眼见未必为实：电子邮件呈现对网络钓鱼易感性的作用

Sijie Zhuo Robert Biddle LucasBetts奥克兰大学 奥克兰大学 奥克兰大学Nalin Asanka Gamagedara Arachchilage YunSing Koh DanielleLottridge奥克兰大学 奥克兰大学 奥克兰大学

Giovanni Russello
奥克兰大学

arXiv:2304.00664v1 [cs.HC] 3 Apr 2023

摘要

网络钓鱼是最常见的社会工程攻击之一，目标既包括组织，也包括个人。了解电子邮件呈现如何影响用户对网络钓鱼攻击的反应至关重要。我们推测，设备和电子邮件呈现可能会发挥作用，尤其是链接的显示方式可能会影响用户的网络钓鱼易感性。我们与某大型组织的 IT 服务部门合作，在一次网络钓鱼培训演练中开展研究，探究设备和链接呈现方式的效应。研究结果表明，移动设备用户和电脑用户点击未隐藏链接的可能性相同；然而，与电脑用户相比，移动设备用户更可能点击伪装链接。这些发现表明，链接呈现方式对用户遭受网络钓鱼攻击的易感性有显著影响。

1 引言

近年来，网络钓鱼攻击已成为一种常见的网络攻击方法。即使存在网络钓鱼过滤器和各种对策，终端用户仍然是抵御此类攻击的最后一道防线。钓鱼邮件一旦突破所有技术防御措施并进入用户的收件箱，用户就必须自行作出正确判断。用户的网络钓鱼易感性会受到多种因素的影响，包括其教育水平、知识和经验。用户识别网络钓鱼邮件并作出明智决策的能力，也会受到其意识、情绪、信念以及阅读电子邮件时的投入程度。电子邮件的特征也会影响用户的决策 [14, 25, 43]。

人们已经开发出各种以人为本的解决方案，以帮助降低用户的网络钓鱼易感性。网络钓鱼培训是帮助人们了解网络钓鱼及其防范方法的最常见方式之一。人们开发了不同的培训工具来帮助用户识别网络钓鱼线索，包括基于文本的材料、视频培训 [37], 和游戏化培训解决方案 [32, 40]。毫无疑问，网络钓鱼培训能够降低用户对网络钓鱼的易感性 [5, 22],，但之后仍需定期开展后续培训，帮助他们维持一定水平的知识和意识 [18, 29]。在实际检查电子邮件时，用户通常会关注邮件内容，并默认将邮件视为合法邮件。只有当邮件中的某些线索令他们起疑时，用户才会改变想法，进而核实邮件的合法性 [39]。阅读电子邮件时，用户看到的是电子邮件客户端呈现出来的内容。我们推测，电子邮件客户端也会影响用户的网络钓鱼易感性。

用于查看电子邮件的设备可能会影响电子邮件的呈现方式以及用户与之互动的方式。计算机与智能手机之间一个常见的区别涉及链接。网络钓鱼者通常会操纵网络钓鱼链接，使其看起来值得信任；他们常将链接隐藏在按钮或文本后面，以降低用户看到可疑网址的可能性。在计算机上，用户只需将鼠标悬停在嵌入式链接上，就能轻松查看其落地页网址。然而，在智能手机上，用户必须点按并按住链接才能查看 URL。这种交互方式对用户而言不够熟悉，也更复杂，因此他们更可能直接点击网络钓鱼链接，从而迈出遭受网络钓鱼攻击的第一步。此外，智能手机的物理尺寸有限，导致电子邮件客户端在设计上做出了一些选择，例如隐藏电子邮件的某些详细信息（如发件人电子邮件地址和功能按钮），这可能会影响用户的判断。这些问题表明，用户在使用移动设备时可能更容易受到网络钓鱼攻击。

本文报告了一项与

版权归作者/所有者所有。允许免费为个人或课堂使用而制作本作品的全部或部分数字副本或纸质副本。*USENIX* 可用隐私与安全研讨会 *(SOUPS)*2022 年。2022 年 8 月 7 日至 9 日，美国马萨诸塞州波士顿。

某大型组织的 IT 服务部门在开展常规网络钓鱼培训演练期间进行的研究。该研究有两个主要目的：a）探究使用不同设备是否会影响用户点击网络钓鱼链接的倾向；b）研究网络钓鱼链接的视觉呈现是否会影响用户的点击行为，进而影响其网络钓鱼易感性。据我们所知，这是首篇大规模探讨这些主题的论文。

本文其余部分安排如下。在第 2 节中，我们介绍用户界面设计对用户行为的影响，以及现有电子邮件客户端在用户界面设计上的差异。在第 3 节中，我们说明研究方法论，以及如何将本研究纳入一项大规模网络钓鱼培训演练中开展。在第 4 节中，我们呈现研究结果及分析。随后，在第 5 节中，我们讨论研究发现并阐述其意义。最后，在第 6 节中，我们总结研究并展望未来方向。

2 相关工作

本节首先回顾研究文献中有关用户界面（UI）设计如何影响用户行为，以及电子邮件客户端的设计如何影响安全风险的证据。接着，我们讨论使用电脑和移动设备查收电子邮件时的差异，包括设备物理特征、交互方式和用户安全意识方面的差异。最后，我们概述以往关于网络钓鱼链接呈现对用户行为及网络钓鱼易感性影响的研究。

用户界面设计的影响力

许多研究表明，用户界面设计会影响用户的行为和选择 [2,4,23,30,31]。例如，Schnei- der 等人的研究 [31] 表明，用户界面设计师可以通过界面设计，在用户无意识的情况下助推他们做出某些选择。这些助推技术已广泛应用于商业网站，以吸引顾客。例如，将某个选项放在一个不吸引人的选项旁边，就能提高该选项的吸引力。

用户界面设计不仅会影响用户对选项的选择，还会影响他们对界面的看法和态度。Anwar 等人的研究 [4] 和 Rendell 等人的研究 [30]均表明，恰当选择图像、样式和配色方案能够提升用户与网站的互动。在在线购物网站的例子中，这将大大提高用户的购买意愿和再次访问意愿。此外，Stojmenovi´c 等人表明，视觉吸引力会影响用户的安全感知 [34]。用户更愿意信任设计精美的网站。

用户界面设计对用户的影响因人而异。Alves 等人的综述 [2] 表明，不同人格特征的用户对用户界面设计和美学有不同偏好，而这些差异会影响他们的任务绩效和信息寻求。研究发现，当界面设计与用户的人格特征相匹配时，用户往往效率更高 [20]。

用户界面设计的影响也适用于电子邮件客户端。通过调整电子邮件客户端中的用户界面元素，可以提升用户的安全意识和识别网络钓鱼邮件的能力。Anderson 的研究 [3] 探讨了钓鱼警告的设计，并指出用户在多次看到警告消息后会逐渐忽视它们。使用多态警告消息可以减缓这种习惯化的形成，从而帮助用户更长时间保持警惕。Petelka 等人 [27] 修改了电子邮件中的嵌入式链接，以帮助用户更多关注着陆页网址。在他们的研究中，最有效的方法是停用链接，并让用户在悬停框中与原始 URL 交互，从而访问着陆页。这些研究表明，通过改变电子邮件客户端的设计，可以提升用户安全表现。

计算机与移动设备

近年来，智能手机和平板电脑的普及使得人们越来越常用它们查看电子邮件 [9]。由于功能和特性不同，用户在不同设备上的交互方式也有所不同。例如，用户通过在智能手机屏幕上直接点击和滑动来进行交互。相比之下，使用电脑时，用户通过控制光标或敲击键盘按键来进行操作。此外，智能手机的屏幕比电脑小，因此一次只能显示有限的内容。设计移动设备电子邮件客户端时，设计人员需要谨慎选择要在小屏幕上显示的重要内容，同时支持交互和可用性的实用组件。这有时会导致某些细节被隐藏，例如发件人的完整电子邮件地址。从安全角度来看，隐藏电子邮件地址意味着用户少了一条可能帮助其识别恶意邮件的线索，从而更容易受到网络钓鱼攻击。

此外，智能手机的移动性意味着人们经常在较为随意的场合或户外环境中使用它们，而这些情境通常比使用电脑时有更多干扰。在充满干扰的环境中，用户表现可能会变差，因为用户必须额外消耗工作记忆来抑制干扰，才能专注于任务 [6]。查看电子邮件时，如果用户投入到电子邮件上的认知努力和注意力较少，就可能导致行为疏忽，降低识别网络钓鱼邮件的可能性，从而更容易成为网络钓鱼的受害者 [25,43]。

研究发现，用户使用不同设备时的心智状态有所不同。Breitinger 等人的研究 [11]显示，用户更担心攻击者通过物理访问入侵自己的智能手机，因此往往会

在使用手机时更关注密码安全和消息安全；而使用电脑时，则更关注安全检测和病毒扫描器，以保护数据和隐私。此外，与使用电脑相比，用户使用智能手机时的信息安全意识（ISA）往往较低。[8,11,13,21,24]许多用户会在电脑上安装安全软件，但只有约三分之一的用户认为在智能手机上安装此类软件是必要的。[11]。

大多数网络钓鱼相关培训主要面向电脑用户，包括培训材料和解决方案。因此，受过培训的用户通常知道使用电脑时该如何处理电子邮件，例如在点击链接前先将鼠标悬停在链接上。然而，许多用户会通过智能手机或平板电脑查看电子邮件。由于缺乏专门面向移动设备用户的培训，这些用户可能不太愿意或不太了解如何在不打开链接的情况下查看其 URL。

网络钓鱼链接的视觉呈现

目前已有一些关于钓鱼邮件视觉呈现的研究。例如，用户更容易信任视觉呈现专业的电子邮件，其中包括徽标、版权声明及其他看似真实的线索 [10, 41]。同一条钓鱼消息在不同客户端中的显示效果可能有所不同，因为电子邮件客户端呈现消息的方式各异。有些电子邮件客户端的设置会禁止下载图像，在这种情况下，用户便看不到徽标。由于屏幕尺寸不同，电子邮件在桌面设备上的电子邮件客户端中显示的效果可能与在移动设备上的电子邮件客户端中不同。

网络钓鱼链接是网络钓鱼邮件中最重要的组成部分之一。对攻击者而言，用户点击网络钓鱼链接可视为网络钓鱼攻击可能成功的指标；该链接还可能使攻击者识别出用户的电子邮件地址。网络钓鱼链接的吸引力对攻击能否成功至关重要。已有研究致力于识别用于操纵网络钓鱼 URL、使其在用户看来更为可信的技术 [1, 15], , 也有研究探讨如何开发工具来帮助用户留意链接 [36]。攻击者通常不会在电子邮件中直接显示完整的网络钓鱼 URL。链接通常会用文本或按钮掩码，因此，除非用户在桌面设备上将鼠标悬停在链接上，或在智能手机上轻触并按住链接，否则就无法看到实际的网络钓鱼 URL。

3 方法

本节首先介绍研究问题和我们的假设。然后，我们说明研究环境、所用材料以及数据收集过程。

3.1 研究问题与假设

我们的研究旨在回答两个研究问题。第一个问题是**研究问题1：用户在查看电子邮件时使用的设备是否会影响其网络钓鱼易感性?** 我们的假设是一级标题：与使用计算机相比，用户使用移动设备上的电子邮件客户端时，更有可能点击网络钓鱼链接。

第二个研究问题是**RQ2：电子邮件中网络钓鱼链接的呈现方式是否会影响用户的网络钓鱼易感性?** 我们假设*H2*：与显示为 *URL* 相比，掩码为按钮或超文本的网络钓鱼链接更容易被用户点击。

按钮和超文本在网站和电子邮件中都很常见。与原始 URL 相比，两者都可以设计得更具视觉吸引力。但总体而言，按钮的视觉呈现设计比超文本更灵活，因此用户可能更容易将按钮与周围的非链接内容区分开来，而不那么容易区分超文本。此外，按钮更具按压和点击的可供性，这可能进一步促使用户点击。因此，我们提出了最后一项补充假设：*H3*：如果网络钓鱼链接隐藏在 *HTML* 按钮中，而非超文本中，用户更有可能点击这些链接。

我们的数据是分类数据，记录了打开电子邮件、点击链接的用户人数以及使用的设备。因此，我们使用卡方检验来确定差异是否显著，并使用皮尔逊 φ (ϕ) 系数衡量效应量；我们的检验自由度为 1，因此，.1 被视为小效应量，.3 为中等效应量，.5 为大效应量 [17]。我们的假设具有方向性，而且列联表为 2×2 结构，因此可以使用卡方残差检验差异是否符合我们的假设方向。

3.2 研究环境

为了了解用户在现实情境中如何与钓鱼邮件互动，我们需要研究用户对通过其真实电子邮件地址收到的真实邮件有何反应。为此，我们与一家大型组织合作，该组织定期开展网络安全培训和钓鱼模拟演练，以教育员工。该组织的 IT 服务部门会向全体员工发送一封模拟钓鱼邮件，点击模拟网络钓鱼链接的员工将被引导至一个介绍网络钓鱼的培训材料网页。

我们与 IT 服务部门合作，在其培训活动中开展了这项研究。我们与组织的网络安全团队合作，并将培训安排在2022年11月，期间他们向组织中的每位员工发送了一封钓鱼邮件。我们帮助团队设计了钓鱼邮件模板和落地页。活动结束后，我们从网络安全团队获得了匿名数据，以供进一步分析。我们的研究方案经本校人类参与者伦理委员会和该组织首席

信息安全官审查并批准。

在正式活动开始之前，我们先与组织网络安全团队的 12 名成员试点测试了钓鱼模拟。随后，我们在拥有 374 名用户的整个 IT服务部门内进行测试，以便在规模更大、组成更多样的群体中开展测试。所有这些都是为了试点测试我们的流程；结果中不会呈现这些步骤的任何数据。主要活动发送至组织内超过 12,000 个员工电子邮件地址。

3.3 研究材料

为研究第二个研究问题，我们使用相同的发件人地址、主题和正文，精心制作了三个版本的钓鱼邮件。邮件声称用户有待处理的邮件消息，必须登录在线系统查看并释放。这模仿了该组织有时会发送的通知。该组织在网络钓鱼培训演练中使用 NIST钓鱼难度量表 [33] 来评估网络钓鱼邮件的检测难度，这限制了我们对钓鱼邮件类型和难度的选择。在本次活动中，组织的 IT服务部门要求我们使用检测难度为中等的钓鱼邮件模板。

这三个版本的区别仅在于网络钓鱼链接的视觉呈现，具体如下：

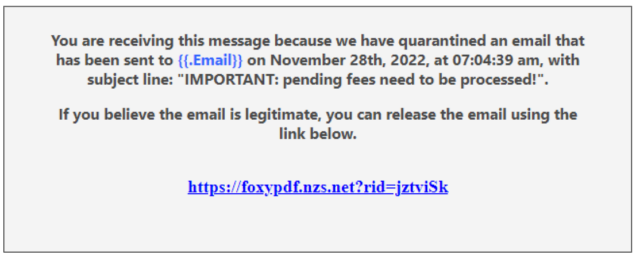
- 版本1（原始 URL）：在电子邮件中将真实（模拟的）网络钓鱼链接“https://foxypdf.nzs.net”显示为可点击链接。请注意，我们稍微修改了该 URL 的域名，以对组织进行匿名化处理。
- 版本2（带文字的按钮）：将网络钓鱼链接显示为一个按钮，按钮文字为“释放暂存邮件”。在 HTML 中，这是通过在超链接标签内放置按钮标签实现的。
- 版本3（超文本）：将“释放暂存邮件”显示为可点击的锚文本，而不是实际 URL。

在图1中，我们展示了这三个版本的电子邮件分别是什么样子。三个版本中的邮件头信息都相同。发件人为：**Security Gateway Notification <security-gateway@onlinesecurity.net>**，主题行为**您有新的暂存邮件**。实际 URL 和着陆页都相同。如果用户打开了着陆页，页面本身会说明这是一次钓鱼模拟，并引导用户查看钓鱼教育材料。

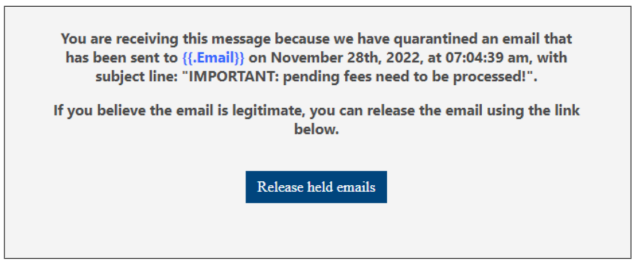
在这次活动中，我们将用户随机分成三组，每组成员收到三种不同版本的钓鱼邮件之一。

3.4 数据收集

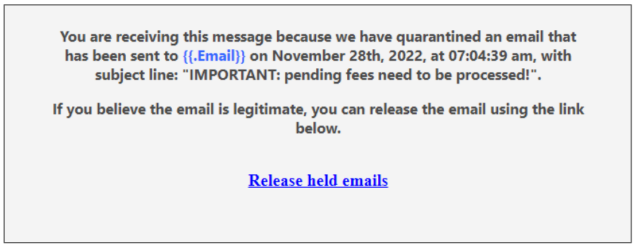
在组织的网络安全团队协助下，我们管理了模拟钓鱼邮件并收集了数据，使用



(a) 原始 URL 版本



(b) 按钮版本



(c) 超文本版本

图1：三种活动邮件：原始 URL、按钮和锚文本

开源钓鱼框架 GoPhish[1]。GoPhish 的安装由网络安全团队完成并管理。

每个与 GoPhish 配合使用的电子邮件地址都会获得一个唯一的匿名 ID。随后，GoPhish 会记录三类事件：邮件已发送、邮件已打开和链接已点击。邮件已打开事件的数据通过在电子邮件中嵌入跟踪图像来收集；访问该图像需要连接 GoPhish 服务器，且该跟踪图像可与跟踪 ID 关联。用户点击电子邮件中的链接（通过原始 URL、按钮或锚文本）并联系 GoPhish 服务器时，会生成链接已点击事件，该事件同样可与跟踪 ID 关联。对于每个邮件打开和链接点击事件，GoPhish 都能记录事件的时间戳、IP 地址和用户代理字符串。随后，可利用用户代理字符串识别发出用户代理请求的应用程序、操作系统、供应商和/或应用程序版本 [12]。

GoPhish 产生的数据首先经过预处理，以移除非用户操作。由于电子邮件

[1]GoPhish：Jordan Wright 开发的开源网络钓鱼框架：https://getgophish.com/

传输系统的复杂性以及不同电子邮件系统的使用，有些打开/点击尝试会在邮件到达收件箱之前产生，从而给数据带来额外噪声。一些电子邮件客户端（例如 Gmail 和 Apple Mail）会通过代理服务器或缓存服务器转发电子邮件，然后再由用户接收，这可能会产生并非由用户执行的打开/点击事件。我们通过检查与事件关联的 IP 地址来过滤这些噪声，并移除了来自托管服务公司的事件。如果 IP 地址的自治系统编号（ASN）属于电子邮件客户端所属的组织或某些托管服务公司，而非用户的本地网络服务提供商，我们便认定该事件很可能并非由用户实际操作所致。

GoPhish 记录的打开和点击事件都包含用户代理数据，但点击事件会显示用于呈现着陆页的客户端软件（通常是网页浏览器）。因此，在对用于打开电子邮件和点击链接的平台进行分类时，我们使用打开事件中的用户代理字符串；该平台通常是电子邮件客户端。

GoPhish 用于确定电子邮件打开情况的图像跟踪系统并不完美。如前所述，有些电子邮件客户端允许用户阻止电子邮件中的图像，这一设置可以由用户选择，也可能默认启用。上文还提到，电子邮件系统（值得肯定地）会通过其他方式采取措施，模糊电子邮件的访问情况。此外，用户代理字符串并非总是可靠，有时也会因隐私和安全原因而被刻意模糊。我们承认，这些问题构成了本研究的局限性。不过，我们没有理由认为，阻止图像的用户或受到其他安全措施影响的用户，在三个电子邮件版本组中的分布会有所不同。因此，我们认为，尽管这些因素可能影响总体数量，我们的各项条件之间的差异仍值得关注。

4 结果

4.1 活动概览

活动于一个工作日周一中午开始，邮件发送至 12,639 个电子邮件地址。我们收集数据至周三下午，历时略多于两天。数据显示，有两千至三千名用户打开了这封电子邮件。这个数字远低于发送的邮件数量，原因有几个。虽然该组织有数千名在职全职员工，但也为许多兼职员工提供电子邮件地址，甚至保留前员工的电子邮件地址，而这些人中许多人可能从不查看自己的电子邮件。也有可能一些用户看到主题行后，认为邮件与自己无关，便直接忽略了。此外，我们只收集了大约两天的数据，因此在数据收集结束后打开邮件的用户也会存在。由于大多数打开电子邮件的用户会在收到邮件后的头几个小时内这样做 [26]，我们预计两天后只会有少量活动，因此认为结果并未受到过多影响。IT 安全团队利用这一有限时间范围来确定 IT 支持团队的工作范围；这些团队负责接收员工举报的网络钓鱼邮件并回答员工的问题。

我们首先检查了数据中是否存在异常活动，因为我们预计，正常的用户行为最多只会在单个电子邮件客户端中产生几次点击。因此，我们从数据集中移除了 27 名进行了超过 20 次交互（包括电子邮件打开活动和链接点击活动）的用户，以及 22 名通过多个电子邮件客户端点击网络钓鱼链接的用户；这两种情况都使我们难以确定单一设备及其行为序列。我们也无法确定与“网页邮件”客户端相关的显示问题，即在网页浏览器中运行的电子邮件客户端。具体而言，我们了解到，该组织将其网页邮件服务的默认设置配置为禁止自动下载图像，这使我们无法准确统计电子邮件打开次数。因此，我们决定聚焦于电子邮件专用应用软件，并筛除在网页浏览器中打开电子邮件的记录。

筛选后，数据显示有 2,375 名用户打开了我们的电子邮件，约占发送总人数的 20%。其中，285 人点击了链接，约占打开电子邮件用户的 12%。这些用户共进行了 3,921 次打开操作，说明许多人不止一次打开了电子邮件；此外还有 304 次点击操作，这意味着少数人使用同一平台点击了不止一次。

4.2 设备使用情况

通过处理每个事件的用户代理字符串，我们提取了执行该事件所用的平台、操作系统和电子邮件客户端。我们根据用于查看电子邮件的设备对数据进行了分组：计算机、移动设备和未分类。未分类类别主要包含使用 Apple Mail 及其他无法根据用户代理字符串识别平台的电子邮件客户端的用户。由于 Apple Mail 的邮件隐私保护机制，无法识别用于打开电子邮件的设备 [2]。据我们观察，截至本文撰写时，所有平台（Mac、iPad 或 iPhone）都使用相同的用户代理（“Mozilla/5.0”）。各组的分布情况见表 1。总数略高于打开电子邮件的用户数，这是因为部分用户会使用多台设备和多个电子邮件客户端打开电子邮件。不过，由于这些用户至多只点击过一种类型的电子邮件客户端，因此我们的数据不会受到影响。

4.2.1 一级标题测试

这些数据使我们能够检验假设H1：用户使用移动设备时更有可能点击网络钓鱼链接

[2] https://www.apple.com/legal/privacy/数据/en/mail-隐私-protection/

表1：活动用户在不同设备上的点击行为分布

	电脑	移动设备	未分类	总计
用户已点击	88	135	62	285
用户未点击了	538	591	1200	2339
Sum	626	726	1262	2614

比在计算机上

我们进行了卡方检验，以考察用户点击链接的行为与用于查看电子邮件的设备之间是否存在关联。进行卡方检验时，我们剔除了未分类组，因为无法确定使用的是哪种设备。结果显著，$\chi^2(1, N = 1352) = 5.02, p = .025$ (皮尔逊残差：+1.4)。此处及下文中，我们报告的是所述第一种条件下的点击次数残差——本例中即移动设备。正值表明，若各类别相同，移动设备上的点击次数高于预期。因此，我们得出结论：假设H1得到支持，用户使用不同设备查看电子邮件时，其行为存在显著差异。然而，我们计算的效应量φ系数为 $\phi = .06$，表明效应非常小，因此我们认为，设备对点击行为造成的差异相当有限。

这些结果也显示在表2的第一行。

我们进一步进行了测试，以探究使用不同设备是否会影响用户的点击行为。我们比较了移动设备和计算机上的数据，并分别考察了每种链接呈现组。对于原始URL，结果为：$\chi^2(1, N = 396) < .01, p = .93$（皮尔逊残差：$-0.1$），因此差异并不显著。换言之，呈现原始 URL 时，设备并不重要。

对于按钮组，结果为：$\chi^2(1, N = 371) = 5.39, p = .02, \phi = .12$ (皮尔逊残差：+1.3)；超文本组的结果类似：$\chi^2(1, N = 585) = 5.98, p = .01, \phi = .10$ (皮尔逊残差：+1.6）。这些结果总体上与我们上文的发现一致：表现出不同用户行为的是链接呈现，而非设备类型。这些结果也显示在表 2 中。

我们观察到，在原始 URL 组中，使用电脑电子邮件客户端打开电子邮件的 163 名用户中，有 8.0% 点击了链接；而在使用移动设备打开电子邮件的用户中，233 人里有 7.7% 点击了链接，这两个点击率相差不大。然而，当网络钓鱼链接对用户隐藏时，我们观察到了差异。在按钮组中，138 名计算机用户中有 10.9% 点击了链接，而移动设备用户中，233 人里有 20.2% 点击了链接。在超文本组中也能观察到类似差异：325 名计算机用户中有 18.5% 点击了

表 2：移动设备与计算机的点击行为：卡方检验结果；显示移动设备点击次数的残差

条件	$\chi^2(1)$ p 值	效应量 ϕ	皮尔逊残差
所有点击行-ior	.025	0.06	+1.4
原始 URL 点击行为	.93	< .01	-0.1
按钮点击行为	.02	.12	+1.3
超文本点击行为	.01	.10	+1.6

链接，而 260 名移动设备用户中有 26.9% 点击了链接。这些结果进一步印证了我们上述的发现：链接呈现会与设备类型相互作用，进而影响用户的行为。

4.3 链接呈现

我们进一步根据用户收到的具体钓鱼邮件，将数据分为三个组。在活动期间，我们还观察到，对于按钮版本，Windows Outlook 应用程序会将按钮显示为超文本。从用户的角度来看，他们看到的是超文本版本，这与将用户归入超文本组的情况相同。因此，我们决定将 Windows Outlook 应用程序的数据从按钮版本中移出，并将其添加到超文本版本中。表 3 显示了每个条件下使用计算机和移动设备打开并点击网络钓鱼链接的用户数量。基于这些数据，我们进行了一系列卡方检验，包括组内不同设备之间的检验，以及不同组之间用户点击行为的检验，如表4。

4.3.1 H2 检验

假设 H2 表述如下：用户看到掩码为按钮或超文本的钓鱼链接时，比看到 *URL* 时更有可能点击该链接。

为检验 H2，我们将按钮组和超文本组合并为一个隐藏文本组，并在所有平台上将其与原始 URL 组进行比较，如表 5所示。随后我们进行了卡方检验，并计算了效应量，结果为：$\chi^2(1, N = 2614) = 34.8, p < .001, \phi = .12$ (皮尔逊残差：+3.1）。因此，H2 得到支持，且效应量较小至中等。由此我们得出结论：用户看到原始链接与看到被按钮或超文本隐藏的链接时，其行为存在差异。

效应量 .12 的解释为小到中等，但我们注意到，差异出现在原始链接

表3：活动用户使用不同设备的点击行为分布

	电脑	移动设备	未分类	总计
原始 URL 已点击	13	18	11	42
Raw URL 未点击	150	215	377	742
按钮点击	15	47	29	91
按钮 not 点击	123	186	401	710
超文本已点击	60	70	22	152
超文本 not 已点击	265	190	422	877
Sum	626	726	1262	2614

表4：所有平台上的点击行为：卡方检验结果；显示第一个条件的残差

条件	$\chi^2(1)$ p 值	效应量 ϕ	皮尔逊残差 针对点击次数
掩码 vs. 原始 URL	< .001	.12	+3.1
按钮与原始内容 URL	< .001	.10	+2.8
超文本 vs. 原始 URL	< .001	.15	+4.0
超文本 vs 按钮	.02	.05	+1.4

情形中，42 人点击、742 人未点击（占总数的 5%）；而在隐藏链接情形中，152 人点击、877 人未点击（占总数的 14%）。在实际中，这可能意味着网络钓鱼易感性存在显著差异。

我们还对两种隐藏文本变体、按钮版本和超文本版本分别与原始 URL 版本进行了卡方检验。结果均具有统计显著性。对于按钮变体，$\chi^2(1, N = 1585) = 17.4, p < .001$，$\phi = .10$（皮尔逊残差：$= +2.8$）；对于超文本版本，$\chi^2(1, N = 1813) = 41.27, p < .001$，$\phi = .15$（皮尔逊残差：$= +4.0$）。

4.3.2 H3 检验

假设 H3 提出：与将钓鱼链接隐藏在超文本中相比，用户更可能点击隐藏在 *HTML* 按钮中的钓鱼链接。

表5：原始 URL 与隐藏文本的列联表

	Raw URL	隐藏 URL	Sum
已点击	42	243	285
未点击	742	1587	2329
Sum	784	1830	2614

为检验假设 H3，我们比较了所有平台上的超文本组和按钮组数据。随后进行了卡方检验，并计算了效应量，结果为：$\chi^2(1, N = 1830) = 5.2, p = .02, \phi = .05$（皮尔逊残差：+1.3）。结果具有统计显著性，但残差显示的方向与我们的假设相反。与按钮版本相比，用户略微更可能点击超文本版本。因此，假设 H3 不成立。

上述结果也显示在表4中。

4.4 总结

如表 6所示，我们提出的三项假设均达到统计显著性水平，α 为。05，但只有 H2 的效应量不可忽略。与显示为原始钓鱼网址相比，用户在网络钓鱼链接显示为按钮或被掩码为文本时更有可能点击。我们观察到，当网络钓鱼链接在视觉上被遮挡时，用户行为存在一个重要差异。若链接一目了然，无论使用何种设备，用户行为都一致。而如果链接被按钮或文本掩码，用户使用移动设备时比使用计算机时更有可能点击该链接。在这两种视觉呈现方式中，我们假设按钮版本会比超文本版本更容易促使用户点击，因为它的可供性和视觉外观。然而，在研究中，我们观察到一种显著但方向相反且效应极小的效应。

表6：假设检验总结

	假设陈述	支持
H1	用户更有可能点击钓鱼—— 点击链接时使用电子邮件客户端 而非使用电脑时，更容易受到影响。	有数据支持, but very 小 效应量
H2	用户更有可能点击钓鱼 链接，如果它们被隐藏在 按钮或超文本中，而不是显示为 URL。	支持, with 小到中等 效应量
H3	如果网络钓鱼 链接通过 HTML 按钮隐藏，用户比起被隐藏 带有超文本。	Not 支持

5 讨论

正如 Steves 等人的研究 [33], 所指出的，“并非所有线索都具有同等作用”。不同的网络钓鱼线索在检测难度和效应方面各不相同。例如，将网络钓鱼链接显示为原始 URL 是一种非常明显的线索，可以帮助用户判断电子邮件是否为网络钓鱼邮件。我们的研究表明，无论人们使用何种设备查看电子邮件，看到原始 URL 版本时，点击的可能性都较低。这种线索之所以容易识别，部分原因在于用户无需与界面进行任何交互（例如悬停），就能看到原始钓鱼链接。如果同一网络钓鱼线索被按钮或超文本掩码，识别起来就会困难得多。当用户看不到明显线索时，他们可能会像处理正常邮件一样处理该电子邮件。只有当他们看到某些线索（例如链接指向一个不熟悉的 URL）时，才可能产生怀疑，并改变心态，开始警惕潜在的网络钓鱼攻击。期待用户悬停在链接上这一额外步骤存在风险。我们的研究发现，链接显示为按钮或超文本时，点击链接的用户更多。可以用将人类思维视为双重加工系统这一概念来解释怀疑如何产生 [19],；该概念已应用于网络钓鱼易感性领域 [16,35,38,42]。这一理论认为，我们的心智有两套推理系统：一套快速、省力，基于启发式；另一套缓慢，需要系统性推理。当用户看到原始钓鱼网址时，启发式系统更可能迅速发出危险信号，直觉地察觉到异常。这会触发系统性推理系统，以更强的意识审视电子邮件，因此用户点击该 URL 的可能性较低。Kahneman 解释说，在缺乏可见信息时，结论往往是所见即所得的信息偏差：“你看到的就是全部。”

使用不同设备会使网络钓鱼呈现问题更加复杂。我们的研究发现，与电脑用户相比，移动设备用户更容易点击链接。这与相关文献的结论一致 [8, 11, 21, 24]。此外，我们的发现也为相关文献增添了新的细节：网络钓鱼链接的呈现方式很重要——移动用户对原始 URL 并未表现出更高的易受骗性，但对隐藏 URL 则表现出更高的易受骗性。这表明，隐藏式呈现对移动用户造成的危险更大。屏幕尺寸、查看完整 URL 的交互机制以及外部环境等因素都可能有所影响。

不同用户检测网络钓鱼线索的能力可能各不相同，因为他们以往的知识和经验会影响其识别线索的能力。在不同组织中，用户对 URL 和网络域名的了解程度各异。这类知识会影响用户判断链接是否合法的能力。

原本预计，按钮的呈现方式会因其可供性和视觉设计而带来更多点击次数。然而，我们发现，链接的超文本呈现方式带来了更多点击次数。组织发送的合法安全通知也使用超文本链接来释放隔离邮件，这可能让超链接对用户而言更熟悉、更值得信任。按钮通常用于执行会影响当前网页的操作，而超链接则用于将用户重定向到其他网页。由于用户并不预期会在电子邮件中直接释放隔离邮件，因此，与会将他们重定向至网站的超链接相比，他们可能较少预期看到按钮。此外，钓鱼按钮和超链接的点击率也可能因情境而异，取决于钓鱼消息的主题。

伪装文本的性质可能会影响用户易受网络钓鱼攻击的程度。在我们的主要研究中，我们使用了“释放暂存邮件”。在试点研究中，我们测试了另一种做法：将钓鱼网址伪装成一个看起来合法、且来自组织内所有员工都熟悉的内部域名的网址。我们将这种做法与原始 URL 版本进行了比较。我们在 IT服务部门的 374 名成员中开展了试点，并将他们随机分为两组，分别测试两种变体。我们观察到两组的用户点击次数差异很大。原始 URL 版本的点击率为 3.8%（打开电子邮件的 79 名用户中有 3 次点击），而隐藏 URL 版本的点击率为 19.6%（打开电子邮件的 56 名用户中有 11 次点击）。这些用户来自 IT服务部门，预计在应对网络钓鱼邮件方面经验更丰富，但我们仍然观察到了显著的点击率差异。我们的试点研究表明，将网址伪装成合法网址会带来危险，并会促使用户点击链接。由于我们关注的是通用钓鱼，因此没有在主要活动中纳入这种“合法网址”变体。了解用户信任且熟悉的内部合法域名，可视为定向钓鱼，这超出了本文的研究范围。此外，我们和 IT服务部门都认为，这种变体对普通人群来说过于复杂。我们会在未来活动中考虑这一点。

同一封钓鱼邮件的呈现方式可能因所使用的电子邮件客户端而异。我们观察到，在 Windows Outlook 客户端中，按钮（通过在超链接标签内使用按钮标签创建）会显示为普通超文本。Windows Outlook 客户端也可以通过其他方法（例如修改超链接的 CSS 样式）正常显示按钮。如果超链接比按钮更能吸引用户点击（正如我们在研究中发现的那样），这意味着 Windows Outlook 用户可能比其他客户端的用户更容易受到网络钓鱼攻击，因为他们看到的可能是更多超链接，而非按钮。

伪装链接会提高用户易受攻击的程度，而这些伪装链接的显示方式因设备和平台而异。电脑网页版邮件用户将鼠标悬停在链接上时，落地页网址会显示在浏览器左下角。相比之下，电脑应用程序用户将鼠标悬停时，落地页网址通常会显示在鼠标光标旁边。

在某些电子邮件客户端（例如 Outlook）中，URL 也会显示在应用程序的左下角。URL 的位置可能会影响其可读性，并导致点击率出现差异。此外，HTML 中的超链接标签可以设置为包含可自定义内容的工具提示。虽然工具提示属性通常不会影响电子邮件客户端应用程序中链接的呈现方式，但当用户将鼠标悬停在链接上时，它可以在网页客户端中模拟悬停框。攻击者可以利用这一技巧，在网络钓鱼链接旁显示“真实的落地页网址”，从而诱使网页客户端用户相信该链接是真的。在极端情况下，网页客户端可能会在用户将鼠标悬停在单个链接上时显示三个不同的 URL：链接本身以一个 URL 的形式显示，工具提示显示第二个 URL，而浏览器则在左下角显示真实 URL（可能是第三个 URL）。

当原始 URL 清晰可见时，可以降低用户的网络钓鱼易感性。然而，显示原始 URL 是以牺牲可用性为代价来换取安全性。HTML 渲染可以让文本更易于理解，也能让链接的用途更加明确，但同时也可能使文本和链接更具欺骗性。尤其是，允许隐藏链接，无异于送给攻击者一份大礼。

我们的研究无法记录悬停行为。评估用户是否将鼠标悬停在链接上，以及这会如何影响其网络钓鱼易感性，将会很有意思。其他研究者曾使用眼动追踪仪来考察人们阅读电子邮件时的注视位置 [28]。遗憾的是，眼动追踪仪目前还不适用于组织级现场研究所需的规模。

在未来的网络钓鱼研究中，电子邮件客户端的设计元素值得更多关注。例如，Gmail 等电子邮件服务提供商 [3] 会在用户回复发件人后隐藏发件人的电子邮件地址。鉴于大多数网络钓鱼邮件都由陌生发件人发送，在电子邮件客户端中突出显示已知和未知发件人之间的差异，或许能为识别网络钓鱼邮件提供有用线索。根据本研究的结果，一种可能的解决方案是在发件人身份不明时显示原始 URL。未来的研究可以调整电子邮件客户端的设计元素，以展现这些设计在帮助用户保护自己免受网络钓鱼侵害方面的潜力。

5.1 局限性

我们这项研究的发现可能看起来显而易见，但我们通过大规模网络钓鱼活动提供了证据，证实用户在使用移动设备时，以及看到以掩码文本形式呈现的网络钓鱼链接时，更容易受到网络钓鱼攻击。这表明存在一种风险，说明有必要开展专项培训或改进电子邮件客户端。

我们的研究存在一些局限性。首先，GoPhish 框架使用不可见的跟踪图像来确定电子邮件是否被打开。如果电子邮件客户端不允许自动下载图片，这种跟踪方法就会失效。因此，我们预计实际的打开尝试次数会多于数据中显示的次数。在分析中，我们剔除了所有无法对应到打开事件的链接点击。实际上，这些点击事件可能是用户的正常操作，但由于我们无法识别对应的打开尝试，也就无法确定与该操作相关联的用户代理。因此，这部分数据在我们的研究中丢失了。

其次，电子邮件客户端和设备的分类依赖于用户代理字符串，而这种字符串并非总是可靠。例如，对于 Apple Mail 用户，默认情况下，他们操作所关联的用户代理在所有设备上都是“Mozilla/5.0”，而且用户可以手动选择发送邮件时使用的用户代理。我们很高兴看到这种做法有助于保护用户隐私，但与此同时，这也增加了我们验证应用程序和设备的难度。

第三，在这项研究中，我们假设所有电子邮件都未被转发。我们承认，可能有一小部分用户会自动将电子邮件转发到其他账户，但我们无法将这些用户与其他用户区分开来。对于这些用户，转发邮件的发件人将是他们自己，这可能会影响他们的行为，因为用户可能不会那么注意邮件的原始发件人。我们假设这些用户会均匀分布在三个组中，因此研究结果不会受到影响。

第四，我们应指出，本研究使用的 URL 并未经过专门设计，使其看起来像用户会识别并信任的链接。相反，我们选择了攻击者采用或劫持来供一般用途的 URL。如今，网络钓鱼所用的域名经常被使用后弃置，通常存续不到 24 小时，以避免被加入阻止列表 [7]。因此，我们认为本研究使用的 URL 对许多攻击而言具有现实性，但并不代表专业化的定向攻击活动。

最后，在本研究中，我们将 Windows Outlook 应用程序用户从按钮版本切换为超文本版本，因为 Outlook Windows 应用程序在两个组中始终都将钓鱼网址显示为超文本。为确保这种数据迁移不会影响我们呈现的研究结果，我们还对所有条件中移除 Windows Outlook 应用程序用户后的数据进行了相同测试，并重新计算以比较结果。如表7所示，结果非常相似。

进一步研究这一领域，将有助于开发更稳健的解决方案，帮助用户识别并避免网络钓鱼诈骗。我们鼓励研究人员重复我们的研究，并在已积累的知识基础上继续深入，为持续提升在线安全的努力贡献力量。

[3] https://support.google.com/mail/answer/1311182?hl=en

表 7：**Mov**情形（将 Windows Outlook 数据从按钮移至超文本）与**Del** 情形（从所有条件中删除 Windows Outlook 数据）的假设检验结果比较。

Case	假设	χ^2	p值	ϕ	resi
Mov	一级标题：全部	5.0	.025	.06	1.39
Del	一级标题：全部	6.5	.011	.08	1.32
Mov	一级标题：仅原始值	<.01	0.927	<.01	-0.06
Del	一级标题：仅原始值	.6	.424	.04	0.39
Mov	H1：按钮 only	5.4	.02	.12	1.29
Del	H1：按钮 only	5.4	.02	.12	1.29
Mov	一级标题：超文本 only	6.0	.014	.10	1.61
Del	一级标题：超文本 only	3.1	.08	.09	.86
Mov	H2：掩码与原始相比	34.8	<.001	.12	3.05
Del	H2：掩码与原始相比	32.8	<.001	.12	2.98
Mov	H2：按钮与 raw	17.4	<.001	.10	2.81
Del	H2：按钮与 raw	20.6	<.001	.12	2.97
Mov	H2：超文本与原始内容	41.3	<.001	.15	3.99
Del	H2：超文本与原始内容相比	36.6	<.001	.15	3.89
Mov	H3：按钮与超文本	5.2	.023	.05	1.40
Del	H3：按钮与超文本	2.8	.092	.04	1.10

6 结论

本文介绍了我们在一个大型组织中开展的网络钓鱼活动研究结果。我们的研究聚焦于电子邮件的视觉呈现及其对用户行为的影响。结果表明，与使用计算机相比，用户使用移动设备时对网络钓鱼略微更易感。更重要的是，我们发现，与显示原始 URL 相比，用按钮或超文本隐藏网络钓鱼链接，更能促使用户点击该网络钓鱼链接。在这些隐藏 URL 条件下，移动用户比计算机用户更易受网络钓鱼影响。我们的研究确定了会影响用户网络钓鱼易感性的全新链接呈现变量。我们建议未来研究进一步探索网络钓鱼邮件的呈现方式，以及如何设计电子邮件客户端来帮助用户保护自己。

致谢

待定。

参考文献

[1] Kholoud Althobaiti、Nicole Meng 和 Kami Vaniea。原来我不需要专家！让网址钓鱼特征更易于人类理解。载于*2021*年*CHI*计算机系统中的人为因素会议论文集，第1–17页，2021年。

[2] Tomás Alves、JoanaNatálio、Joana Henriques-Calado 和 Sandra Gama。在用户界面设计中融入人格特征：一篇综述。《人格与个体差异》，155：109709，2020年。

[3] Bonnie Anderson、Anthony Vance、C Brock Kirwan、David Eargle 和 Jeffrey L Jenkins。用户如何感知并回应安全信息：神经信息系统研究议程与实证研究。《欧洲信息系统期刊》，25(4)：364–390，2016年。

[4] Aizza Anwar、Ali Waqas、Hafiz MuhammadZain 和 Daisy Mui Hung Kee。音乐和色彩对顾客情绪状态的影响：一项关于在线商店的实验研究。《亚洲商业研究期刊》，10(1):104–125，2020年。

[5] Aurélien Baillon、Jeroen De Bruin、Aysil E mirmahmuto- glu、Evelien Van De Veer 和 Bram Van Dijk。提供信息、模拟经验，或两者兼有：一项关于网络钓鱼风险的现场实验。《公共科学图书馆·综合》，14(12):e0224216，2019年。

[6] Lisa Feldman Barrett、Michele M Tugade 和 Ran- dall W Engle。工作记忆容量的个体差异与心智的双加工理论。心理学通报，130(4):553，2004年。

[7] Simon Bell 和 Peter Komisarczuk。对网络钓鱼黑名单的分析：Google 安全浏览、OpenPhish 和 PhishTank。载于澳大拉西亚计算机科学周多会议论文集，ACSW '20，美国纽约，2020年。计算机协会。

[8] Ron Bitton、Andrey Finkelshtein、Lior Sidi、Rami Puzis、Lior Rokach 和 Asaf Shabtai。移动用户安全意识分类体系。《计算机与安全》，73:266–293，2018年。

[9]Email Blaster。桌面设备与移动设备——哪种更适合您的电子邮件营销活动? https://www.emailblasteruk.com/blog/desktop-vs-mobile-which-is-best/。

[10] Mark Blythe、Helen Petrie 和 John A Clark。《F代表伪造：关于我们如何上钩的四项研究》。载于*SIGCHI*计算机系统人为因素会议论文集，第3469–3478页，2011年。

[11] Frank Breitinger、Ryan Tully-Doyle 和 Courtney Hassenfeldt。《智能手机用户的安全选择、意识与教育调查》。《电脑与安全》，88:101647，2020年。

[12]MDN贡献者。用户代理。
h
t
tps://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/User-Agent。

[13] Adrienne Porter Felt 和 David Wagner。移动设备上的网络钓鱼。2011年。

[14] Anjuli Franz、Verena Zimmermann、Gregor Albrecht、Katrin Hartwig、Christian Reuter、Alexander Benlian 和 Joachim Vogt。《Sok：海中仍有大量网络钓鱼——面向用户的网络钓鱼干预措施分类体系及未来研究方向》。载于 第十七届可用隐私与安全研讨会（{*SOUPS*}*2021*年，第339–358页，2021年。

[15] Sujata Garera、Niels Provos、Monica Chew 和 Aviel D Rubin。《网络钓鱼攻击的检测与测量框架》。载于 *2007*年美国计算机协会重复出现的恶意代码研讨会论文集，第1–8页，2007年。

[16] Brynne Harrison、Arun Vishwanath、Yu Jie Ng 和 Raghav Rao。考察在场感对个体网络钓鱼受害的影响。载于*2015*年第*48*届夏威夷国际系统科学会议，第3483–3489页。电气电子工程师学会，2015年。

[17] James F Hemphill。解读相关系数的大小。《美国心理学家》，58(1)，2003年。

[18] Daniel Jampen、Gürkan Gür、Thomas Sutter 和 Bernhard Tellenbach。切勿点击：迈向有效的反网络钓鱼培训。一项比较性文献综述。《以人为中心的计算与信息科学》，10(1)：1–41，2020年。

[19] Daniel Kahneman。《思考，快与慢》。Farrar, Straus and Giroux，纽约，2011年。

[20] Valho Kostov 和 S Fukuda。基于用户偏好的人机界面开发。载于*2001*年*IEEE*国际控制应用会议论文集（*CCA'01*）（目录号：*01CH37204*），第1124–1128页。电气电子工程师学会，2001年。

[21] Murat Koyuncu 和 Tolga Pusatli。智能手机用户的安全意识水平：一项探索性案例研究。《移动信息系统》，2019年，2019年。

[22] Daniele Lain、Kari Kostiainen 和 Srdjan Capkun。组织中的网络钓鱼：一项大规模长期研究的发现。*arXiv* 预印本 *arXiv:2112.07498*，2021。

[23] Caroll P Lau、Joanne L Harbluk、Peter C Burns 和 Yue El-Hage。界面设计对自动驾驶中驾驶员行为的影响。*CARSP*（加拿大道路安全专业人士协会）：加拿大不列颠哥伦比亚省维多利亚，2018年。

[24] Tanya McGill 和 Nik Thompson。旧风险，新挑战：探讨家用计算机与移动设备使用在安全方面的差异。行为与信息技术，36(11)：1111–1124，2017年。

[25] Gareth Norris、Alexandra Brookes 和 David Dowell。互联网欺诈受害的心理学：系统性综述。警务与犯罪心理学杂志，34(3)：231–245，2019年。

[26] Adam Oest、Penghui Zhang、Brad Wardman、Eric Nunes、Jakub Burgis、Ali Zand、Kurt Thomas、Adam Doupé 和 Gail-Joon Ahn。从日出到日落：大规模分析网络钓鱼攻击的端到端生命周期及其有效性。载于第*29*届*USENIX*安全研讨会，2020年。

[27] Justin Petelka、Yixin Zou 和 Florian Schaub。《把警告放在链接旁：改进并评估电子邮件网络钓鱼警告》。载于*2019*年 *CHI* 计算机系统中的人为因素会议论文集，第 1–15 页，2019年。

[28] Kevin Pfeffel、Philipp Ulsamer 和 Nicholas H Müller。《用户阅读网络钓鱼邮件时究竟会看哪里——一项眼动追踪研究》。载于人机交互国际会议，第 277–287 页。施普林格，2019年。

[29] Benjamin Reinheimer、Lukas Aldag、Peter Mayer、Mattia Mossano、Reyhan Duezguen、Bettina Lofthouse、Tatiana Von Landesberger 和 Melanie Volkamer。《网络钓鱼意识与教育的长期研究：何时以及如何最好地提醒用户》。载于第十六届 *USENIX*可用隐私与安全会议论文集，第 259–284 页，2020年。

[30] Ashlea Rendell、Marc TP Adam、Ami Eidels 和 Timm Teubner。《用户界面设计中的自然意象：对用户信任感知与美学感知的影响》。《行为与信息技术》，第 1–17 页，2021 年。

[31] Christoph Schneider、Markus Weinmann 和 Jan Vom Brocke。数字助推：通过界面设计引导在线用户选择。《美国计算机协会通讯》，61(7):67–73，2018年。

[32]Steve Sheng、Bryant Magnien、Ponnurangam Kumaraguru、Alessandro Acquisti、Lorrie Faith Cranor、Ja- son Hong 和 Elizabeth Nunge。反钓鱼 Phil：一款教人们避免上当受骗的游戏的设计与评估。载于第三届可用隐私与安全研讨会论文集，第88–99页，2007年。

[33] Michelle Steves、Kristen Greene 和 Mary Theofanos。人类网络钓鱼难度分类：钓鱼量表。《网络安全杂志》，6(1)，2020年。[34] Milica Stojmenovi´c、Eric Spero、Miloš Stojmenovi´c 和 Robert Biddle。美观即安全。《美国计算机协会隐私与安全汇刊》，25(4)：1–30，2022年。[35] Arun Vishwanath、Brynne Harrison 和 Yu Jie Ng。网络钓鱼易感性的怀疑、认知与自动化模型。《传播研究》，45(8)：1146–1166，2018年。[36] Melanie Volkamer、Karen Renaud、Benjamin Reinheimer 和 Alexandra Kunz。Torpedo 的用户体验：工具提示驱动的钓鱼邮件检测。《计算机与安全》，71：100–113，2017年。

[37] Melanie Volkamer、Karen Renaud、Benjamin Rein- heimer、Philipp Rack、Marco Ghiglieri、Peter Mayer、Alexandra Kunz 和 Nina Gerber。开发并评估一段五分钟的网络钓鱼意识视频。载于数字商务中的信任、隐私与安全：第十五届国际会议，*TrustBus 2018*，德国雷根斯堡，*2018*年*9*月*5*日至*6*日，论文集 *15*，第119–134页。施普林格，2018年。

[38] Jingguo Wang、Yuan Li 和 H Raghav Rao。网络钓鱼检测中的应对反应：对前因与后果的研究。*Information Systems Research*，28(2):378–396，2017年。

[39] Rick Wash。《专家如何识别钓鱼诈骗邮件》。美国计算机协会人机交互论文集，4(CSCW2):1–28，2020年。

[40] Zikai Alex Wen、Zhiqiu Lin、Rowena Chen 和 Erik Andersen。《What. hack：通过角色扮演式网络钓鱼模拟游戏开展引人入胜的反网络钓鱼培训》。载于*2019*年*CHI*计算机系统中的人为因素会议论文集，第1–12页，2019年。

[41] Emma J Williams 和 Danielle Polage。《钓鱼邮件有多大的说服力？真实设计、影响力和时事在邮件判断中的作用》。《行为与信息技术》，38(2):184–197，2019年。

[42] Ryan T Wright、Matthew L Jensen、Jason Bennett Thatcher、Michael Dinger 和 Kent Marett。《研究札记——网络钓鱼攻击中的影响技巧：对易受攻击性与抵抗力的考察》。*Informationsystems research*，25(2):385–400，2014年。[43] Sijie Zhuo、Robert Biddle、Yun Sing Koh、Danielle Lottridge 和 Giovanni Russello。《综述：以人为中心的网络钓鱼易感性》。美国计算机协会隐私与安全汇刊，2022年12月。