

组织中的网络钓鱼：一项大规模长期研究的结果

Daniel Lain、Kari Kostiainen 和 Srdjan Capkun

瑞士苏黎世联邦理工学院计算

机科学系

{daniele.lain, kari.costs, srdjan.capkun} @inf.ethz.ch

摘要——在本文中，我们展示了我们与合作伙伴公司合作进行的大规模和长期网络钓鱼实验的结果。我们的实验持续了 15 个月，在此期间，超过 14,000 名研究参与者（公司员工）在其正常工作环境中收到了不同的模拟网络钓鱼电子邮件。我们还在公司的电子邮件客户端部署了一个报告按钮，允许参与者报告他们收到的可疑电子邮件。我们测量了网络钓鱼电子邮件、提交凭据等危险操作以及报告的可疑电子邮件的点击率。

我们的实验结果提供了三种类型的贡献。首先，我们的一些研究结果支持以前的文献具有更高的生态有效性。此类结果的一个示例是电子邮件警告的良好效果。其次，我们的一些结果与先前的文献和常见的行业惯例相矛盾。令人惊讶的是，我们发现，当今行业普遍采用的模拟网络钓鱼练习中的嵌入式培训并没有使员工更能抵御网络钓鱼，反而会产生意想不到的副作用，使员工更容易受到网络钓鱼的影响。第三，我们报告新发现。特别是，我们率先证明将员工用作集体网络钓鱼检测机制在大型组织中是可行的。我们的结果表明，这种众包可以快速检测新的网络钓鱼活动，组织的运营负荷是可以接受的，员工长期保持活跃。

I. 介绍

网络钓鱼仍然是 Internet 上的一个主要问题 [1]。欺骗用户执行不安全操作的欺骗性电子邮件变得越来越复杂 [2]、[1]，并且在过去二十年中，网络钓鱼没有任何放缓的迹象 [3]。网络钓鱼工具包的开发使网络犯罪分子的工作变得容易，这种软件能够自动创建流行网站的欺骗性副本 [4]、[5]、[6]。更糟糕的是，COVID-19 大流行已将工作、购物和其他活动转移到网上，这反过来又创造了新的网络钓鱼机会并增加了网络钓鱼 [7]。

几十年来，研究人员一直在研究网络钓鱼（请参阅 [8]、[9]、[10]、[11] 以了解对早期作品的广泛评论），并提出了从电子邮件过滤器 [10]、[12] 到检测网络钓鱼网站的各种防御措施 [13]、网络钓鱼活动的模式 [14]、促使人们陷入网络钓鱼的触发器 [15] 以及教育用户的方法 [16]、[11]。在过去十年中，还出现了提供网络钓鱼防护产品和服务的公司的整个生态系统。常见的商业产品包括培训和教育服务 [17]、[18]、[19]、[20]、已知 URL 的数据库以及使用的电子邮件

通过网络钓鱼攻击 [21]、[22]、[23] 和由专家收集的威胁情报和客户报告 [24]、[18]、[19] 提供支持的电子邮件过滤器。

我们的研究和贡献。在本文中，我们研究网络钓鱼，特别关注组织中的网络钓鱼。我们通过以下四个问题来探讨这个话题——所有问题都与网络钓鱼的人为因素有关。首先，我们感兴趣了解大型组织中哪些员工最容易受到网络钓鱼的攻击。我们通过员工人口统计和工作类型等常见方面来检查这一点。其次，我们探索了该组织的网络钓鱼漏洞是如何随着时间的推移而演变的。例如，我们研究了有多少员工会因持续接触网络钓鱼而最终落入网络钓鱼的陷阱。第三，我们研究组织如何帮助其员工预防网络钓鱼。特别是，我们分析了当前流行工具的好处，例如嵌入式网络钓鱼培训和可疑电子邮件上的警告。第四，我们探讨员工是否可以集体帮助组织预防网络钓鱼。关于这个问题，我们专注于将员工用作集体网络钓鱼检测传感器——这一想法之前曾被提出 [25]、[23]，但在我们开展工作之前，其有效性和可行性尚未在真正的大型组织中进行过公开评估。

为了回答这些问题，我们与合作伙伴公司合作设计并进行了一项大规模的长期网络钓鱼研究。我们的研究持续了 15 个月（2019 年 7 月至 2020 年 10 月），期间有 14,773 名公司员工参与了我们的实验。我们的研究涉及向参与者发送模拟网络钓鱼电子邮件，参与者在正常工作流程和上下文中收到这些电子邮件。我们测量了他们的点击率、凭据提交和附件启用宏。我们还在公司电子邮件客户端部署了一个报告按钮，使我们的研究参与者能够轻松报告他们发现可疑的电子邮件，并分析报告的电子邮件。

据我们所知，我们的实验是对同时大规模（14000 名参与者）、长期（15 个月）、现实（我们测量真实员工的网络钓鱼行为）的组织中的网络钓鱼行为的首次研究实际工作环境）和多样化（包括不同公司部门和工作角色的参与者）。所有可比较的、以前的研究要么规模较小 [26]、[27]、[28]、[29]、[30]、[31]、[32]、[33]、[34]、[35]、[36]，[37]，[38]，[16]，

[39], 较短的 [36], [35], [26], [16], [33], [27], 基于角色扮演 [40], [41], [29], [32], [31], 或多样性较低的 [41]、[34]、[29]、[28]、[27], 我们将在第二部分详细说明。

我们的实验结果提供了三种类型的贡献。首先, 我们报告了几个支持先前文献的结果, 这些结果具有更高的生态有效性 (例如, 更多的研究参与者、更长的研究持续时间或更现实的研究环境)。其中, 我们发现电子邮件警告是有效的, 并且在我们的实验中观察到许多“重复点击者”[42]。其次, 我们的研究发现了一些发现, 这些发现与先前的学术研究结论和常见的行业实践相矛盾。特别是, 我们发现当今行业普遍使用的嵌入式网络钓鱼训练可能会导致意想不到的副作用, 甚至不利于网络钓鱼预防。这是一个重要的发现, 因为这种做法在行业中得到广泛使用。

第三, 我们的结果为组织中的网络钓鱼提供了新的见解。特别是, 作为本文的主要贡献之一, 我们的实验首次证明了众包网络钓鱼检测可以在很长一段时间内有效、快速和可持续。在我们的实验中, 员工报告了数以千计的可疑电子邮件, 这些电子邮件代表了数百个真实的和以前未见过的网络钓鱼活动。我们模拟的网络钓鱼电子邮件的报告速度表明, 可以在启动后的几分钟内检测到新的活动。我们设计了一个简单的处理管道, 结合了对报告电子邮件的自动和手动分析。我们的实验表明, 通过这种技术, 即使在大型组织中, 处理所有报告的电子邮件的操作负载也可以降低。我们的实验还表明, 庞大的员工群体可以在很长一段时间内共同保持足够高的报告率。总之, 本文首次证明众包网络钓鱼检测对于许多组织来说是一种实用且有效的选择。

总而言之, 本文做出以下贡献:

- 1) 对大型组织中网络钓鱼和网络钓鱼预防的人为因素进行广泛的测量研究。
- 2) 对先前几项研究结果的支持性结果具有更高的生态有效性。
- 3) 矛盾的发现挑战了先前研究的结论和流行的行业实践。
- 4) 对众包网络钓鱼报告的大规模评估显示了快速检测、小运营开销和持续的员工报告活动。

论文大纲。本文组织如下。在第二部分中, 我们定义了我们的研究问题并概述了我们的发现。我们在第 III 节中描述了我们的实验设置。我们在第 IV 节中报告了与员工人口统计相关的结果。第五部分展示了在我们的研究中网络钓鱼漏洞是如何随着时间的推移而演变的。第六节解释了我们与警告和嵌入式训练相关的结果。第七节分析了众包网络钓鱼检测。在第八节中, 我们讨论了我们研究的有效性。第 IX 节回顾相关工作, 第 X 节总结本文。

II. 研究问题和主要发现

在本节中, 我们首先定义了我们的研究旨在回答的研究问题, 然后总结了我们的主要发现, 两者都在表 I 中进行了总结。

A. 研究问题

RQ1: 哪些员工上当受骗? 我们实验的第一个目标是了解大型组织中的哪些员工最有可能陷入网络钓鱼。特别是, 我们想了解组织可以轻松获得的员工特征, 例如年龄、性别和在一个人的工作类型中假定的计算机使用水平, 与网络钓鱼的敏感性有何关联。

RQ2: 随着时间的推移, 组织对网络钓鱼的脆弱性如何演变? 我们实验的第二个目标是了解网络钓鱼的持续存在如何随着时间的推移影响组织。我们研究的主题包括最终落入网络钓鱼的员工基数有多大, 以及有多少人反复落入网络钓鱼 [42]。

RQ3: 网络钓鱼警告和培训的效果如何? 我们的第三个目标是了解大型组织如何帮助其员工识别网络钓鱼电子邮件, 从而抵御网络钓鱼。如今, 组织可以从为此目的设计的一系列工具和教育措施中进行选择。在我们的研究中, 我们专注于评估可以以适中的成本部署到大型员工群的工具, 因为这些工具在实践中很常用。

我们决定检查其有效性的第一个工具是在可疑电子邮件之上发出警告。许多流行的电子邮件客户端和服务 (如 Gmail [43]) 都使用警告: 它们显示在自动网络钓鱼检测机制已在电子邮件中识别出一些危险或可疑特征的电子邮件顶部, 但它无法将电子邮件标记为网络钓鱼具有足够高的置信度 (通常将电子邮件过滤器调整为宽松以避免太多误报)。我们要测试的第二个工具是模拟网络钓鱼练习 [32]、[11] 结合嵌入式训练 [33]。在过去十年中, 模拟网络钓鱼演习已成为一种常见的行业做法 [18]、[19]、[17]、[20]。在模拟网络钓鱼练习中, 该组织向其员工发送模拟真实网络钓鱼电子邮件的电子邮件, 然后跟踪哪些员工执行了不安全的操作, 例如单击链接或向网页泄露凭据。通常, 此类练习与嵌入式培训 (有时也称为情境培训) 相结合, 在练习中失败的员工 (例如, 通过单击链接或披露其证书) 将被转发到信息资源, 例如提供有关教育材料的网页网络钓鱼。 **RQ4:** 员工能否帮助组织进行网络钓鱼检测? 我们实验的第四个目标是了解庞大的员工群是否可以共同帮助组织预防网络钓鱼。更准确地说, 我们想了解是否将员工用作众包网络钓鱼

表 I：我们研究问题和主要结果的总结，包括支持先前文献的发现、与先前研究相矛盾的发现以及新见解。本文的两个最重要的贡献以粗体标记。

	支持先前文献研究的发现	与以往文献研究相矛盾的发现	组织中网络钓鱼的新发现
RQ1：哪些员工爱上了网络钓鱼？ （第四节）	年龄和计算机技能相关具有网络钓鱼敏感性 [40], [41], [34], [36], [35], [29], [11], [26]	性别与网络钓鱼敏感性（与 [36]、[30]、[40]、[41] 相矛盾）	计算机使用类型更具预测性网络钓鱼漏洞比电脑使用量
RQ2：组织如何网络钓鱼的脆弱性不断发展 随着时间的推移？（第五节）	有几个“重复答题器”在大型组织中 [42]		许多员工最终会倒下如果持续暴露，则用于网络钓鱼
RQ3：网络钓鱼的效果如何警告和培训？ （第六节）	可疑电子邮件之上的警告有效 [38]、[37]、[39]	志愿嵌入式培训模拟网络钓鱼练习不是有效 （与 [33]、[32]、[34] 相矛盾）	更详细的警告就不多说了比简单的有效
RQ4：员工能否帮助网络钓鱼组织检测？ （第七节）			众包钓鱼邮件去tection是既有效又feasible祝福

在大型组织中，检测机制是高效的（是否可以足够快地检测到网络钓鱼活动？）、实用的（处理所报告的电子邮件的管理负担是否仍然可以接受？）和可持续的（员工会随着时间的推移继续报告电子邮件吗？）。此外，我们的目的是了解反馈机制的存在是否会鼓励员工更多地报告可疑电子邮件。

B. 主要发现摘要

接下来，我们概述了我们实验的主要发现，并简要讨论了这些结果与先前研究文献的关系（对相关工作的更详细调查在第 IX 节中给出）。我们的研究结果支持先前研究的主张，具有更高的生态有效性；与之前的结论和普遍的行业惯例相矛盾；并提供与大型组织中的网络钓鱼相关的新见解。

与 RQ1 相关的调查结果。我们的实验结果支持之前的工作，该工作表明年龄 [40]、[41]、[34]、[36]、[35]、[29] 和计算机技能 [11]、[26] 都与网络钓鱼相关漏洞。与之前的研究类似，我们还发现年长和年轻的员工以及计算机技能较低的员工面临的风险更大。我们的实验提高了这些研究的生态有效性，这些研究规模较小 [36]、[35]、[30]、[34]、[29]、[26]，持续时间较短 [36]、[35]、[26]]、多样性较低的特色人群（例如，主要是大学生和员工 [41]、[34]、[29]，年龄偏斜 [35]），或仅特色角色扮演或测验式研究 [40]、[41]]，[29]。与之前的文献 [36]、[30]、[40]、[41] 相反，我们没有发现性别与网络钓鱼易感性相关。我们观察到的相关性可以通过不同类型工作在性别之间的偏斜分布得到更好的解释。我们通过在日常工作环境中报告更大、更多样化的人群来改进这些研究。

作为一项新发现，我们的研究表明，最脆弱的员工是那些每天使用计算机进行重复性工作的员工

仅使用专门软件的任务，而不是那些在日常工作中不需要计算机的员工。也就是说，在我们的实验中，计算机使用的类型比数量更能预测网络钓鱼漏洞。我们将在第 IV 节中更多地讨论这些主题。

与 RQ2 相关的调查结果。与之前的研究类似，我们发现了几个多次未能通过模拟网络钓鱼练习的“重复点击者”[42]。我们还发现，如果组织中继续暴露于网络钓鱼，最终很大一部分员工将落入网络钓鱼的陷阱。我们在第五节详细说明了这些结果。

与 RQ3 相关的调查结果。我们的结果支持之前的研究，这些研究发现上下文警告有效 [38]、[37]、[39] 以及使用此类警告的常见行业实践 [43]。由于更大、更普遍的人群和严格的对照组，我们改进了这些研究。

有趣的是，与先前的研究结果 [33]、[32]、[34] 和常见的行业实践 [19]、[17]、[20]、[18] 相矛盾，我们发现模拟网络钓鱼练习和自愿嵌入的组合培训（即不要求员工完成培训）不仅不能提高员工的网络钓鱼抵御能力，反而使员工更容易受到网络钓鱼的影响。与我们的实验相比，以前的研究参与者较少 [33]、[31]、[28]、[16]、[32]、[27]，时间较短 [16]、[33]、[27]、人口多样性很少 [31]、[28]、[27] 或仅测试角色扮演设置 [32]、[31]。我们的结果表明在设计嵌入式培训时要谨慎：我们在第 VI 节中详细讨论了这个问题有点令人惊讶和非直觉的发现的可能原因（例如对公司 IT 安全的错误认识）和实际影响。

我们研究的另一个新发现是，在上下文警告中添加更多细节（例如，解释电子邮件被标记为可疑的原因）不会显着降低网络钓鱼的有效性。

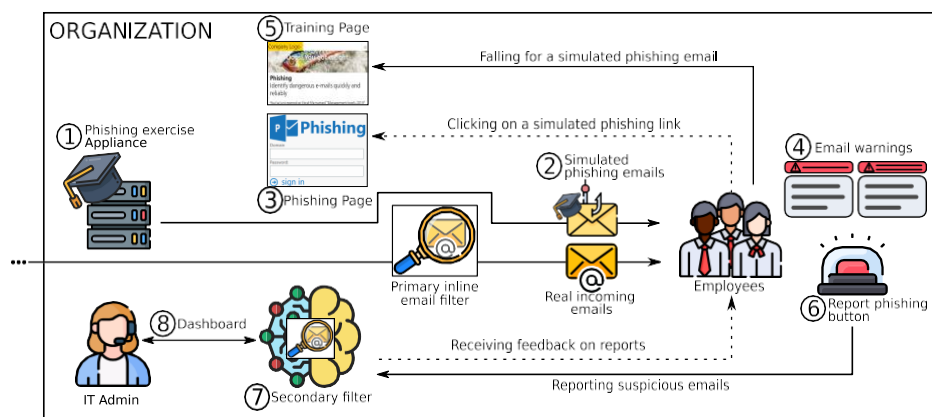


图 1：我们在合作伙伴公司部署的测量基础设施概览。

与 RQ4 相关的调查结果。本文的主要贡献之一是我们通过实验证明众包网络钓鱼检测在大型组织中可以高效且可持续。之前的论文 [25]、[23] 已经提出了对员工进行众包网络钓鱼检测的想法。我们的贡献是，我们是第一个在一个真正的大型组织的背景下长期评估这个想法的人。¹ 我们的实验表明，众包网络钓鱼检测使组织能够检测到大量以前看不见的真实网络钓鱼活动从活动开始后有短暂的延迟。我们作为实验的一部分开发的处理管道还表明，即使在大型组织中，网络钓鱼报告处理的操作负载也可以保持在较低水平。我们的研究还表明，有足够多的员工在很长一段时间内主动报告可疑电子邮件。总之，我们表明，众包网络钓鱼检测为许多组织提供了一个可行的选择。第七节提供了对该主题的完整讨论。

三、实验装置

在本节中，我们将解释我们如何与合作伙伴公司合作开展这项研究。

A. 学习组织

合作公司。在这项研究中，我们与一家拥有超过 56,000 名不同技术技能、年龄段和工作岗位的员工合作。我们的合作伙伴公司是一家大型上市公司，从事物流、金融、运输和 IT 服务。他们雇用不同职责的人：现场工作人员、在前端商店工作与公众接触的分店工作人员，以及从 IT 到营销和会计的不同资格的办公室工作人员。

¹用户报告网络钓鱼是一种广泛使用的行业惯例。例如，有些服务提供商从他们的许多商业客户 [24]、[19] 收集数据，大型电子邮件提供商收集报告以提供机器学习模型 [44]。然而，在我们开展工作之前，尚未公开评估是否可以有效利用单个组织的员工群作为网络钓鱼检测机制。

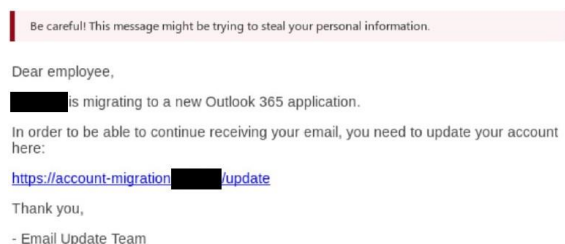
按照常见的行业惯例 [19]、[17]、[20]、[18]，在研究计划时，我们的合作伙伴公司已经在开展网络钓鱼意识活动，其中包括模拟网络钓鱼电子邮件和上下文（嵌入式）培训。

我们的角色。对于这项研究，我们利用现有的网络钓鱼意识活动作为我们研究问题的试验台。更准确地说，我们以两种方式与我们的合作伙伴公司合作。首先，作为帮助设计实验的科学顾问。通过为不同的员工部署不同的工具和条件，我们能够使用现有的活动来解决我们的研究问题。在研究结束时，我们从该公司批量收到匿名数据并进行分析。其次，我们积极参与，对随机选择的员工进行问卷调查并分析答复。

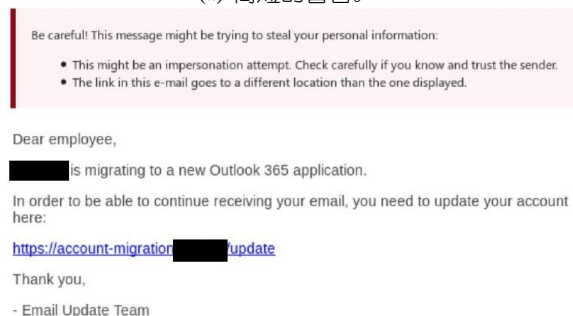
公司的作用。公司的作用有三：设计所有的模拟钓鱼邮件；提供用于发送模拟网络钓鱼电子邮件和测量点击等危险行为的基础设施；并托管嵌入式培训资源（向执行危险操作的员工展示的教育网页）。该公司与一家专门从事网络钓鱼意识和教育的外部服务提供商已有合作关系。该服务提供商协助该公司进行网络钓鱼电子邮件和上下文培训页面设计。该研究由公司的 CISO 发起并批准。

B. 测量基础设施

网络钓鱼练习组件。我们的合作伙伴公司部署了一个网络钓鱼练习组件，如图 1 中的 G) 所示，由专门从事网络钓鱼意识和培训的服务提供商实施，发送由人类专家制作的模拟网络钓鱼电子邮件。这些电子邮件可能链接到欺骗性网站（由 component ® 托管）或附加恶意文件，目的是欺骗参与者进行危险操作，例如提交他们的凭据或在附件上启用宏。



(a) 简短的警告。



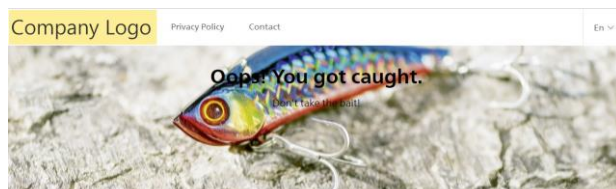
(b) 详细警告。

图 2：我们在模拟网络钓鱼电子邮件之上添加到选定参与者的电子邮件客户端的警告。

已部署警告。根据我们的建议，该公司部署了两种类型的警告^①，它们可以被触发显示在员工电子邮件客户端（Outlook）上的模拟网络钓鱼电子邮件之上。作为基准，我们部署了简短的警告（图 2a），在视觉上与员工习惯的标准 Outlook 警告相同，包含类似的通用句子，警告收件人要小心，因为电子邮件“看起来可疑”。

我们还开发并部署了详细的警告，如图 2b 所示，在视觉上与 Outlook 警告相同，但添加了电子邮件可能可疑的原因列表，例如，发件人的电子邮件与显示的名称不匹配，或显示的链接和指向的域。当没有足够的把握阻止电子邮件时，此类信息可以在部署中自动生成，该部署会向看似可疑的电子邮件添加警告。

部署培训。网络钓鱼练习组件还托管了一个关于网络钓鱼^②的培训网页，该网页是在有人执行模拟网络钓鱼电子邮件的危险操作后显示的。这个内部公司网页（图 3 中显示的部分内容）向员工详细解释了发生的事情（即，他们未能通过其组织的网络钓鱼活动）、电子邮件中应该注意的具体提示、提示以后避免网络钓鱼、教学视频以及有关网络钓鱼的进一步测验和学习材料。培训页面是由外部服务提供商根据学术界 [45]、[31] 和工业界 [19]、[17] 的最佳实践开发的；我们在附录 A 中提供了一个摘录。培训页面已交付给员工，因此没有强制执行员工必须



Phishing
Identify dangerous e-mails quickly and reliably

图 3：上当模拟钓鱼邮件后显示的上下文训练意识网页的标题。

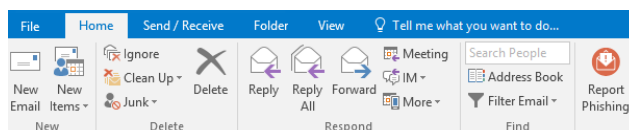


图 4：公司电子邮件客户端（Outlook）的菜单栏，修改为包含报告可疑电子邮件的按钮。

阅读整个网页或参加测验。

报告按钮。我们的合作伙伴公司部署了一个按钮^③来报告可疑电子邮件。这个按钮是在 Outlook 客户端中引入的，如图 4 所示，实验开始前在公司内部新闻中进行了宣传。报告可疑电子邮件时，员工可以切换复选框以报告他们也打开了附件或访问了电子邮件中的链接，以通知 IT 部门可能发生的事件。

报告的电子邮件处理。我们的研究参与者报告的所有电子邮件都由商业反网络钓鱼设备（J）进行分类，该设备运行更详细的二次分析。对报告的电子邮件执行的二次分析在两个方面不同于公司的主要在线过滤器：（a）执行了更耗时的检查，例如以下链接，以及（b）分析设置被调整得更积极，因为在这点上，我们不需要避免太多误报。二次分析的结果通过仪表板呈现给公司的 IT 部门，其中可以根据手动分析^④确认或推翻设备判断。此外，该设备可以向员工返回反馈，表明所报告的电子邮件是否确实是恶意的。

C. 研究参与者

公司招募了 14,733 名员工参与实验：我们将他们称为参与者。参与者是从整个公司的员工群中随机选择的，包括许多不同的工作类型，从会计师、IT、营销和管理角色到技术含量较低的工作（例如，物流或零售店工作）。参与者总共来自公司的 28 个组织组，代表 3,827 个不同的团队。

出于我们研究的目的，我们根据参与者的年龄、性别和当天的计算机使用情况对参与者进行了分类——

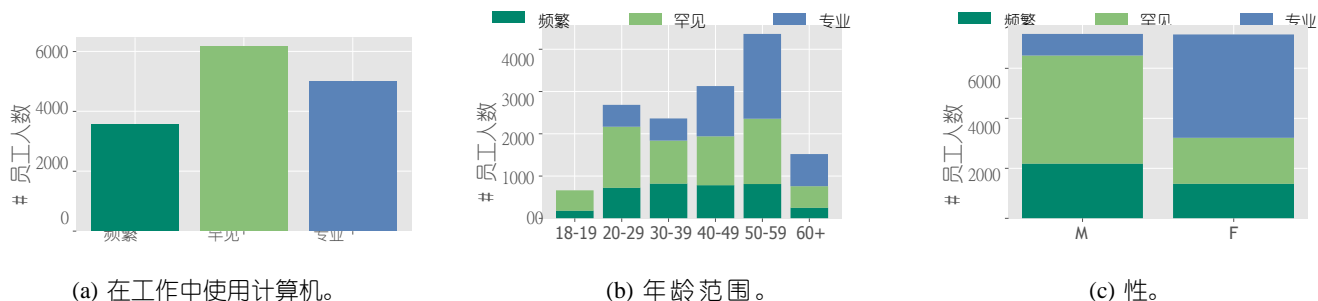


图5：研究参与者的人口统计信息。年龄和性别在工作中因计算机使用而进一步划分。

今天的工作。参与者按计算机使用情况（如图5a所示）分为三个不同的类别：（i）每天使用计算机的办公室工作人员，无论是在与IT相关的工作中，还是在营销和会计等使用计算机的工作（经常使用）；（ii）就业角色，例如与公众接触的零售店工作人员，他们主要使用销售点软件并从中配置服务（专用）；以及（iii）拥有公司电子邮件帐户但很少在职责中使用计算机的后勤现场工作人员的团队负责人等角色（不经常使用）。研究参与者的年龄范围为18-73岁，所有年龄组在我们的参与者中都有很好的代表性（图5b）。参与者的性别分布（图5c）是平衡的：7,377名男性，7,356名女性，与公司员工基础的分布相似。我们观察到性别和年龄使用计算机的不平衡：大多数使用一个专业程序的分支机构工作人员都是女性，并且偏向于老年人，而使用或不使用计算机的用户分布更均匀。

D. 研究组抽样

根据我们的建议，该公司将 14,733 名参与者中的每一个分配到通过组合为不同测试工具和机制管理的设置生成的 12 个不同用户组之一：

- 警告（3 种设置）：每个参与者在其模拟网络钓鱼电子邮件上收到三种可能设置之一：简单警告；详细警告；或无警告，作为控制设置。
- 训练（2 种设置）：每个通过执行危险操作而失败的模拟网络钓鱼攻击的参与者都可以重定向到培训页面；或未接受此类培训，作为控制设置。
- 报告反馈（2种设置）：在报告可疑电子邮件后，参与者始终可以收到报告结果作为反馈；或者，仅当他们报告合法电子邮件作为控制设置时，他们才能收到结果。

例如，组 1 在正确报告网络钓鱼后管理简单的警告、培训且没有反馈，而组 2 具有相同的配置，但接收复杂的警告，依此类推。每个参与者都是随机的

分配到 $3 \times 2 \times 2 = 12$ 组之一，因此它们的大小大致相同：从较小的 1,223 名参与者到较大的 1,231 名参与者。

E. 实验执行

从 2019 年 7 月到 2020 年 10 月，该公司向 14,733 名参与者中的每个人发送了 8 封不同的模拟网络钓鱼电子邮件。参与者在实验的前12个月（2019年7月至2020年7月）以随机顺序和随机时间间隔[16]收到前6封电子邮件。他们从 2020 年 8 月到 2020 年 10 月收到了最后两封网络钓鱼电子邮件²，同样以随机顺序和随机时间间隔。参与者没有特别意识到我们的研究，不改变他们的行为[47]，[48]；但是，他们知道公司可能偶尔会向其员工发送网络钓鱼练习。

这 8 种难度不同的电子邮件活动旨在模拟针对整个组织的广泛网络钓鱼活动，而不是复杂的、单独制作的鱼叉式网络钓鱼。每封不同的电子邮件都代表一个典型的网络钓鱼场景，例如提示检查其公司凭据，将其电子邮件帐户迁移到新系统，或将包裹递送单作为附件，并使用不同的触发器，例如权威感或紧迫感或利用人们的好奇心[27]。五封电子邮件包含指向网络钓鱼网站的链接，而三封电子邮件则带有附件。我们在附录B中提供了所选电子邮件的英文版本。

在实验过程中，我们的合作伙伴公司记录了与模拟电子邮件的以下交互：

- 点击电子邮件中包含的链接；
- **危险操作**：通过向链接的网站提交凭据或在附加文档上启用宏来进一步陷入网络钓鱼。

该公司还记录了参与者对可疑电子邮件的报告。对于每封报告的电子邮件，他们都会存储它是否是我们模拟的网络钓鱼电子邮件之一，反网络钓鱼设备的二次分析结果，以及IT部门是否有任何员工查看了此类结果并确认或推翻了其裁决。在过去 5 个月内

²最后一封电子邮件应该是三封；但是，模拟的CEO欺诈网络钓鱼攻击[46]在公司内部造成了不必要的混乱，并且此特定的模拟网络钓鱼电子邮件被取消。

在实验中，该公司还记录了在报告日期前后的 20 天内有多少入站电子邮件与报告的电子邮件相似。

在实验结束时，我们对 1000 名随机选择的参与者进行了问卷调查，其中包含 27 个封闭式问题。接受回复的参与者被告知，他们的回复是匿名记录的，并且不会进一步与他们的雇主分享，以鼓励诚实的回答。第一个问题询问参与者有关网络钓鱼和其他电子邮件威胁的知识、有关电子邮件警告的问题、报告网络钓鱼的按钮、上下文培训，以及他们是否记得上当过网络钓鱼。我们在附录 C 中报告了从问卷中选择的问题。我们收到了 151 份完整的答案。

F. 道德与安全

研究批准。本研究由我们的合作伙伴公司的 CISO 发起并批准。在研究期间，我们从未访问过任何 PII，并且仅在公司收集后才允许访问匿名数据（参见第 III-A 节）。由于根据我们机构的指南，匿名数据的分析不需要 IRB 批准，因此我们没有提交正式请求。

参与者的风险。我们的合作伙伴公司会告知其员工他们的网络钓鱼意识活动，其中包括网络钓鱼练习。因此，我们的研究参与者普遍意识到公司可能会向他们发送模拟钓鱼邮件。该公司没有具体告知参与者有关作为本研究的一部分发送的模拟网络钓鱼电子邮件（即，没有知情同意或汇报）。不在嵌入式培训组的参与者没有被特别告知模拟网络钓鱼电子邮件，而嵌入式培训组的参与者被告知，如果他们上当，该电子邮件是网络钓鱼邮件。

作为该实验的一部分，我们的参与者受到的风险最小：他们没有比他们在日常生活中遇到的风险更大 [49]，因为他们经常收到真正的网络钓鱼和其他恶意电子邮件。像我们在这里进行的实验这样的实验可能会产生负面影响，例如浪费员工的时间或造成对公司的不信任 [49]。该实验是公司现有培训计划的一部分；鉴于这种情况，我们认为我们实验的科学影响值得这些潜在的负面影响

数据收集和保护。在研究期间，我们的合作伙伴公司收集了有关点击和危险行为的数据，以及参与者报告为网络钓鱼的电子邮件数据。如果研究参与者在模拟网络钓鱼网页上输入密码，我们的合作伙伴公司不会记录输入的凭据，也不会检查它们是否正确。在我们合作伙伴公司的 IT 安全部门工作的少数员工可以访问收集到的数据集，并通过双因素身份验证进行保护。

收集的数据集以匿名格式提供给我们，因此只有性别、年龄和级别等属性

保留了计算机使用。我们的合作伙伴公司在内部使用该数据集来评估其对网络钓鱼威胁的总体暴露程度，并向我们保证该数据集不会用于任何其他目的，例如员工绩效评估。被举报的邮件不携带任何 PII：每份报告都记录了被举报的邮件是否是模拟邮件，以及反钓鱼设备的评分和判定。这些信息都不能链接到邮件的原始发件人、主题或内容。

G. 实验统计

总体而言，研究参与者点击了 117,864 个模拟网络钓鱼中的 6,680 个 (5.67%)。在这 15 个月中，4,729/14,733 名参与者 (32.10%) 至少点击了一次网络钓鱼。危险行为的趋势相似，数字略低：参与者因 4,885 封模拟钓鱼邮件而倒下（占发送邮件总数的 4.14%，占所有点击的模拟钓鱼邮件的 73.13%），以及 3,747/14,733 名参与者 (25.43%) 用户至少做了一项危险操作。

有 4,260 名研究参与者至少报告了一封电子邮件。参与者总共报告了 14,401 封电子邮件，其中 11,035 封是我们的模拟电子邮件。报告网络钓鱼的按钮也被部署到 6300 名未参与实验但可以报告网络钓鱼的员工：其中 1,543 人报告了至少一封可疑电子邮件，他们报告了 4,075 封电子邮件。因此，我们在 15 个月内收到的报告电子邮件总数为 18,476 封。

四、哪些员工容易上当网络钓鱼？

在本节中，我们分析实验数据以了解哪些员工最有可能陷入网络钓鱼 (RQ1)。回想一下第 III 节，我们根据频繁、不频繁和专业使用对参与者进行分类。我们根据人口统计数据和工作类别计算点击链接和危险操作的数量（见图 6）。对于我们接下来的分析，我们定义以下三个假设：

- H1: 员工在工作中使用计算机与上当网络钓鱼有关。
- H2: 员工的年龄与网络钓鱼有关。
- H3: 员工的性别与网络钓鱼有关。为了分析测量的数字，我们拟合了一个具有 III 型平方和的线性模型来单独分析人口统计属性，并捕获交互作用

他们之中。这种统计工具使我们能够衡量自变量（即人口统计属性）对因变量的影响：点击链接和危险行为的数量，我们将其用作网络钓鱼敏感性的代理。我们将模型与人口统计属性的所有组合相匹配，并排除不重要的因素，直到我们获得具有以下结果的最终模型。结果支持 H1：与计算机使用的相关性。从图 6a 可以看出，工作类型涉及专业计算机使用的参与者（例如，主要使用单一专用程序的分支机构工作人员）点击了更多钓鱼邮件中的链接并执行了更多危险操作

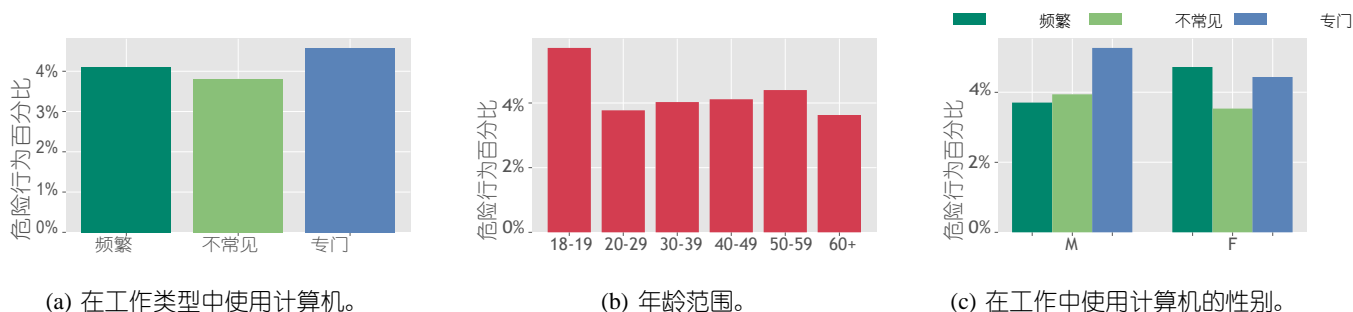


图 6：在发送的所有网络钓鱼电子邮件中执行的危险操作的百分比，除以不同的人口统计数据。频繁使用计算机但在非常专业的环境中，以及年轻人和老年人都会影响对网络钓鱼的敏感性。

比其他可比组（频繁和不频繁使用）的参与者。我们的拟合模型显示计算机使用很重要（点击： $F(2, 14710) = 11.01, p < 0.001$ ；危险行为： $F(2, 14710) = 9.45, p < 0.001$ ）和 Tukey HSD 事后测试证实 Specialized use 和其他两组之间的区别对于点击和危险操作都很重要。但是，频繁使用和不经常使用之间的区别并不显著。因此，虽然我们支持之前显示网络钓鱼敏感性与技术知识之间关系的工作 [11]，但最后的观察结果需要谨慎，因为这种关系似乎更加微妙。虽然通常会利用

计算机在参与者工作中的使用作为技术技能的代表，我们的结果表明计算机使用的类型和对工作的期望也可能影响网络钓鱼的敏感性。例如，我们合作伙伴组织中的专业使用参与者可能会比不经常使用的参与者更多地与电子邮件进行交互，因此他们可能对传入的电子邮件更加怀疑。

结果支持 H2：与年龄相关。最年轻的员工点击次数更多，执行的危险动作也更多。我们的模型证实了年龄和网络钓鱼敏感性之间的相互作用（点击率 $F(5, 14710) = 4.70, p < 0.001$ ；危险行动率 $F(5, 14710) = 3.84, p < 0.001$ ）。我们运行了 Tukey HSD 测试来分析哪些群体风险更高，并确认图 6b 显示的内容：18-19 岁的参与者比任何其他年龄组更有可能点击网络钓鱼链接并执行危险操作；50-59 岁年龄段的参与者也比 20-29 岁和 60 岁以上表现最好的参与者面临更高的风险。这一结果支持了之前的文献 [40]、[41]、[34]。

结果不支持 H3：与性别相关。我们参与者的电脑使用 w.r.t. 他们的性别不统一（回想一下图 5c）。因此，通过使用计算机进一步划分两性的交互显示，同一性别之间存在很大差异，如图 6c 所示，并由我们的模型证实：性别和计算机使用的组合是显著的（点击率 $F(2, 14710) = 13.06, p < 0.001$ ），但性别本身不是（点击率 $F(2, 14710) = 0.23, p = 0.63$ ）。事实上，图 6c 向我们展示了虽然经常使用女性

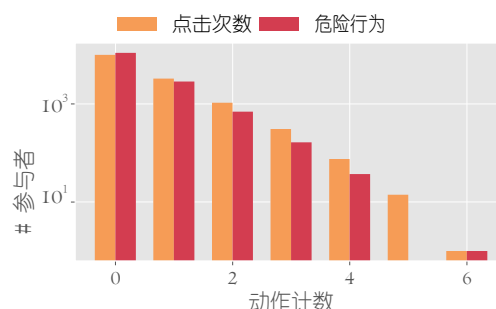


图 7：参与者点击或执行危险操作的模拟网络钓鱼电子邮件的数量（最多 8 个；缺失的条表示零个参与者）。

比经常使用的男性更容易受到影响，专门使用的男性比女性更容易受到影响。因此，通过考虑工作类型的不平衡，可以更好地解释参与者的网络钓鱼敏感性，这与之前的一些研究相矛盾 [36]，[30]。

五、随着时间的推移网络钓鱼漏洞

在本节中，我们利用为期 15 个月的研究来分析组织的网络钓鱼敏感性如何随时间演变 (RQ2)。为此，我们分析了随着时间的推移点击和危险行为的趋势：参与者与网络钓鱼交互了多少次（最多 8 次），以及随着时间的推移有多少参与者最终至少这样做了一次。重复的答题器。我们在图 7 中报告了有多少参与者在给定次数的模拟中单击或执行危险操作的直方图。共有 1,448 名 (30.62%) 参与者点击了两个或更多网络钓鱼，896 名 (23.91%) 对两个或更多网络钓鱼执行了危险操作——一名参与者甚至在 8 次模拟中落入 6 次。因此，我们观察到会有少数员工多次点击或陷入网络钓鱼电子邮件，支持之前的初步研究 [42]。类似于点击和危险动作的原始数量，我们观察到年龄组和点击之间的相关性 (Welch 校正方差分析

$F(5, 4199) = 5.72, p < 0.001$) 或对多于一封模拟钓鱼邮件执行危险操作 ($F(5, 4186) = 3.66, p = 0.002$)。在这两种情况下, Tukey HSD 测试表明, 年龄在 18-19 岁的年轻参与者群体脱颖而出, 因为他们更有可能多次点击。

如果不断暴露, 许多员工最终会陷入网络钓鱼。在我们的实验中, 14,733 名参与者中有 4,729 名 (32.10%) 单击了我们模拟的网络钓鱼电子邮件中的至少一个链接或附件。类似的高数字适用于危险行为: 14,733 人中有 3,747 人 (25.43%) 至少进行过一次。这些结果表明当暴露于网络钓鱼电子邮件足够长的时间时, 整个员工群中的很大一部分将容易受到网络钓鱼的攻击。我们是第一个大规模展示这种结果的人。

VI. 警告和培训的有效性

在本节中, 我们分析了从我们的实验中收集的数据, 以回答与网络钓鱼警告和培训的有效性相关的 RQ3。

A. 警告的有效性

回想一下第三部分, 我们试验了两种类型的警告 (简短的和详细的), 以及一个没有看到任何警告的对照组。为了分析这两种警告类型的有效性, 我们使用以下假设:

- H4: 在可疑电子邮件之上添加警告有助于用户检测网络钓鱼。

- H5: 详细警告比简短警告更有效。结果支持 H4: 警告帮助用户。图 8 显示了不同警告配置的点击率和危险动作率。我们观察到, 这两种类型的警告都极大地帮助参与者避免点击我们模拟的网络钓鱼电子邮件中的链接, 并且不会因执行危险操作而上当网络钓鱼。考虑到点击率, 没有警告的组点击了 3,964 次, 相比之下, 短点击为 1,427 次, 长警告点击为 1,289 次 (Welch 校正方差分析 $F(2, 7485) = 564.71, p < 0.001$)。危险动作率相似: 2,994 次危险动作没有警告, 分别为 998 次和 893 次危险动作 ($F(2, 7461) = 392.58, p < 0.001$)。图 9 显示了有多少参与者点击了给定次数的模拟网络钓鱼的直方图。我们观察到收到任何警告与不点击或多次执行危险操作之间存在很强的相关性 (点击: $F(2, 9287) = 358.88, p < 0.001$, 危险操作: $F(2, 9194) = 239.68, p < 0.001$)。我们的结果支持这种广泛的行业实践 [43]。

结果不支持 H5: 详细警告并不比简短警告更有效。为了检查简短警告和详细警告之间是否存在任何差异, 我们在所有组之间进行了 Tukey HSD 测试并观察到, 虽然这两种警告都与较低的总点击次数和危险操作相关, 但简短警告和详细警告之间没有显著差异。因此, 我们向用户提供额外信息的方式 (通过模仿当前的行业惯例,

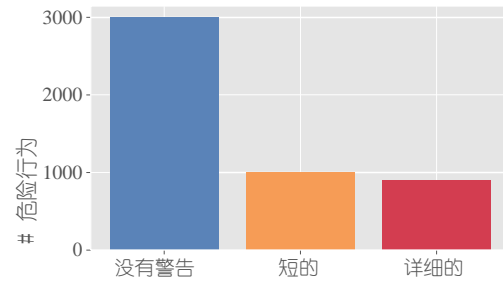
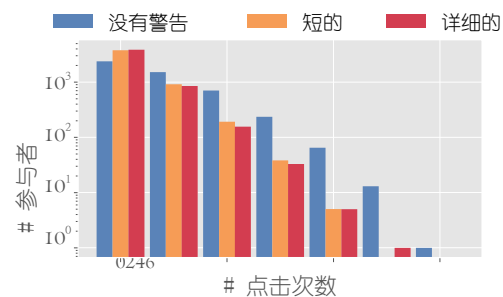


图 8: 管理警告的危险行为。两种警告类型都对参与者有很大帮助。



训练组中的那些人要么从未看过训练页面，要么在执行了他们唯一的危险动作后才看到它。然而，如果我们关注失败两次或更多次的参与者（因此，关注训练组中在显示培训页面后再次因网络钓鱼而失败的参与者），我们会看到参与者的分布更偏向右侧训练组。事实上，点击两封或更多钓鱼邮件的参与者中有 647 人没有接受过培训，801 人接受过培训。这表明所提供的培训页面与点击网络钓鱼电子邮件甚至不止一次执行危险操作之间存在很强的相关性（Welch corrected ANOVA for clicking: $F(1, 14592) = 18.37$, $p < 0.001$ ；危险行为: $F(1, 14279) = 33.80$, $p < 0.001$ ）。

这个可能令人惊讶的结果需要仔细解释。我们的实验表明，这种提供自愿培训的特殊方式行不通。相反，这种训练方法可能会导致意想不到的负面影响，例如增加对网络钓鱼的敏感性。这一发现意义重大，因为被测试的网络钓鱼培训交付方法是一种常见的行业惯例 [19]、[17]、[20]、[18]，并且培训材料（参见第 III 节）是由一家专业公司根据参考以前工作中的已知指南和最佳实践 [31]、[34]、[45]。研究其他可能的方式来提供情境培训（例如，强制与提供的培训材料进行互动的方式）是否会更好地工作将很有趣。我们的研究没有测试强制培训的有效性。为了深入了解为什么转发到培训页面的参与者对网络钓鱼的敏感性增加，我们分析了实验后问卷的答案。问卷回复中出现的一种可能的解释是与部署的培训方法相关的错误安全感：在记得看过培训页面的受访者中，43% 选择了选项“看到培训网页让我感到安全”，40% 的人选择了“公司正在保护我免受不良电子邮件的侵害”选项。探索这是否是由于对培训页面的误解（即参与者是否认为他们受到保护免受真正的攻击），或者这是否是因为对组织的 IT 措施过于自信仍然是未来工作的一个悬而未决的问题一般而言，正如过去在类似环境中观察到的那样 [39]、[50]、[51]。

最终，我们的结果表明，组织在使用这种培训方法时需要小心，并注意可能出现的意外副作用。

VII. 员工可以帮助组织吗？

我们现在分析从我们的实验中收集的数据来回答 RQ4，与组织中的众包网络钓鱼检测相关。这种方法需要满足以下要求才能有用：

- **可持续性**：员工需要在很长一段时间内不断报告可疑电子邮件。
- **有效性**：员工的报告需要足够准确和及时，以便组织可以足够快地停止新的活动。

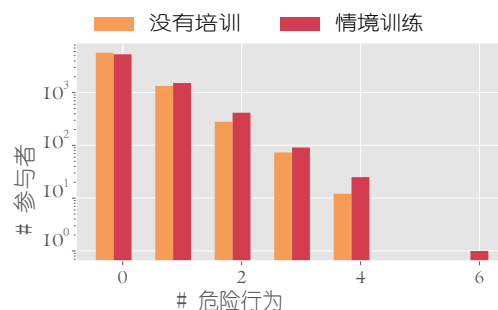


图 10：参与者通过管理的上下文培训对其执行危险操作的不同模拟网络钓鱼电子邮件的数量。缺失的条表示 0。

- **实用性**：处理所有报告的电子邮件的操作工作量需要保持在可接受的范围内。

A. 报告员工的可持续性

回想一下第三部分，我们决定尝试两种类型的反馈：(i) 总是收到他们报告的结果；或 (ii) 仅在（错误地）报告合法（非网络钓鱼）电子邮件时收到结果。为了调查报告的可持续性，我们检查了员工报告可疑电子邮件的活动如何随着时间的推移而演变，以及经过测试的鼓励报告的方法是否有效。我们使用以下两个假设来检验这些问题：

- H7：随着时间的推移，员工保持稳定的报告率
- H8：对报告提供反馈鼓励将来再次报告

我们计算所有报告并分析它们随时间变化的比率，并比较在收到两种不同类型的反馈后报告更多电子邮件的参与者数量。

结果支持 H7：员工继续报告电子邮件。图 11 显示了整个实验期间报告的可疑电子邮件数量。³我们观察到报告的稳定收入并没有放缓（甚至在 2020 年 8 月发布两封新的网络钓鱼电子邮件时有所增加），因为每天报告的模拟电子邮件的常数部分显示。我们进一步分析了图 12 中显示的报告频率分布。虽然 90% 的报告可疑电子邮件的员工报告了 6 次或更少，但仍有不可忽略的非常活跃的用户。我们得出的结论是，在我们为期 15 个月的实验中，没有出现明显的“报告疲劳”，这表明，如果报告变得容易，员工可以在很长一段时间内积极地继续报告可疑电子邮件。

此外，我们通过拟合具有 III 型平方和的线性模型来检查是否有任何人口统计影响报告的数量。与网络钓鱼易感性类似，年龄和计算机在工作中的使用以及性别和计算机在工作中的使用的组合很重要（年龄和计算机

³这些数字包括收到按钮的所有 21,000 名员工。

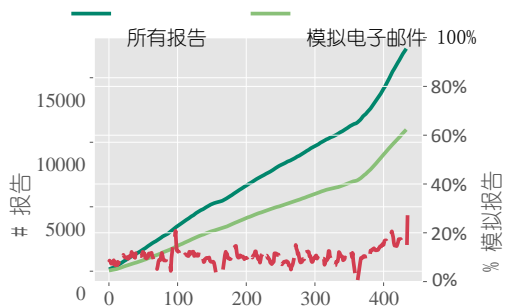


图 11: 随时间推移累积的电子邮件报告。红色虚线显示每天报告的模拟电子邮件的百分比。

使用 $F(10, 14710) = 6.49, p < 0.001$ ；性别和计算机使用 $F(2, 14710) = 11.35, p < 0.001$ 。考虑到计算机使用的分布不均，我们认为这是主要的影响因素。事实上，我们发现经常使用计算机的参与者报告了他们收到的所有模拟电子邮件中非常令人鼓舞的 22%，而不经常使用的参与者报告的比例仅为 10.20%，专门使用的参与者报告为 7.60%。我们的结论是，非常直观地，具有最佳计算机技能的员工也是最活跃的报告者。然而，有趣的是，不经常使用的参与者更多比专业的活跃。

结果支持 H8: 正反馈鼓励员工报告更多。我们发现管理反馈类型和报告的电子邮件数量之间存在显著的相互作用。为了衡量这一点，我们首先排除了所有从未报告过任何电子邮件的参与者。然后我们计算实际收到正面反馈的组和只收到虚假报告反馈的组报告了多少封电子邮件。前者（2,046 名参与者）由总是收到反馈并报告至少一封恶意或模拟电子邮件（因此收到积极反馈）的小组参与者组成。后者（2,201 名参与者）由未收到积极反馈的组中的人员以及可以收到积极反馈但仅报告合法电子邮件（因此从未收到积极反馈）的组中的人员组成。我们运行了 Welch 校正方差分析 ($F(1, 3224) = 31.62, p < 0.001$) 确认看到积极反馈的参与者更有可能报告更多电子邮件。

B. 众包网络钓鱼检测的有效性

为了从整体上分析众包网络钓鱼检测机制的有效性，我们分析了报告的及时性和准确性。除了足够高的报告活动外，组织还需要快速和足够准确的报告，以便能够检测和阻止通常短暂的新型网络钓鱼活动 [14]。

我们注意到，由于我们没有同时发送数千份相同的网络钓鱼电子邮件，因此我们无法直接衡量此类大规模网络钓鱼活动的报告速度

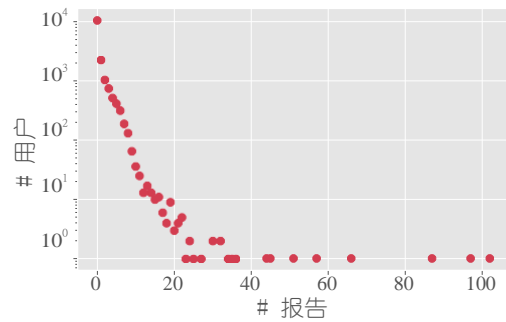


图 12: 每个用户的报告数量分布。

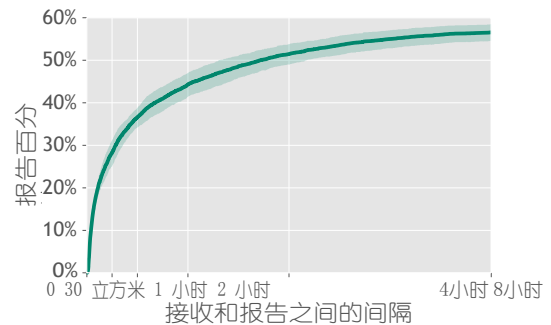


图 13: 报告的模拟电子邮件的平均每个用户组累积分布函数作为电子邮件接收和报告之间的间隔的函数，标准差作为彩色区域。

并因此被检测到。相反，我们测量了参与者报告我们随机定时的模拟网络钓鱼电子邮件的速度。基于这些数字，我们可以估计检测到真正的大规模活动的速度和准确度。

及时性。我们在图 13 中显示了在发送后不久到达的模拟电子邮件报告的百分比。我们可以观察到整个员工群的反应时间很快：平均约 10% 的报告在 5 分钟内到达；15 以内20%；30 分钟内减少 30% 到 40%。我们观察到不同模拟电子邮件活动的报告时间之间没有显著差异：尽管所有报告的总数不同（从报告最多的 2,538 份报告到报告最少的 832 份报告），所有报告的数量始终相似在前 30 分钟内报告传入。

将这些数字应用于一家拥有 1,000 名员工的假设公司，其中 100 名员工成为网络钓鱼活动的目标，我们将收到 8 到 25 份员工电子邮件报告——其中一份很可能在 5 分钟内发生，而更多30 分钟内。

准确性。报告的平均准确率很好：68%，如果垃圾邮件也应报告，则最高可达 79%。⁴我们观察到

⁴作为基本事实，我们在这里考虑二级反网络钓鱼设备的结果，并由公司的 IT 部门更正和验证。

员工报告准确度的分布很广：虽然超过 60% 的报告员工准确度达到 80% 或更高，但仍有相当一部分员工总是错误的（如果应报告垃圾邮件，则为 13%；22 % 否则）——然而，它主要包括仅报告一封电子邮件的员工。报告 6 封或更多电子邮件的非常活跃的前 10% 的员工（回忆第 VII-A 节）的准确性比考虑所有员工高约 5%。我们进一步注意到，非常高的报告准确性并不重要。如果使用辅助反网络钓鱼设备对报告进行分类，就像我们在实验中所做的那样，可以鼓励员工过于谨慎，并在有疑问时（不仅是在绝对确定时）报告电子邮件，因为该设备可以作为第一次检查在电子邮件中，并保持可接受的操作工作量，如下所述。

事件意识。此外，我们还分析了员工作为安全事件受害者的意识。我们首先注意到，在我们的模拟电子邮件上执行危险操作的参与者中有 6% 立即报告了该电子邮件，从而意识到他们是网络钓鱼攻击的受害者。⁵这些参与者中只有 3.7% 没有切换复选框报告按钮，允许员工报告他们是否访问了电子邮件中包含的链接，或打开了其附件。有趣的是，我们观察到一些参与者过于谨慎：13% 的模拟网络钓鱼电子邮件报告表示他们打开了链接或附件，尽管他们并没有这样做。

C. 组织的实用性

我们观察到，对报告进行分类的辅助设备使增加的工作量变得合理：在 15 个月的 7,191 封非模拟报告电子邮件中，只有 689 (9%) 的决定是由人类管理员做出的，并且实际上推翻了设备做出的决定只有 50 次（占处理案件总数的 7%）。此辅助设备的主要目标是过滤掉明确的良性电子邮件或垃圾邮件等轻微威胁的报告，其中包括我们收集的大部分报告：在 7,191 份不属于我们练习的电子邮件报告中，3,531 份是良性的，并且 2,371 份是垃圾邮件或不需要的时事通讯。因此，每天大约只有 1.5 封电子邮件需要 IT 部门手动处理——对于从超过 21,000 名用户收集报告的大型组织来说，这显然是可以接受的工作量。

D. 寻找真正的网络钓鱼活动

我们通过分析我们是否捕获了发送给公司员工的任何真实网络钓鱼活动（除了我们的模拟网络钓鱼电子邮件之外），进一步验证了我们的众包网络钓鱼检测方法。我们使用二级过滤器的判断和 IT 专家的人工检查来查找报告的网络钓鱼和其他恶意电子邮件。在过去的 5 年中，我们观察到 918 份关于真实网络钓鱼电子邮件的报告

⁵我们只对中了模拟网络钓鱼后未接受培训的参与者进行测量，因为他们必须自己了解发生了什么——培训材料明确说明这是模拟网络钓鱼攻击。

我们部署的几个月。借助电子邮件相似性技术，我们测量了有多少与报告的电子邮件相似的电子邮件传入，并发现了 252 起大规模网络钓鱼活动，其中包括 28,830 封电子邮件，以及 1,534 封带有恶意软件的电子邮件，我们的众包方法可以在短时间内从他们的开始。

VIII. 研究有效性

模拟电子邮件限制。回想一下，我们的 8 封电子邮件中有 3 封带有恶意附件，其中的危险操作是启用宏。虽然该公司可以通过对监控基础设施的网络调用来监控宏何时启用，但它无法知道参与者何时仅单击，即，在不启用宏的情况下简单地打开和关闭附件。因此，对于附件，我们通过将其设置为危险操作的次数来低估点击次数。

该公司没有记录打开模拟邮件的时间，因此我们不知道打开邮件到点击和危险操作的转化率。

出于数据保护的考虑，没有记录员工是否向模拟钓鱼网站提交了有效凭证。因此，我们记录的执行某些危险操作（例如提交凭证）的员工数量可能被高估了，因为我们无法过滤掉提交虚假凭证的员工。电子邮件警告限制。我们的合作伙伴公司在模拟的网络钓鱼电子邮件之上添加了警告，但没有在使用的内联过滤解决方案认为可疑但无论如何都会通过的电子邮件之上添加警告。这可能会导致一些参与者因我们的模拟网络钓鱼电子邮件而跌倒，随后将警告的存在与肯定可疑的电子邮件相关联，甚至更糟，与培训练习相关联。需要对这种有前途的警告添加到合法但看起来可疑的电子邮件之上进行进一步研究，以消除潜在的偏见。

活动成功率。如图 14 所示，不同的模拟网络钓鱼电子邮件活动具有不同的成功率。由于两个原因，这种差异不会影响我们对 RQ1-RQ4 的分析。首先，我们总是计算所有活动的点击总数或危险操作总数，并比较总数。其次，管理活动的顺序是随机分配给大组中的每个参与者的。适用于不同的公司。我们的合作伙伴公司在许多不同的领域开展业务，拥有多元化的员工队伍和庞大的规模。因此，我们相信我们的结果可以推广到各种类似规模（大型）的公司。目前尚不清楚我们的结果是否适用于拥有非常专业的 IT 员工的公司，例如软件工程公司，或者适用于非常小的组织。

IX. 相关工作

网络钓鱼和人口统计。年龄是网络钓鱼分析最多的因素之一，因为它在直觉上通常与技术技能相关。研究表明，非常年轻 [40]，

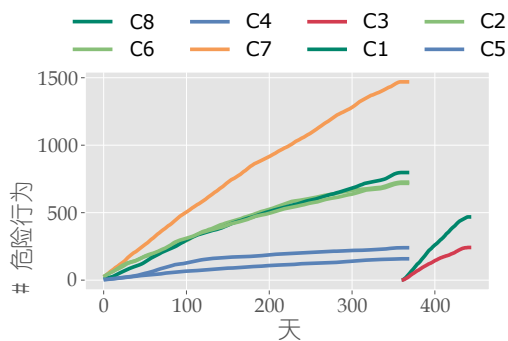


图 14：实验期间每个活动的危险动作累计数。

[41]、[34] 和老年人 [36]、[35]、[29] 更容易受到网络钓鱼的威胁。初步研究表明，年龄增长会增加对网络钓鱼的敏感性 [35]，但仅测试了两个极端（非常年轻和年长的人），而不是整个年龄段。此外，不同的年龄段容易受到不同类型的网络钓鱼电子邮件的影响 [15]、[36]。根据最近的一项文献调查 [11]，性别是一个更具分裂性的人口统计数据，但确实发现影响的研究表明女性更容易受到伤害 [36]，并且可以检测到更少的网络钓鱼企图 [30]。使用计算机的经验 [11]、之前网络钓鱼尝试的经验 [29] 以及在组织中的资历 [26] 也会对网络钓鱼免疫力产生积极影响。

在工作场所进行网络钓鱼。之前的一些研究表明，在组织的边界内，员工会感到更安全并且通常信任他们公司的措施，从而降低他们的注意力 [39]、[50]，并且存在极有可能被网络钓鱼的“重复点击者”[42]。其他研究发现，帮助员工预防网络钓鱼变得困难，因为他们努力遵守公司安全政策并且经常忽视它们 [52]，[53]。

网络钓鱼培训和警告。人们普遍认为培训应该是积极的，例如安全游戏 [54]。一种流行的机制是运行模拟网络钓鱼练习，几家公司采用了这种方法 [19]、[18]、[17]、[20]，并获得了有希望的研究结果 [32]、[33]、[34]，其中（可能没有意识到 [47]、[48]）随着时间的推移，员工会收到模拟的网络钓鱼电子邮件，最好是随机发送 [16]。这种做法通常与嵌入式培训相结合：立即将陷入网络钓鱼的员工重定向到一个专门的网页，解释他们刚刚陷入的模拟攻击并提供有关网络钓鱼的信息 [34]。

以前的研究表明，培训应该是连续的，因为知识保留的时间从几天 [33]、[45] 到最多几个月 [34]。然而，研究工作的外部有效性不明确，因为大多数工作使用的人口较少 [33]、[31]、[28]、[16]、[32]、[27]，时间较短 [16]、[33]，[27]，人口多样性很少 [31]，[28]，[27] 或仅测试角色扮演设置 [32]，[31]——最近的一项研究质疑这些结果是否会转移到

公司环境 [55]。此外，围绕嵌入式网络钓鱼训练 [19]、[18]、[17]、[20] 出现的商业生态系统在最近的协作报告 [2] 中声称由于训练的好处而有所改进，但没有报告实验结果在受控环境中 [56]。

网络钓鱼警告已在浏览器上下文中得到广泛研究（例如，[57]、[58]）。最近的一些作品 [37] 还评估了电子邮件客户端上显示的不同类型的警告。虽然过于频繁的警告容易让人习惯并

尽管随着时间的推移会失去一些有效性 [59]，但文献一致认为，精心安排的警告通常是有效的。众包网络钓鱼检测。一些公司已经提供了报告网络钓鱼电子邮件的工具，以使用跨多个客户的聚合信息快速检测新攻击 [19]，[24]。同一家公司报告说，随着时间的推移，用户在报告网络钓鱼尝试方面有所改进 [2]、[1]，但是，其他工作表明，由于流程缺乏透明度，用户不愿向 IT 报告网络钓鱼尝试 [60] 和系统缺乏快速响应 [39]。在我们开展工作之前，尚不清楚员工作为封闭场景中的众包机制，例如在内部管理报告的网络钓鱼的公司，是否能够在可接受的运营工作量下有效工作。最近的一些作品也提出了这个概念，但没有对其进行评估 [25]、[61]。

十、结论和未来的工作

由于我们的长期和大规模实验，在本文中，我们支持了几个先前的发现，例如警告的有效性和生态有效性的提高。此外，我们发现当今行业普遍部署的嵌入式网络钓鱼培训效果不佳，实际上可能会产生负面影响。在这方面，我们的结果与先前的文献和常见的行业惯例相矛盾。最后，我们是第一个通过实验证明众包网络钓鱼检测在单个组织中有效且实用的人。基于这些结果，我们鼓励组织采用警告等网络钓鱼预防工具，这些工具已经过广泛研究，并且现有文献绝大多数支持它们的有效性。我们呼吁谨慎部署嵌入式网络钓鱼练习和培训等方法，现有文献对其有效性的看法不太一致，我们的研究发现了潜在的负面影响。我们建议组织考虑将众包网络钓鱼检测作为一种新的补充方式来提高组织的整体网络钓鱼防御能力，因为它的有效性看起来很有希望并且操作工作量仍然很低。

我们的工作还确定了需要更多研究的主题。我们的研究表明，网络钓鱼练习和培训的有效性尚未得到充分衡量，并且提供嵌入式网络钓鱼培训的最有效方法是什么仍然未知。还需要进行更多研究，以更好地了解嵌入到员工正常工作环境中的网络钓鱼练习和培训的（心理）影响，以及这些影响如何影响员工未来处理真实网络钓鱼电子邮件的方式。

这项研究得到了苏黎世信息安全和隐私中心（ZISC）的部分支持。

参考文献

- [1] Verizon, “2012 年数据泄露调查报告”, <https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report>. pdf, 2020, [在线; 2021 年 3 月 20 日访问]。
- [2] —, “2019 数据 违反 调查 报 告”, <https://enterprise.verizon.com/resources/reports/2019/2019-数据泄露-调查-报告.pdf>, 2019, [在线;访问 20 2021 年 3 月]。
- [3] J. Hong, “网络钓鱼攻击的状态”, ACM 通讯, 第一卷。 55, 没有。 1, 第 74–81 页, 2012 年。
- [4] A. Oest, Y. Safei, A. Doupe, G.-J. Ahn, B. Wardman 和 G. Warner, “网络钓鱼者的内心深处: 通过网络钓鱼工具包分析了解反网络钓鱼生态系统”, 2018 年 APWG 电子犯罪研究 (eCrime) 研讨会。 IEEE, 2018 年, 第 1–12 页。
- [5] M. Cova, C. Kruegel 和 G. Vigna, “没有免费的网络钓鱼: 对“免费”和实时网络钓鱼工具包的 分析。” WOOT, 卷。 8, 第 1–8 页, 2008 年。
- [6] X. Han, N. Kheir 和 D. Balzarotti, “Phisheye: 沙盒网络钓鱼工具包的实时监控”, 2016 年 ACM SIGSAC 计算机和通信安全会议论文集, 2016 年, 第 1402–1413 页。
- [7] M. Bitaab, H. Cho, A. Oest, P. Zhang, Z. Sun, R. Pourmohamad, D. Kim, T. Bao, R. Wang, Y. Shoshitaishvili, A. Doupe 和 G.-J. Ahn, “诈骗大流行: 攻击者如何通过网络钓鱼利用公众的恐惧”, 电子犯罪研究电子犯罪研讨会, 2020 年。
- [8] M. Khonji, Y. Iraqi 和 A. Jones, “网络钓鱼检测: 一项文献调查”, IEEE Communications Surveys & Tutorials, vol. 15, 没有。 4, 第 2091–2121 页, 2013 年。
- [9] A. Aleroud 和 L. Zhou, “网络钓鱼环境、技术和对策: 调查”, 计算机与安全, 卷。 68, 第 160–196 页, 2017 年。
- [10] A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg 和 E. Almomani, “网络钓鱼电子邮件过滤技术调查”, IEEE 通信调查和教程, 卷。 15, 没有。 4, 第 2070–2090 页, 2013 年。
- [11] D. Jampen, G. Gür, T. Sutter 和 B. Tellenbach, “不要点击: 进行有效的反网络钓鱼培训。比较文献综述”, 以人为中心的计算和信息科学, 卷。 10, 没有。 1, 第 1–41 页, 2020 年。
- [12] I. Fette, N. Sadeh 和 A. Tomasic, “学习检测网络钓鱼电子邮件”, 第 16 届万维网国际会议论文集, 2007 年, 第 649–656 页。
- [13] G. Xiang, J. Hong, C. P. Rose 和 L. Cranor, “Cantina+ 用于检测网络钓鱼网站的功能丰富的机器学习框架”, ACM 信息和系统安全交易 (TISSEC), 卷。 14, 没有。 2, 第 1–28 页, 2011 年。
- [14] A. Oest, P. Zhang, B. Wardman, E. Nunes, J. Burgis, A. Zand, K. Thomas, A. Doupe 和 G.-J. Ahn, “日出到日落: 大规模分析网络钓鱼攻击的端到端生命周期和有效性”, 第 29 届 USENIX 安全研讨会 (USENIX 安全 20), 2020 年, 第 361–377 页。
- [15] J. Wang, T. Herath, R. Chen, A. Vishwanath 和 H. R. Rao, “研究文章网络钓鱼敏感性: 针对目标鱼叉式网络钓鱼电子邮件处理的调查”, IEEE 专业交流交易, 卷。 55, 没有。 4, 第 345–362 页, 2012 年。
- [16] R. Wash 和 M. M. Cooper, “谁提供网络钓鱼培训? 事实、故事和像我这样的人”, 载于 2018 年 chi 计算系统人为因素会议论文集, 2018 年, 第 1–12 页。
- [17] Proofpoint, “Proofpoint 安全意识培训”, <https://www.proofpoint.com/us/products/security-awareness-training>, 2021, [在线; 2021 年 3 月 20 日访问]。
- [18] Cofense, “Cofense 网络钓鱼解决方案和产品”, <https://cofense.com/产品概览/>, 2021, [在线; 2021 年 3 月 20 日访问]。
- [19] Rapid7, “网络钓鱼意识培训”, <https://www.rapid7.com/解决方案/网络钓鱼意识培训/>, 2021, [在线; 2021 年 3 月 20 日访问]。
- [20] KnowBe4, “网络钓鱼”, <https://www.knowbe4.com/phishing>, 2021, [在线; 2021 年 3 月 20 日访问]。
- [21] PhishTank, “加入打击网络钓鱼的斗争”, <http://phishtank.org/>, 2021, [在线; 2021 年 3 月 20 日访问]。
- [22] OpenPhish, “网络钓鱼情报”, <https://openphish.com/>, 2021, [在线; 2021 年 3 月 20 日访问]。
- [23] T. Moore 和 R. Clayton, “评估人群评估网络钓鱼网站的智慧”, 国际金融密码学和数据安全会议。斯普林格, 2008 年, 第 16–30 页。
- [24] 证明点, “介绍 网络钓鱼警报, Woms 一键式电子邮件报告按钮,” <https://www.proofpoint.com/us/security-awareness/post/介绍-phishalarm-wombats-一键式电子邮件报告按钮>, 2015, [在线; 2021 年 3 月 20 日访问]。
- [25] P. Burda, L. Allodi 和 N. Zannone, 在 2020 年 IEEE 欧洲安全和隐私研讨会 (EuroS&PW) 上, “不要忘记人类: 一种自动响应和遏制鱼叉式网络钓鱼攻击的众包方法”。 IEEE, 2020 年, 第 471–476 页。
- [26] P. Burda, T. Chotza, L. Allodi 和 N. Zannone, “在工业界和学术界测试定制网络钓鱼技术的有效性: 现场实验”, 第 15 届可用性、可靠性和安全性国际会议论文集, 2020 年, 第 1–10 页。
- [27] A. Burns, M. E. Johnson 和 D. D. Caputo, “桶中的鱼叉式网络钓鱼: 来自有针对性的网络钓鱼活动的见解”, 组织计算和电子商务杂志, 卷。 29, 没有。 1, 第 24–39 页, 2019 年。
- [28] A. Carella, M. Kotsoev 和 T. M. Truta, “安全意识培训对网络钓鱼点击率的影响”, 2017 年 IEEE 大数据国际会议 (Big Data)。 IEEE, 2017 年, 第 4458–4466 页。
- [29] B. E. Gavett, R. Zhao, S. E. John, C. A. Bussell, J. R. Roberts 和 C. Yue, “老年人和年轻人的网络钓鱼可疑性: 执行功能的作用”, PLoS one, 第一卷。 12, 没有。 2, 页。 e0171620, 2017。
- [30] C. Iuga, J. R. Nurse 和 A. Erola, “上钩: 影响网络钓鱼攻击敏感性的因素”, 以人为中心的计算和信息科学, 卷。 6, 没有。 1, 第 1–20 页, 2016 年。
- [31] P. Kumaraguru, Y. Rhee, S. Sheng, S. Hasan, A. Acquisti, L. F. Cranor 和 J. Hong, “让用户关注反网络钓鱼教育: 保留和转移的评估”, 载于反网络钓鱼工作组第二届年度电子犯罪研究人员峰会, 2007 年, 第 70–81 页。
- [32] P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong 和 E. Nunge, “Protecting people from phishing: the design and evaluation of an embedded training email system”, 载于 SIGCHI 计算系统人为因素会议论文集, 2007 年, 第 905–914 页。
- [33] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor 和 J. Hong, “反网络钓鱼培训真实世界评估的经验教训”, 2008 年电子犯罪研究人员峰会。 IEEE, 2008 年, 第 1–12 页。
- [34] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. A. Blair 和 T. Pham, “网络钓鱼学校: 反网络钓鱼培训的真正评估”, 第 5 届研讨会论文集可用的隐私和安全, 2009 年, 第 1–12 页。
- [35] T. Lin, D. E. Capecci, D. M. Ellis, H. A. Rocha, S. Dommaraju, D. S. Oliveira 和 N. C. Ebner, “对鱼叉式网络钓鱼电子邮件的敏感性: 互联网用户人口统计和电子邮件内容的影响”, ACM 人机交互交易 (TOCHI), 卷。 26, 没有。 5, 第 1–28 页, 2019 年。
- [36] D. Oliveira, H. Rocha, H. Yang, D. Ellis, S. Dommaraju, M. Muradoglu, D. Weir, A. Soliman, T. Lin 和 N. Ebner, “针对老年人和年轻人剖析鱼叉式网络钓鱼电子邮件: 关于影响力武器和生活领域在预测网络钓鱼易感性方面的相互作用”, 2017 年会议记录chi 计算系统人为因素会议, 2017 年, 第 6412–6424 页。
- [37] J. Petelka, Y. Zou 和 F. Schaub, “将警告放在链接所在的位置: 改进和评估电子邮件网络钓鱼警告”, 载于 2019 年 CHI 计算系统人为因素会议论文集, 2019 年, 第 1– 页15。
- [38] M. Volkamer, K. Renaud, B. Reinheimer 和 A. Kunz, “鱼雷的用户体验: 工具提示支持的网 络钓鱼电子邮件检测”, 计算机与安全, 卷。 71, 第 100–113 页, 2017 年。
- [39] E. J. Williams, J. Hinds 和 A. N. Joinson, “探索工作场所网络钓鱼的敏感性”, 《国际人机研究杂志》, 第 1 卷。 120, 第 1–13 页, 2018 年。
- [40] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor 和 J. Downs, “谁会上钩? 网络钓鱼 敏感性和干预有效性的入口统计分析”, SIGCHI 计算系统人为因素会议论文集, 2010 年, 第 373–382 页。
- [41] M. Blythe, H. Petrie 和 J. A. Clark, “F 代表假话: 关于我们如何陷入网络钓鱼的四项研究”, 载于 SIGCHI 计算系统人为因素会议论文集, 2011 年, 第 3469–3478 页。

- [42] M. Canham, M. Constantino, I. Hudson, S. M. Fiore, B. Caulkins 和 L. Reinerman-Jones, “重复答题器的持久之谜”, 第十五届可用隐私和安全研讨会 (SOUPS 2019)。USENIX 高级计算系统协会, 2019 年。
- [43] G. Workspace, “高级网络钓鱼和恶意软件防护”, <https://support.google.com/a/answer/9157861>, 2021, [在线:访问 20 2021 年 3 月]。
- [44] Gmail, “避免并报告网络钓鱼电子邮件”, <https://support.google.com/邮件/答案/8253>, 2021, [在线:2021 年 3 月 20 日访问]。
- [45] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor 和 J. Hong, “教约翰尼不要上当受骗”, ACM 互联网技术交易 (TOIT), 卷。10, 没有。2, 第 1-31 页, 2010 年。
- [46] S. Mansfield-Devine, “模仿游戏: 商业电子邮件妥协诈骗如何抢劫组织”, 计算机欺诈与安全, 卷。2016 年, 没有。11, 第 5-10 页, 2016 年。
- [47] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius 和 C. Jerram, “网络钓鱼研究的设计: 研究人员面临的挑战”, 计算机与安全, 卷。52, 第 194-206 页, 2015 年。
- [48] R. C. Dodge Jr., C. Carver 和 A. J. Ferguson, “提高用户安全意识的网络钓鱼”, 计算机与安全, 卷。26, 没有。1, 第 73-80 页, 2007 年。
- [49] P. Finn 和 M. Jakobsson, “设计道德网络钓鱼实验”, IEEE 技术与社会杂志, 卷。26, 没有。1, 第 46-58 页, 2007 年。
- [50] K. K. Greene, M. Steves, M. Theofanos 和 J. Kostick, “用户上下文: 网络钓鱼敏感性的解释变量”, Proc. 2018 年研讨会可用安全性, 2018 年。
- [51] D. Conway, R. Taib, M. Harris, K. Yu, S. Berkovsky 和 F. Chen, “银行员工信息安全和网络钓鱼体验的定性调查”, 第十三届可用隐私和安全研讨会 (SOUPS) 2017 年, 2017 年, 第 115-129 页。
- [52] H.-y. S. Tsai, M. Jiang, S. Alhabash, R. LaRose, N. J. Rifon 和 S. R. Cotten, “了解在线安全行为: 保护动机理论视角”, 计算机与安全, 卷。59, 第 138-150 页, 2016 年。
- [53] M. Siponen, M. A. Mahmood 和 S. Pahlila, “员工遵守信息安全政策: 一项探索性实地研究”, 信息与管理, 卷。51, 没有。2, 第 217-224 页, 2014 年。
- [54] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong 和 E. Nunge, “Anti-phishing phil: 一款教导人们不要上当的游戏的设计和评估”, 第 3 届可用隐私和安全研讨会论文集, 2007 年, 第 88-99 页。
- [55] D. D. Caputo, S. L. Pfleeger, J. D. Freeman 和 M. E. Johnson, “Going spear phishing: Exploring embedded training and awareness”, IEEE 安全与隐私, 卷。12, 没有。1, 第 28-38 页, 2013 年。
- [56] H. Siadati, S. Palka, A. Siegel 和 D. McCoy, “衡量嵌入式网络钓鱼练习的有效性”, 第 10 届 USENIX 网络安全实验和测试研讨会 (CSET 17), 2017 年。
- [57] S. Egelman, L. F. Cranor 和 J. Hong, “你已被警告: 网络浏览器网络钓鱼警告有效性的实证研究”, 载于 SIGCHI 计算系统人为因素会议论文集, 2008 年, 第 1065 页-1074 页。
- [58] D. Akhawe 和 A. P. Felt, “警告地带的爱丽丝: 浏览器安全警告有效性的规模实地研究”, 第 22 届 USENIX 安全研讨会 (USENIX 安全 13), 2013 年, 第 257-272 页。
- [59] A. Vance, B. Kirwan, D. Bjornn, J. Jenkins 和 B. B. Anderson, “对于警告的习惯是如何随着时间的推移发生的, 我们真正了解多少? 习惯和多态性警告的纵向 fMRI 研究”, 2017 年 CHI 计算系统人为因素会议论文集, 2017 年, 第 2215-2227 页。
- [60] Y. Kwak, S. Lee, A. Damiano 和 A. Vishwanath, “为什么用户不报告鱼叉式网络钓鱼电子邮件?” 远程信息处理和信息学, 卷。48 页 101343, 2020。
- [61] C. Nguyen, M. L. Jensen, A. Durcikova 和 R. T. Wright, “众包网络钓鱼警告系统的功能比较”, 信息系统杂志, 2021 年。

附录

我们在这里报告我们在实验中使用的材料: 模拟网络钓鱼电子邮件、参与者在执行危险操作时查看的嵌入式培训网页, 以及我们在研究结束时管理的问卷。

由于篇幅限制, 我们仅报告每种材料的样本: 一个为特定模拟电子邮件量身定制的嵌入式培训网页; 四封模拟网络钓鱼电子邮件, 以及让我们在本文中报告的一些见解的调查问卷问题。我们相信这个示例足以全面了解我们的设计。

A. 嵌入式培训网页

我们在图 15 中显示了当员工执行一封模拟网络钓鱼电子邮件的危险操作时显示的上下文培训网页。它包含量身定制的信息、有关宣传活动的解释, 并且选项卡还包含有关电子邮件威胁的信息和教学视频。

B. 模拟钓鱼邮件

图 16 显示了我们发送给参与者的四封模拟网络钓鱼电子邮件。报告的电子邮件要么旨在让参与者单击指向恶意网页的链接, 而恶意网页又旨在让参与者执行不安全的操作 (例如, 提交他们的凭据), 或者旨在让参与者下载附件, 例如, 提示启用宏的文档。每封电子邮件都使用不同的触发器来敦促参与者点击, 例如好奇心或对后果的恐惧。

C. 调查问卷

问卷包括 27 个封闭式问题, 例如是/否问题, 以及参与者可以选择多个答案的多项选择题。每个问题都提供不知道或不记得等答案, 也可以让受访者不作答。我们可以将问题分为五个主要类别:

- 熟悉计算机和电子邮件安全威胁。
- 电子邮件警告。
- 在电子邮件客户端中报告网络钓鱼的按钮。
- 记住可疑的电子邮件和安全事件。
- 情境培训网页。

关于电子邮件警告、报告按钮和上下文培训网页的问题组之前是对该工具的回忆, 例如, 我们在其问题之前显示了培训网页的屏幕截图。

有关已部署工具 (电子邮件警告、报告按钮、上下文培训网页) 的问题是在向受访者回忆之前, 例如, 我们在询问相关问题之前立即显示了培训网页的屏幕截图。他们询问受访者是否记得在过去 12 个月内注意到并使用过该工具, 以及他们对该工具的看法。

我们在下面报告有关培训页面的问题作为样本。


- Q22: 您还记得在过去的 12 个月里看过这个培训页面吗?
 - 是的; 不; 我不知道
- Q23: 您看到培训页面时的感受如何?
 - 尴尬的。我明白我犯了一个错误。

- 担心的。我意识到我已经危及了我自己和我的 com 在线安全。
 - 安全的。我觉得该组织在网上保护我。
 - 不感兴趣。看到培训页面并没有引发任何情绪反应。
 - 我不记得了。
- Q24: 您估计您在培训页面上花费了多少时间？
 - 一分多钟。我仔细阅读了整页。
 - 不到一分钟。我简要浏览了提供的信息。
 - 几秒钟。我打开了页面，但没有阅读其内容。
 - 我不记得了。
- Q25: 您觉得培训页面的内容可信吗？
 - 是的。我认为它来自组织的 IT 部门等合法来源。
 - 不，培训页面在我看来很可疑（可能是骗局）。
 - 我不记得了。
- Q26: 您觉得培训页面的内容有用吗？
 - 是的。我发现它很好地提醒了恶意电子邮件的威胁。
 - 否。所提供的信息对我没有帮助。
 - 没有把握。
- Q27: 访问培训页面后，您对可疑邮件的态度有变化吗？
 - 是的。我了解了更多有关如何检查可疑电子邮件的信息。
 - 是的。我意识到可疑电子邮件可能是公司培训活动的一部分。
 - 是的。我觉得该组织正在保护我免受不良电子邮件的侵害。
 - 不，我已经知道网页上的信息了。
 - 否。页面内容不清晰或信息不详。
 - 不记得了。

Company Logo

Privacy PolicyContact

En



Phishing

Identify dangerous e-mails quickly and reliably

You've just opened an Excel file named "Management levels 2019" and enabled the macros included in the document by clicking "Enable editing" and "Activate content" in the status bar. When you enabled editing, your computer could have been infected with malware (malicious software) in the worst-case scenario.

The e-mail appeared to originate from within the company and prompted you to open an attachment claiming to be a new management list following internal reorganization. You were prompted to activate the macros in the attached document. You did as you were asked without noticing the alarm signals.

You could have seen through this particular "management list" attack. To begin with, the sender looked suspicious and was indeed fake (██████████). The fact that such sensitive information was sent by e-mail, without encryption and using an incorrect address should have led you to doubt its authenticity. When you were then asked to activate the macros, you should definitely have become suspicious.

Do not open any e-mail attachments if you are not sure what they contain!

Note: This attack was part of a ██████████ awareness campaign. No data was transferred and no malware was installed.

Tips

Information

Video

Preventing the attack

Never enable active content, such as the Word macros in this case, if you are not sure that the document comes from a reliable source. In this attack, just opening the Word file would not have caused any damage.

Be wary of all e-mails that arrive in your inbox:

- How does the sender know your address and why are you receiving the e-mail?
- Do you know the sender, does the content make sense and does the language sound like the sender?
- Are you being pressured into doing something or is something being offered to you in a pushy manner?

Strengthen your knowledge with our phishing exercise.

Start the exercise now

图 15：在对模拟网络钓鱼电子邮件进行危险操作后向员工显示的示例上下文培训网页。

Password change



Dear employee

Your password expires in two days!

Last password change: 6th January 2019

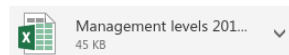
Please click [here](#) to change your password. You could lose access to important systems if you do not change your password.

This is an automated email.

Best regards
User Help Desk
[redacted]

(a) 提示更改组织密码的电子邮件。

Assignments to management levels



Download

To all department heads

As announced in the newsletter of April 5, 2021, as part of the reorganization, the management levels must be adjusted. Since some employees will be downgraded, this will probably lead to considerable discussions.

Attached is a list of all changes. You can filter by department, etc., simply activate the macros.

Many greetings
[redacted]

(b) 带有恶意宏附件的电子邮件。

Private data found - Your action is required!



Private Data

We found a lot of private data on user drives on the [redacted] infrastructure. This consumes too much disk space on servers and backup systems get overloaded.

IMPORTANT: Every file identified as private data will be deleted on April 19, 2021 at 3pm.

You may choose to view your private data and save it to a local drive if you wish. Please log on with your personal account to do so:

[http://\[redacted\]](http://[redacted])

Best regards
Service Desk

(c) 电子邮件提示检查公司驱动器中的文件。

IMPORTANT: Virus found



A virus was found on your computer:

K8Stba-trojan.vbs

The virus can not be deleted automatically due to insufficient user rights. Please start the scan manually to remove the virus.

[http://\[redacted\]](http://[redacted])

Best regards
Virusscan [redacted]

(d) 电子邮件提醒假定的恶意软件。

图 16: 模拟钓鱼邮件样本。我们报告了三封包含恶意网页链接的电子邮件（例如，要求提供凭据或提示下载），以及一封带有恶意附件的电子邮件。