

防网络安全心得体会 8 篇

(经典版)

编制人：_____
审核人：_____
审批人：_____
编制单位：_____
编制时间：____年____月____日

序言

下载提示：该文档是本店铺精心编制而成的，希望大家下载后，能够帮助大家解决实际问题。文档下载后可定制修改，请根据实际需要进行调整和使用，谢谢！

并且，本店铺为大家提供各种类型的经典范文，如总结报告、心得体会、讲话致辞、条据文书、合同协议、策划方案、规章制度、教学资料、作文大全、其他范文等等，想了解不同范文格式和写法，敬请关注！

Download tips: This document is carefully compiled by this editor. I hope that after you download it, it can help you solve practical problems. The document can be customized and modified after downloading, please adjust and use it according to actual needs, thank you!

Moreover, our store provides various types of classic sample essays, such as summary reports, insights, speeches, written documents, contract agreements, planning plans, rules and regulations, teaching materials, complete essays, and other sample essays. If you want to learn about different sample formats and writing methods, please pay attention!

防网络安全心得体会 8 篇

不管是谁在写心得体会的时候都是要将自己的思路梳理好的，在写心得的时候，一定要确定好深刻的主题，这样才能保证它的意义，本店铺今天就为您带来了防网络安全心得体会 8 篇，相信一定会对你有所帮助。

防网络安全心得体会篇 1

我从网上学习《网络学习安全教育心得》得出感触。观看聆听了各位领导、专家老师关于学校安全教育培训的讲座后，我对安全教育工作有了更为深刻的认识，反思自己学校的实际情况谈点体会：

一、要提高全校师生对安全管理的认识

1、要加大安全教育的宣传力度

要全面提高教师与每位家长的安全责任意识，积极主动地向学生和家长宣传学校所潜在的诸多安全隐患以及各类重大安全事故教训。在校园醒目的地方张贴悬挂安全教育图片、标语，在楼梯、校门、操场、实验室、厕所、等容易发生安全问题的地方设置警示标志或标语。要利用校园板报、壁报、专栏、主题班会、征文、演讲等活动宣传安全知识，在校园形成事事想安全，处处有警示、人人抓安全的浓厚的安全育人氛围。

2、经常排查学校安全隐患

我校位于村庄的西北侧，与村庄连为一体。学校主要存在以下几个方面的隐患：

(1) 交通隐患为主要。出去校门口几乎就是公路，来往车辆比较多；跑校的学生也不少；

(2) 学生自身突发隐患；

(3) 学生上下楼梯极易出现踩空、歪脚等事故。

(4) 学校与村庄连为一体，学校周围的治安问题；

3、要不断加强安全教育，预防和减少事故的发生

加强对学生的安全教育，让学生自己懂得安全知识，增强安全意识，掌握防范技能，从根本上预防和减少安全事故的发生。利用每学期的开学初、放假前的一周和每次大型集会时间对学生进行安全知识教育，要积极利用综合实践课开展安全知识讲座、演讲、讨论等多种形式的安全教育活动，同时要与家庭、社会密切配合，形成学校、家庭、社会三位一体的安全教育网络，坚持不懈地把各项安全教育开展下去，有效预防各类安全事故的发生。

二、要加强领导，强化安全责任

学校安全责任重于泰山，本着一保安全，二保稳定，三保发展的原则，对学校安全高度重视，狠抓责任落实，真正形成校长亲自抓，分管领导重点抓、班主任及相关部门各司其职，各负其责的工作机制。同时，将学校安全工作纳入目标管理，制订目标管理细则，逐级签订安全责任书，做到层层把关，责任到人，真正做到谁主管、谁负责。

(1) 建全领导机构。校长亲自任组长，分管领导、各班班主任以及各科任老师为成员负责学校的安全。

(2) 学校与每位教师签订安全目标责任书，各班主任和每位学

生签订安全目标责任书。

(3) 专设门卫负责来往客人的登记，同时兼管外来人员对学校
的破坏。

(4) 建立健全防范安全事故的规章制度，制订完善的安全应急
预案。

(5) 建立健全安全工作检查制度。每学期开学、放假前都要进
行一次拉网式的安全工作大排查，并做到全面检查与重点检查相结合，
定期检查和日常防范相结合，对发现的事故隐患及时整改。

(6) 建立健全并严格执行重特大突发事件和安全事故报告制度，
建立健全预警和应急处理工作机制，制定切实可行的工作预案。

(7) 实行安全工作例会制度，每周至少召开一次安全工作专题
会议。

三、一定要采取得力措施，严防易发事故的发生

安全事故主要集中在交通、食物中毒、火灾等方面。研究掌握事
故的规律，采取有力措施防止事故的发生。

1、加强学校安全设施建设。加大学校的监管力度，严把教学、
生活用房的设计、监管和质量验收关，不留任何安全隐患。

2、防止发生各种食物、药物中毒事件。落实各项规章制度。

3、防止各种火灾的发生。加强对学校消防安全设施的检查 and 配
备，加强对实验室、电脑室的线路检查，特别是要对校舍设施陈旧使
用时间较长的电路进行检查，对老化陈旧的电线、电缆要及时更新。

4、严防溺水事件的发生。各班主任要求学生不要到河边去玩耍，

杜绝溺水事故的发生。

5、积极开展心理健康教育，防止有心理障碍学生造成的偏激行为。学校要求每位班主任要对本班个别心理素质差的学生进行长期地心理辅导，保证学生的心理健康。

6、加大安全工作的检查力度，建立常抓不懈的学校安全工作机制。我校在安全这方面一直做得较好，每天有领导带班，坚持早检查，午检查和下午放学检查。

7、继续加强学校及校园周边治安综合治理，抓好安全排查和整治工作，防止交通事故的发生。学校要积极配合公安、文化、卫生、工商、建设等部门，大力整顿学校周边的秩序，坚决防止校外犯罪分子侵入校园，伤害师生事件发生。同时要认真搞好学生的交通安全教育，关爱生命、远离危险宣传教育活动，并贯穿到学校日常的教学管理之中。

总之，学校的安全工作一定放在第一位，以后我校在安全方面要进一步努力，确保学校师生不出现大的安全事故，让老师们轻松愉快的工作，让学生安安全全健康成长。

读书破万卷下笔如有神，以上就是本店铺为大家整理的 5 篇《网络安全教育心得体会》，希望对您的写作有一定的参考作用。

防网络安全心得体会篇 2

随着电信行业的发展，利用电信工具和电信技术实施诈骗的事件越来越多，我身边一个朋友的经历就是典型的案例，她被诈骗的具体过程是这样的：

一天下午，她接到一个陌生的异地电话，对方声称是某购物网站的客服，并告诉我朋友她在他们网站所购买的某某商品由于尺码缺失，要进行退款。朋友当时有所顾虑，但是见对方将自己购买的网站甚至物品具体信息都讲述的分毫不差，便放松了警惕，随后添加了对方提供的一个 qq 号码，对方也将订单的具体信息在 qq 上再发了一遍，并留下了一个退款的网站。朋友照着点了进去，登录页面和自己当时购买的网站看不出任何分别，但是网址却不是官方的网址，朋友向对方提出了这个疑问，电话里的人解释说这是他们临时做的网站。朋友便也没有过多怀疑。接下来朋友填写了自己的银行卡的信息，对方谎称为了安全验证，欺骗朋友把银行卡的密码也填了进去。随后，验证码发到了朋友的手机上面，这时候，对方在电话里要朋友快速填入验证码，否则会超时无法退款，朋友便在洗脑般的状态下填写了两次 95533 发送的付款的验证码。随后朋友登录自己的网上银行，发现银行卡里面近万元的存款已被转走，这才恍然大悟被诈骗了。

通过我朋友这次案例，我认为导致这次诈骗事件的关键所在，就是受害者对于电信诈骗的防范意识不够。首先，对于陌生电话，网站等一定要慎重再慎重，不要轻易相信他们的话，如果确认他们提供的消息无误，最好自己拨打购物网站的官方热线询问有关消息。其次，对银行卡的了解不够，在收款的时候，无论如何是不需要告知银行卡密码的，密码泄露，骗子便可以知道你银行账户的所有信息。最后，验证码作为银行卡支付的最后一道屏障，一定不能泄漏给任何人，验证码一旦透露给对方，钱立马就会被转走。

如果钱被转走，当事人应该在第一时间马上报警，要求警方联系银行，调查钱款汇入的银行卡账户，及时冻结，避免更多的损失。对此，我们要对电信诈骗的种种手段有一定的了解，在遭遇时做到有效防范，及时发现，尽早纠错。

作为银行工作人员，在为客户开卡，办理电子产品等业务时，必须要加强审核是否本人办理，同时向签约电子产品的客户发放风险提示卡，并告知客户不能随意点击不明网址，不要轻易相信和回复不明信息和电话，增强客户安全意识，防范于未然，让犯罪份子无机可趁。

防网络安全心得体会篇 3

21 世纪是信息时代，互联网的诞生给了全世界人民带来了方便。在生活中，我们学生经常要查资料。但是在茫茫书海中，也有找不到资料的时候，而且查书颇费时间。但如果在电脑前轻轻地点击鼠标，需要的资料立刻出现在眼前，快捷方便。

通过网络，我们可以与世界建立联系，获取外界信息，可以更全面地了解世界，直接面对信息社会。网络还可以提高我们自身各方面的能力，比如：可以提高打字速度，可以增强我们的理解能力，所以，上网是件好事。

可是，上网也有坏处。上网容易着迷，一旦着了迷，就像走火入魔似的，不能自拔。有人一旦着迷，就整日泡在网吧里，对其他的事情失去了兴趣，自然也影响学习。上网过度伤神，耗费精力，同学们就会恍恍惚惚精神不振，最终成绩一落千丈。

我举几个典型的例子吧：像我们班有几位网虫，他们是专门用网

络打游戏的人。每当我在扫地的时候，往往会听见林智霖与郑涵都在讲一些奇葩的话：你打刀战杀多少人，你怎么打枪战啊！玩都不会玩。等。还有两个人是游晓成与陈昊，游晓成呆在班上，上课一言不发，也没有心思读书，恍恍惚惚的，我总觉得这里面一定有问题，于是，我就来了一个洞旁观火之计，经过调查发现，原来游晓成上课都在幻想着游戏中一幅幅精彩的画面，以至于无心听课。

在网络上，还有一些不文明的网站，网站上有许多不健康的内容。这些不健康的内容侵袭着同学们的头脑，使抵抗力低的同学们，渐渐逃避现实，性格异化，最后玩物丧智，从而断送了自己的美好前途。在网吧，某位男同学由于打游戏输得很惨，没钱去网吧，便用刀刺向了那位最疼他爱他的奶奶。本来可以拥有美好前途的少年，就这样断送了自己的美好前程。

一天，我无意中看见一句话：网络是一个自由，平等的世界，是没有政府、警察、没有军队。没有等级、没有贫富、没有歧视的世外桃源。但我却认为网络世界并非真正的世外桃源，也并非是一片净土。它只是一个虚拟的世界，进入网络犹如进入一个地球村，五彩缤纷的信息应有尽有，它是信息的海洋，但也可以称之为信息垃圾场。尤其是学生，很容易因为网络误入歧途。

所以，上网是件严肃的事情，请三思而后行！

防网络安全心得体会篇 4

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没有得到合理的保障，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被别人所监视，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

（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隐蔽的木马，类似我们见到的 autorun 。exe 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

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路的功能，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** 空间设路了访问限制，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解决 **qq** 空间解决又会发现 **n** 多的解决方法，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**照就是别人解决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，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

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，

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/685013311232011340>