实验策略下青少年网络素养课程的开发与实践——以《剖析钓鱼手段——互联网安全意识》一课为例

Design and Practice of an Experimental Cyber Literacy Curriculum for Adolescents: A Case Study of the Lesson 'Deconstructing Phishing Tactics—Raising Internet Security Awareness

马静[1]，赵琪旻[2*]，杨爽[3]，刘文文[4]，李青轩[5]
[1,2,3,4,5]北京市人大附中航天城学校
chimmyzh@foxmail.com

【摘要】 数字时代下青少年网络素养教育不容忽视。本案例通过实验剖析网络“钓鱼”原理，引导学生认识“钓鱼”本质上是心理诱骗，人处于信息安全核心地位，最终达到提升网络素养的目的。创新点在于秉持“技术融合人文”的设计理念，搭建了贴近学生真实生活的模拟“钓鱼”场景，带领学生学习“硬”知识的同时提升自身“软”素养。

【关键词】 网络素养；实验；“钓鱼”；真实生活

Abstract: *Teenagers' network literacy education cannot be ignored in the digital age. This case analyzes the principle of network "fishing" through experiments, and guides students to understand that "fishing" is essentially psychological deception, and people are at the core of information security, and finally achieve the goal of improving network literacy. The innovation lies in adhering to the design concept of "integrating technology with humanity", building a simulated "fishing" scene close to students' real life, leading students to learn "hard" knowledge while improving their "soft" literacy.*

Keywords: Network literacy, Experiment, Phishing, Real life

1. 前言

当前中小学校网络素养教育形式单一，影响有限，主要依赖校园宣传和课堂案例分析，缺乏深度互动与心灵触动，导致教育效果平面化。此外，网络安全技术教育与素养教育脱节，学生仅知“禁令”而不知“为何”，知识难以应用于实际。

为解决此问题，本案例采用实验改革，聚焦网络“钓鱼”安全问题，搭建模拟场景，结合真实域名、交互式视频及丰富案例，深入剖析“钓鱼”事件，强化学生心理认知，积累经验以降低风险。同时，揭示技术背后的人文因素，促进网络素养教育的深度与实用性。

2. 青少年网络素养课程的研究现状

包含网络素养的青少年媒介素养教育在国外已有九十多年历史，英国、美国、加拿大、澳大利亚等是青少年媒介素养教育起步早、发展比较成熟的国家，如表 1 所示。

表 1. 国外网络素养课程现状

国 家	课程形式	课程对象	课程内容特点	课程开展方式
英国	独立式课程	从幼儿到成人	保护主义、甄别与判断、接受、阶段性	以学生讨论为主
美国	融入式课程	K-12（幼儿园-高中）	批判接受、媒体剖析、自我表述	以探究活动为主
加拿大	融入式课程	1~12 年级	媒介批判、媒介形式、利用媒介	以实践活动为主
芬兰	融入式课程	8 岁及以下	认识媒介的理念、使用媒介的方法	以体验活动为主

国外网络素养课程的相同点是：

（1）网络素养课程由理论研究转为与其他学科课程融合的实践过程的研究。

（2）网络素养课程更关注教师与学生，更多的关注学生的兴趣认知等。

（3）从抵抗式防御走向向融合与和谐共生的“参与式”网络素养教育模式发展。

与国外发达国家几十年的媒介素养教育发展历史相比，我国青少年网络素养教育研究起步较晚，相应的网络素养课程的研究与实施就少，在课程研究、实施、资源三方面处于初步探索阶段，课程资源很不完善 、不系统、非常匮乏，并且主要是分散的短视频、小范围公开课，急需加快课程资源的建设与发展，探索“立体”的网络素养教学方式。

3. 实验活动是网络素养形成的途径

学科活动包括两个部分，即实践活动（注重动手，提供感性认知）和认知活动（注重动脑，提供理性认知），具有实践性、思维性和自主性三个特性。学科活动通过教学层级的跃迁、学科知识的挖掘和大单元主题的推进“三大”抓手促进学科核心素养的形成，如图 1 所示。信息科技实验教学属于实践活动，教师在为学生提供直观的体验的同时，应当借助“三大”抓手，达成落实核心素养的目标[4]。

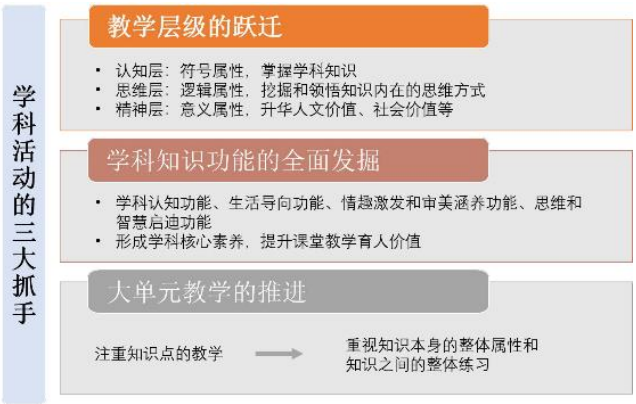

图 1. 学科活动的三大抓手

4. 案例课程设计思路

基于实验教学策略，结合信息科技、道德与法治课标以及心理学科教学指导意见，开发了《剖析钓鱼手段——互联网安全意识》这一案例课程。现具体说明课程设计情况。

4.1. 厘清课程定位

本课程针对中学生网络素养不足及缺乏正确网络安全观的问题，主要表现为：

（1）技术与责任意识不匹配：中学生网络操作熟练，但网络安全意识滞后。

（2）价值观引导手段不足：现有教育方式偏重理性，缺乏感性实操体验。

（3）课堂教育缺失：网络素养未充分融入课堂教学，学生参与度低。

（4）学科割裂：技术素养与人文素养教育分离，影响综合素养培养。

为解决上述问题，本课程设计将技术素养（网络知识）与人文素养（安全观、价值观）等思政元素融入信息科技课程，实施跨学科融合教学，涵盖信息科技、心理及道德与法治等内容（如图 2 所示）。

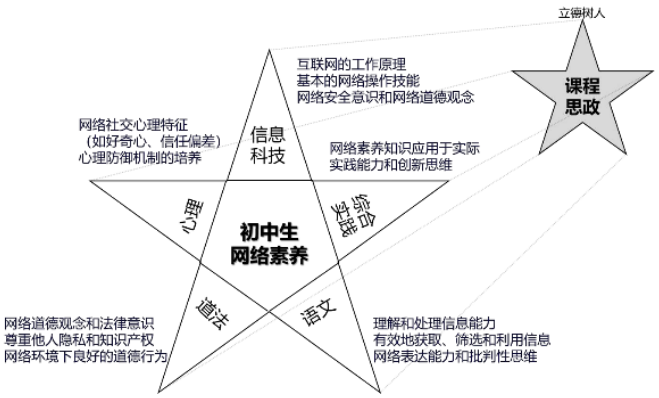

图 2. 网络素养课程的跨学科教学属性

第一课时以网络“钓鱼”手段为例，明线分析技术手段，暗线探讨心理诱骗，旨在从技术与人文双维度增强学生防骗意识，保护个人信息及隐私。本课程设计以素养为先导，旨在促进后期知识与技能的合理运用。

4.2. 课程实施过程

4.2.1. 课程预热

4 月份为学校的“网络安全宣传月”，升旗仪式中学生代表向全体学生宣传了网络安全的途径、危害以及防护措施，以此拉开本年度网络安全学习的序幕；校园中张贴国家安全和网络安全相关主题海报，营造网络安全学习氛围，增加主题活动情境记忆点。

4.2.2. 课程执行

主题课程以培养学生网络安全素养为目的，帮助学生应对数字化时代下可能存在的网络安全问题，以“体验+讨论”的“做中学”策略帮助学生在学习网络安全知识的同时树立正确的社会价值观。课程活动设计为 6 个环节，缘起于学生填写中小学生综合素质平台的真实生活情境，类比百度搜索资源的经历，让学生在实操中感受网络诈骗的原理，最终提高安全意识。接下来，介绍 6 个环节的具体内容。

（1）体验“被”钓鱼，唤醒安全意识

活动内容：学生尝试登录模拟的“北京学生综合素质评价平台”，填写活动照片等材料。

体验结果：学生发现登录异常（如网址问题），无法直接登录，需要再次填写信息后才能进入。

原理解释：模拟的钓鱼网站与真正的综素平台网站高度相似，但域名不同。学生在钓鱼网站上填写的信息会被后台记录下来，导致账号和密码被盗取。

引出主题：通过网络“钓鱼”的例子，引出主题活动的三个核心问题：“网络钓鱼是什么”、“如何让人上钩” 、“如何避免”。

（2）观看“315”视频，理解“钓鱼”概念

活动内容：播放 315 晚会关于手机短信诈骗的案例视频。

思考问题：引导学生思考钓鱼网站的载体、目的和特点，以及为什么受害者会上当受骗。

原理解释：钓鱼网站通常通过伪装成正规网站或发送虚假信息来诱骗用户点击，目的是获取用户的个人信息或进行欺诈活动。受害者往往因为缺乏警惕或识别能力而上当受骗。

生活实例：学生分享生活中的“钓鱼”诈骗例子，总结常见手段。

（3）类比百度访问，剖析“钓鱼”原理

活动内容：利用百度访问流程图解释服务器的功能和信息流动。

类比分析：请学生思考综素平台登录过程的信息流动图，并与百度访问流程图进行类比。

原理解释：当用户在浏览器中输入网址时，浏览器会向 DNS 服务器发送请求，将域名解析为 IP 地址。如果用户点击的是钓鱼网站的链接，DNS 服务器会将域名解析为钓鱼服务器的 IP 地址。用户的信息（如账号、密码等）会发送到钓鱼服务器，并被钓鱼者收集。钓鱼服务器可能会模拟真正的网站界面，让用户误以为自己正在与正规网站进行交互。在某些情况下，钓鱼网站可能会将用户重定向到真正的网站，以掩盖其欺诈行为。

深入分析：分析钓鱼网站的信息流动过程，以及为什么用户难以察觉信息的泄露。用户为何会不慎点击假冒网页的原因，主要归结为网页克隆与域名欺骗两大技巧。网页克隆使得假冒网页与真实网页几乎难以分辨，而域名欺骗则利用相似域名诱导用户误入歧途。

（4）识别“钓鱼”话术，增强心理防线

“钓鱼”诈骗不仅依赖技术手段，更擅长利用心理诱骗。这些诈骗信息往往针对人性弱点，如生活关联、个人利益或诱惑性内容。学生将参考提供的钓鱼话术，结合对同学的了解，使用临时邮箱 tempmail 撰写一封模拟钓鱼邮件，尝试诱骗对方下载含病毒的附件，以此提升对钓鱼邮件的识别能力。

随后，展示一个教师设计的钓鱼邮件案例，其中包含一个虚构网址“rdfzhtc.xyz”，该网址实际指向一个匿名且低安全的聊天室，内部可发送支付二维码、病毒软件，甚至散布谣言。这再次强调，无论是信息中的链接、邮件中的软件，还是聊天室里的支付请求，都应保持警惕，时刻绷紧网络安全这根弦。

（5）总结交流，提炼防骗策略

通过阅读小刘受骗的案例，学生将分析受骗原因和交易中的可疑点，培养批判性思维能力。在此基础上，引导学生从客观（如技术防范）和主观（如心理防范）两方面归纳防骗措施，形成一套实用的自我保护策略。

（6）视频互动，深化网络安全认知

在掌握个人防“钓鱼”技巧后，学生将进一步理解网络安全的社会意义。通过交互式视频，他们将认识到网络诈骗不仅是个人信息的威胁，更是社会信息安全的隐患。以西工大被攻击事件为例，说明网络安全与社会安全、国家安全的紧密联系。观看网络安全宣传片，学生将深刻理解国家安全与个人网络安全的相辅相成，意识到每个人都是国家信息安全防线的一部分，高度的网络安全意识是维护国家安全不可或缺的力量。

通过这一系列课程环节，学生不仅能够提升网络安全技能，还能在心理层面建立坚固的防线，更重要的是，他们将认识到网络安全的社会责任，成为维护网络安全的积极参与者。

5. 案例总结

（1）技术防范与心理防范并重：在案例实践中，我们发现技术层面的防范虽然重要，但心理层面的防范同样不可或缺。学生在面对模拟钓鱼邮件时，往往因为好奇心或信任感而轻

易点击，这反映了心理防范的薄弱。

（2）批判性思维的培养：通过分析受骗案例，我们意识到学生在面对网络信息时缺乏足够的批判性思维。他们往往容易相信表面的信息，而缺乏对信息真实性和来源的深入探究。

参考文献

罗生全和欧露梅.(2012).国外中小学媒介素养教育新进展.中国电化教育,(07),23-28.
王雨馨.(2013).加拿大青少年媒介素养教育的经验与启示(硕士学位论文,郑州大学).
王振武.(2016).浅析加拿大青少年媒介素养教育及其当代启示.河北青年管理干部学院学报,28(05),24-27.
周建华.(2023).课堂教学促进学科核心素养形成的策略.新课程教学(电子版),(02),1-4+10.

本论文为北京市数字教育研究课题《基于 DOK 理论的中学多元连续性精准教学的实证研究》（课题号为 BDEC2023080003）的成果。