

2024-2025 学年初中信息技术（信息科技）七年级 下册苏科版（2023）教学设计合集

目录

一、第五单元 互联网安全维护——争做网络安全推广员

1.1 一、项目分析

1.2 二、项目探索

1.3 三、项目开展

1.4 本单元复习与测试

二、第六单元 互联网与创新——制作数字化变革全景图谱

2.1 一、项目分析

2.2 二、项目探索

2.3 三、项目开展

2.4 本单元复习与测试

第五单元 互联网安全维护——争做网络安全推广员一、项目分析

授课内容

授课时数

授课班级

授课人数

授课地点

授课时间

设计意图

本节课旨在通过分析互联网安全维护的实际案例，帮助学生深入了解网络安全的重要性，培养他们自觉维护网络安全的意识。结合初中信息技术（信息科技）七年级下册苏科版（2023）第五单元的内容，让学生在掌握网络安全基础知识的基础上，通过项目实践，提高网络安全防护能力，为争做网络安全推广员做好准备。

核心素养目标

培养学生信息意识，使其能够主动关注网络安全问题，识别网络风险，提高自我保护能力；发展计算思维，通过分析网络安全案例，学会运用逻辑推理和创造性思维解决问题；增强信息社会责任感，培养积极参与网络安全宣传和维护的行动力，为构建清朗网络空间贡献力量。

学习者分析

1. 学生已经掌握了哪些相关知识：

学生在之前的学习中已经接触了计算机基础操作、网络基本概念以及简单的网络应用，对互联网有初步的了解和认识。

2. 学生的学习兴趣、能力和学习风格：

学生对互联网充满好奇心，对网络安全有一定的兴趣。他们具备一定的逻辑思维能力和问题解决能力，喜欢通过实践操作来学习新知识。学生中有些倾向于独立探索，有些则更偏好团队合作。

3. 学生可能遇到的困难和挑战：

学生可能对网络安全的专业术语和复杂概念感到困惑，需要通过具体案例来加深理解。此外，将理论知识应用于实际操作时，可能会遇到技术操作上的困难，需要老师的耐心指导和鼓励。同时，对于网络安全意识较强的学生，可能会对网络环境中的风险和挑战感到担忧，需要引导他们以科学的态度对待网络安全问题。

教学方法与策略

采用讲授与案例研究相结合的方法，通过讲解网络安全基础知识，辅以实际案例进行分析，使学生理解网络安全的重要性。设计角色扮演活动，让学生模拟网络安全推广员角色，提高参与度和互动性。利用小组讨论，鼓励学生分享网络安全知识和个人经验。同时，运用多媒体教学资源，如网络安全宣传视频，增强学生的学习兴趣 and 视觉效果。

教学流程

1. 导入新课（5分钟）

详细内容：通过展示一组网络安全的新闻图片或视频，引发学生对网络安全问题的关注，提问学生：“你们在生活中遇到过网络安全问题吗？是如何解决的？”以此引出本节课的主题“互联网安全维护——争做网络安全推广员”。

2. 新课讲授（15分钟）

详细内容：

- 讲解网络安全的基本概念，包括网络安全的重要性、常见的网络威胁和攻击手段。
- 介绍网络安全防护的基本方法，如设置复杂密码、定期更新系统、使用安全软件等。
- 分析网络安全案例，让学生了解网络安全问题的实际影响和应对策略。

3.

实践活动（15分钟）

详细内容：

- （1）分组进行网络安全知识问答游戏，通过抢答方式检验学生对网络安全知识的掌握。
- （2）模拟网络安全推广员角色，每组设计一份网络安全宣传海报或宣传口号，并进行展示。
- （3）进行网络安全模拟演练，让学生在模拟环境中识别网络风险，并采取相应防护措施。

4. 学生小组讨论（10分钟）

内容举例回答：

- （1）讨论网络安全风险识别的方法，举例：如何识别可疑邮件和链接？
- （2）讨论网络安全防护措施的实用性，举例：为什么需要定期更新系统和软件？
- （3）讨论如何有效地推广网络安全知识，举例：如何制作吸引人的网络安全宣传材料？

5. 总结回顾（5分钟）

内容：回顾本节课所学内容，强调网络安全的重要性，总结网络安全防护的基本方法。提醒学生将所学知识应用到实际生活中，争做网络安全推广员。强调网络安全是一个持续的学习过程，鼓励学生在课后继续关注网络安全动态。

总用时：45分钟

教学资源拓展

拓展资源：

1. 拓展网络安全知识，包括但不限于以下内容：

- 网络病毒的传播途径和预防措施
- 个人信息保护的方法和策略
- 网络诈骗的常见形式和识别方法
- 网络隐私权的相关法律法规
- 国内外网络安全事件案例分析

2. 拓展网络安全技术，包括以下方面：

- 防火墙和入侵检测系统的原理和应用
- 加密技术的种类和应用场景
- 安全漏洞的识别和修补
- 网络安全监测和应急响应

3. 拓展网络安全意识培养，包括以下内容：

- 网络安全意识的内涵和重要性
- 网络安全教育与培训的方法
- 网络安全文化的建设和推广
- 网络安全宣传活动的策划和实施

拓展建议：

1. 鼓励学生阅读网络安全相关的书籍和杂志，如《网络安全技术与应用》、《网络安全与隐私保护》等，以加深对网络安全知识的理解。
2. 推荐学生参加网络安全知识竞赛和讲座，如“全国青少年网络安全竞赛”、“网络安全公益讲座”等，以提高网络安全技能和意识。
3. 建议学生关注网络安全领域的最新动态，如订阅网络安全相关的博客、微博、微信公众号等，以保持对网络安全信息的敏感度。

引导学生参与网络安全社区和论坛，如“FreeBuf”、“知道创宇”等，与其他网络安全爱好者交流学习，共同进步。

5. 鼓励学生在生活中实践网络安全知识，如定期更新个人设备的操作系统和应用程序，使用复杂密码，不随意泄露个人信息等，将网络安全意识转化为实际行动。

6. 提倡学生参与网络安全志愿服务活动，如协助社区开展网络安全宣传活动，为老年人提供网络安全培训等，以实际行动维护网络安全。

作业布置与反馈

作业布置：

1. 网络安全知识问答：设计一份包含 10 道选择题和 5 道简答题的问卷，内容涵盖本节课所学的网络安全基础知识、防护措施以及案例分析。要求学生在课后独立完成，以检验对课堂内容的理解和掌握。

2. 网络安全宣传方案：要求学生结合本节课所学，设计一份网络安全宣传方案。方案应包括宣传主题、目标受众、宣传方式（如海报、视频、讲座等）、预期效果评估等。鼓励学生发挥创意，将所学知识应用于实际。

3. 网络安全日志：要求学生记录一周内的网络安全行为，包括使用的防护措施、遇到的网络安全问题及解决方法。通过日志记录，让学生养成良好的网络安全习惯。

作业反馈：

1. 对于网络安全知识问答，我将及时批改并记录学生的得分情况。针对错误较多的题目，我将提供详细的解释和指导，帮助学生理解正确的答案和解题思路。

2. 对于网络安全宣传方案，我将重点关注学生的创意和实际可行性。我将提供个性化的反馈，指出方案的亮点和需要改进的地方，如宣传方式的创新性、目标受众的准确性等。

3. 对于网络安全日志，我将检查学生的记录是否详尽、真实。我将给出建议，如如何提高日志的条理性和分析性，以及如何从日志中发现自身的网络安全习惯漏洞。

在作业批改过程中，我将注意以下几点：

- 对学生的作业给予积极的评价，鼓励他们的努力和进步。
- 针对存在的问题，提供具体的改进建议，帮助学生明确下一步学习方向。
- 对于表现优秀的学生，我将给予表扬，并鼓励他们继续深入研究网络安全领域。
- 定期与学生进行一对一交流，了解他们在完成作业过程中的困惑和需求，提供个性化的指导。

教学反思与改进

在完成“互联网安全维护——争做网络安全推广员”这一课后，我进行了深入的教学反思。我设计了一个反思活动，通过学生的反馈、作业完成情况以及课堂互动情况来评估教学效果，并识别出了以下几个需要改进的地方。

首先，我发现学生在网络安全知识问答环节的参与度不高，部分学生对理论知识感到枯燥。这提示我需要在未来的教学中加入更多的互动环节，比如小组竞赛、游戏化学习等，以提高学生的参与度和兴趣。

其次，在网络安全宣传方案的设计上，学生的创意和实际操作能力有待提高。我意识到可能是我没有给予足够的指导和支持。因此，我计划在未来的教学中，提供更多的案例分析和设计指导，帮助学生打开思路，提升他们的创新能力和实践能力。

另外，学生在网络安全日志的记录上，内容较为简单，缺乏深入分析和反思。我认为这可能与学生对于网络安全重要性的认识不足有关。接下来，我将加强对学生网络安全意识的培养，通过讨论网络安全事件的影响，让学生更加深刻地理解网络安全的重要性。

针对以上反思，我制定了以下改进措施：

1. 引入更多的互动式教学方法，如小组讨论、角色扮演等，让学生在互动中学习和思考，提高他们的学习积极性。
2. 在网络安全宣传方案的设计环节，提供更多的案例分析和设计指导，同时鼓励学生进行头脑风暴，激发他们的创意思维。
3. 加强网络安全意识的培养，通过分析网络安全事件，让学生认识到网络安全问题的严重性，从而更加重视网络安全日志的记录和反思。
4. 定期组织网络安全知识竞赛和讲座，让学生在活动中不断巩固和更新网络安全知识。
5. 加强与学生的沟通，了解他们在学习过程中遇到的问题，及时调整教学策略和方法，确保教学内容的适宜性和有效性。

典型例题讲解

例题 1：设计一份网络安全宣传海报，要求包含以下元素：主题、网络安全知识普及、防护措施、互动环节。

答案：海报主题：“网络安全，人人有责”。内容包含：介绍网络安全的重要性，普及个人信息保护、密码设置、网络诈骗防范等知识；提供一系列实用的防护措施，如定期更新系统、使用安全软件等；互动环节可以设计一个网络安全知识问答游戏，吸引参观者参与。

例题 2：分析以下网络诈骗案例，指出诈骗手段及预防措施。

案例：某学生收到一条短信，称其在中奖活动中获得了一台笔记本电脑，要求提供银行账户信息以便发放奖金。

答案：诈骗手段：利用中奖为诱饵，诱使学生提供银行账户信息。预防措施：不轻信来历不明的中奖信息，不透露个人银行账户信息，及时向相关部门举报。

例题 3：编写一个简单的网络安全脚本，用于检测计算机系统中是否存在未更新的软件。

答案：脚本示例：

```
...  
# 检测系统中未更新软件的脚本  
updated = true  
software_list = ['Firefox', 'Chrome', 'Adobe Reader']  
for software in software_list:  
version = get_software_version(software)
```

```
if version < latest_version(software):
print(f"{software} is not up-to-date.")
updated = False
if updated:
print("All software is up-to-date.")
else:
print("Some software needs to be
```

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/628132010020006135>