当前，青少年网络安全教育已经成为世界各国普遍关注的问题，国家的未来在青少年，网络的未来也在青少年。然而，我国在青少年网络信息安全意识教育方面缺乏体系化的知识架构、丰富的教育资源、科学的教育实施方案，高效的教育培养策略，这些都严重制约了国家网络强国梦和网络安全全民化、普及化的深入需求。

为了有效强化学生的信息安全意识，提升其信息安全防护能力，首先， 综合分析了国内外信息安全意识研究现状及研究意义；其次，针对当前教育资源存在的问题，结合学生自身特点，构建了相对健全的教育知识体系；接着，为了有效实现既定的教育目标，制订了一套科学、高效的教育实施方案，包括充足的实施准备和有序的实施过程；最后，进行具体的实证性研究，经过基础学习、实践训练、竞赛强化三个阶段的实践，采取多元评估模型验证分析实施成效，结果表明：该教育课程的科学实施可在一定程度上提高学生的信息安全意识水平，促进其认知、技能、道德三方面协调发展。

中国已是名副其实的网络大国，根据中国互联网信息中心的报告，截至2018 年 6 月，我国网民规模达 8.02 亿，互联网普及率高达57.7%，全球排名第一。但另外一些数据显示，中国与网络强国的目标仍有差距，主要表现在信息化程度滞后、核心技术受制于人、信息安全防护能力低、政策法规体系不完善、国民网络安全意识淡薄等等 。

在网络信息安全防护方面，信息安全意识已被公认为信息安全防护的第一道防线。为顺应时代的发展，贴合国家对于网络安全全民化、普及化的不断深入需求， 重点是为高中阶段信息技术教育引入全面的、全新的、实用的信息安全资源及科学有效的教育实施理念。以国家网络安全宣传周为契机、借助学校信息技术教学平台、运用好教育资源、加强网络安全教育、提升学生信息安全意识水平，已成为中小学信息安全教育发展和改革的必然趋势。

**1 信息安全意识教育现状及反思**

**1.1 国外研究现状**

为应对信息技术日新月异，网络形式复杂多变的现实挑战，世界各国特别是欧美国家均将加强网络信息安全意识教育作为提升网络安全保障能力的有效手段。经过十数年的努力， 现已从防御型网络安全教育步入全方位、多层次的教育阶段，目标明确、体系完备、活动丰富、主题鲜明。

**1.1.1 美国的信息安全意识教育**

早在 1999 年，美国政府制定的《国家信息安全战略框架》中就明确提出了信息空间安全意识教育，启动了国家信息安全教育培训计划（NIETP）[4]。从 2013 年起，将网络空间安全课程纳入中小学 PRE-K12 教育课程体系之中，实现了真正意义上信息安全教育从娃娃抓起。

此外，美国政府设立了多重项目以支持信息安全意识的培养，例如，中小学拓广项目。美国高校积极开展了一系列的信息安全意识培训项目。多所大学的信息安全办公室都建有主题教育网站。如：佐治亚大学使用 SecureUGA安全意识培训模型来培养学生和教职员工，建立个人意识的极端重要性。SecureUGA 中包括 10 个模块。分别为密码安全（PasswordSecurity）、社交网络（SocialNetworking）、合法下载（Legal Downloading）等。培训者可依次学习模块中的内容，完成测验，测验的分数必须达到 80 分及以上。

为了加强公民网络安全自我保护教育，提升网络设施的恢复力，美国政府从 2009 年开始将每年 10 月定为国家网络安全意识月，每年设定特定主题，并且意识月的每一周都设定关键议题 。之后，从 2011 年开始将每年 1月定为国家数据隐私月，旨在保护数据隐私，控制数据足迹。

**1.1.2 欧盟的信息安全意识教育**

欧盟也极具代表性，早在 1999 年，欧盟委员会就成立了“加强网络安全”项目（SIP）， 致力于提升青少年的自我防护能力，以达到趋利避害的目的 。在其中小学阶段设有网络安全课程，且体系设置有所不同，中学阶段以更加结构化的方式呈现，分类合理、特色鲜明，其中有9 个主题被重点强调。分别为在线安全行为、个人隐私、网络欺诈、下载和版权、会见网友、手机安全、电游成瘾、网购安全、病毒防御等。

为应对网络信息安全方面的挑战，2013 年起，欧盟委员会正式将每年 10 月定为“欧洲网络安全月”（ECSM），目标在于强化威胁认识、提高安全意识。

**1.2 国内研究现状**

为了改变现状，奋力变革，针对我国信息安全目前所面临的复杂形势，政府方面，2014 年中央网络安全和信息化领导小组成立，组长习近平总书记指出“没有网络安全就没有国家安全，没有信息化就没有现代化”，彰显我国的信息安全问题已经上升到了史无前例的战略高度 。

从 2016 年起将每年九月第三周确定为国家网络安全宣传周，并设计 7 个主题日，举办高峰论坛、创意视频大赛等活动。企业方面，国内的一些公司借鉴了国外优秀的信息安全意识培训项目，开发了相应的培训软件，形式也比较丰富，但他们主要针对公司企业员工，如： 谷安天下、亭长朗然。

在学校教育方面，部分包含在信息素养教育体系中，且国家侧重于专业技术人才的培养，关注大学生信息安全意识教育的较多，而关注中小学生的较少，比较有特色的则集中于北京、上海、深圳等一些发达城市，一方面，他们主要是借助网络安全公司以及警局的力量，聘请安全工程师和网警进校园开展主题教育、技术指导；另一方面，政府主导，公司配合建立网络安全主题教育基地， 开展游戏体验、网络攻防实验区等，寓教于乐。

虽然这些方式方法都值得其他城市学习借鉴， 但这需要政府大力支持、还需具备优越的条件。单从学校教育的角度来看，尚未形成体系化的知识架构，并制订完整的计划和实施方略，方便普通学校予以开展实施。

截至 2018 年 11 月， 笔者在多种文献数据库检索关键词“青少年、中学生”并与“信息安全意识、信息安全素养、网络安全意识”相关的研究论文，仅有 15 篇，具有代表性的有 7 篇 。

综上所述，通过分析欧美此方面的举措，不难看出，要实施国家网络安全战略，就务必重视信息安全意识教育，构建标准化知识体系， 将其纳入信息技术课程总体规划之中，通过意识教育促进信息安全核心素养的发展。

因此，我们要吸纳世界文明成果，汲取成功经验，引进先进的教育理念。通常情况下，关于信息安全意识的通识教育主要趋向于理论课程，而对于实践性课程来说，往往是专业性很强的大学学院才能够开设。这样很不利于普通学生整体意识能力水平的提升，与国家提出的关于提高学生综合分析以及解决问题的核心素养不相吻合。

因此笔者认为课程体系的构建应该理论与实践并重，而实践课程并非要像专业性的本科院校那样，学习密码技术、网络攻防、入侵检测等技能，而可以结合国情，紧密联系青少年在生活、家庭、社会中可能会遇到的一些信息安全问题， 加大对网络信息安全基本技术操作的教育。例如计算机基础性安全、无线网络安全配置等等。

**2 信息安全意识教育体系建设**

学生信息安全意识，即在日常学习生活中， 察觉、识别、发现、解决与自身紧密联系的信息安全问题的能力，以及严格规范自我安全行为的修养，具体可包括认知、技能、道德等方面的素质，最终确保个人设备、计算机信息网中的硬件、软件、数据安全，形成牢不可破的防护体系 。依据基本概念，遵循学生自身发展需要，并融合欧美信息安全意识教育文化和现代资源建设理念，构建相对健全的知识体系。

**2.1 理论知识教育体系**

主要包括三大类 31 项基础知识，内容涵盖指导方针、安全概念、风险与提示 。指导方针即青少年在网络世界应该遵守的道德准则和文明公约等政策法规，如表1 所示；安全概念即介绍信息安全领域的一些专业术语及其概念， 如：病毒、特洛伊木马、网络钓鱼、恶意软件、社会工程攻击等，如表 2 所示；风险与提示即青少年使用互联网或数码设备存在的信息安全风险，以及相应的防范措施或小贴士，如表3 所示。

表 1 指导方针内容表

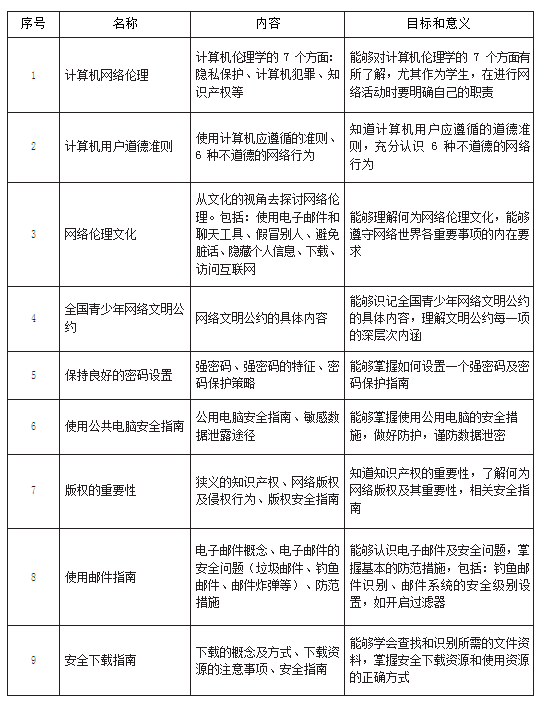


表 2 安全概念内容表

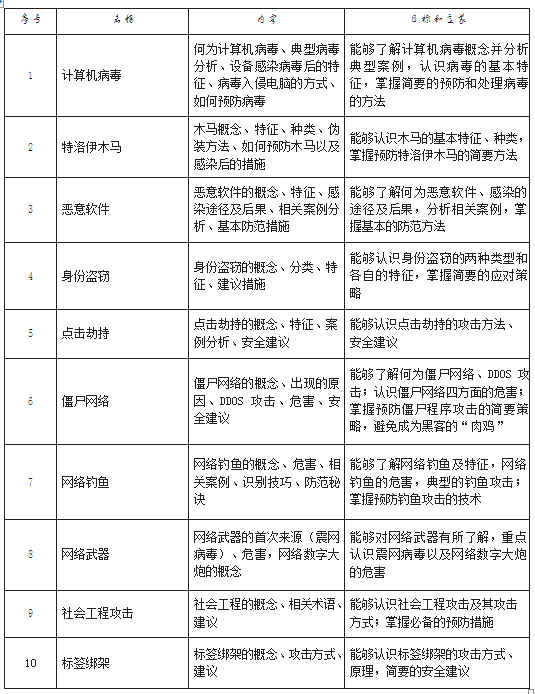
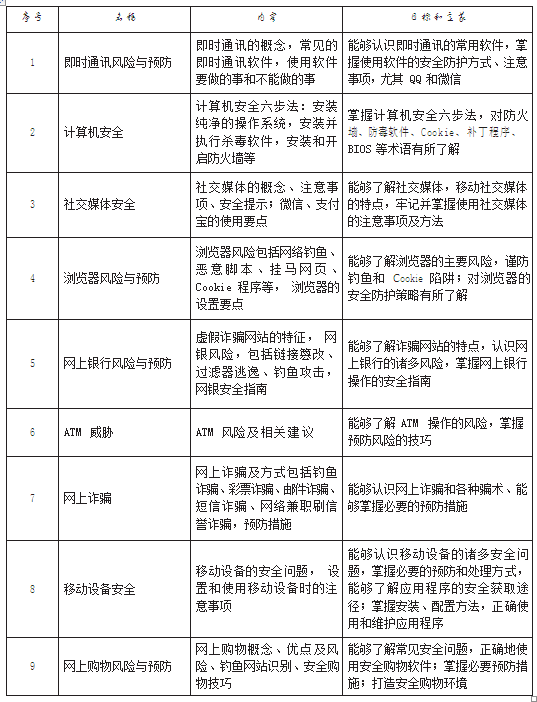
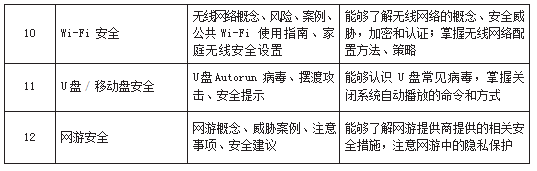


表 3 风险和提示内容表

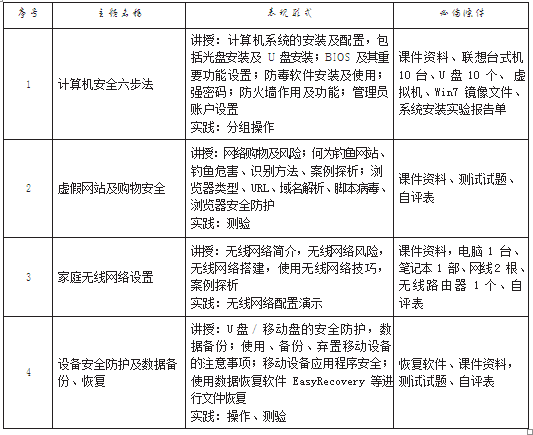




**2.2 实践活动教育体系**

主要分为四个主题，如表 4 所示。通过四个主题的重点讲解和实践练习，能够使学生对生活、家庭关系密切的信息安全问题有更深入的认识，提升其认知水平，并增强其最基本的技术操作能力。

表 4 信息安全意识实践课程体系



**3 信息安全意识教育实施方案**

目标：明晰青少年信息安全意识的概念，认识网络信息安全是每个人的责任，学习网络信息安全知识，了解网络攻击者的常用伎俩， 掌握基本的防治方法，并遵循必要的安全指南， 养成良好的设备使用习惯，增强保护数据和隐私的行为，提升信息安全防范意识。

方案包括两方面：一是实施准备。具体包括思想准备、条件保障、组织分工；二是实施过程。具体包括理论学习、实践训练、竞赛强化。

**3.1 实施准备**

**3.1.1 条件保障**

学校不仅应加强信息中心的建设，还要制作、开发各种优质的实体资源。

信息安全实验室主要依托信息技术中心来建立。其一，基本设备齐全。其二，为学生搭建真实的实践操作平台。其三，打造精品实验室， 精心设计布置，将每年的培训资料，学生创作的作品等重要资料归档整理，集中展示此方面的突出业绩。

信息安全意识手册。主要借助 Indesign 进行设计，浓缩了学生日常生活中可能遇到的各种信息安全问题、以及针对相应问题的防治方法、解决对策，通过翻阅和学习，可在无形之中激活学生的认知敏感度。

信息安全认知在线，如图 1 所示。主要采用LAMP架构进行开发，网站中应提供两项内容：主题教育和测评工具。包括三大类主题 31 项基础知识、微课 8 个、安全意识视频 10 个、测试题 70 道、电子书 4 册、课件 10 个等，总数据量约450M。



*图 1 信息安全认知在线*

认知在线与教育读本结合学习，可发挥出主题网站最大的效果。网站既可供学生自行浏览，也可经教师指导性学习。考虑到学生在浏览的过程中存在“惰性”，自控能力可能不强，学校可统一开放三周时间，便于学生集中学习， 三大类主题每项基础知识规定固定时间，教师可稍做讲授、点拨，并让学生完成基础知识后面的诊断性测试题，上传至服务器端，以备教师检查。

最后需留出40 ～ 50 分钟时间，自主浏览资源库中的电子书、课件等内容，并利用测评工具进行自主测试，教师可通过管理员账号查看成绩及未通过学生的情况，督促其学习相应知识，再次测试，直至成绩合格。

**3.1.2 思想准备**

思想统一、重视，行动方能一致，在九月中旬，应适时的开展一次动员大会，侧重于传达及研讨课程实施的细则，此外，在新生信息技术教学中宣讲国家有关网络信息安全的相关法律、法规及重大的活动事项等内容，重点是应结合当地特色、学生特点宣传开展信息安全教育的意义，让学生认识到加强此方面教育的重要性，以及作为新时代的学生应掌握哪些知识、技能，达到什么目标，最终让学生通过接受一系列的教育培养， 从而具备高度的社会责任感，形成积极向上的价值观，提升整体素质。

**3.1.3 组织分工**

组织分工主要是组织、协调学校相关处室， 统筹兼顾，助推学生信息安全意识教育有效开展。

教导处主要负责信息安全意识教育实施计划、各项规章制度的制定；对教育教学进行有效分工；负责组织信息中心开发信息安全学习网并架设服务器、制作并发放资料，征订课外读物，张贴海报供学生观看学习；检查知识考查、意识测验、技能测试、竞赛评比等的实施情况与工作质量；做好资料整理、总结工作。

政教处主要负责信息安全方面道德伦理、法律、法规宣传教育。借助主题班会、课间集会集中学习《未成年人网络保护条例》等法规知识，进行主题征文比赛、开展板报设计，多管齐下， 全面提高学生的网络信息安全价值观的形成。

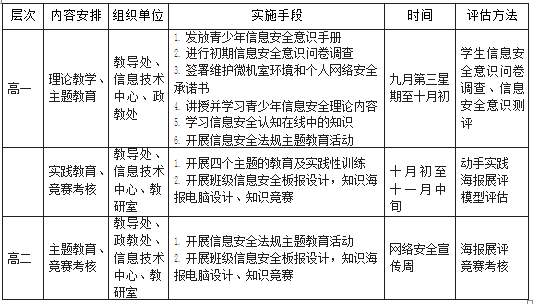
信息技术中心主要负责向全体学生宣讲国家网络安全相关政策，开展网络安全知识讲座及网络安全防范技能培训；负责信息安全意识教育体系的设计、课程讲授；网站资源的更新； 整合素材，制作学习手册、宣传海报；知识考查、意识测验、竞赛评比的实施；撰写总结性报告和相关资料上交。

教研室主要联合信息技术中心进行信息安全知识竞赛的实施工作，包括试题的搜集、整理、编创、制版、考核、分析等工作。

**3.2 实施安排**

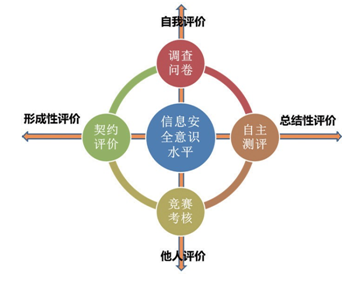
表 5 是具体的实施安排，主要通过分层次、分阶段来完成，20 学时左右，各学校可根据自身情况进行调整。

表 5 教育实施安排表



**4 信息安全意识教育实施成效**

为了检验应用效果，一方面利用 8 周时间，在本校内进行整体课程的实施；另一方面利用3周时间选取三所兄弟高中进行理论课程的教育及测评。共计 2390 人。在课程实施的基础上，结合契约、测验、竞赛三种手段对学习情况进行评价。依据课程教育目标，笔者设计了自我评价与他人评价相结合，形成性评价与总结性评价相结合，传统评价与信息化评价相结合的四位一体、三结合多元评估模型，如图 2 所示。



*图 2 信息安全意识多元评估模型*

**4.1 契约评价**

契约评价来源于学习契约论，是指学生在受教育之前与学校签订协议或承诺书，建立一种遵守规则的契约，起到约束以及修正自身行为的作用。在进入微机室及实验室学习之前， 签订《维护微机室环境和个人网络安全承诺书》， 如学习期间没有违反，则此项评价为优秀，如果出现了问题，则按照责任书的要求进行惩罚。大多数学生自律性较高，能够严格遵守契约内容，较认真地完成学习任务。

**4.2 自主测验**

利用测评工具进行测试。工具主要通过Quizmaker 制作完成，Quizmaker 属于 E-learning 开发软件 ArticulateStudio中的一个模块，用其设计的测评软件，可用于快速评估学生成绩，且试题种类齐全、形式新颖，PC 端和移动端皆可使用，如图 3 所示。

测试题严格按照理论指标体系的各知识要点设计，共计70 题项，每次测试将会随机抽取 60 题，回答正确率达到 80%方可通过。据后台数据统计，有78% 的学生一次性通过测试，剩余的则经过第二次测试顺利通过，从某种程度上反映学生已基本掌握基础知识，信息安全意识水平得到初步提升。

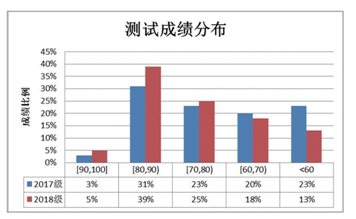


*图 3 信息安全意识测评工具页面*

**4.3 竞赛考核**

竞赛考核重点在于检验课程学习后的效果。主要利用预先设计的网络信息安全知识竞赛两套试题，百分制，其中一套难度稍高。此外， 将实践科目的知识点融入案例分析题中。分析题分别涉及个人电脑安全、Wi-Fi 安全、移动设备安全、网购安全等。通过初步分析考核情况，得出一些理想的数据。如图 4 所示。

进一步分析案例题的解答情况，可知大部分学生对基础概念性及技巧性的知识掌握得较理想，能够比较有条理地列出设置及防范要点。例如：个人计算机安全，多数同学不仅能够详细地列出六步法，根深蒂固、密码防护、百毒不侵、火之铠甲、安全视窗、自强不息，而且还能够进一步写出 BIOS 和防火墙的基本功能及强密码的设置要求。



*图 4 竞赛考核成绩分布*

研究结果表明：该信息安全意识课程的科学实施能够在一定程度上提高学生的信息安全意识水平，促进其认知能力、应用防护、道德规范等方面协调发展。

通过本次研究，已初步形成一整套从理论、实践到实施和评价的教育体系，可帮助学生识别信息安全威胁、规避信息安全风险、加强道德伦理和法律法规教育，提高其基本的信息安全防护能力，为国家将来培养高素质、优秀的专业人才奠定扎实基础。

（1）将研究锁定于信息安全意识教育，在分析了国内外信息安全意识、素养教育等相关资料的基础上，针对知识架构不健全、资源建设不完善等问题，上升至难题破解，教育培养的高度。突破了以往研究只分析学生信息安全意识现状及对策，而没有重点设计课程体系和开发适合学生学习的资源。

（2）形成了一套完整的课程体系，包括理论知识教育体系和实践活动教育体系。此外还包括一套科学、高效的教育实施方案，针对性地提出基础学习、实践训练、竞赛强化三步法则以及信息安全意识多元评估模型，实现对学生信息安全意识各要素协调发展、整体水平稳步提升。

将教育资源与实际应用相结合。选取一定区域范围内的学生为实验对象，进行跟踪调查、实证研究、验证假设，充分体现教育资源的应用价值，为意识教育提供有力的运用支撑，为高中信息安全教育开辟新的天地。

**5 结语**

青少年是国家的未来和希望，国家的未来在青少年，网络的未来也在青少年。在建设网络强国，携手共建网络命运共同体的关键时期，不仅需要政府主导、典范带动，更需要全民参与，汇聚正能量，贡献中国大智慧。只希望本研究能为其他学校开展网络信息安全教育提供借鉴，能抛砖引玉，引来更多教育实践者在此方面的开拓与创新，使其真正的全民化、大众化、常态化、规范化。

**作者简介**

董李鹏，理学硕士，全国未来科学家创新大赛优秀指导教师。研究方向为信息技术与教育应用，青少年信息安全意识培养研究。

*选自《信息安全与通信保密》2019年第十一期 （为便于排版，已省去原文参考文献）*

声明：本文来自信息安全与通信保密杂志社，版权归作者所有。文章内容仅代表作者独立观点，不代表安全内参立场，转载目的在于传递更多信息。如有侵权，请联系 anquanneican@163.com。

链接：https://www.secrss.com/articles/15539