arXiv:2305.03062v1 [cs.CR] 4 May 2023

用于模拟网络攻击以教授网络安全的严肃游戏

Christopher Scherb 瑞士西北应用科学与艺术大学
christopher.scherb@fhnw.ch

Luc Bryan Heitz 瑞士西北应用科学与艺术大学
luc.heitz@fhnw.ch

Frank Grimberg
瑞士西北应用科学与艺术大学
frank.grimberg@fhnw.ch

瑞士西北应用科学与艺术大学
Hermann Grieder
hermann.grieder@fhnw.ch

Marcel Maurer
Muuri Solutions，瑞士伯尔尼州伯尔尼
info@muuri.solutions

2023年5月8日

摘要

随着勒索软件攻击、网络间谍活动等网络攻击日益增多，教育非网络安全专业人士识别威胁变得比以往任何时候都更加重要。然而，传统培训方法（如网络钓鱼意识宣传活动、培训视频和测评）已被证明效果会随着时间推移而降低。因此，是时候重新思考网络安全意识培训的方法了。本文提出一种替代方案——严肃游戏，用于普及常见网络攻击的相关知识。尽管已有许多用于网络安全教育的严肃游戏，但它们采用的方式都非常相似：展示网络攻击对玩家自身系统或公司网络造成的影响。例如，这类游戏中的一项主要任务就是筛选钓鱼邮件。我们开发并评估了一种新型网络安全游戏：攻击模拟器，从不同视角展现整个场景。玩家不再筛选钓鱼邮件，而是要编写钓鱼邮件诱骗潜在受害者，并使用其他形式的网络攻击。我们的游戏会解释每种攻击的意图，并展示攻击成功后的后果。我们希望借此帮助玩家更好地了解如何检测网络攻击。

关键词：网络安全、严肃游戏、教育、意识、网络钓鱼

1 引言

过去几年，全球网络攻击数量显著上升。随着业务流程日益数字化、家庭自动化技术的发展、互联城市的兴起以及远程办公的普及，网络犯罪分子找到了利用计算机网络、计算机系统和人类漏洞的新方法，而且手段更加复杂。从网络钓鱼诈骗和勒索软件攻击，到数据泄露和身份盗窃，网络攻击已成为企业、政府和个人共同面临的重大隐患。新冠疫情进一步加剧了这一问题，网络犯罪分子利用线上活动增加的机会，对易受攻击的个人和组织发起定向攻击。随着技术不断进步，网络攻击的威胁很可能会持续增长，因此个人和组织必须保持警惕，并采取积极措施保护自己免受这些数字威胁。

与此同时，大众媒体中对黑客攻击的描绘，例如电视剧《NCIS》[1] 和电子游戏《看门狗》[2] 中的相关情节，往往经过戏剧化处理，与现实并不相符。在这些影视作品和游戏中，黑客攻击通常被描绘成一种光鲜亮丽、轻而易举的活动，黑客只需敲击几下键盘，就能入侵高度安全的系统。尽管这些影视作品和游戏可能颇具娱乐性，但它们可能会延续一种误解，即黑客攻击是一种无害的活动，从而导致人们对网络安全相关风险缺乏足够的认识。事实上，黑客攻击是一种复杂且往往违法的活动，可能给黑客和受害者双方带来严重后果。媒体往往未能准确呈现黑客攻击造成的负面影响，包括身份盗窃、金融欺诈以及关键基础设施遭到破坏，同时还会营造一种无助感，让人觉得一旦成为黑客的目标，就只能束手无策。然而，如果大多数非技术岗位的员工接受了良好的安全意识教育，并具备良好的安全意识，那么大多数攻击原本都是可以避免的。

因此，降低网络攻击风险的最重要方式之一，就是向员工传授网络安全最佳实践 [3, 4]。员工往往是抵御网络威胁的第一道防线；如果缺乏适当的培训，他们可能会无意间泄露公司的敏感信息，或成为网络钓鱼诈骗的受害者 [5]。通过为员工提供全面的网络安全培训，企业可以帮助他们识别并报告可疑活动、保护设备和账户，并遵循数据保护最佳实践。这有助于防止代价高昂的数据泄露和网络攻击，同时在整个组织中培育安全意识文化。简而言之，在员工网络安全教育方面进行投资，是在当今数字环境中保护公司宝贵资产和声誉的关键一步。

然而，网络安全教育是一个相当复杂的课题，大多数员工认为培训和意识宣传活动令人厌烦，因此参与时往往不够积极。此外，近期研究表明，网络钓鱼宣传活动等意识培训只能产生短期效果 [6]，无法从长远角度提高员工抵御钓鱼邮件的能力。造成这一现象的原因之一是，网络钓鱼电子邮件变得越来越复杂，使其更难被检测出来。攻击者利用社会工程、伪造合法电子邮件地址以及创建具有迷惑性的虚假网站等手段，诱骗毫无防备的受害者。此外，一些员工可能并未认真对待网络钓鱼威胁，或者由于工作繁忙，无法仔细审查收到的每一封电子邮件。即使接受了培训并参与了意识宣传活动，员工仍然可能落入钓鱼邮件的陷阱。此外，网络钓鱼意识宣传活动本身也可能助长员工的轻率行为，因为在处理来自网络钓鱼意识宣传活动的邮件时，即使随意点击其中的链接，也可能不会造成任何危害。因此，员工可能逐渐习惯于低估网络钓鱼相关风险，从而使真正的钓鱼邮件变得更加危险。

通过了解攻击者使用的策略，例如社会工程和鱼叉式网络钓鱼，个人可以更好地识别并避免网络钓鱼攻击尝试。此外，认识到成为网络钓鱼受害者可能造成的后果，可以促使个人采取必要的预防措施，保护自己的敏感信息。许多人并不了解点击电子邮件或链接不仅会对自己的系统造成什么危害，还会对整个网络造成什么危害，因为他们从未见过诸如系统被勒索软件加密、公司机密被窃取或发生金融欺诈等后果。

因此，我们设计了一款网络安全教育游戏，让玩家从攻击者的视角体验网络攻击 [7]。玩家扮演一名攻击者，需要获取信息、发送钓鱼邮件、使用漏洞利用程序及其他形式的网络攻击来攻击一家公司 [8]。整个过程尽可能真实地呈现。用户必须在模拟的暗网商店中搜索受害者的电子邮件地址、用于网络钓鱼攻击的虚假网站，并购买漏洞利用程序。每次攻击所造成的后果都会得到展示和解释，从而帮助玩家更深入地理解网络攻击的动机及其不同形式，并以此增强抵御真实网络攻击的能力。
本文接下来的章节安排如下：第 2 节回顾相关文献，向读者介绍研究背景，并为本文提供背景知识。第 4 节概述我们的严肃游戏，并详细介绍每个已实现的场景。第 5 节呈现并讨论一项短期调查的结果。第 6 节总结本文，并指出未来可能的研究方向。

2 文献综述

本节将介绍并总结相关研究和背景研究。

[1] https://www.imdb.com/title/tt0364845/[2] https://www.ubisoft.com/en-us/game/watch-dogs/watch-dogs

2.1 ENISA 威胁态势报告

ENISA威胁报告[3] 是欧盟网络安全局（ENISA）每年发布的报告。报告概述了欧洲及全球网络安全威胁的现状和趋势，分析了上一年度发生的重大网络安全事件，并指出可能影响个人、组织和关键基础设施的新兴威胁与漏洞。

该报告还提出了改善网络安全的建议，例如风险管理和事件响应方面的最佳实践。报告面向广泛的受众，包括政策制定者、IT专业人员和公众，旨在提高人们对当前网络安全态势的认识，并帮助利益相关者就如何保护其数字资产作出明智的决策。

ENISA威胁报告是重要的资源，有助于任何有兴趣了解当前网络安全状况以及如何降低潜在风险的人；它也有助于确定降低网络攻击暴露风险所需的重要技能。

2.2 NIST 网络安全框架

NIST 网络安全框架 [9] 是一套由美国国家标准与技术研究院（NIST）制定的指南、标准和最佳实践，旨在帮助组织管理和降低网络安全风险。该框架包含五项核心职能：识别、保护、检测、响应和恢复。每项职能都包含一系列类别和子类别，为组织可以采取哪些具体行动来增强其网络安全态势提供详细指导。政府机构、私营企业和各种规模的组织广泛认可并采用该框架，以改进其网络安全实践并降低网络威胁风险。

该框架于2014年由 NIST 首次发布，此后已被医疗保健、金融和能源等各行业的组织广泛采用。无论规模或所属行业如何，该框架都旨在灵活适应各组织的独特需求和风险概况。

该框架的五项核心功能如下：

- 识别：此功能旨在帮助组织了解其系统、资产、数据和风险。相关活动包括盘点硬件和软件资产、识别漏洞和威胁，以及评估网络安全事件可能造成的影响。
- 保护：此功能侧重于实施安全防护措施，以抵御网络威胁。相关活动包括访问控制、数据加密以及面向员工的安全意识培训。
- 检测：此功能旨在尽可能快速地识别网络安全事件。相关活动包括持续监控、异常检测和事件响应规划。
- 响应：此功能旨在立即采取行动，遏制并减轻网络安全事件造成的影响。相关活动包括事件响应、业务连续性规划和灾难恢复。
- 恢复：此功能涉及在网络安全事件发生后恢复正常运行。它包括系统恢复、损害评估和事件后审查等活动。

NIST 网络安全框架进一步明确了一系列技能，这些技能对于开发人员和计算机系统的一般用户更好地防范网络风险至关重要，具体如下：

- 通过不可信网站防范恶意软件
- 通过电子邮件网络钓鱼传播恶意软件的防范
- 通过访问不可信网站防止个人身份信息盗窃
- 通过电子邮件网络钓鱼防止个人身份信息盗窃
- 通过社交媒体防止个人身份信息泄露
- 防止通过 USB 或存储设备利用造成信息系统遭入侵
- 防止通过密码利用造成未经授权的信息系统访问

该框架旨在作为改进组织网络安全实践的工具，而不是一套适用于所有情况的解决方案。它是一份持续更新的文档，可以随着时间的推移进行更新和定制，以反映技术、威胁和业务需求的变化。

[3] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

2.3 组织中的网络钓鱼：一项大规模长期研究的发现

研究项目《组织中的网络钓鱼：大规模长期研究的发现》 [6] 在一家拥有超过 14,000 名员工的公司开展了一项大规模实验。研究旨在了解某些员工是否比其他员工更容易遭受网络钓鱼攻击、公司整体易受网络钓鱼攻击的程度如何随时间变化、网络钓鱼警告和培训的效果如何，以及众包网络钓鱼检测在公司中的应用效果如何。研究证实了以往的发现，即年龄和计算机技能都与个体是否容易受到网络钓鱼攻击有关。此外，研究还发现，最容易受到网络钓鱼攻击的员工，是那些每天使用计算机、仅借助专业软件执行重复性任务的员工。研究中一个更令人担忧的发现是，模拟网络钓鱼演练和自愿培训不仅未能提高员工的防范能力，反而适得其反，使员工更容易遭受网络钓鱼攻击。如果再结合另一项观察，即长期接触网络钓鱼攻击可能导致更大比例的员工容易受到此类攻击，那么这一发现的严重性就更加突出。积极的一面是，研究证明，众包网络钓鱼检测能够在大型组织中有效发挥作用。

2.4 网络安全培训：网络安全严肃游戏综述

在论文《网络安全培训：网络安全严肃游戏综述》中， [10] 开展了一项调查，研究对象是专注于网络安全的学术和非学术严肃游戏。该研究强调，尽管人们在技术安全方面投入了大量精力，但对于如何更好地教育用户所投入的关注却少得多，而用户被认为是安全链中最薄弱的环节。研究还指出，有效的大规模措施更倾向于面向技术受众，而对于如何消除“网络安全只属于精通技术人士”的观念，所做的工作却很少。与实践培训方法相比，基于游戏的学习允许学生，甚至鼓励学生，在无风险环境中犯错并从中学习 [11]。此外，研究认为，设计良好的严肃游戏能够保留传统培训和实践培训的所有优势，同时保持较低成本。调查得出的结论是，面向网络安全的严肃游戏似乎很有前景，但目前缺乏对这些游戏的适当评估，因此无法对其有效性作出确切结论。

3 研究设计

我们的网络攻击模拟器旨在提升社会大众对网络攻击的认识。因此，我们设计了一项研究，在玩家游玩游戏前后分别进行提问，以了解游戏对其网络攻击知识的影响。相关问卷采用结构化形式，问题为是非题或范围题，范围从一到五。问题主要聚焦于游戏中的网络钓鱼部分，因为我们认为大多数人都曾接触过网络钓鱼 [12]。我们向两个不同研究机构的学士生以及其他随机招募的人士发放了问卷。游戏开始前的第一次调查侧重于参与者在网络攻击领域已有的知识。游戏结束后的第二次调查用于验证游玩游戏是否提升了参与者对网络攻击的认识，因此其中的问题几乎与第一次完全相同。调查以匿名方式进行，我们没有追踪每位参与者在游戏前后所提交的答案。本研究仅分析了短期效果，因为我们没有在游玩游戏一段时间后（例如半年或一年后）进行任何评估。

4 游戏设计

本节将介绍我们网络攻击模拟器的游戏设计。我们重点关注游戏中最重要的部分——场景。之后，我们将讨论游戏的实际设计，例如图形和风格。

该游戏的核心目标是让玩家亲自实施攻击，从而更好地理解网络犯罪分子如何发动网络攻击以及如何接近目标，无论他们是否具备技术知识。以攻击为核心的游戏并不少见，常用于教授网络安全技能，常见形式是夺旗赛（CTF）游戏。其缺点是，这类游戏通常要么需要丰富的技术知识，要么需要投入大量时间。我们采用严肃游戏的方式，旨在让更多人能够轻松体验网络安全游戏，并让他们自由探索，无需担心犯错。游戏分为多个场景，每个场景都对应恶意行为者在现实世界中使用的攻击。玩家可以与角色 Nate 互动，选择先体验哪个场景。选定场景后，玩家需要将自己的角色移动到游戏中的一台计算机前，并从那里发起所选攻击。以下小节将首先介绍 NIST 框架与我们的场景之间的对应关系，然后介绍并说明目前可供玩家探索的场景。

4.1 将网络安全技能映射到游戏场景

我们以 NIST 框架（见第 2.2 节）为基础设计场景，并将成功应对网络攻击所需的不同技能总结为四个类别。

我们首先将技能归纳为类别。

1. 第一个场景是添加网络钓鱼/社会工程，涵盖以下技能：通过电子邮件网络钓鱼防止恶意软件、通过电子邮件网络钓鱼防止个人身份信息盗窃、通过访问不可信网站防止个人身份信息盗窃，以及通过社交媒体防止个人身份信息泄露。该场景将引导玩家体验一次典型的网络钓鱼攻击，以了解攻击者的思维方式，并帮助他们认识钓鱼邮件中应当识别的相关特征。2. 第二个类别更侧重于开发人员，涵盖通过密码利用防止未经授权的信息系统访问这一技能。该场景将引导玩家体验这样一种情境：攻击者能够从不安全的网站窃取信息。3. 第三个类别与 Metasploit [13], 有关。Metasploit 是一种用于渗透测试的攻击框架，但也可能被攻击者滥用。该类别涵盖打补丁和更新关键系统的重要性。这也是一个更侧重于开发人员和系统工程师的场景，其内容依据 ENISA 威胁态势报告（参见第 2.1 节）中的建议，并涵盖通过不可信网站防止恶意软件这一技能。4. 第四个也是最后一个类别与恶意 USB 密钥有关。该类别涵盖通过 USB 或存储设备利用防止信息系统遭到入侵这一技能，并引导玩家了解攻击者如何从暗网获取恶意软件，以及如何利用 USB 密钥找到进入公司网络的途径。

为每个类别创建一个场景。下一节将对所有场景进行更详细的描述。目前，这些场景是我们根据 NIST 框架和 ENISA威胁态势中的信息创建的示例场景，用于涵盖并评估基础技能。未来将开发更多场景，以涵盖更高级的攻击场景。

4.2 社会工程与网络钓鱼

社会工程这一术语描述的是这样一种行为：通过与个人建立联系以获取其信任和信赖，诱骗其泄露敏感信息、获得未经授权的访问权限或实施欺诈。[4] 为了说服受害者提供信息或服务，社会工程师严重依赖影响力的六项原则 [14]。基于这些原则，社会工程师会稍作调整后采用以下手段：权威、恐吓、共识/社会认同、稀缺性、紧迫性以及熟悉/喜好。通常，攻击者会通过电子邮件与目标接触；一般情况下，这称为网络钓鱼，而当攻击针对特定组织或个人时，则称为鱼叉式网络钓鱼。Verizon数据泄露调查报告 [5] 指出，欧洲、中东和非洲超过 60% 的数据泄露事件都包含社会工程要素；尽管开展了意识宣传活动和演练，仍有许多人会上当于钓鱼邮件。社会工程是攻击者最常用的入侵途径，如果对員工进行适当教育，也是最容易避免的攻击方式。此外，防御网络钓鱼所需的技术知识非常少，因此任何人都可以且必须接受适当的相关培训。

在我们的游戏中，玩家首先通过使用社交媒体收集目标对象的信息，从而发起社会工程攻击。在社交媒体上找到企业电子邮件地址后，玩家接下来会检查该电子邮件是否曾出现在已知的数据泄露事件中，以及是否有密码被泄露。由于该电子邮件并未出现在任何泄露事件中，玩家便获得了发起网络钓鱼攻击的选项。随后，游戏使用 SocialPhish[6]，逐步引导玩家完成一次经过简化但真实的网络钓鱼攻击。为了提高用户友好性，游戏将较为复杂的命令和搜索操作替换为点击操作和特定文本输入。为了获取目标对象的登录凭据，游戏利用紧迫性原则，发送一封伪装成来自 Facebook 的虚假电子邮件，告知目标对象其账户即将过期。目标对象上当并点击了网络钓鱼电子邮件，随后，被窃取的凭据便显示在屏幕上。

4.3 SQL 注入

2021年，基于注入的攻击在 OWASP 的十大风险排名中位列第三 [15], ，该排名是一份面向开发人员的标准安全意识文档，介绍了十大 Web 应用程序安全风险。在此前的 2017年 排名中，注入攻击位居第一。SQL 注入是一种特殊类型的基于注入的攻击，其攻击目标是数据库。通过注入 SQL

[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf [5] https://www.verizon.com/business/resources/reports/dbir/ [6] https://github.com/xHak9x/SocialPhish

语句转换为输入数据，攻击者试图操纵查询，以篡改或泄露敏感数据。成功攻击还可能导致攻击者在数据库管理系统中执行管理员命令，试图窃取数据库中存储的文件内容，在某些情况下甚至能够在底层操作系统上执行命令。如果软件与 SQL 数据库进行交互、接收来自不可信来源的数据（例如网站上的用户输入），并动态使用这些数据构建查询，那么该软件就容易受到 SQL 注入攻击 [16]。
由于这是一个更具技术性和复杂性的概念，我们的游戏仅通过引导玩家逐步实施一次攻击并解释其底层原理，简要介绍 SQL 注入的概念。通过注入攻击，玩家可以绕过登录验证，访问测试服务器并搜索其中的文件。通过查看不同的文件夹（及其内容），游戏会解释可能采取的后续操作及其目的。

4.4 Metasploit

Metasploit 框架 [9] 是一种用于针对指定机器创建和执行漏洞利用程序的工具。其核心是一个已知漏洞和有效载荷的集合，旨在帮助渗透测试人员更好地测试系统，并始终拥有一份最新的攻击选项目录。使用该框架执行攻击时，它会提供已知漏洞利用程序的基本框架，并允许用户手动设置特定目标和选项。此外，该框架还提供了 Meterpreter，这是一种能够接管受害者系统控制权的有效载荷。Metasploit 框架和 Meterpreter 均向公众开放，因此，它们不仅被安全专家用于以合法方式攻击系统，也被攻击者用于实施非法活动。

场景从玩家使用 Nmap [17], 进行网络扫描开始。Nmap 是一款广受欢迎的安全扫描工具，可扫描网络中的主机及其运行的服务。完成初步扫描后，玩家将学习如何在 Metasploit 框架中按常规步骤设置漏洞利用程序，并进行配置，以便使用选定的有效载荷攻击特定目标。输入 run 后，漏洞利用程序成功执行，并在目标设备上启动 Meterpreter 会话。接着，玩家利用该会话查找并下载敏感数据。场景最后提醒玩家，此时系统已严重暴露，攻击者可以实施各种恶意操作，例如在目标主机上安装恶意软件。

4.5 恶意 USB

恶意 USB 也称为 Rubber Ducky，是 Hak5[7], i 制造的一种恶意 USB。这种攻击通过使用经过改装的 USB 闪存盘攻击系统。这些 USB 闪存盘通常内置可编程微控制器，攻击者可以对其进行编程 [18]。插入系统后，恶意 USB 会模拟键盘，并立即被目标系统识别为键盘。随后，该设备会向目标系统输入按键并发送命令。这些命令可以是打开终端并下载勒索软件、查找并窃取敏感数据，也可以是无害地恶作剧，比如关闭目标系统。要成功实施攻击，攻击者只需将 USB 插入目标系统，或说服他人代为插入。还有一种大规模攻击方式：攻击者将 USB 设备作为礼物寄给目标公司的员工。向数百名员工寄送恶意 USB 后，很可能有人在不久的将来将其用于公司设备，从而为攻击者进一步攻击目标提供入口 [19]。

要启动此场景，玩家首先需要找到放在房间桌上的 USB 闪存盘。随后，游戏会解释恶意 USB 攻击的运作方式，并让玩家选择如何继续。第一个选项是利用零日漏洞对其进行刷写。所谓零日漏洞，是指软件生产商尚未发现的漏洞。游戏会引导玩家前往暗网购买此类漏洞利用程序，展示网络犯罪分子如何获取这类漏洞。游戏还会解释网络犯罪分子如何在使用在线黑市时保持匿名。购买零日漏洞后，场景会让玩家选择如何在 USB 闪存盘上贴标签，标签上的文字旨在诱使发现它的员工将其插入电脑。

第二个选项的恶意程度较低，其中包含一个会打开 Microsoft Word 5 次的批处理脚本。游戏还会解释，可以将此脚本与一张图片关联，以提高有人意外执行它的可能性。虽然此场景使用的是无害示例，但脚本可以替换，且其中可以包含恶意得多的内容。选择此选项后，玩家最终会继续选择前面提到的零日漏洞选项。

4.6 游戏实现

游戏的设计受到 Cybersiege [20, 21, 22] 的启发，因此构思了一段简短的叙事，随后展示了各种真实网络攻击的场景。游戏采用 3D 形式，玩家可以在房间里自由行走

[7] https://shop.hak5.org/

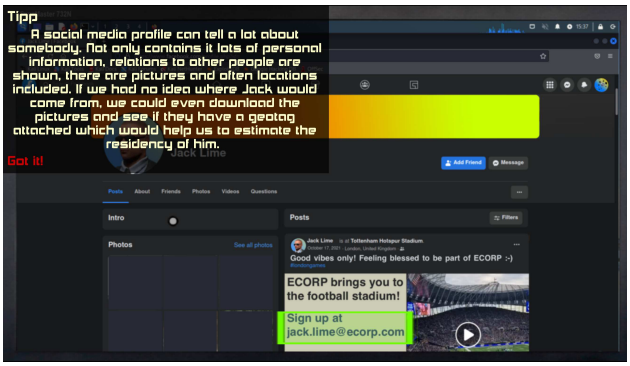

图 1：已实现的网络钓鱼场景截图。

并探索房间。游戏使用 Adventure Creator[8], 开发，这是一款 Unity[9]游戏引擎插件，可通过可视化脚本编程来开发游戏。当玩家与游戏中的电脑互动时，场景会切换到伪 2D 环境，仅显示屏幕。为了能在浏览器中通过 WebGL 运行，游戏经过大幅压缩，体积为 190MB。图 1 展示了游戏中的网络钓鱼场景截图，游戏在其中向玩家介绍了在社交媒体上发布敏感信息可能带来的风险。

5 评估

为了评估我们的游戏，我们开展了一项短期调查（见第 3 节），请参与者在游戏开始前和结束后填写一份表格。与通常的前测和后测调查一样，我们收到的前测结果多于后测结果。为保护参与者的隐私，我们没有在每份表格中添加个人标识符，因此无法将游戏前填写的表格与游戏后填写的表格对应起来。从图 2 可以看出，几乎所有参与者都知道什么是钓鱼邮件。

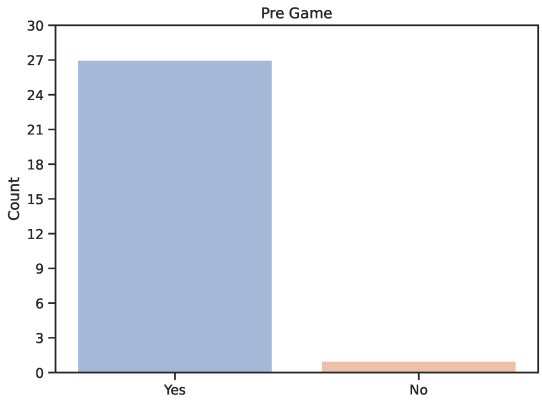

图 2：对问题“你知道什么是钓鱼邮件吗？”的回答

然而，如图 3 所示，在玩我们的游戏之前，大多数参与者对网络钓鱼攻击是如何实施的知之甚少，甚至一无所知。游戏后的结果显示，参与者对网络钓鱼攻击的实施方式有了明显更深入的了解。尽管前测和后测结果数量不平衡，但从绝对数量来看，我们可以得出结论：参与者通过玩我们的游戏加深了理解。如图 4 所示，我们还询问参与者是否知道网络钓鱼攻击者如何获取他们的电子邮件。这里同样可以看到，参与者对攻击者如何获取受害者电子邮件的认识有所提高。在调查结束时，我们询问参与者，他们总体而言是否通过我们的游戏对网络攻击和风险有了更多了解。从图 5 可以得出结论，平均而言，这款游戏让玩家对网络攻击和网络风险有了更深入的认识。

[8]https://adventurecreator.org/[9]
https://unity.com

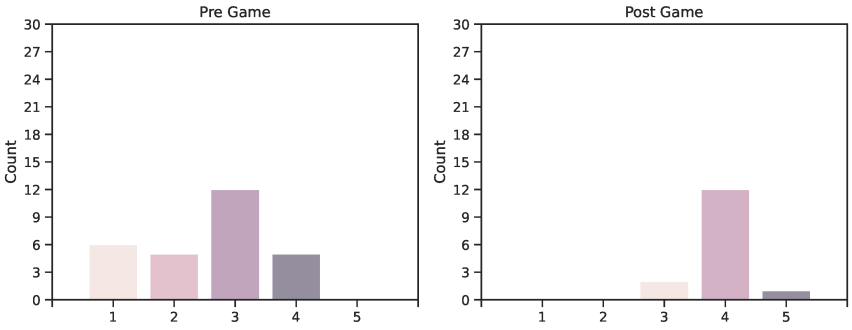

图 3：对问题“你知道网络钓鱼攻击是如何实施的吗？”的回答

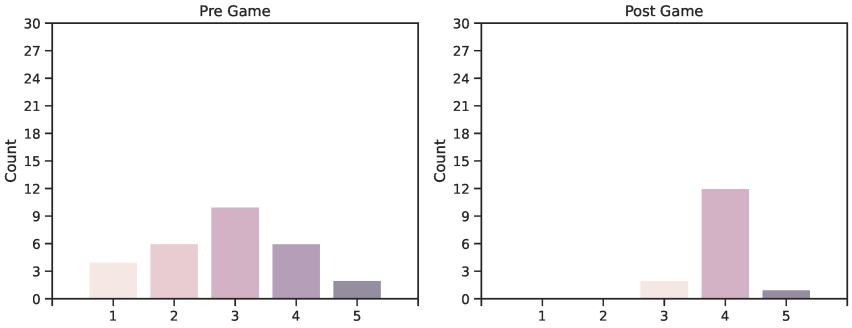

图 4：对问题“你知道网络钓鱼攻击者如何获取你的电子邮件地址吗？”的回答

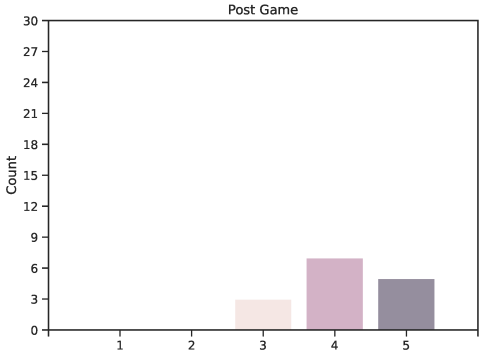

图 5：对问题“你认为游戏《The get in》是否帮助你更好地了解网络攻击和网络风险？”的回答

6 结论与未来工作

本文重点介绍了员工在日常工作中面临的常见网络威胁及其可能造成的相关后果。此外，我们强调，对于网络钓鱼和社会工程这两种网络犯罪分子最常用的入侵途径，目前采取的预防措施实际上反而降低了员工抵御此类攻击的能力 [6]。为了提高员工对常见网络威胁的意识和理解，我们提出了一种严肃游戏，而非意识宣传活动。在这款游戏中，玩家扮演攻击者的角色，深入了解攻击者如何接近目标，以及如何利用常见的疏忽和漏洞。基于攻击的游戏在网络安全领域非常流行，通常以夺旗赛（CTF）的形式出现。这些游戏化场景通常对应真实场景，具有显著的学习效果，但往往需要较深厚的技术知识，因此难以让更广泛的受众参与。我们的方法采用交互式流程，引导玩家逐步经历不同的攻击场景，从而提高游戏的可参与性。在攻击的每个步骤中，都会解释攻击者的思考逻辑以及相应的预防措施选项。

根据我们在第 5 节中的评估，我们得出结论：我们的游戏对提升网络安全意识具有积极的短期效果。此外，几乎所有玩过这款游戏的参与者都表示，他们很享受游戏过程。为了缓解游戏前后回答不一致的问题，我们可以在游戏前表单中添加一个随机生成的会话标识符，供玩家在游戏中和游戏后表单中使用。通过这些措施，我们可以筛除不完整的结果，并得出更可靠的结论。需要注意的是，我们并未在参与者玩游戏前后开展网络钓鱼意识宣传活动，以验证游戏在实际中的教育效果。问卷本身也更侧重于短期结果。正如 [10] 所指出的，目前尚无针对网络安全场景中严肃游戏效果的长期评估。我们也将这一问题留待未来研究。

目前，这款游戏仍处于开发阶段，需要进一步完善。此外，3D场景除了模仿3A级游戏之外，是否还能带来其他特定益处，也值得商榷。对于不习惯玩3D游戏的人来说，更复杂的移动控制可能会分散他们对突出网络风险这一实际目标的注意力。由于游戏的重点在于发生在计算机上的场景（即 2D场景），3D图形给游戏玩法带来的复杂性大于益处。与其将时间花在开发3D游戏所增加的复杂工作上，不如将其用于打造更精细的2D场景、为每个场景增加不同的难度选项，或提升图像质量。

参考文献

[1] Christopher Scherb、Pascal Bürklin 和 Christian Tschudin。《Scoiot：物联网的群体计算》。载于《2021年国际计算机通信与网络会议（ICCCN）》，第1–6页。IEEE，2021年。[2] Christopher Scherb、Dennis Grewe、Marco Wagner 和 Christian Tschudin。《通过命名函数在边缘实现物联网联网的解析策略》。载于《2018年第15届IEEE年度消费者通信与网络会议（CCNC）》。IEEE，2018年。[3] Nurul Amirah Abdul Rahman、I Sairi、NAM Zizi 和 Fariza Khalid。《学校网络安全教育的重要性》。《国际信息与教育技术期刊》，2020年。[4] Valdemar Švábensk`y、Jan Vykopal 和 Pavel ˇCeleda。《网络安全教育论文的主题是什么？SIGCSE 和 ITiCSE 会议的系统性文献综述》。载于《第51届ACM计算机科学教育技术研讨会论文集》，第2–8页，2020年。[5] Zainab Alkhalil、Chaminda Hewage、Liqaa Nawaf 和 Imtiaz Khan。《网络钓鱼攻击：近期综合研究与新型剖析》。《计算机科学前沿》，3：563060，2021年。ˇ[6] Daniele Lain、Kari Kostiainen 和 Srdjan Capkun。《组织中的网络钓鱼：大规模长期研究的发现》。载于《2022年IEEE安全与隐私研讨会（SP）》，第842–859页。IEEE，2022年。[7] Marcel Maurer。《面向非网络安全专业人士的攻击模拟严肃游戏》。技术报告1，FHNW硕士论文，fhnw.ch，2022年12月。FHNW硕士论文。用于开展网络安全教育的严肃游戏设计与开发。[8] Bruce Schneier。《黑客之心》。W. W. Norton，2023年。[9] Kevin M Stine、Kim Quill 和 Gregory A Witte。《改进关键基础设施网络安全的框架》。2014年。[10] Jin-Ning Tioh、Mani Mina 和 Douglas W. Jacobson。《网络安全培训：网络安全严肃游戏综述》。载于《2017年IEEE教育前沿会议（FIE）》，第1–5页，2017年。

[11] Kurt Squire。《教育中的电子游戏》。International Journal of Intelligent Simulations and Gaming，2：49–62，2003年10月。[12] Rana Alabdan。《网络钓鱼攻击调查：类型、途径与技术方法》。Future Internet，12(10)：168，2020年。[13] David Kennedy、Jim O'gorman、Devon Kearns 和 Mati Aharoni。《Metasploit：渗透测试人员指南》。No Starch Press，2011年。[14] Roselle L. Wissler、Robert B. Cialdini 和 N J Schweitzer。《影响力科学：运用六项说服原则，更有效地进行谈判与调解》。2002年。[15] OWASP 十大风险。https://owasp.org/Top10/ 访问日期：2023年3月23日。[16] William G Halfond、Jeremy Viegas、Alessandro Orso 等。《SQL 注入攻击及对策分类》。载于 IEEE 国际安全软件工程研讨会论文集。IEEE，2006年。[17] Nmap。https://nmap.org/ 访问日期：2023年3月23日。[18] Stella Vouteva、Ruud Verbij 和 Jarno Roos。《恶意 USB 的可行性与部署》。阿姆斯特丹大学系统与网络工程硕士研究项目，2015年。[19] Rohan Scanavez。《恶意 USB：为什么企业必须讨论这一威胁？》。Research Review，2(3)：561–567，2021年。[20] Michael F. Thompson 和 Cynthia E. Irvine。《通过 CyberCIEGE 电子游戏进行主动学习》。发表于 CSET，2011年。[21] Michael F. Thompson 和 Cynthia E. Irvine。《CyberCIEGE 场景设计与实现》。Genetics Selection Evolution，2014年。[22] Michael F. Thompson 和 Cynthia E. Irvine。《CyberCIEGE：一款用于建构式网络安全教育的电子游戏》。2016年。

此图“test.png”可从以下位置获取 PNG格式：

http://arxiv.org/ps/2305.03062v1