网络安全防范知识精选 15 篇

网络安全防范知识（精选篇 1）

笔者近年供职于中国信息安全研究院，深入参与了国家网络安全顶层设计和标准编制等工作，目睹了国际和国内网络安全政策、产业和技术的重要变革，对产业政策、产业现状和需求，以及网络安全技术体系进行了深入研究。*结合近年工作经验与高教研究，以打造网络安全体系性人才为目标，对网络安全专业的教学特点、教学内容、教学方法和考核方式等进行了一系列探索。

一、网络安全专业的教学特点

网络安全专业涉及范围广，涵盖了计算机、通信、电子、数学、生物、法律、教育和国际贸易等多学科内容，属知识密集型专业，具有很强的专业性、广泛性和实践性，随着物联网、云计算、大数据等新技术新应用的出现，网络安全专业的特点更加突出。

1.内容涉及范围广。网络安全专业涉及信息系统软硬件的本质安全，以及应对网络威胁、数据传输等方面的动态过程安全，在安全访问领域涉及密码学和生物学等，在网络安治理方面涉及法律学，在网络安全服务方面涉及教育学和管理学等，WTO 第二十一条“国家安全例外”等内容涉及国际贸易学。

2.知识和技术迭代速度快。网络安全由传统意义上的信息安全演变而来。狭义的信息安全重点关注内容安全，即确保信息的完整性、可用性和保密性。随着新技术新应用的层出不穷，异构信息系统和复杂多变的网络威胁带来了新挑战。除具备网络安全基础知识和技能以外，了解和掌握更多新技术知识是网络安全专业对学生提出的新要求。

3.对实际操作能力要求高。网络安全对实践操作能力有很高要求，构建具有本质安全的自主可控软硬件系统需要丰富开发经验和集成适配能力。应对复杂多

变的网络安全威胁，需要提前具备应急响应和灾难恢复能力；面对国际贸易中技术壁垒的挑战，需要深入研究国际贸易保护下的信息安全产业和政策竞争策略等。

二、教学内容设置

对于网络安全专业学生和非网络安全专业学生，在设置网络安全专业课程和教学内容时应予以区分，以使不同发展方向的学生在毕业以后将在校期间学习的知识充分发挥，适应未来职位对其知识储备的差异化需求。

（一）网络安全专业学生

网络安全涵盖本质安全和动态过程安全两大部分。对于网络安全专业的学生，在教学内容设置上，应鼓励学生通过理论和实践，构建网络安全体系观念，并依据个人爱好，深耕具体技术方向，使网络安全专业毕业生具备顶层大局观和技术优势。

1.本质安全方向。近年来，“棱镜门”等事件充分说明美国政府可利用其全球大型 IT 或互联网企业的技术、产品和服务，甚至对产品植入后门，来窃听、窃取各国数据和信息，这促使我国政府和产业界高度重视本质安全。本质安全涉及包括 CPU、芯片、操作系统、数据库、整机、网络设备等软硬件技术产品的自主研发，目前我国党政军和“8+2”对以上技术产品渴求度很大，人才队伍建设亟待加强，因此在课程内容应增强核心硬件和基础软件知识的普及力度，使学生在本质安全基础理论、产品设计和集成适配等方面有所突破。

2.过程安全方向。学习了本质安全相关知识后，就可了解如何构建一个相对完整、安全的信息系统，但在信息系统运行过程中，还需要针对系统构建运维服务体系，从加强整个信息系统的安全性和健壮性。过程安全相关的教学内容包括容灾备份、追踪溯源、安全访问等技术，在过程安全教学内容中，可以以聚合式的思维来教授相关知识，以使学生具备完整的运维服务体系思维。 （二）非网络安全专业学生

1.专业与网络安全有交互的学生。本部分以涉及网络安全的国际贸易和法律专业为例，阐述如何面向专业与网络安全有交互的学生进行教学。

对于国际贸易专业学生，引导学生加强国际 IT 贸易问题研究，特别是 WTO 第二十一条“国家安全例外”，即从国家安全考量出发，深入研究世界主要国家限制其他国家企业在其本土投资的案例，以及外国企业如何规避 WTO 限制，在我国广泛开展 IT 投资，总结国际贸易争端经验，为未来围绕“技术性贸易壁垒”的国际贸易纠纷做好充分准备。

对于法律专业学生，鼓励学生加强《中华人民共和国网络安全法》法理研究，深入学习互联网治理和网络安全相关法律和法规，培养网络安全法人才，为党政军和相关产业提供网络安全法律力量支撑，提升国家和企业的国际竞争力。

2.其他专业学生。对于其他专业学生，设置网络安全知识普及课程，通过案例分析和实践体验等手段，培养学生安全使用互联网的习惯，提升网络安全意识，了解和掌握网络安全防范和处理基本方法，巩固意识形态，促使学生做到文明上网、安全使用、加强防护，构建和谐清朗网络空间。

三、创新教学方法

教学方法和理念因学校和教师的不同而千差万别。总的来看，现代教学方法秉承以学生为主体、互动教学和构建体系化知识三项原则[1]，重视创新性和突破性，符合新时代和新形势对我国高等教育提出的要求。本节结合网络安全专业的特点，总结了三个面向该专业的创新教学方法。（一）教法和学法结合

网络安全专业涉及范围广且实践性很强，因此在教学方法上需要创新，将教法和学法进行有机结合，构建学生的理论和技术体系，提高实践能力。

PPT 教授法。教师精炼教材重点，利用互联网和多媒体手段，将要点和案例以图文并茂的 PPT 展示，并结合课堂上的口头表述将知识展现给学生。比如利用信息系统模拟工控系统运行环境，利用 DDOS 进行持续攻击，使学生从各生产节

点和控制系统观察受攻击时的状态，调动学生的注意力，加深学生的印象，使学生随着教师思路来学习。

互动提问法。在课堂上利用互动提问法可启发学生的思维，调动学生积极性和学习热情，促进学生提高注意力和快速学习到重要知识点，避免无精打采或溜号走神等现象发生。同时，提问法给学生提供了讨论、发表个人观点的机会，也促进了学生表达能力的提升。比如讲到构建本质安全信息系统时，可以首先向学生提问，构建该系统需要具备什么样的要素，请学生总结自己认为的具有本质安全信息系统的构造，以此增加师生间的互动，培养探究意识和发现问题的敏感性。

分组发表法。将学生分组并布置特定研究方向，鼓励学生利用互联网资源来获取知识、查找案例，并编制集文字、图片和视频等素材为一体的 PPT，在课堂上进行发表，通过教授的点评和同学的提问促使学生深入了解该方向内容， 做到专；通过聆听其他组的同学做发表，可以了解其他人的研究成果，并可通过课堂提问和课下交流来深入了解其他网络安全技术知识， 做到广。例如学习网络安全政策时，可组建学生小组，基于学生网络安全基础技术和知识，深入研究包括 FedRAMP、美关键基础设施保护总统令或国防部云计算安全指南等网络安全政策，并在课堂上做发表，与师生共同分享和研讨美国的网络安全治理经验。

（二）传统授课和网络授课结合

目前，采用传统教学模式依然是我国教育的主要方式，作为“以教师为中心”的课堂教学模式，传统授课模式通过教师在课堂上当面将知识教授给学生，可以促进有意义的学习、加深学生的理解和记忆，也有利于未来对知识的提取。而网络授课的教学模式在传统课堂教学模式的基础上融合了互联网的优势，该模式相较传统教授模式具有更好的灵活性、互动性和广泛性。特别是对于教师资源相对匮乏的地域，可以依托互联网基础设施，通过网络授课的模式将发达地区的优质教育资源引入到地方课堂，使学生享受到公平的先进的网络安全教育资源。

（三）注重实训体系建设

依托网络安全企业或其他专业机构建设网络安全实训基地，与高校等人才培养单位联合，对网络安全专业学生进行实践技能训练。实训基地对于我国网络安全人才培养具有重要意义。首先，实训基地可解决我国网络安全人才培养和使用相“脱节”、学生实际动手能力严重不足等问题。其次，实训基地涵盖技术、战略、法规等多个领域，有利于培养跨学科、复合型人才。

实训基地培训既要涵盖网络安全技术，也要涵盖网络安全战略规划和法律标准等。针对网络安全专业的不同研究方向，有针对性地分类建设攻防、追踪溯源、容灾备份、安全测评、自主可控等实训场景；针对网络安全战略规划，针对性地研究世界主要国家网络安全战略规划，分析各国目前网络安全现状和未来发展重点；针对法律标准，深入研究 WTO“国家安全例外”、 中美网络安全相关标准，为未来工作找到技术和法律依据。

四、改进考核方式

按照网络安全专业的特点，学生除了具备相应专业基础知识以外，还需要具备很强的实践能力。诸如学生出勤率、课堂表现、作业完成情况、参加实验和完成实验情况和考试成绩等传统的考核方式不能完全评判学生实际能力，还需增加对学生实践能力的考核，同时分配好各项考核要素权重。传统考核方面，鉴于出勤不一定认真听课，因此可将出勤率和课堂表现考核结合，作业和实验完成情况相结合，再辅以笔试，这样可以较好地评判学生对网络安全知识了解程度。实践考核方面，加强网络安全关键环节的考核内容，传统网路安全专业考核主要是以编程为主。面对新形势，实践考核可针对网络安全体系中的关键节点进行实践考核，例如对持续监控和处理信息系统网络安全问题的综合能力进行考核，增强学生网络安全的系统性实践能力。

在教育部提出加强网络空间安全专业建设的新形势下，网络安全学科建设应以培养具有网络安全体系化思维人才为导向，对不同专业的学生采取差异化授课的方式，并结合创新性教学方法和考核机制，来提升专业人才培养效果，为国家安全提供基础性和专业性人才保障。

网络安全防范知识（精选篇 2）

根据省委高校工委、省教育厅《关于组织开展 20--年国家网络安全宣传周活动的通知》的精神，我校自 20--年 9 月 17 日至 9 月 23 日开展了主题为“网络安全为人民，网络安全靠人民”的网络安全宣传周活动。通过主题宣传教育活动，普及网络安全知识，增强师生们网络安全意识，提高网络安全技能，加强个人信息保护，号召大家共同维护国家网络安全，营造网络安全人人有责、人人参与的良好氛围，切实做好了我省教育系统倡导的“网络安全宣传周”活动。现将活动情况汇报如下：

一、深入学习，强化意识

为切实抓好网络安全宣传周活动，学校党委行政高度重视网络宣传安全周活动，第一时间研究部署。活动由党委宣传部具体统筹，对于开展网络安全宣传周的活动要求作详细的布置，明确活动的目的，突出宣传的实效性和思想性，下发《关于组织开展 20--年国家网络安全宣传周活动的通知》，要求各党委、党总支、直属党支部和校直各单位充分利用培训会、知识竞赛、签名活动、宣传教育等有效形式，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活动的参与意识和责任意识。

二、精心组织，狠抓落实

为确保网络安全宣传周活动达到预期效果，学校强化措施，狠抓落实，确保了活动取得实效。我校成立了宣传活动领导小组，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。宣传部负责督导各单位，全力按照工作要求，确保了本次宣传周活动有序开展并圆满完成。

三、形式多样，内容丰富

（一）通过多种渠道的宣传方式提升网络安全意识

为在全校范围内广泛开展网络安全知识的宣传，宣传部发挥线上线下多渠道的宣传优势，全方位多角度的对网络安全意识的提升加以宣传。

1. 通过校园大屏幕滚动播放网络安全视频让全校师生学习；

2. 通过宣传专栏系统的介绍网络安全知识；

3. 通过校园广播电台让全校学生在课余时间对相关知识深入了解；

4. 通过发动各个学院的微信公众平台传播网络安全知识；

5. 各院系还相继展出了以“网络安全为人民，网络安全靠人民”为主题的网络安全宣传板。

通过以上切实有效的宣传活动，使全校师生强化了网络安全自我保护意识，同时师生们也纷纷宣传并转载了关于“网络道德和网络素养”的*，将其运用到学习生活中，以便更好的创造和谐的网络环境。

（二）通过积极参与知识竞赛的方式深化网络安全教育

组织全校师生参加教育部思政司开展的”全国大学生网络安全知识竞赛”和“全国大学生网络安全知识答题闯关”活动。通过网络答题方式普及网络安全知识。各地各校要组织高校学生积极参与竞赛，激发学生学习网络安全知识兴趣，提升网络安全防护技能。在竞赛活动中，师生们纷纷展现出了较高的积极性，数千名师生参加了竞赛答题。通过开展网络知识竞赛，掀起了师生们学习网络安全知识的热潮。

（三）通过教育主题系列活动的开展提高师生网络素养

为进一步提升我校师生的网络安全意识和安全防护技能，营造安全健康文明的校园网络环境。我校各单位在 9 月 17 日至 9 月 23 日期间积极组织开展了“网络安全为人民，网络安全靠人民”教育主题系列活动。

1. 网络安全知识抢答赛。法学院、金融学院和数学与信息科学学院举行了网络安全知识抢答比赛决赛。法学院在 17、18 级学生中全面开展，动员 15、16 级学生积极参加，共收取 17、18 级学生参与竞赛截图 545 张，取得了良好效果；金融学院通过组织开展“全国大学生网络安全知识答题闯关”活动，让学生网络答题方式普及网络安全知识；数学与信息科学学院组织学生积极参加竞赛。通过参与网络安全知识抢答赛，不仅激发学生学习网络安全知识的兴趣，而且提升网络安全的防护技能。

2. 新媒体平台宣传教育。法学院和数学与信息科学学院积极利用新媒体平台宣传网络安全。法学院在其团委微博（____财经政法大法学院团委）、微信公众号（法学青年号）网络安全相关知识；数学与信息科学学院通过学院的微信、微博积极宣传在全国网络安全和信息化工作会议上的重要讲话精神，向师生发送相关网络安全知识，运用网站、微信、微博等媒体积极宣传网络安全法律、法规和技术知识。

3. 网络安全知识培训会。9 月 24 日，法学院在教学科研楼 B 座 429 教室开展团属新媒体网络安全培训会，会议由学院学生团委副书记主持，学院各级新媒体账号负责人参与此次会议。会议上，老师强调了网络安全的重要性，讲解了网络安全技巧，提醒学生要加强网络安全意识，并指出要加大舆论引导，责任落实到个人。学院新媒体负责人表示会跟学生强调注意网络安全，减少网络安全事故。

4. 主题班会活动。金融学院各班召开以“网络安全”为主题的专题班会，利用多媒体教学宣传网络安全知识，让同学们深刻理解这次活动的意义和必要性。学生们也积极踊跃的发言讨论。不仅增长学生的网络安全知识，而且提高学生的网络安全防范意识。

5. 主题日签名活动。9 月 18 日是网络安全教育主题日，由我校宣传部主办的“网络安全为人民，网络安全靠人民”签名活动在一餐广场展开。我校党委宣传部、外语学院、文化传播学院、会计学院、公共管理学院、财政税务学院、国际经济与贸易学院、计算机与信息工程学院的老师们，以及上万名学生积极参与

了此次签名活动，营造了网络安全人人有责、人人参与的良好氛围。本次签名活动，我校同步发放了《网络安全法》书籍，通过宣传展板宣传“上网安全”和“计算机安全”相关知识，传播文明上网常识，增强全校师生文明安全上网意识。此次活动的举办，增强了我校师生网络安全防范意识，提高了网络安全技能，有利于营造良好的校园网络使用的氛围，同时加强了我校师生对于维护网络安全的责任感和使命感。

四、效果突出，深入人心

1. 网络安全教育全新认知。通过本次活动，全校师生对网络安全教育又有了更深层的认识，既加强了网络安全宣传教育，又提升了师生们的网络安全意识和基本技能，构筑出了网络安全的第一道防线，在增强师生们的网络安全防范意识和自我保护技能方面都取得了较好的效果。

2. 网络安全意识显著提高。通过本次活动，号召师生们做“网络安全为人民，网络安全靠人民”的践行者、宣传者、保护者和捍卫者，教师们树立网络安全教育理念，弘扬正能量，传播网络安全理念，学生们认识到学习掌握网络安全知识的重要性，加强个人信息保护，共同创建安全的网络环境。

3. 网络安全素养有力提升。通过本次活动，教育师生们要敢于担当，大胆地同网络上的杂音噪音、歪风邪气作斗争，增强自己明辨是非、判别对错的能力，并提升网络文明素养，不参与有害和无用信息的制作和传播，切实履行应有的社会责任。师生们倡议携手共行，积极响应党中央关于净化网络文化环境的号召，传播文明、倡导文明、净化网络、引领风尚，争当网络“文明使者”。

网络安全防范知识（精选篇 3）

网络安全不仅涉及物理安全和技术安全，更涉及信息安全和意识形态安全。长期以来，高校的网络建设普遍存在重技术轻教育、重运用轻管理的现象，给网

络安全留下了隐患，这既不利于大学生的成长成才，还会对校园稳定和国家安全形成威胁。面对无处不在的网络安全威胁，大学生网络安全教育就非常必要了。

一、我国大学网络安全教育的问题分析

（一）网络安全教育认知不全面

网络安全教育的目的在于培养我国大学生基本的网络安全常识，掌握一定的网络安全知识与能力，进而正确应对和解决或降低网络安全事件带来的伤害，从而确保大学生的健康成长，然而我国的网络安全教育在实际教育过程中，教师、学校对网络安全意识认知不全面，未能形成一套系统、完善的教育方案，也严重缺乏相关机制，“重安全管理，轻安全教育”的现象严重，对学生进行网络安全教育时，也只是单一地宣讲安全意识防范的规章制度，并未做到实质性的安全教育和贯彻落实。

（二）大学生网络安全教育内容的单一性

我国严重缺失大学生网络安全教育的课程设置，极少部分设置网络安全教育课程的学校，其课程内容也局限于：计算机公共课，让学生们掌握计算机操作的基础知识；思想政治教育，为学生讲解网络道德等知识；各类讲座、宣传等进行案例分析。在实际教育过程中，这些课程实施机会较少或并未实施，导致大学生网络安全教育课程体系严重缺失。同时，我国大学网络安全教育内容不全面，严重缺乏网络安全教育实践，导致当前网络安全防范仅局限于不全面的理论知识，严重缺乏实际的防范操作，学生在发生网络安全事故后不能进行及时、正确地处理，从而导致学生个人信息的安全隐患。

（三）大学生网络安全教育资源的缺失

目前我国大学生网络安全教育在师资队伍建设和管理体系等方面严重缺失。学生要切实学习和掌握专业、扎实的网络安全防护知识与技能，就需要有专业、高水平的网络安全教育师资队伍，而我国大多部分高校网络安全教师都是辅导员、班主任、管理教师或是任课教师，专业知识和专业技能不全面、不扎实。网

络安全监管体系是保障大学生网络安全的关键。而我国高技网络安全监管体系还处于初期的基础形成阶段，对网络病毒、客攻击等方面的防御功能还有待提升，整个体系对网络安全的监督与管理功能未能得到充分发挥。

二、提升我国大学生网络安全教育的有效措施

（一）强化对大学生网络安全教育的认知

网络信息化在方便大学生学习、生活和社交方式的同时，也带来许多新的挑战。因此，要进一步提升大学生网络安全教育就需要强化社会和学校对大学生网络安全教育的认知，从国家安全和人才培养的高度明确网络安全教育的重要性。政府部门或社会团体要积极借助各种网络媒介进行安全教育宣传。高校要对结合高等教育的要求和大学生的特点，通过外部宣传和内部监管结合的方式进行大学生网络安全教育，提升高校网络安全教育的认知，有效提升大学生网络安全教育的效率。

（二）优化大学生网络安全教育内容

大学生网络安全教育的关键在于教育内容的优质性。因此，要加强大学生网络安全意识，就需要进一步优化网路安全教育的内容。充实网络心理健康和道德教育，网络安全法制教育，网络信息保护和防护意识教育，以及案例和实践教育等内容，提升大学生对网络信息的认识和辨别能力，加强大学生网络安全防护的理论知识，并通过案例和实践强化理论知识，强化实际操作能力，全面保障大学生的网络安全，确保大学生健康上网，健康成长。

（三）构建大学生网络安全教育体系

构建大学生网络安全教育体系是一项系统工程，需要坚持“全员育人”的理念，做好顶层设计和具体落实。

加强大学生网络安全教育的组织管理。建立学校和院系两级组织管理体系。高校应成立由校领导挂帅，党委宣传部、网络管理中心、学生处、教务处和保卫

处等部门负责人组成的网络安全教育领导小组，具体负责网络安全教育规划和制度的制定，定期研究和解决网络安全的重大事宜。党委宣传部具体负责全校内网络安全教育的宣传工作，育工作的思想方向；网络管理中心具体负责网络安全的监管和技术保障；学生处具体负责网络安全教育的培训和活动开展，提升网络安全教育的能力和效果等。院系应建立网络安全领导负责制，发挥辅导员、班主任的作用，配合好各职能部门的工作部署，将大学生网络安全教育落实落细。

加强大学生网络安全教育的制度建设。根据国家法律法规的规定，结合高校的育人目标和教育教学的实际，科学制定《高校网络安全教育规划》和《大学生网络安全教育和管理办法》。各院系结合学生特色，制定明确、操作性强的《大学生网络安全教育实施细则》和《大学生网络安全防护预案》。通过科学系统的制度，确保大学生网络安全教育长期有效的开展。

加强大学生网络安全教育的队伍建设。大学生网络安全教育的目标是强化大学生网络安全的认识、认同和意志，认识认同是形成意志的基础。在实现目标的过程中，认识和认同的形成过程中都离不开教育者的教育引导。 因此，大学生网络安全教育必须加强队伍建设。发挥理论课老师的主要作用，强化思想政治理论课和计算机基础课的教学。发挥辅导员和班主任贴近学生的优势，强化对学生的日常思想政治教育，及时发现并帮助解决学生的思想和实际问题。加强对任课老师、辅导员和班主任的培训，充实他们网络安全教育的理论储备；选拔他们中的优秀分子，担任学校的网络宣传员或评论员。严格对校内青年教师的选聘和培训，保证社会主义办学方向，杜绝不良言论。建立一支政治可靠强、技术精的网络安全监管队伍，净化网络空间。

创新大学生网络安全教育的阵地建设。面对互联网的复杂形势，高校必须主动出击，发出自己的声音，利用丰富多彩的新媒体和健康向上的内容吸引学生，打破网络上的西方霸权。建设融思想性、知识性、服务性和趣味性于一体的校内网站，根据大学生的需求，及时提供教育和服务。开辟网络安全防护专栏，重点介绍网络安全威胁和应对策略，提供网络安全技术指导。开辟网络互动平台，培

育有学生工作经验老师或者辅导员担任网络评论员，就大学生关注的意识形态或价值观的冲突斗争给予教育引导，就学生关心的时事政治事件给予科学理性的分析；在解决思想问题的同时，帮助大学生解决实际问题，宣传各项资助管理政策。与此同时，充分利用微博、微信和 QQ 群等新媒体，在质和量上牢牢掌握网络安全教育的主动权和话语权。

互联网所具有的技术特征使互联网本身在不同国家行为体之间没有偏向性的立场。然而，互联网可以借助国家对自己的使用和发展，逐步改造国际体系的权力结构。这就是互联网的“非中性”特征，服务于国家权力和国家利益。美国是互联网的创造者，至今掌握着互联网的核心技术和全球网络空间的制网权。随着中美实力差距缩小，美国对中国的战略骚扰和防范增多。这在美国借助网络加强对我国意识形态和价值观的渗透中表现尤为明显。网络安全已经构成对国家安全的威胁。大学生现在是我国网络的主要使用者，由于学识、阅历和技术的限制，他们比其他群体更容易受到网络安全的威胁。网络威胁不仅会影响大学生成长成才，还有可能危及国家事业。因此，对大学生的网络安全教育亟待加强。按照“积极利用、科学发展、依法管理、确保安全”的思路，加强大学生网络安全教育，为国家培养和输送合格建设者和可靠接班人。

网络安全防范知识（精选篇 4）

为贯彻落实全国网络安全和信息化工作会议的重要讲话精神，根据市委网信办《关于印发的通知》（雅委网信办 10 号）《石棉县国家网络安全宣传周活实施方案》文件要求，围绕“网络安全为人民，网络安全靠人民”的主题开展宣传活动，现将我乡宣传工作情况报告如下。

一、网络安全宣传工作开展情况

(一)高度重视，提高认识，确保网络安全宣传活动有序开展。成立由乡党委书记为组长，乡党委副书记、乡长和纪委书记为副组长的回隆彝族乡的国家网络安全宣传活动领导小组，对全乡网络安全宣传活动统一领导。由乡司法所和综治办等站所具体分工，明确职责，确保活动有序推进。

(二)精心组织，稳步推进，确保网络安全宣传活动保质保量。我乡高度重视本次网络安全宣传活动，通过干部职工会议传达全国网络安全会议的重要讲话精神。及时制定网络安全宣传学习活动实施方案，以村为单位有序开展工作。

(三)加强宣传，营造氛围，确保网络安全宣传活动达到目标。充分利用会议、标语横幅、宣传栏、LED 显示屏、微信群、到学校宣讲和发放传单等线下线上、室内与室外相结合的宣传方式，营造浓厚氛围，提高群众知晓率。

(四)深入基层，做好思想发动，确保活动取得实实在在的效果。开展志愿服务，组织乡、村青年深入农家、企业和学校开展网络安全宣传活动，在全乡小学通过开展主题班会、发放宣传资料等多种宣传方式，进一步宣传网络安全知识。

二、网络安全宣传活动取得的实效

1、思想认识得到提高。

通过网络安全宣传活动的开展，群众、企业、乡干部认识到网络便利生活工作的同时，存在手机中毒和账号密码、个人隐私等重要信息的泄漏等危害，认识到本次国家网络安全宣传活动的重要性。

2、加强了青少年教育。

通过开展网络安全进校园活动，强化了学生的网络安全意识，提高了防范网上有害信息的能力。

3、营造浓厚氛围。

通过线上和线下、室内和室外等宣传方式，在全乡营造网络安全的浓厚氛围，明确网络安全为人民，网络安全靠大家的主题，着力营造人人关注网络安全的良好氛围。四是长效机制得到确定。通过网络安全学习活动，初步建立起回隆乡网络安全工作制度，明确职责、分工，把网络安全宣传工作长期有效的开展，增长群众网络安全知识，提高警惕，预防网络诈骗。

网络安全防范知识（精选篇 5）

一、网络金融安全风险

（一）业务风险

网络金融建立于网络传输的高效、便捷的基础之上，互联网的金融服务因为其快捷的交易方式得到了迅速的发展。网络去联系交易方，有一定的虚拟性，从这个角度来看，这也加大了交易者身份的验证难度，无法避免出现交易者身份证明的交易误差，且信用评价不够透明，进一步增大了网络金融的使用风险。除此之外，还有一个重要问题是交易的信息风险，由于金融机构之间的信息不对称、传递信息的滞后性以及网络时代的信息污染，进一步对信息造成了影响。互联网金融作用于虚拟网络中，很多信息都是通过网上的数据进行的，比以往的传统金融业务方式更具有便捷的方式，同时也会随着用户的激增，带来大量的垃圾广告，影响到互联网金融企业的信息传递，最终带来信息风险。

（二）管理风险

目前我国缺乏独立自主的网络信息安全技术，我国的互联网金融企业所使用的配套硬件、软件系统都是****于发达国家，从本质上来看，我们缺乏对信息系统的了解程度和掌握程度，这就使得一些国外的不法分子很容易利用自身先进的技术侵入我国的金融系统当中。网络安全当下是金融行业发展遇到的一个比较棘手的问题，在互联网技术不断引进国内的同时，我们还会受到网络病毒的干扰，

进而对网络的使用造成一定程度的干扰。当下我过已经有了自主研发的原生态系统，但因为技术尚不成熟，存在着大量的漏洞和不稳定因素，这些都会威胁到使用的稳定性和安全性。所以，网络金融在良好的发展势头下没有成熟的技术支持，是当下其发展一个重要的问题。网络金融建立于互联网上，互联网本身的安全性和用户的操作规范有着较强的关联性，具体的风险可能因为系统的不完善以及有关产品设计的缺漏等等，会对自身的运营造成威胁。

二、网络金融安全的防范措施

（一）业务风险防范

任何事情在未到来前就要做好应对的准备，对于金融行业的风险防范更是如此。通常情况下，金融行业的事故之所以会发生，会造成大范围的影响，都是因为应急措施不够到位，在处理体系的设置上存在漏洞。所以，要想竭力避免有关的金融事故，就需要从根源降低业务处理的风险，建立健全系统处理机制，当下我国的业务风险防范主要从完善信用审核制度入手。近些年来，个人信用征信制度的投入使用使得我国的个人信用体系空白得到了弥补。在我国快速发展的金融行业，建立健全个人和企业的征信体系，更有助于促进网络金融行业的发展。这可以进一步降低网络金融的虚拟性问题，减少法律调节的障碍和成本。利用个人、企业的信用调查、认证、评级等服务，逐步实现征信的透明化，让一些信用不好的企业和个人，在互联网金融中难以立足，减少信用的使用风险。

（二）管理风险防范

随着社会的不断发展，金融行业的拓展规模越来越大，其管理的内容也越来越复杂。庞大的信息体系让我们感到无所适从，从传统的管理方式来看，一些管理方法和管理思路已经跟不上时代的发展。在大数据时代，海量的银行交易数据，再加上产品的功能和系统是金融行业处理风险的重要掌控点，在办理相关业务时，工作人员需要有谨慎的工作态度，避免出现工作的事物。企业方面也需要进一步提升功能和系统的稳定性、可靠性，配备上强有力的监控系统，使得整个互

联网金融可以得到正常的运行。金融软件的开发设计上，需要工作人员进一步严格要求自己，企业管理者要严格控制工作人员的开发产品质量，从而使其更好地投入运营和使用当中。大数据时代的特征为金融工作带来了诸多挑战，电子数据的高度集合化，使得金融行业的传统模式无法得到充分的发挥。由于金融工作的数量巨大，数字信息并不利于金融从业人员寻找重点，以此影响到金融从业人员的判断。数据结构的多样复杂性，使得数据内涵并不能再短时间内为金融工作者所理解和掌握，数据类型的多样性，使得金融从业人员的非结构化采集能力、分析能力都有待提升。

加大互联网的支付风险防范控制力度，因为支付作为互联网金融防范的重要环节，所以要进一步建立健全计算机的防火技术，建立网络安全管理制度，优化企业的内部管理和专人管理。掌握核心的技术，更好地应用于电子信息产品的开发。

三、结束语

随着经济全球化的进一步发展，我国金融市场也在不断践行对外开放的政策，在网络时代，金融的安全问题成为我们化解金融风险的重要问题。从一定程度上来说，网络具有较强的破坏力，比以往的呆账、烂账的危害更大，一旦出现了不可控的风险，则对于金融行业的打击是具有毁灭性的。所以，网络时代，金融行业要更加重视自身的安全防范体系构建，只有将其控制在手中，才能够更稳健地推进有关工作。

参考文献：

[1]陈秋颖，罗军.金融一体化、网络经济与金融会计风险防范－－以商业银行公司金融业务创新为案例[J].西南金融，20--，07：1-5

网络安全防范知识（精选篇 6）

随着计算机网络技术在社会生活中的各个领域的广泛应用，计算机网络技术提供巨大的信息含量和交互功能，提高了各个领域的工作效率，但是计算机网络安全问题也日益严重。

1 计算机网络信息安全的重要性

网络信息安全已成为国家、企业、个人都时刻关心的问题，一个脆弱的网络系统往往成为信息间谍、敌对势力、恐怖集团、国家之间信息战攻击的目标。随着美国正式开始实施“信息战”战略，网络安全已提升到维护国家、保护国家安全的高度。信息安全保障体系研究和信息安全支撑软件及平台研究已经列为国家“863”重点项目、应急项目。所以采用目前先进的信息安全技术，建成一个信息通畅、指挥灵活、反应快速、防范严密、易于管理的的全方位的信息安全防护体系，保障计算机网络能够安全、稳定、可靠地运行，并实现了信息安全是十分必要的。

2 计算机各种网络风险分析

2.1 计算机病毒

计算机病毒是指人为编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码，就像生物病毒一样，计算机病毒有独特的复制能力。它是网络安全的头号大敌。计算机病毒具有传染性、寄生性、隐蔽性、触发性、破坏性等特点。按其破坏性分为良性病毒和恶性病毒，计算机病毒可以破坏硬盘、主板、显示器、光驱等。计算机病毒在网络上传播后，会造成网络瘫痪，严重影响网络的正常运行。因此，提高对计算机病毒的防范刻不容缓。

2.2 黑客

黑客是在未经许可的情况下通过特殊技术登录到他人的网络服务器甚至是连接在网络上的单机，并对网络进行一些未经授权的操作的人员。黑客分为最传统的黑客和骇客。黑客攻击网络的手段是多种多样的，其中包括在 Cookie 中夹

杂黑客代码、隐藏指令、取得网站的控制权、制造缓冲区溢出和种植病毒等。其洛伊木马程序技术是最常用的黑客攻击手段，是在正常程序运行过程中央杂着额外操作代码，通过在用户的电脑系统隐藏一个会在 Windows 启动时运行的程序，从而达到控制用户电脑的目的。

2.3 系统漏洞

应用软件或操作系统软件在逻辑设计上的缺陷或在编写时产生的错误称为系统漏洞。系统漏洞可以被不法者或者电脑黑客利用，通过植入木马、病毒等方式来攻击或控制整个电脑，从而窃取电脑中的重要资料和信息，甚至破坏系统。这就使我们的计算机处于危险的境地，一旦连入网络，将严重威胁网络的安全。

2.4 配置漏洞

服务器、路由器、交换机、防火墙等配置不当造成安全漏洞。例如，服务器的配置不正确，导致它成为网络的瓶颈，存在极大的安全隐患，严重影响网络的传输效率。路由器配置不当将导致客户端无法上网，给用户造成不可估量的损失。

3 计算机网络安全防范对策

3.1 增强计算机网络安全管理

3.1.1 提高安全意识，建立专业的管理队伍

对于计算机个人用户而言，要不断加强网络安全意识的培养，对应用程序进行合法的操作，依据职责权利选择不同的口令，杜绝其他的用户越权访问网络资源。要重视对计算机病毒的防范，及时更新杀毒软件和安装补丁。而对于计算机网络管理人员要求更高些，增强安全意识的同时加强职业道德和工作责任心的培养，还要不断提升管理人员的专业技能，增强对网络的监察和评估。

3.1.2 落实网络安全管理的各项工作

网络安全维护除了应用先进的软件防御需要把网络管理的各项工作落到实处，加大网络评估和监控力度，对网络运行全过程进行监控，针对网络安全存在的风险提出修改意见，完善网络安全运行管理机制，营造优良的网络环境，做好设备维护工作，制定应急预案，确保计算机网络安全工作的科学性和时效性。

3.2 计算机网络安全技术防范措施

3.2.1 外部网络入侵的防范

计算机一旦联网，信息泄密的风险和防范难度就大大增加。外部网络入侵可以像幽灵一样游走在网络中，随心所欲地非法访问任意一台电脑，而不为人察觉。与外部实体入侵相比，外部网络入侵的方法更为隐蔽，手段更为多样，攻击范围更大。

针对外部网络入侵的特点，不仅需要建立健全安全制度，对网络入口进行严格管理和控制，还需要采取各种技术手段，及时发现网络入侵活动，杜绝网络入侵行为。目前阻止外部网络入侵的产品有杀毒软件和防火墙产品、数字证书和身份认证产品、漏洞扫描和入侵监测产品等，以及文件加密、密码机、传输加密、外部访问控制等产品。

3.2.2 防火墙技术

防火墙指的是一个由软件和硬件设备组合而成，在内部网和外部网之间，专用网与公共网之间的界面上构造的保护屏障。能够限制外部用户内部访问，以及管理内部用户访问外界网络。有效的控制信息输入输出是否符合安全规则，对包含不安全的信息数据进行过滤，防止内网数据和资源的外泄，强化计算机网络的安全策略，是保障计算机网络安全的基础技术。

3.2.3 计算机病毒防范技术

由于计算机病毒的破坏性和危害性很大，许多时候我们采取了各种措施仍然无法抵御计算机病毒、系统非法入侵、数据泄密、木马植入、漏洞非法利用等信

息安全事件的发生。所以在平时要使用防火墙保护数据防止外部入侵的攻击，使用防病毒软件防止病毒的破坏，及时进行病毒的更新，定期进行杀毒，在上网时要时刻注意网络的安全。

3.2.4 信息加密技术

随着互联网的应用也越来越普及，像 MAIL、QQ、MSN、BT 等即时通信工具和 P2P 工具都成了现代人工作的必备工具，然而 MAIL/QQ/MSN 的使用很容易造成文件泄密，还有 BT、电驴、ftp 等工具也有这种文件泄密的可能。所以要应用信息加密技术，保障信息数据传输的安全。

3.2.5 数据安全

主要涉及三个方面。一个是对重要数据的备份，二是对重要数据的恢复，三是文件删除后，是否进行了文件粉碎处理，以防删除的文件被恢复而泄密。

3.2.6 应用系统的安全

应用系统的安全主要是指各种业务应用软件，不同的单位之间有很大区别。这些应用系统完成各种业务功能，一旦运行出现故障，将使业务瘫痪。同时其数据是极其重要的，一旦丢失或泄密，可能导致严重后果。因此如何保障应用系统的正常运行和数据安全是信息安全的核心任务。为保障应用系统的正常运行，一是要登录授权控制，二是要保障系统安全，三是要做好数据备份。

结束语

计算机网络安全是一个有机的整体，疏漏任何一个环节其安全性就大打折扣，在这信息越来越发达的今天，对于防范网络的安全需要采取综合性技术手段就显得更为重要，信息安全的核心内容是保护数据的安全，所以要提高网络的安全意识，提高计算机技术知识，通过加强安全管理，才能保证由安全产品和安全技术组成的安全防护体系能够被有效的使用，为人们营造一个安全的网络环境。

网络安全防范知识（精选篇 7）

网络应用于教育领域，使教育信息的传播方式发生了改变，从而促使教育理念、教育模式、教学方法等发生极大的改变。网络教学已成为当今信息时代的一种重要的教学方式，在网络教学环境中课程转化为网络课程这种新的表现形式。网络课程是通过网络表现的某门学科的教学内容及实施的教学活动的总和[1]。

高职院校培养目标的定位是高端技能型、应用型人才，其核心竞争力在于培养的人才具有良好的专业综合素质和机敏的应变能力，而这样的人才所应具备的知识和技能在有限的课堂教学中是无法获取的。在《安全学基础》课程教学改革中，引进现代化教学手段和技术，教学方式采用课堂教学和网络教学混合学习[2]，意在拓宽安全知识的信息量，提高学生的学习兴趣。要通过网络来辅助课堂教学，关键要有一个适合教师与学生互动交流的网络平台，如何建立这个平台，又如何利用网络来实施辅助教学，这是教师首先要思考和研究的课题。基于以上考虑，*将对《安全学基础》网络课程的建设与教学实施过程进行探讨，并针对实施过程提出几点体会，希望能为同类院校的《安全学基础》网络课程的建设与发展提供参考。

1 《安全学基础》网络课程建设的内容

《安全学基础》课程是我院航空港安全检查专业的一门专业基础理论课程。课程目标是培养安检专业学生的安全意识，增强在工作岗位中预防和控制事故的技能。

该课程理论性较强，为增强学生的学习兴趣，并结合网络学习的特点，在网络课程建设上，以企业岗位要求为指导，采用内容模块化的组织方式，将知识点或教学单元作为学习主线，来组织构建课程内容，重视课程内容的可用性和可视性。