安全科学与工程学报
Journal of Safety Science and Engineering
第 3 卷◆第 2 期◆版本 1.0◆2025 年
文章类型：论文丨刊号（ISSN）：2972-4716(P) / 2972-4724(O)

针对高校教师的钓鱼邮件演练实战与分析

孙浩宇　王爱国　胡海　朱宇楠　王晓露
宿迁学院信息化建设与管理中心
DOI:10.12238/jsse.v3i2.13453

[摘　要] 本研究通过学校网络中心自制钓鱼邮件对教师群体进行网络安全意识演练,结果显示点击邮件比例达16.8%,打开邮件内钓鱼连接比例为7.6%。这一结果凸显了高校教师群体在网络安全意识方面存在的严重不足。本文深入分析演练结果,探讨背后原因,并从提高网络安全意识和阻拦恶意访问两个角度提出针对性策略,旨在为提升高校整体网络安全水平提供参考。
[关键词] 钓鱼邮件；网络攻击；网络安全；实战演练
中图分类号：TN915.08　**文献标识码**：A

Practice and Analysis of Phishing Email Drills Based On University Teachers

Haoyu Sun　Aiguo Wang　Hai Hu　Yu'nan Zhu　Xiaolu Wang
Suqian University Informationization Construction and Management Center

[Abstract] In this study, the school network center self-made phishing emails were used to conduct a network security awareness drill among the teaching staff. The results showed that the proportion of those who clicked on the emails reached 16.8%, and the proportion of those who opened the phishing links within the emails was 7.6%. This result highlights the serious deficiencies in the network security awareness of the teaching staff in colleges and universities. This paper analyzes the drill results in depth, explores the reasons behind them, and proposes targeted strategies from two perspectives: improving network security awareness and blocking malicious access, aiming to provide references for enhancing the overall network security level of colleges and universities.
[Key words] Phishing emails; Network attacks; Network security; Practical drills

1 研究背景

随着信息技术的飞速发展,网络已成为高校教学、科研和管理的重要支撑。然而,网络安全问题也日益严峻,钓鱼邮件作为一种常见的网络攻击手段,给高校师生的信息安全带来了巨大威胁。

电子邮件安全领域知名企业Cofense公司发布的《2024 年度邮件安全报告》[1]相关数据显示,电子邮件在当下依旧是网络犯罪领域最为主要的威胁媒介。据统计,高达90%的数据泄露事件均起始于网络钓鱼行为,而电子邮件作为网络钓鱼的主要实施途径,相较于2022年,2023年恶意电子邮件数量增长了37%;与2021年相比,这一数据更是增长了310%。恶意钓鱼邮件无疑在网络犯罪威胁体系中占据着核心地位。

网络安全领域知名企业Check Point公司发布《2025年全球网络安全现状》[2]年度报告。报告主要调查结果如下：勒索软件持续演变,数据泄露与勒索取代基于加密的攻击,成为主要勒索软件攻击手段,此类攻击实施简便且非法获利高,边缘设备常被利用,受感染的路由器、VPN等边缘设备是攻击者关键切入点。在目标行业方面,教育行业连续五年成为首要攻击目标,攻击次数同比增长75%。

1.1研究意义和目标

本研究旨在达成三个层面的目标。首先,长期以来,学校针对网络攻击始终采取严格防御策略,在校园网络边界部署了防火墙、防毒墙、入侵检测系统(IDS)以及入侵防御系统(IPS)等一系列网络安全防护设备。本研究欲探究在此基础上,校园内部教师群体的网络安全防范意识水平。

其次,通过深度剖析演练结果,能够精准定位教师群体在应对网络安全威胁时存在的薄弱环节,从而制定并实施行之有效的策略,增强教师网络安全意识,有效阻止恶意访问行为。

最后,本研究致力于协助学校强化校园网络安全保障体系,提升校园网络整体的安全防范能力与水平,以应对日益复杂的网络安全挑战,确保校园网络环境的稳定与安全。

2 相关理论和研究综述

2.1钓鱼邮件的定义与影响

所谓钓鱼邮件攻击,是指攻击者使用社会工程学手法伪装

身份,向攻击目标发送具有诱骗性的电子邮件“诱饵”,利用人们的好奇、贪婪和猎奇等情绪和心理,通过诱导攻击目标降低戒备心、其目的是诱使用户泄露敏感信息(如用户名、密码、银行卡号、身份证号等)、下载恶意软件或执行其他有害操作,从而给用户带来经济损失或其他不良后果。

一般钓鱼邮件攻击者首先会收集目标用户的相关信息,如邮箱地址、工作单位、兴趣爱好等,以便更好地定制钓鱼邮件内容,提高欺骗成功率。根据收集到的信息,攻击者精心制作钓鱼邮件,包括选择合适的伪装身份、编写具有欺骗性的内容、设置钓鱼链接或恶意附件等。攻击者利用大量的僵尸网络或购买的邮件列表,向目标用户发送钓鱼邮件。为了避免被邮件服务器拦截,他们可能会采用一些技术手段来隐藏邮件的真实来源。当用户收到钓鱼邮件并点击链接或打开附件后,就可能会泄露敏感信息或导致设备被感染恶意软件。攻击者会收集这些信息,并用于进一步的诈骗活动,如盗刷用户银行卡、窃取用户账号资金、进行身份盗窃等。钓鱼邮件共计流程如图1所示。

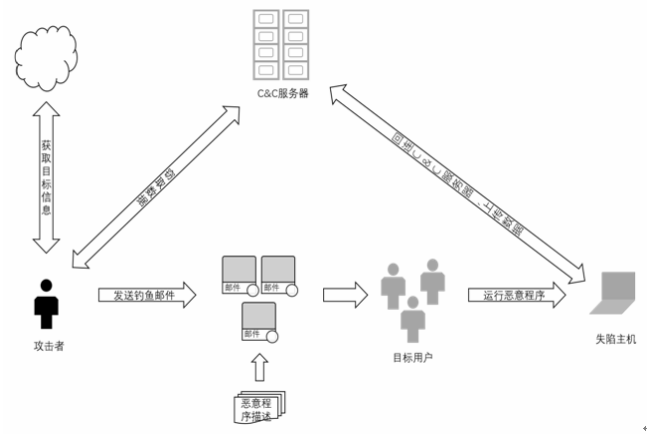

图1 一般钓鱼邮件攻击过程

钓鱼邮件的影响从个人层面上,用户可能会遭受经济损失,如银行账户被盗刷、信用卡信息泄露导致被盗用等。同时,个人的隐私信息如身份证号、家庭住址、电话号码等也可能被泄露,给用户带来骚扰和潜在的安全风险。

从企业层面上,员工若不慎点击钓鱼邮件,可能会导致企业内部的敏感信息泄露,如商业机密、客户数据、财务信息等,给企业带来巨大的经济损失和声誉损害。此外,还可能使企业的网络系统受到攻击,导致业务中断、生产停滞,影响企业的正常运营。

2.2钓鱼邮件的研究综述

文献[3]提出了一种基于智能体工作流的钓鱼邮件检测方法——PhishingAgent。该方法结合多源知识库和安全工具,充分发挥LLM的推理能力,在保证检测精度的前提下提高了检测效率。文献[4]主要分析了钓鱼邮件的特征及攻击过程,阐述了钓鱼邮件的检测技术和防范措施,从而提高公司员工对钓鱼邮件的防范意识,降低因钓鱼邮件攻击造成的损失。文献[5]设计了一套针对企业员工的钓鱼邮件演练方案,利用VPS云服务器、Gophish和Postfix等工具,在生产环境中开展实战演练。该方案的目的在于提高企业员工的网络安全意识和企业网络安全防范能力。文献[6]为激励用户积极举报网络钓鱼邮件,基于三方演化博弈理论,以邮件服务提供平台、用户和网信办为博弈主体,并假设主体有限理性,构建演化博弈模型,并对模型中的参数进行敏感性分析及赋值仿真分析。研究结果表明：用户对举报策略的选择受到举报成本、平台激励以及平台和网信办策略选择的影响,通过调节敏感参数的大小可以稳定三方主体的策略选择。

3 针对校园教师的钓鱼邮件演练设计

3.1钓鱼邮件演练的目标

本次演练是在真实校园网络环境的基础上架设相关演练环境,最大程度地模拟在网络环境下真实的攻击场景,并且不影响正常业务运作为原则,从而达到以下演练目标：

(1)识别与排列人为风险优先级,从而有针对性地对症下药；(2)改变教师的不安全行为,降低人为风险；(3)提升教师的安全意识成熟度。

3.2钓鱼邮件演练的设计步骤和流程

(1)在互联网上部署蜜罐平台服务器,部署仿真蜜罐,展示虚假的教师节&中秋节联合抽奖活动web页面。(2)在一台互联网服务器部署攻击者邮件服务器,攻击者通过该服务器发送钓鱼邮件,邮件中包含了钓鱼链接。(3)企业员工收到并打开钓鱼邮件后,可点击访问邮件中由蜜罐仿冒的链接。(4)蜜罐平台获取到企业员工做蜜罐访问的记录。

3.3钓鱼邮件演练方案的具体内容和形式

本次演练由学校网络中心自制钓鱼邮件,模仿教师节&中秋节联合抽奖活动邀请函,邀请函中包含一个伪装成正常链接的钓鱼链接,钓鱼邮件以活动助手的名称被发送给学校所有教师工作邮箱。考虑到日常的办公行为,此次后台统计的截止日期是次日当时,只统计一天内的点击量。

4 结果分析和讨论

4.1演练结果的统计

本次钓鱼攻击演练共发送1344封钓鱼邮件,发送成功1344封钓鱼邮件,打开邮件人数为226,点击邮件钓鱼仿冒链接人数为102。此次模拟演练钓鱼邮件点击率为16.8%,钓鱼链接中招率为7.6%。根据深信服科技公司的安全意识评定参考表1所示,安全意识一般。这一结果表明,大部分教师对邮件来源缺乏足够的警惕性,且在面对邮件中的链接时,未能有效识别其潜在风险。

表1 深信服科技股份有限公司安全意识评定参考表

安全意识评定参考	0%~2%,安全意识非常好
	2%~5%,安全意识较好
	5%~10%,安全意识一般
	10%~15%,安全意识较差
	>15%,安全意识非常差

进一步的，钓鱼邮件后台统计结束后，对中招教师得到邮箱账号进行进一步与教师信息数据库进行过滤，分别统计了各个年龄段以及各学院教师的打开邮件和点击链接的数据。统计了各学院打开邮件与点击链接的数量，考虑到各学院的人数会有所不等，所以改成中招人数占本学院的比例会使结果更公平。各学院的中招数据如图2所示。

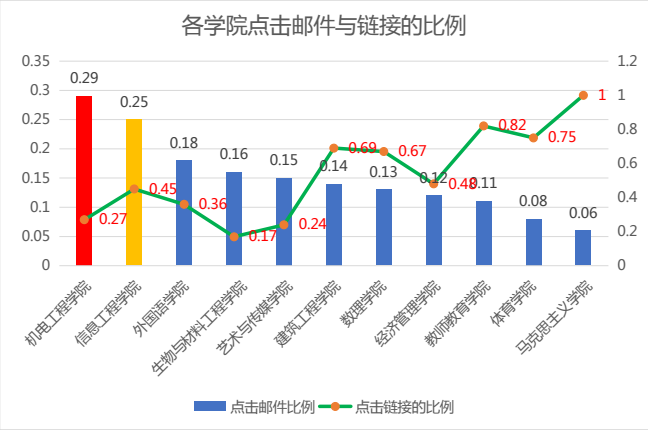

图2 各学院打开邮件和点击链接的比例混合图

4.2演练结果的分析

分析数据可知，打开邮件人数较多的30-44岁年龄段，在工作中往往承担着重要职责，工作内容涉及大量的沟通协作，邮件是重要的工作工具，因此打开邮件的需求较大。在处理邮件时相对急切，更容易忽略邮件的安全性，从而增加了遭受钓鱼邮件攻击的风险。26－29年龄段的刚参加工作，工作往来使用邮箱沟通较少，使用微信与QQ更多。55-59岁以及60-64岁年龄段人数极少，一方面可能是他们对电子设备和网络的熟悉程度更低，另一方面，这个年龄段的人可能已经退休，工作相关的邮件需求大幅减少。

机电工程学院、信息工程学院这类理工科类学院，点开邮件的比例相对较高，这是由于专业学习和研究需求，他们频繁接收各类学术资料、项目通知等邮件，邮件成为日常学习与工作不可或缺的工具。然而，他们打开链接的比例却并不高，这或许得益于理工科学生和教师严谨的思维方式以及相对较高的技术素养。他们在面对邮件中的链接时，会更倾向于从技术角度分析链接的安全性，如查看链接的域名、分析链接的参数等，从而降低了被钓鱼链接欺骗的概率。

体育、教师教育、马克思主义学院：这几类学院点开邮件的比例较低，可能因为其教学和研究工作对邮件的依赖程度不如理工科类学院，日常沟通方式更多样化，如面对面交流、即时通讯工具等。但令人担忧的是，他们打开链接的比例却很高。这可能是因为这些学院的师生在网络安全知识方面的储备相对不足，缺乏对链接潜在风险的敏感性。同时，他们在面对邮件内容时，可能更容易受到情感因素的影响，比如邮件中以紧急教学事务、重要学术交流机会等说辞，更容易引发他们的关注并点击链接。

4.3演练结果的启示

4.3.1开展定期培训

各大高校应定期组织网络安全培训课程，邀请专业的网络安全专家为教师进行授课，尤其是文科类专业的教师。培训内容应包括网络安全基础知识、钓鱼邮件的识别方法、常见网络攻击手段及防范措施等。通过培训，提高教师的网络安全意识和防范能力。

4.3.2加强宣传教育

利用学校的官方网站、微信公众号、宣传栏等渠道，定期发布网络安全相关的知识和案例，向教师宣传网络安全的重要性和防范方法。同时，通过举办网络安全宣传周等活动，营造浓厚的网络安全氛围。

4.3.3模拟演练常态化

除了本次的钓鱼邮件演练外，学校应将类似的模拟演练常态化。定期发送模拟钓鱼邮件，对点击邮件和打开链接的教师进行针对性的提醒和教育，让教师在实践中不断提高识别和防范钓鱼邮件的能力。

5 研究展望

网络战作为一种无形却极具杀伤力的战争形式，已成为国家间战略博弈的重要领域。我国在网络发展进程中起步相对欧美国家较晚，因此，强化网络边界防护显得尤为关键且迫切。对于校园网络安全运营而言，除了加强宣传和教育之外，以下几个方面的防护措施不容忽视。

5.1邮件过滤系统升级

学校应升级邮件过滤系统，采用更先进的技术和算法，对收到的邮件进行全面的安全检查。过滤系统应能够识别钓鱼邮件的特征，如异常的发件人地址、可疑的链接等，并将其拦截在教师的收件箱之外。

5.2网络访问控制

加强学校网络的访问控制，限制教师访问可疑的网站和链接。可以通过引入人工智能进行内容识别、使用入侵检测系统等方式，对网络流量进行监控和过滤，及时发现并阻拦恶意访问。

5.3安全审计与监测

建立完善的安全审计与监测机制，对教师的网络行为进行实时监测和审计。一旦发现异常的网络访问行为，如访问钓鱼网站、下载可疑文件等，及时发出警报并采取相应的措施。

6 结论

本次钓鱼邮件演练结果显示，高校教师的网络安全意识亟待提高。通过开展定期培训、加强宣传教育和模拟演练常态化等措施，可以有效提高教师的网络安全意识。同时，通过升级邮件过滤系统、加强网络访问控制和建立安全审计与监测机制等技术手段，可以阻拦恶意访问，保障学校网络的安全稳定运行。学校应高度重视网络安全工作，将提高教师网络安全意识和阻拦恶意访问作为一项长期的任务来抓，不断完善网络安全管理体系，为高校的发展提供坚实的网络安全保障。

[参考文献]

[1]Cofense Inc.2024 Cofense Annual State of Email SecurityReport[EB/OL].(2024-02)[2025/02/20].https://cofense.com/getmedia/db5a5ad7-b39a-45f5-bab7-eb165b9a0685/2024-cofense-annual-state-of-email-security-report.pdf.

[2]Check Point Software Technologies Ltd. The State of Cyber Security 2025[EB/OL].(2025-01)[2025-02-20].

[3]金建栋,黄正,胡占宇,等.基于智能体工作流的高级钓鱼邮件检测方法[J].通信学报,2024,45(S2):59-68.

[4]高静.钓鱼邮件的分析与防范[J].广播电视网络,2024,31(02):82-85.

[5]石宏庆,侯庆,蓝善根,等.针对企业员工的钓鱼邮件演练方案设计与实践[J].网络安全技术与应用,2024,(01):113-116.

[6]王志英,索小姣.基于三方演化博弈的网络钓鱼举报激励机制研究[J].网络安全技术与应用,2024,(04):68-75.

作者简介：

孙浩宇(1997--),男,汉族,江苏睢宁人,硕士研究生,助理工程师,研究方向：网络工程与网络安全方向。