中华民族新的历史机遇，我们必须毫不动摇的把握机遇，将建设网络强国与“两个一百年”奋斗目标同步推进，实现“网络基础设施基本普及、自主创新能力显著增强、信息经济全面发展、网络安全保障有力”，达到“技术先进、产业发达、攻防兼备、制网权尽在掌握、网络安全坚不可摧”。

(二)把握“两对关系”

首先是平衡好信息化发展和网络安全的关系。我国信息化发展已经进入“促发展”与“保安全”并重的阶段，适应阶段特征，把握客观实际，处理好发展与安全的关系尤为关键。习近平总书记指出“安全是发展的前提，发展是安全的保障，安全和发展要同步推进。”一方面，要认识到信息化发展“不进则退、慢进亦退”，发展中的问题要通过发展解决，不发展才是最大的不安全，在各国都着力抢占网络空间制高点的时期，信息化发展慢人一步，就会导致我国在信息时代的再次落后。另一方面，也要认识网络安全基石不牢固，信息化发展越快，存在的隐患也越大。网络安全是底线、红线，网络安全出了问题，核心网络和关键数据遭遇入侵和泄露，其他方面做得再好也失去了意义。

第二是处理好对外开放和产业自主的关系。掌握网络空间“制网权”，实现由“跟跑者”向“领跑者”转变，既要坚持开放竞争，又要走自主创新的道路，两者并不矛盾。习近平总书记明确指出：“自主创新首先是技术自主，要分清哪些技术可以站在别人肩膀上搞好引进消化吸收再创新，做好安全可控就行;哪些技术必须自主创新、自立自强”。因此，在保障安全的基本前提下，既要充分引进国外先进技术提升国内产业发展水平，也要给国产技术和设备充分的尝试空间，构建起内部外部“双轮驱动”，相互切磋、相得益彰的良性循环。

当前，我国正处于全面建成小康社会的决胜阶段，经济大调整、大转型成为时代主旋律，同时，全球新一轮信息技术产业变革蓬勃兴起，关键技术交叉融合、群体跃进，与我国加快转变经济发展方式形成历史性交汇。在这一背景下，网络空间与现实世界从逐步交叉走向全面融合，网络空间的行为特点、思维方式及组织模式等向现实社会渗透，网络安全态势呈现新特点、新趋势。一方面，境内外网络攻击活动日趋频繁，网络攻击的来源越来越多样化，网络攻击的手法更加复杂隐蔽，攻击类型也从短时间、突发性攻击向高级别、持续性攻击转变，网络攻击和安全防御在信息层面、手段层面的不对称现象都十分突出。另一方面，新技术新业务带来的网络安全问题逐渐凸显。云计算、大数据、物联网、网络功能虚拟化等快速发展，带动信息系统软硬件架构的全新变革，在软件、硬件、协议等多方面引入未知的威胁隐患;规模化数据采集、网络和用户数据向云端不断集中、大规模跨境服务，导致数据和用户隐私安全威胁不断涌现。新形势下，坚持多措并举、重点突破、全面推进，加快建成完善有力的网络安全保障体系，维护国家网络安全，意义重大，任务艰巨。

(一)积极推进网络安全顶层设计和法制化建设

古语有言，“先谋后事者昌，先事后谋者亡”。面对网络安全这一重大问题，要充分发挥战略的牵引和带动作用，完善制度建设和立法保障。一是积极参与制定《国家网络空间安全战略》等顶层设计工作，公开阐释我国网络空间的基本主张、重大立场。二是建立健全网络安全相关法律法规制度体系，积极推动出台《网络安全法》、《关键信息基础设施安全保护办法》等，加快推进用户信息安全保护、跨境数据流动分类监管等立法。三是适应云计算、物联网、大数据、下一代互联网等新技术新业务发展要求，加快推进相关网络安全管理制度的研究与制定。

(二)加快完善网络和数据安全保障体系

一是强化关键信息基础设施保护。将关键信息基础设施保护提升到国家战略高度，明确关键信息基础设施保护的原则、目标和制度措施，探索建立关键信息基础设施清单制度，健全分级保护、动态调整的关键信息基础设施网络安全防护体系，强化风险管理，在关键领域大力推进自主创新、安全可控的软硬件应用。二是加强网络数据和用户信息保护。完善网络数据资产保护制度，加强网络数据全生命周期的安全保护，明确企业数据采集、传输、存储、使用、共享等各环节的主体责任和具体要求，督促企业落实用户个人信息防窃密、防篡改等安全防护措施;督促落实数据资产分类分级保护要求，建立健全敏感数据操作审计机制和数据安全评估认证体系。三是构建全局性、整体化的态势感知体系，变被动应对为主动防御。建设完善的网络防御能力体系，积极开展网络空间大数据挖掘和分析，提升对国家级、有组织网络攻击威胁的发现、预警和防御能力。加强网络安全突发事件预警能力建设，强化应急预案演练，提升应急状态下的网络安全事件应对以及协同处置能力。

(三)做大做强自主可控的信息技术产业

习近平总书记强调，“我们要掌握我国互联网发展主动权、保障互联网安全、国家安全，就必须突破核心技术这个难题”。突破核心技术，要坚定不移地实施创新驱动发展战略，提升信息通信关键技术、产品的自主研发和产业化能力。一是夯实信息产业基础。落实好《国家集成电路产业发展推进纲要》，做好引导产业发展、政策支持和公共服务，着力解决自主产业发展面临的突出问题。大力支持关键基础网络设备的研发和应用，重点支持高端服务器、路由器等核心网络设备产业发展，提升安全性和可靠性。二是顺应大众创业、万众创新趋势，加强网络安全产业政策引导，以政府采购为引导，推动形成安全产品与服务均衡理念，统筹优化安全产品和服务市场格局;引导建设区域性安全产业基地，促进产业集聚发展，推动加快安全技术和企业孵化速度。三是壮大国内企业，构建全产业链协同发展格局。加快发展和形成一批掌握关键核心技术、创新能力突出、国际竞争力强的跨国大公司，促进中小企业向“专、精、特、新”方向发展，与大企业共同构建合理分工体系，加强企业间的良性互动和协同发展，推动形成密切合作的研发体系，壮大企业集群，形成产业集聚优势。

(四)强化网络安全人才队伍建设

网络空间的竞争，归根结底是人才竞争。保障网络安全和国家安全，没有一支优秀的人才队伍，没有人才创造力迸发、活力涌流，是难以成功的。一是创新网络安全人才培养方式。积极推进网络空间安全学科建设，深化网络安全领域产教结合，依托高校、科研机构、企业的智力资源和研究平台，建立一批联合培训基地，加快跨学科、跨领域的人才培养。二是用好用活网络安全人才。人尽其才百事兴，只有把广大网络安全人才的积极性充分调动起来，创新成果才会源源不断涌现。要探索建立适应网络安全事业发展特点的人事制度、薪酬制度，把优秀人才凝聚到技术部门、研究部门、管理部门中来。建立灵活的人才激励机制，让作出贡献的人才有成就感、获得感，让更多优秀人才能够脱颖而出、一展身手。三是推进国际人才交流合作。在人才选拔上要有全球视野，加大高精尖人才引进力度，改进人才引进相关配套制度，吸引更多海外的领军人才、紧缺人才在我国从事网络安全相关教学科研活动，构建具有全球竞争力的人才制度体系。

**信息安全的心得体会篇八**

作为信息技术的从业者，无论是个人还是企业，信息安全都是必须重视的。现在，我们的生活和工作几乎离不开互联网，信息泄露和黑客攻击越来越常见。保护好个人和企业的信息安全已经成为我们的应有之责。下面，我将分享自己在日常工作中总结出的几点经验和体会。

一、重视密码安全。

从电子邮件、网银到各种APP，无论是个人的账号还是公司的帐户，都需要设定密码。这些密码的安全性，直接影响到其他信息、甚至财产安全。密码不宜过于简单，最好采用纯数字、字母、字符组成的复杂密码，并定期更换。

二、定期备份数据。

备份是信息安全的最后一道防线。定期备份数据可以防止数据丢失，同时可以在被攻击时快速恢复数据。例如，个人数据可以备份到云端，而企业的重要业务数据则需要定期备份至离线存储介质中。

三、安装有效的杀毒软件和防火墙。

电脑和手机等设备需要安装杀毒软件和防火墙抵御网络攻击，减少受到恶意软件、病毒和木马等威胁的风险。同时，定期更新安全补丁也是非常必要的。

四、不轻易相信陌生人的信息。

现在，电信诈骗越来越多，往往通过社交软件或电子邮件等方式冒充熟人骗取信息。为了避免被骗，我们需时刻保持清醒的头脑，不轻易相信陌生人的信息。

五、加强员工的信息安全意识。

企业内部信息泄露和外部攻击是信息安全的另一大风险，漏洞总是在人性弱点中出现。为此，企业应该加强员工的信息安全意识，培养良好的保密习惯并加强内部管理。企业领导可以倡导建立信息安全文化，让员工知晓信息安全的重要性，并且严格执行信息安全计划。

总之，信息安全对于个人和企业来说都是至关重要的。在日常的工作生活中，我们必须牢记以上几点，尽可能减少受到网络攻击和数据泄露的风险，保护我们自己和家人的财产和隐私安全。同时，企业也要加强信息安全领域的投入，提高保护自身信息资产的能力。

**信息安全的心得体会篇九**

第一段：引言（200字）。

信息安全是我们在当今数字化时代面临的重要问题之一。作为一个信息安全小白，我在学习过程中深刻体会到了信息安全的重要性以及如何保护个人信息安全的方法。在这篇文章中，我将分享一些自己的心得体会，希望可以为其他信息安全小白提供一些指引。

第二段：了解信息安全（200字）。

在学习信息安全的过程中，我首先明确了信息安全的概念和重要性。信息安全涉及到我们在网络上与人交流、存储个人资料，时刻要警惕那些可能侵犯我们隐私和造成损害的风险。了解了这些基本概念后，我开始关注自己在日常生活中可能面临的信息安全问题。

第三段：保护个人信息安全的方法（300字）。

为了保护个人信息安全，我开始采取一系列的预防措施。首先，我注意了密码安全，始终使用复杂且不易破解的密码，同时定期更换密码，并不在多个平台使用同一密码。其次，我注重保护隐私，不随便在公共场所或社交媒体上泄露个人的敏感信息，如住址、手机号等。另外，我也尽量避免点击可疑的链接和附件，以防止遭遇钓鱼网站和恶意软件的攻击。此外，我还安装了可靠的防病毒软件和防火墙，对设备进行定期检查和更新，确保自己的设备和信息受到全面的保护。

第四段：提高信息安全意识（300字）。

除了采取个人保护措施，提高信息安全意识也非常重要。我认为，了解常见的网络攻击手段和识别欺诈行为，比如诈骗电话和电子邮件，是必要的。此外，我还提高了对隐私政策和服务条款的关注度，不随意接受各种应用或网站的信息采集请求。同时，我也尽量使用官方的应用商店来下载应用，以减少恶意软件的风险。通过不断学习和实践，我逐渐形成了自己的信息安全意识。

第五段：结语（200字）。

通过学习和实践，我认识到信息安全对个人和社会的重要性，并且采取了一系列的措施来保护自己的个人信息。与此同时，我也愿意将我所学到的知识和经验分享给其他信息安全小白，希望可以共同提高信息安全意识，共建一个更加安全的网络环境。信息安全不仅仅是个人的事情，也是每个人应该关注和行动的重要问题。只有我们共同努力，才能打造一个更加安全的信息世界。

**信息安全的心得体会篇十**

作为一个网络时代的人，信息安全对于我们来说是非常重要的。在我的使用电脑和网络的过程中，我深刻体会到了信息安全的重要性，也明白了一些信息安全知识。在这篇文章中，我将分享我的心得体会。

第一段：了解信息安全的重要性。在我初次接触网络时，并没有意识到信息安全的重要性，很多时候我甚至将个人信息泄露给一些不熟悉的人。后来，我发现一些不法分子会利用这些信息进行犯罪活动，比如诈骗、盗取个人隐私等。这些经历让我深刻体会到信息安全的重要性。我们不仅要意识到信息的重要性，还需要加强信息安全的保护措施。

第二段：信息保护知识的重要性。为了更好地保护个人信息的安全，我开始了解一些信息保护知识。比如，不要使用简单的密码，不要将个人信息随意公开等等。此外，定期更换密码也是非常重要的。当然，不能够完全避免遇到信息安全问题，但我们需要加强信息安全保护措施，以减少信息被盗取的危险。

第三段：信息安全与网络社交。在社交网络上，我们经常发布一些个人信息，比如姓名、性别、出生日期等。其实，在社交网络上公开个人信息很危险，模拟用户进行诈骗活动的不法分子可能在这些信息中寻找目标。解决这些问题的一个办法是仔细阅读隐私政策，合理设置隐私设置，并避免公开敏感信息。

第四段：软件安全性的重要性。不良软件是信息安全的重要威胁之一。需要我们安装有信誉保证的软件，并保持升级到最新版本。在下载和安装软件时要小心谨慎，并免费下载不知名软件。最好使用正版软件和防病毒软件。这样可以避免操作系统和软件的漏洞被利用，从而更好地保护信息安全。

第五段：信息安全与注意力的平衡。在网络上，我们经常在寻找有用信息的同时容易分散注意力，而不注意信息安全问题，这是非常危险的。我们不能因为追求网络世界中的有趣和有用的信息而牺牲了我们自身的信息安全。我们需要平衡注意力，注意信息安全和人身安全的保护，在适当的时候更加警惕和小心。

总之，信息安全是网络时代中极为重要的问题，我们应该充分认识到信息安全的重要性，并加强保护措施。同时，要注意到信息安全与注意力的平衡，尽量防止被网络上的有趣和有用信息所迷惑。通过学习更多的信息安全知识，我们可以更好地保护个人信息的安全，避免受到信息泄露的风险。

**信息安全的心得体会篇十一**

二十世纪末的今天，世界继新技术以后，又掀起了一场以加速社会信息化为宗旨的信息高速公路建设的浪潮。信息正以其前所未有的迅猛态势渗透于社会的方方面面，改变着人们原有的社会空间。作为信息传播的重要媒介计算机互连网络正在成为人类社会的重要组成部分，为人们的学习、生活和工作提供了前所未有的便利和快捷。然而，计算机网络也像其它事物一样，在产生积极影响的同时，必会产生一些负面效应。随着网络的飞速发展部分人也迈入了小活并拥有了电脑。而随着计算机网络技术的快速发展，计算机功能的多样化与信息处理的复杂程度也显著提高。越来越多的人学会了上网，通过网络购物，购买虚拟产品等，然而，随之而来的便是网络的安全和道德问题。越来越多的人在网络上被欺骗，有很多的网络诈骗，让人民受害，也有很多负面的网络信息、网络需要我们正确面对。学会维护自己的合法权益，网络是一把举世闻名的“双刃剑”。剑一出鞘就光彩四照，人人都喜欢、赞叹；可挥舞起来就“不见血”，人人谈它色变。所以当我们使用它时一定要慎重：一方面可以利用它好的一面来帮助自己，另一方面要时刻提高警惕，树立保护自己的意识，防止被这把“双刃剑”“刺”伤。

首先我们应该加强网络公德自律，个人认为需要加强以下几个方面：一是正确使用学习；二是要健康进行网络交往；三是自觉避免沉迷网络；四是要养成网络自律精神。另外还要对于网上出现的病毒要加以防范，由于网路储存信息量大，一些东西是有害、虚假、的同时信息道德问题应受到关注，例如知识产权、个人隐私、信息安全、信息共享等都要进行尊重。在网络中，为了很好的保护自己的信息安全，我认为应该做到以下几点：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、诺顿、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、在安装从网上下载的软件时一定要一步步来，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软件，软件又是极不容易卸载的，这些软件可能会修改你的注册表，修改你的主页，定期打开某一网页，在ie中增加令人感到恶心的工具条等等，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的偏好，随时给我们发过来垃圾广告。所以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。姑且就某些破坏性的病毒可能导致移动存储设备损坏不说。单说安全性上我们通过上文的论述也可以看出，使用移动存储设备带来的信息被窃取的威胁有多大，有些公司为了防止商业机密被窃取甚至直接要求员工把电脑中的usb接口封死，利用光盘刻录的方法进行相互之间资料信息的传播，可谓是用心良苦。我们在使用u盘之类的存储设备时也要小心谨慎。

**信息安全的心得体会篇十二**

二十世纪末的今天，世界继新技术革命以后，又掀起了一场以加速社会信息化为宗旨的信息高速公路建设的浪潮。信息正以其前所未有的迅猛态势渗透于社会的方方面面，改变着人们原有的社会空间。作为信息传播的重要媒介计算机互连网络正在成为人类社会的重要组成部分，为人们的学习、生活和工作提供了前所未有的便利和快捷。然而，计算机网络也像其它事物一样，在产生积极影响的同时，必会产生一些负面效应。随着网络的飞速发展部分人也迈入了小康生活并拥有了电脑。而随着计算机网络技术的快速发展，计算机功能的多样化与信息处理的复杂程度也显著提高。越来越多的人学会了上网，通过网络购物，购买虚拟产品等，然而，随之而来的便是网络的安全和道德问题。越来越多的人在网络上被欺骗，有很多的网络诈骗，让人民受害，也有很多负面的网络信息、网络言论需要我们正确面对。学会维护自己的合法权益，网络是一把举世闻名的“双刃剑”。剑一出鞘就光彩四照，人人都喜欢、赞叹;可挥舞起来就“杀人不见血”，人人谈它色变。所以当我们使用它时一定要慎重：一方面可以利用它好的一面来帮助自己，另一方面要时刻提高警惕，树立保护自己的意识，防止被这把“双刃剑”“刺”伤。首先我们应该加强网络公德自律，个人认为需要加强以下几个方面：一是正确使用网络工作学习;二是要健康进行网络交往;三是自觉避免沉迷网络;四是要养成网络自律精神。另外还要对于网上出现的病毒要加以防范，由于网路储存信息量大，一些东西是有害、虚假、反动的同时信息道德问题应受到关注，例如知识产权、个人隐私、信息安全、信息共享等都要进行尊重。在网络中，为了很好的保护自己的信息安全，我认为应该做到以下几点：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、诺顿、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、在安装从网上下载的软件时一定要一步步来，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，流氓软件又是极不容易卸载的，这些流氓软件可能会修改你的注册表，修改你的主页，定期打开某一网页，在ie中增加令人感到恶心的工具条等等，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的偏好，随时给我们发过来垃圾广告。所以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。姑且就某些破坏性的病毒可能导致移动存储设备损坏不说。单说安全性上我们通过上文的论述也可以看出，使用移动存储设备带来的信息被窃取的威胁有多大，有些公司为了防止商业机密被窃取甚至直接要求员工把电脑中的usb接口封死，利用光盘刻录的方法进行相互之间资料信息的传播，可谓是用心良苦。我们在使用u盘之类的存储设备时也要小心谨慎。

本学期我选修了信息安全导论这门课，自从上了第一堂课，我的观念得到了彻底的改观。首先，老师不是生搬硬套，或者只会读ppt的reader，而是一位真正在传授自己知识的学者，并且老师语言生动幽默，给了人很大的激励去继续听下去。其次，在课堂上了解到了保护自己信息安全的重要性，而且知道了不良分子窃取信息的诸多荫蔽方法，不禁让人有些后怕，以前从来没有注意到过这类事情，尽管也没有什么特别有价值的文献资料之类的东西，但是对自己的隐私还是十分看重的。此外，看到老师提出的关于期末考试成绩优秀有奖品的事实也十分吸引人，上了2年选修课还从来没有遇到过这种事情，自小的争胜心告诉我，我一定要好好学习这门课，期末得到那个最好的公仔。

信息安全顾名思义，是指所掌握的信息不被他人窃取的安全属性。由于现代社会科技高速发展，信息的数量以指数级别增加，而科技的进步也催生出很大窃取信息的技术方法，给我们信息安全带来了极大的威胁，不光说我们的个人隐私我发得到合理的保障，甚至一些商业机密乃至国家机密也都收到了潜在盗窃者的威胁。因此，如何防范信息的窃取正确的有效的保护自己信息隐私的安全性，如何处理信息被盗所造成的损失，如何亡羊补牢都是亟待解决的问题。信息安全概论这门课正是给我们提供了这样一个学习交流的平台，给了我们应对新时期信息安全问题一条出路。

现在的上网环境可谓是“布满荆棘”，正如老师上课时举的例子所说，一项实验，不开杀毒软件的电脑“裸奔”上网，2小时之内就会陷入崩溃，足见上网环境的恶劣，这中间可能是因为访问某个网站时给自己电脑中上了木马、修改了注册表、沾染了病毒，还可能是因为从某个网站上下载的应用软件中自带了木马、病毒，在你不知不觉中已经使电脑陷入了危险，这些病毒有一部分会占用你的资源，破坏你的系统，属于完全是没事找抽型的破坏性病毒，但是另外一些病毒和大部分木马却是居心不良，有些可以监视你键盘的动作，也就是说你在键盘上的输入会及时的别人所监视，同时也有的会强迫打开你的摄像头(前提是你有摄像头并且安装了驱动)来偷窥你所有的动作，我们经常会在一些视频网站或者新闻上看到这样的报道，一对夫妻在房内被另一个城市的无耻网友通过安装木马自动打开摄像头偷拍并被敲诈勒索的事件，这就是这类木马做的坏事。还有的木马会通过你的电脑再次传播，比如老师上课所讲的植入木马成为僵尸电脑，进而被控制攻击其它电脑，还有就是我们最常见的qq“尾巴”，首先在qq的对话框中给你说什么我在上看到了一段视频(这类视频前面一般加一些吸引人的定语，如我跳舞的视频，美女视频等等)然后建议你也去看一下，我敢说凡是头一次遇到这种情况的qq使用者80%都会去点开这个网站，于是不点不要紧，点了之后你也会中木马并肆意传播，我就是受害者之一，所以对它更是深恶痛绝(不是抵不住诱惑，每个人心里都有好奇心，所以就点开了)。

就算不上网也有信息被盗取的可能性。首先，是最常见的u盘盗取，有的时候电脑不上网但是需要用u盘或者移动硬盘拷贝一些资料或者其他什么信息，这时候如果有人事先在电脑中给你植入了一类荫蔽的木马，之类的，直接感染到电脑硬盘，然后偷偷地从你电脑中copy信息，等到下次在此插入u盘时带走，或者有些是你上网时就通过互联网悄悄的传输出去。其次，现在很多磁存储设备删除信息过程中可能留下痕迹，然后被某些居心不良的人用一些特殊技术就可以还原过来，比如数码相机中的照片，硬盘中的文档等等，这样在已经确认删除的情况下一般会放松警惕进而被钻空子，信息被窃取。最后，问题可能处在我们自己身上，换言之，我们自己的保密意识不强也会导致信息被窃取，很多时候我们的电脑并不设臵访问密码，任何人只要在我们不在的时候都可以访问，这样岂不是给某些不良分子行了方便。还有就是我们对某些重要的文档信息进行加密时过于疏忽，我就曾经遇到过这类事情，我对某个文件夹用超级兔子的文件伪装功能进行了加密，只要输入密码不正确怎么都不会打得开，后来过了段时间我自己把密码给忘了，于是抱着试一试的心里在百度中搜了一下“超级兔子文件解密”，结果发现很多绕过密码打开文件的方法，其中一种竟然可以利用winrar直接暴力修改文件后缀，达到完全去除密码设臵的功能，还好是我自己发现，不然隐私岂不是有可能被人窃取?!另外一个例子就是有些人相册或者qq空间设臵了访问限制，不输入密码或者不是主人好友禁止访问，这时候上网搜一下“相册密码”“qq空间”又会发现n多的方法，当然我没有那么无聊去偷看别人的什么东西，但是网上时常报料出一些新闻还是不得不引起我们的注意，如前段时间曝光的“伊莱克斯经理x照”就是别人了相册空间把照片窃取出来的，我们姑且不从伦理道德的角度对照片上的人做什么评论，单单就这个事情已经让我们毛骨悚然了，不知道以后还有谁敢发一些比较私密的照片到互联网上去。另外一个例子就是最近时常出现于报端的“网络暴民”，这些人通过在互联网上发布“通缉令”之类的方法，对他人展开人身攻击，我知道的最出名的就是mop的“人肉搜索”，也就是根据“暴民”提供的一些个人信息，搜到被通缉人的各类私人信息诸如住址、身份证号、电话号码、真实姓名、家属姓名、工作单位等等，最著名的例子就是mop上的“虐猫事件”直接找到了视频中女性的工作单位，还有“铜须”也是公布了当事人的照片和所在学校，给当事人造成了极大的伤害，这些隐藏在互联网后面的“网络暴民”企图想绕过法律给他人造成巨大伤害，如果我们没有一个很好的保护自己信息安全、自己在互联网上隐私的方法，也许下一个被通缉的人就是我们之中的谁。

为了很好的保护自己的信息安全，我认为应该做到以下几点：

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、诺顿、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、在安装从网上下载的软件时一定要一步步来，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，流氓软件又是极不容易卸载的，这些流氓软件可能会修改你的注册表，修改你的主页，定期打开某一网页，在ie中增加令人感到恶心的工具条等等，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的偏好，随时给我们发过来垃圾广告。所以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。姑且就某些破坏性的病毒可能导致移动存储设备损坏不说。单说安全性上我们通过上文的论述也可以看出，使用移动存储设备带来的信息被窃取的威胁有多大，有些公司为了防止商业机密被窃取甚至直接要求员工把电脑中的usb接口封死，利用光盘刻录的方法进行相互之间资料信息的传播，可谓是用心良苦。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。

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！