

附件 1

课程思政教学案例
(2024 年度)

案例名称	慧眼识诈——网页诈骗防范		
课程名称	HTML5	负责人	秋彦芳
开课单位	计算机信息工程系	依托专业	计算机应用技术

课程名称： HTML5

课程代码： 010020034

课程学分： 3

总 学 时： 72 (理论学时： 0 实践学时： 72)

授课对象： 二年级

课程类型： 专业技能课

一、授课教师基本情况

秋彦芳，中共党员，副教授，骨干教师。从教 20 载，坚定政治立场，爱岗敬业，以德育人。积极教改，成果丰硕，发表论文 10 篇，参编教材 7 本，获专利 3 项。指导学生获一带一路技能创新大赛佳绩。深受学生爱戴。

二、课程及案例简介

本课程旨在通过剖析网络诈骗的常见类型与防范策略，提升学生的网络安全意识和自我保护能力。课程结合思想政治教育，引导学生树立正确的价值观，增强社会责任感，培养理性消费和谨慎行事的良好习惯。以“守



护财产安全”为主线，将思想政治教育融入网络诈骗防范的各个环节。通过案例分析、小组讨论、角色扮演等多种教学方式，让学生在实践中感受诚信的重要性，增强社会责任感，提升自我保护能力。课程以理论讲授为基础，结合实际案例分析，引导学生深入理解网络诈骗的危害和防范策略。通过互动式教学，激发学生的学习兴趣 and 参与度，培养他们的批判性思维和解决问题的能力。实施效果显著，学生的网络安全意识和自我保护能力得到明显提升。

三、结合章节

本案例结合《互联网应用开发技术（HTML5）》课程中，项目 4 运用 float、position 和 flex 属性完成网页布局相关知识点。

四、教学目标

思政目标：培养学生的诚信意识和社会责任感，反对任何形式的欺诈行为。引导学生树立正确的价值观，理性消费，谨慎行事。

知识目标：掌握内外边距的用法、overflow 属性属性的用法、文本阴影、盒子阴影的用法。

能力目标：能独立完成文化主题网页架构设计，能够识别网络诈骗的常见手段、具备基本的网络诈骗防范能力。

素质目标：提升学生的网络安全意识和自我保护能力。培养学生的批判性思维和解决问题的能力。

证书目标：为学生考取前端开发相关证书奠定基础，提升学生的职业竞争力。

五、案例意义

本案例通过剖析网络诈骗的常见类型和防范策略，将思想政治教育融入网络安全教育中。案例选用的意义在于：一方面，帮助学生提升网络安



全意识和自我保护能力；另一方面，引导学生树立正确的价值观，增强社会责任感，培养理性消费和谨慎行事的良好习惯。

六、教学过程实施

本课程的教学过程实施以“以学生为中心”为核心理念，通过网络诈骗案例，将思想政治教育有机融入网络诈骗防范教学中，旨在提升学生的网络安全意识、自我保护能力以及思想政治素质。

（一）了解学生基础，精准定位教学起点

在课程开始前，通过与学生谈话，全面了解学生对网络诈骗的认知程度、防范意识以及他们在网络使用中的实际行为。基于这些信息，课程设计能够更精准地定位教学起点，确保教学内容贴近学生实际，教学方法符合学生学习习惯。

（二）教学内容设计：专业性、前沿性与思政性的融合

1. 专业性与前沿性并重

教学内容涵盖网络诈骗的常见类型、技术手段、防范策略等多个方面，既包括传统的刷单返利、虚假投资等诈骗类型，也涉及最新的 AI 换脸诈骗、虚拟货币诈骗等前沿案例。通过深入剖析这些案例，学生不仅能够掌握网络诈骗的基本特征，还能了解诈骗手段的不断演变趋势，提升对新型诈骗的识别能力。

2. 思政性贯穿始终

在教学内容中融入思想政治教育元素，引导学生树立正确的价值观和消费观。例如，在分析诈骗案例时，强调诚信、法治、责任等价值观的重要性，引导学生认识到任何形式的欺诈行为都是对社会的伤害，都是违背社会主义核心价值观的。

（三）教学方法：参与式、互动式与体验式的有机结合



参与式教学：通过小组讨论、案例分析等方式，鼓励学生积极参与课堂活动。例如，将学生分成若干小组，每组负责分析一种网络诈骗类型，从诈骗手段、受害者心理、防范策略等多个角度进行深入探讨。小组讨论后，各组选用相应的素材来制作诈骗网页，这种教学方式不仅激发了学生的学习兴趣，还培养了他们的团队合作能力和批判性思维。

互动式教学：利用在线平台，开展实时问答、投票等互动环节。例如，在讲解网页内容诈骗防范策略时，通过在提问的问题，引导学生思考并回答。增强防范意识。

（四）教学理念与创新：以学生为中心，促进主动学习

以学生为中心的教学理念：课程设计充分体现“以学生为中心”的理念，注重学生的主体性和参与度。在教学过程中，教师扮演引导者和支持者的角色，鼓励学生主动探索、积极思考。同时，根据学生的反馈和需求，及时调整教学内容和方法，确保教学过程的针对性和有效性。

混合式教学模式的创新：结合线上和线下教学优势，构建混合式教学模式。线上教学提供丰富的学习资源，如视频讲座、案例分析、互动测试等，方便学生随时随地学习。线下教学则通过小组讨论、角色扮演、案例分析等方式，深化学生对知识的理解和应用。这种教学模式不仅提高了教学效率，还满足了学生个性化学习的需求。

持续评估与反馈机制的建立：通过网页制作的作业、测试、项目等多种方式，持续评估学生的学习效果。同时，建立及时的反馈机制，根据学生的评估结果，调整教学策略，提供个性化的学习建议。这种评估与反馈机制不仅有助于提升教学质量，还能激发学生的学习动力，促进他们的主动学习。

（五）课程思政融入



本案例通过深入剖析网络诈骗的常见类型、技术手段及防范策略，将诚信教育、法治观念和社会责任感等思政元素自然融入其中。在讲解诈骗网页制作过程中，通过展示真实的网络诈骗案例，比如有人收到短信声称中奖了，需要点击链接领取奖金；或者有人在网上购物时，遇到了低价促销的陷阱，付款后却收不到商品。这些案例都是学生们在日常生活中可能遇到的，因此他们很容易就能产生共鸣。另外，让学生讨论诈骗者是如何设计陷阱的，他们利用了人们的哪些心理弱点；为什么有些人会轻易上当受骗，他们在面对诱惑时缺乏了哪些判断力。通过这样的分析，学生们不仅能更深入地了解网络诈骗的危害，还能逐渐认识到诚信、谨慎和理性思考的重要性。通过这个思政融入的教学案例，学生们不仅学到了如何防范网络诈骗的知识和技能，还深刻理解了诚信、法治和社会责任等价值观的重要性。

案例效果：



警惕网络诈骗，守护财产安全

网络诈骗手段层出不穷，以下是一些常见的诈骗类型，请务必提高警惕，保护自己的财产安全。



刷单返利类诈骗

展示“刷单返利”界面，以“高额返利”诱惑用户点击，实则骗取钱财。



虚假网络投资理财类诈骗

展示“高收益投资平台”界面，以“快速致富”宣传语诱导用户投资，实则平台虚假。



虚假购物、服务类诈骗

展示“低价促销”购物界面，吸引用户下单，但付款后可收不到商品或服务。



冒充电商物流客服类诈骗

以“商品质量问题”、“物流异常”等理由，诱导用户点击链接或提供个人信息。



贷款、代办信用卡类诈骗

以“低门槛、高额度”为诱饵，吸引用户申请，随后以各种名义收取费用。



虚假征信类诈骗

声称可以花钱消除不良征信记录，实则骗取用户钱财。



冒充领导、熟人类诈骗

以“紧急情况”或“帮忙转账”为由，要求用户转账，实则对方为骗子冒充。



冒充公检法类诈骗

声称用户涉嫌违法犯罪，要求配合调查并转账至“安全账户”。



网络婚恋、交友类诈骗

展示“交友平台”界面，诱导用户充值会员或购买虚拟礼物，实则与用户聊天的可能是“托”或机器人。



网络游戏产品虚假交易类诈骗

展示“游戏装备交易”界面，诱导用户点击链接或转账，实则交易平台为虚假。



小测试：你能识别诈骗吗？

假设你收到一条短信，声称你中奖了，需要点击链接领取奖金。你应该怎么做？

保持警惕，不点击链接

立即点击链接领取奖金

防范指南

- 不轻信陌生信息，尤其是涉及金钱的请求。
- 保护个人信息，不随意透露给陌生人。
- 遇到可疑情况，及时与家人、朋友或老师商量。
- 安装并更新防病毒软件，定期检查账户安全。
- 如遇诈骗，立即报警并保留相关证据。

遇到诈骗怎么办？

如果你或身边的人遇到诈骗，请立即采取以下措施：

1. 保留所有相关证据，如聊天记录、转账记录等。
2. 立即拨打110报警，或向当地公安机关报案。
3. 如需网络举报，可访问[中国互联网举报中心](#)。

七、实施效果

通过本案例的教学实施，学生的思想政治素质得到明显提升。他们更加注重诚信和社会责任，能够理性消费，谨慎行事。同时，学生的网络安全意识和自我保护能力也得到显著增强，能够有效识别和防范网络诈骗。

八、教学考核评价

采用多元考核评价方式，包括课堂表现、小组讨论、案例分析报告等。

设立过程性考核和终结性考核相结合的评价体系。

考核目标与课程目标对应：

课堂表现：评价学生的参与度、思维活跃度等。

小组讨论：评价学生的团队合作能力、批判性思维等。

案例分析报告：评价学生的分析能力、解决问题的能力等。



九、创新与示范

典型经验和做法：将思想政治教育融入网络安全教育，实现知识传授与价值引领的有机结合。采用案例分析法、小组讨论法、角色扮演法等多种教学方式，提升教学效果。引入互动式教学，激发学生的学习兴趣 and 积极性。本案例的成功经验可逐步推广到其他课程形成具有示范意义的思政教学模式。

十、案例反思

本案例通过剖析网络诈骗的常见类型和防范策略，有效提升了学生的网络安全意识和自我保护能力。同时，通过思想政治教育的融入，培养了学生的诚信意识和社会责任感。

存在的问题及改进思路：

案例更新速度需加快，以适应网络诈骗手段的不断变化。需进一步加强学生的实践操作能力