# 网络安全宣传口号(推荐)

来源：网络 作者：眉眼如画 更新时间：2024-09-29

*网络安全宣传口号(推荐)一一、加强网络安全认真部署师生网络安全意识为切实抓好这次活动，学校召开了校委会，对整个网络信息安全宣传活动作了详细的布置，明确了人员的职责，会后下发了《后柳镇中心小学网络信息安全教育宣传周活动计划》。要求各负责人充分...*

**网络安全宣传口号(推荐)一**

一、加强网络安全认真部署师生网络安全意识

为切实抓好这次活动，学校召开了校委会，对整个网络信息安全宣传活动作了详细的布置，明确了人员的职责，会后下发了《后柳镇中心小学网络信息安全教育宣传周活动计划》。要求各负责人充分利用各种会议、活动、课堂等有效形式，在全校广泛宣传和普及网络安全教育的法律、法规政策和相关知识，强化全校师生对网络安全教育工作的参与意识和责任意识。

二、精心组织狠抓落实

为确保宣传周活动不走过场，达到预期效果，全校各部门强化措施，狠抓落实，确保了活动取得实效。成立了以副校长为组长的宣传活动领导小组，全面负责本次宣传活动的方案拟定、工作部署、组织协调等工作。校委成员各负其责，全力配合学校做好本次宣传周的活动。

三、形式多样内容丰富

1、针对活动意义和活动目的，利用电子屏打出本次活动的主题：共建网络安全，共享网络文明。

2、充分利用班队会、统一集会广泛宣传网络安全教育相关知识。

3、学校电教中心，在网上下载有关网络安全的教育视频，组织学生观看，对学生进行网络安全教育，上好网络安全第一课。

4、全校进行了一次校园网络安全隐患大排查。

5、学校还印发了《网络安全知识告家长书》，加强家长的网络安全和网络道德意识，发挥家长对孩子的监护和指导的作用。

**网络安全宣传口号(推荐)二**

青少年的健康成长，关系到社会的稳定，关系到民族的兴旺和国家的前途。因此，教育和保护好下一代，具有十分重要的意义。中学阶段是一个人成长的重要时期，中学教育尤其是中学生安全教育的成败直接关系到一个人将来是否成为人才。

随着信息时代的到来，形形色色的网吧如雨后春笋般在各个城镇应运而生。它们中有一些是正规挂牌网吧，但多数是一些无牌的地下黑色网吧，这些黑色网吧瞄准的市 场就是青少年学生。一些学生迷上网络游戏后，便欺骗家长和老师，设法筹资，利用一切可利用的时间上网。

有许许多多原先是优秀的学生，因误入黑色网吧，整日沉迷于虚幻世界之中，学习之类则抛之脑后，并且身体健康状况日下。黑色网吧不仅有学生几天几夜也打不“出关”的游戏，更有不健康、不宜中学生观看的黄色网页。

抓好中学生的网络安全教育与管理，保障中学生的人身财产安全，促进中学生身心健康发展，是摆在我们面前的一个突出课题。

针对这种情况，一是要与学生家长配合管好自己的学生，二是向有关执法部门反映，端掉这些黑色网吧，三是加强网络法律法规宣传教育，提高中学生网络安全意识，在思想上形成一道能抵御外来反动、邪恶侵蚀的“防火墙”。 四是组织学生积极参与学校的安全管理工作 ，让中学生参与学校的安全管理工作是提高中学生安全防范意识的有效途径。最后，争取相关部门协作，整治校园周边环境，优化育人环境。

学校在加大对校园安全保卫力量的投入、提高保卫人员素质和学校安全教育水平的同时，要积极争取地方政府、公安机关的支持，严厉打击危害学校及中学生安全的不法行为，切实改善校园周边治安状况，优化育人环境。对校门口的一些摊点，校园附近的一些黑色网吧，对中学生存有安全隐患的一切问题，该取缔的取缔，该打击的打击，该解决的尽快解决。

对校内发生的治安事件或安全事故，要依法处理，及时通报。对违反安全规章的学生应予以批评教育，甚至必要的纪律处分，对已发现的安全隐患及时采取有效的防范措施，以此创造一个安全、文明的育人环境，为提高教育教学质量和我国教育事业的发展做出新的贡献。

综上所述，对中学生进行安全教育是一项系统工程，在外部，需要社会、学校、家庭紧密配合;在内部，需要学校的各个部门通力合作、齐抓共管，组织学生积极参与，这样才能达到对中学生进行安全教育的目的。

**网络安全宣传口号(推荐)三**

1 引言

随着计算机网络技术的飞速发展，无线网络技术以独特的优点，被许多企业、政府、家庭所使用，但在其安装、使用便利，接入方式灵活的同时，由于无线网络传送的数据是利用无线电波在空中辐射传播，这种传播方式是发散的、开放的，这给数据安全带来了诸多潜在的隐患。无线网络可能会遭到搜索攻击、信息泄露攻击、无线身份验证欺骗攻击、网络接管与篡改、拒绝服务攻击等安全威胁，因此，探讨新形势下无线网络安全的应对之策，对确保无线网络安全，提高网络运行质量具有十分重要的意义。

2 无线网络存在的主要安全威胁

无线网络存在的主要安全威胁有两类：一类是关于网络访问控制、数据机密性保护和数据完整性保护而进行的攻击；另一类是基于无线通信网络设计、部署和维护的独特方式而进行的攻击。对于第一类攻击在有线网络的环境下也会发生。可见，无线网络的安全性是在传统有线网络的基础上增加了新的安全性威胁。

2.1 攻击者侵入威胁

无线局域网非常容易被发现，为了能够使用户发现无线网络的存在，网络必须发送有特定参数的信标帧，这样就给攻击者提供了必要的网络信息。入侵者可以通过高灵敏度天线在合适的范围内对网络发起攻击而不需要任何物理方式的侵入。因为任何人的计算机都可以通过自己购买的ap，不经过授权而连入网络。很多部门未通过公司it中心授权就自建无线局域网，用户通过非法ap接入给网络带来很大安全隐患。还有的部分设备、技术不完善，导致网络安全性受到挑战。这些挑战可能包括窃听、截取和监听。以被动和无法觉察的方式入侵检测设备的，即使网络不对外广播网络信息，只要能够发现任何明文信息，攻击者仍然可以使用一些网络工具，如airopeek和tcpdump来监听和分析通信量，从而识别出可以解除的信息。

2.2 相关无线网络保密机制存在缺陷

wep机制用来提高无线网络安全性，但长期的运行结果是该机制存在一定的安全缺陷，值得影响大家的关注。加密算法过于简单。wep中的iv由于位数太短和初始化复位设计，常常出现重复使用现象，易于被他人解除密钥。而对用于进行流加密的rc4算法，在其头256个字节数据中的密钥存在弱点，容易被黑客攻破。一个是接入点和客户端使用相同的加密密钥。如果在家庭或者小企业内部，一个访问节点只连接几台pc的话还可以，但如果在不确定的客户环境下则无法使用。让全部客户都知道密钥的做法，无疑在宣告wlan根本没有加密。不同的制造商提供了两种wep级别，一种建立在40位密钥和24位初始向量基础上，被称作64位密码；另一种是建立在104位密码加上24位初始向量基础上的，被称作128位密码。高水平的黑客，要窃取通过40位密钥加密的传输资料并非难事，40位的长度就拥有2的40次方的排列组合，而rsa的解除速度，每秒就能列出2.45×109种排列组合，很容易就可以被解除出来。

虽然wep有着种种的不安全，但是很多情况下，许多访问节点甚至在没有激活wep的情况下就开始使用网络了，这好像在敞开大门迎接敌人一样。用netstumbler等工具扫描一下网络就能轻易记下mac地址、网络名、服务设置标识符、制造商、信道、信号强度、信噪比的情况。作为防护功能的扩展，最新的无线局域网产品的防护功能更进了一步，利用密钥管理协议实现每15分钟更换一次wep密钥，即使最繁忙的网络也不会在这么短的时间内产生足够的数据证实攻击者破获密钥。然而，一半以上的用户在使用ap时只是在其默认的配置基础上进行很少的修改，几乎所有的ap都按照默认配置来开启wep进行加密或者使用原厂提供的默认密钥。

2.3 搜索攻击威胁

进行搜索也是攻击无线网络的一种方法，现在有很多针对无线网络识别与攻击的技术和软件。netstumbler软件是第一个被广泛用来发现无线网络的软件。很多无线网络是不使用加密功能的，或即使加密功能是处于活动状态，如果没有关闭ap（无线基站）广播信息功能，ap广播信息中仍然包括许多可以用来推断出wep密钥的明文信息，如网络名称、ssid（安全集标识符）等可给黑客提供入侵的条件。同时，许多用户由于安全意识淡薄，没有改变缺省的配置选项，而缺省的加密设置都是比较简单或脆弱，容易遭受黑客攻击。

除通过欺骗帧进行攻击外，攻击者还可以通过截获会话帧发现ap中存在的认证缺陷，通过监测ap发出的广播帧发现ap的存在。然而，由于802.11没有要求ap必须证明自己真是一个ap，攻击者很容易装扮成ap进入网络，通过这样的ap，攻击者可以进一步获取认证身份信息从而进入网络。在没有采用802.11i对每一个802.11 mac帧进行认证的技术前，通过会话拦截实现的网络入侵是无法避免的。

2.4 网络身份冒充

网络身份冒充是采取假冒相关用户的身份，通过网络设备，使得它们错误地认为来自它们的连接是网络中一个合法的和经过同意的机器发出的。达到欺骗的目的，最简单的方法是重新定义无线网络或网卡的mac地址。由于tcp/ip的设计原因，几乎无法防止mac/ip地址欺骗。只有通过静态定义mac地址表才能防止这种类型的攻击。但是，因为巨大的管理负担，这种方案很少被采用。只有通过智能事件记录和监控日志才可以对付已经出现过的欺骗。当试图连接到网络上的时候，简单地通过让另外一个节点重新向ap提交身份验证请求就可以很容易地欺骗无线网身份验证。

3 无线网络安全对策探讨

提高无线网络安全等级，必须首先从思想要高度重视，提出有效的应对举措，确保无线网络安全。

3.1 科学进行网络部署

选择比较有安全保证的产品来部署网络和设置适合的网络结构是确保网络安全的前提条件，同时还要做到如下几点：修改设备的默认值；把基站看作 ras（remoteaccessserver，远程访问服务器）；指定专用于无线网络的ip协议；在ap上使用速度最快的、能够支持的安全功能；考虑天线对授权用户和入侵者的影响；在网络上，针对全部用户使用一致的授权规则；在不会被轻易损坏的位置部署硬件。

3.2 合理配置网络的接入点设备

要对无线网络加装防火墙，并且在进行网络配置时，要首先确保无线接入点放置在防火墙范围之外，提高防火墙的防御功效。同时，要利用基于mac地址的acls（访问控制表）确保只有经过注册的设备才能进入网络。mac过滤技术就如同给系统的前门再加一把锁，设置的障碍越多，越会使黑客知难而退，不得不转而寻求其他低安全性的网络。

3.3 重视发挥wep协议的重要作用

wep是802.11b无线局域网的标准网络安全协议。在传输信息时，wep可以通过加密无线传输数据来提供类似有线传输的保护。在简便的安装和启动之后，应立即更改wep密钥的缺省值。最理想的方式是wep的密钥能够在用户登录后进行动态改变，这样，黑客想要获得无线网络的数据就需要不断跟踪这种变化。基于会话和用户的wep密钥管理技术能够实现最优保护，为网络增加另外一层防范。此外，所有无线局域网都有一个缺省的ssid（服务标识符）或网络名，立即更改这个名字，用文字和数字符号来表示。如果企业具有网络管理能力，应该定期更改ssid：即取消ssid自动播放功能。

**网络安全宣传口号(推荐)四**

为贯彻落实好党的xx大提出的“健全基层社会管理体制”精神，在全面整合现有各类行政资源的基础上，以层级负责为基础，以细分区域为平台，以长效机制为抓手，以提高效率为目标，全名推行“三级网格、五项机制”网格化管理模式，实现城乡管理由粗放向精确、静态到动态、分散到集中、局部到全面的转变，逐步实现管理的全覆盖与服务全方位，加强和提升基层管理与服务的综合水平。

本着“各司其职、各负其责”的精神，构建“排查报送、处置反馈、信息管理、督查考核、奖惩表彰”配套工作机制，保障三级网格化的正常运转。

现将各级网格职责分解如下：

一级网格：指导基层的管理与服务等综合工作;协调的重大事宜定期深入社区内听取居民的意见和建议，并及时将其反馈至城乡相关部门给予解决;督促和指导下级网格责任人工作落实情况。

二级网格：协助管理与服务等综合工作，列席工作例会;每个工作日不少于1小时深入社区收集居民的意见和建议;及时将各类动态情况反馈至上级相关部门与责任人，并协助其给予解决;督导下级网格责任人工作落实情况，检查其网格工作记录等。

三级网格：收集与整理责任区内民生、经济、稳定、计生等各类信息资源，建立网格化管理台帐系统;每个工作日不少于2小时深入责任片，巡查网格内市政、消防等硬件设施情况;将责任区内各类动态情况反馈至相关责任人，督促并协助其给予解决;指导和动员相关责任人工作;认真做好网格化工作记录。

(一)排查报送机制

1、结合社区工作实际，将工作领域所需求的信息内容分解至社区，各级网格责任人须切实履行工作职责，按规定要求定期在责任网格内开展信息排查工作。

2、三级网格责任人应当整合责任区内各类信息资源，创建网格化管理系统台帐，并实行动态化管理。认真排查，做好信息记录工作，如实填写网格化管理工作日志，全面掌握责任区内基本情况。将排查收集的问题与信息，整理后按“区分责任、分口处理”的原则，属于社区职责范围内的报送社区责任干部，督促并协助该责任人在规定时限内给予解决和反馈;属于社区职责范围外的上报二级网格责任人与职能科室。

(二)信息管理机制

1、信息台帐系统坚持以“一个网格一本台帐、一项工作一组数据”为原则，使网格内各类数据信息科学、直观。三级网格责任人应将信息台帐系统实行动态管理，坚持做到有变化时即时充实更改，无变化时定期调整维护，使信息台帐系统随着工作的进展而变化。

2、信息台帐系统实行分类管理，以工作性质为尺度区分为党群组织、经济财政、综治司法、社会事务、人口计生、劳动保障、城市管理、文教体育等八大项，以及若干小项。实行电子版本与纸质版本相结合，电子版本作为数据更新库;纸质版本便于深入网格排查时随手携带。

(三)处置反馈机制

排查收集的各类信息与问题，必须本着“务实、快速、高效”的原则给予处置。

2、在处置责任上，涉及到驻区单位之间、居民与驻区单位之间、居民与居民之前的事务，原则上由网格责任领导牵头处理;涉及到市、区职能部门的事务，原则上由城乡职能科室牵头处理。

3、在处置时效上，属社区职责范围内的，一般在3个工作日内给予解决，属城乡职能科室职责范围内的，一般在5个工作日内给予解决，如特殊情况短期内难以解决，应当及时注明原因。

4、在处置协调上，如问题超出城乡职责范围，应当在1个工作日内报送区相关职能部门，并及时将处置进展情况给予反馈。

5、在处置反馈上，所有问题处置办理结果应当向群众公示，接受群众监督。

(四)督查考核机制

城乡对网络化管理运转情况实行督查考核，确保该管理模式做到有效、实效、高效;

城区督查考核组采取听、看、议相结合的方式负责督查下级网格运转情况，实行一季一排名，年度总评比，年度评比考核与社区工作考核一并实施，考核内容：贯彻落实城乡党工委、办事处布置的各项工作;执行城乡社区网格化管理运转情况;排查各类信息是否全面、准确、及时;处置各类问题的时效与实效情况等。

(五)奖惩表彰机制

城乡对网络化管理运转情况实行激励机制，奖惩以督查考核结果为依据;

1、考核奖励：

①在网络化管理中表现突出的给予表彰。

②在网络化管理中表现突出的个人，优先参评市、区、城乡各级先进荣誉，作为继续聘用的重要依据。

2、考核惩罚：

①对不能切实履行职责掌握网格动态情况者，给予通报批评;因未能及时掌握信息与问题而给城区造成影响者，给予警告一次。

②在平台管理上，更新不及时、不准确，特别是数据虚假者，给予通报批评;

③在处置反馈上，不能按规定时限办结并反馈者，给予通报批评;因处置失当而给城乡造成影响者，城区党工委视情节给予处分。

④在督查排名上，连续三次在季度评比中位列后两名的社区，给予通报批评等相应处罚。

3、奖惩表彰细则另行规定。

城区社会管理网格化工作组(签字)

社区居委会网格长(签字)

20xx年x月

**网络安全宣传口号(推荐)五**

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和配备，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。

**网络安全宣传口号(推荐)六**

根据《中华人民共和国计算机信息系统安全保护条例》(国务院令第号)、《计算机信息网络国际联网安全保护管理办法》(公安部令第33号)和《信息安全等级保护管理办法》(公通字[]号)等规定，为加强政府网站的网络安全保护工作，由公安机关与政府网站安全责任单位共同签订责任书，明确和落实网站开办单位的安全管理责任及公安机关的安全监管责任。具体内容如下：

一、网站开办单位要高度重视网站安全保护工作，按照“谁主管、谁负责，谁运营、谁负责”的原则，明确责任，落实网站各项安全保护措施，保障网站的安全稳定运行。

二、政府网站建设和应用要与网络安全同步规划、同步建设、同步实施，开展信息安全等级保护定级备案、安全测评、安全建设整改和安全自查等工作。

三、网站开办单位要制定完善网站安全应急预案，定期开展应急演练。建设安全监测手段，开展实时监测。对重要数据和系统，建设相应的备份措施。做好技术力量、资源的储备，应对重大突发事件的发生。

四、网站开办单位应配合公安机关开展安全检查，与公安机关建立重大网络安全事件(事故)发现、报告、应急处置等工作机制。

五、公安机关应加强对网站开办单位网络安全工作的指导，定期进行现场安全检查和远程技术检测，对网站存在的安全漏洞和隐患及时通报预警，对发生的案事件及时进行调查侦查，打击攻击政府网站的违法犯罪活动。

六、对网站安全责任和工作要求不落实的，或网站被不法分子攻击、篡改及传播、链接有害信息的，公安机关应督促网站开办单位及时整改，情节严重的，依法追究相关单位及责任人的法律责任，并进行通报。

七、本“责任书”一式四份，网站开办单位、公安机关和双方监察部门各存一份。

网站安全责任单位领导(签字)：公安机关分管领导(签字)：

网站单位(盖章)公安机关(盖章)

**网络安全宣传口号(推荐)七**

同学们，上网就像步入社会，你可以在这个虚拟的空间里，学到有益自己身心健康成长的东西，学到课本里没有学不到的东西，在这里你可以得到世界上成千上万的网友的帮助。但在这里也可能受到一些内容不健康的网站的影响，思想受到的侵害，也有可能做出犯法的事。为此，请大家熟记以下上网安全守则：

1、没有经过父母同意，不要把自己及父母家人的真实信息，如姓名、住址、学校、电话号码和相片等，在网上告诉其他人。

2、如果看到不文明的信息或图片，应立即告知父母。

3、进入聊天室前要告知父母。必要时由父母确认该聊天室是否适合学生使用。不要在各个聊天室之间“串门”。在聊天室中，如果发现有人发表不正确的言论，应立即离开，自己也不要在聊天室散布没有根据或不负责任的言论。

4、不要在聊天室或bbs上散布对别人有攻击性的言论，也不要传播或转贴他人的违反中小学生行为规范甚至触犯法律的内容。

5、尽可能不要在网上论坛，网上公告栏、聊天室上公布自己的e-mail地址。如果有多个e-mail信箱，要尽可能设置不同的密码，未经父母同意，不和任何网上认识的人见面。如果确定要与网友见面，必须在父母的同意和护送下，或与可信任的同学、朋友一起在公共场所进行。

7、如果收到垃圾邮件(不明来历的邮件)，应立即删除。包括主题为问候、发奖一类的邮件。若有疑问，立刻请教父母、老师如何处理。

8、如遇到网上有人伤害自己，应及时告诉父母或老师。

9、根据与父母的约定，适当控制上网时间，一般每次不要超过1小时，每天不超过3小时。

上网要注意安全，如果不加防范，网络的危害并不小，以下几方面应当引起同学们的足够重视。

一、网上娱乐谨防过度。

二、网上交友谨防受骗。

三、对网上内容要有取舍，自动远离发布不良信息的网站。

四、网上逗留谨防“毒黑”。也就是要防范病毒侵扰和黑客攻击，不要随便下载不知名网站的程序和附件。

**网络安全宣传口号(推荐)八**

我区接到市信息化领导小组办公室下发的《xx市信息化工作领导小组办公室关于开展重点领域网络与信息安全检查的通知》后，高新区管委会领导十分重视，及时召集相关人员按照文件要求，逐条落实，周密安排自查，对机关各部局配备的计算机网络与信息安全工作进行了排查，现将自查情况报告如下:

一、领导高度重视、组织健全、制度完善

近年来，高新区网络与信息安全工作通过不断完善，日益健全，管委会领导十分重视计算机管理组织的建设，本着“控制源头、加强检查、明确责任、落实制度”的指导思想，成立了由管委会副主任为主管，办公室主任为负责人的网络安全工作小组，并设有专门的信息管理人员，所有上传信息都由办公室主任负责审查其合法性、准确性和保密性。高新区会在有关部门的监督和指导下，根据《中华人民共和国计算机信息系统安全保护条例》和《计算机病毒防治管理办法》等法规、规定，建立和健全了《安全管理责任制度》、《计算机及网络保密管理规定》和《文书保密工作制度》等防范制度，将计算机信息系统保密工作切实做到防微杜渐，把不安全苗头消除在萌芽状态。

按照文件要求，高新区及时制定了高新区门户网站安全突发事件应急预案，并根据应急预案组织应急演练。

二、强化安全教育，定期检查督促强化安全教育

高新区在开展网络与信息工作的每一步，都把强化信息安全教育放到首位，使管委会全体工作人员都意识到计算机安全保护是高新区中心工作的有机组成部分，而且在新形势下，网络和信息安全还将成为创建“平安高新、和谐高新”的重要内容。为进一步提高人员网络安全意识，我们还经常组织人员对相关部局进行计算机安全保护的检查。通过检查，我们发现部分人员安全意识不强，少数计算机操作员对制度贯彻不够。对此，我们根据检查方案中的检查内容对不合格的部局提出批评，限期整改。各部局在安装杀毒软件时全部采用国家主管部门批准的查毒杀毒软件适时查毒和杀毒，不使用来历不明、未经杀毒的软件、u盘等载体，不访问非法网站，自觉严格控制和阻断病毒来源。单位电脑设备外送修理时，有指定人员跟随联系。电脑报废处理时，及时将硬盘等存储载体拆除或销毁。

三、信息安全制度日趋完善在网络与信息安全管理工作中，我们就树立了以制度管理人员的思想，制定了网络信息安全相关制度，要求高新区管委会各部局提供的上传内容，由各部局负责人审查签字后报送至信息管理员，经办公室主任审核同意后上传;重大内容发布报管委会领导签发后再上传，以此作为高新区计算机网络内控制度，确保网站信息的保密性。

对照《通知》要求，高新区网站在以往的工作中，主要作了以上几方面的工作，但还有些方面要急待改进。

一是要今后还要进一步加强与市政府信息中心联系，

以此来查找差距，弥补工作中的不足。

二是要进一步加强对高新区管委会工作人员的计算机安全意识教育和防范技能训练，提高防范意识，充分认识到计算机网络与信息安全案件的严重性，把计算机安全保护知识真正融于工作人员业务素质的提高当中。

三是要进一步健络与信息安全管理制度，提高管理人员工作技能，经常聘请专业人员对管理人员进行培训，把学到的知识真正融于网络与信息安全保护工作中，而不是轻轻带过;做到人防与技防结合，真正设置起一道网络与信息安全工作的一道看不见的屏障。

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