电子邮件欺骗攻击的端到端测量

胡航和王刚，弗吉尼亚理工大学

https://www.usenix.org/conference/usenixsecurity18/presentation/hu

这篇论文包含在第 27 届 USENIX 安全研讨会论文集中。

2018 年 8 月 15-17 日 • 美国马里兰州巴尔的摩

书号 978-1-939133-04-5

开放获取第 27 届 USENIX 安全研讨会论文集
由 USENIX 赞助。

电子邮件欺骗攻击的端到端测量

杭胡弗吉尼亚
理工大学
hanghu@vt.edu

王刚弗吉尼亚理
工大学刚
ang@vt.edu

摘要

鱼叉式网络钓鱼一直是对用户和组织的持续威胁，但电子邮件提供商仍然面临验证传入电子邮件的主要挑战。因此，攻击者可以应用欺骗技术来冒充受信任的实体来进行极具欺骗性的网络钓鱼攻击。在这项工作中，我们研究电子邮件欺骗以回答三个关键问题：(1) 电子邮件提供商如何检测和处理伪造的电子邮件？(2) 伪造的邮件在什么情况下可以越过防御到达用户收件箱？(3) 一旦伪造的电子邮件进入，电子邮件提供商如何警告用户？警告真的有效吗？

我们通过对 35 家流行的电子邮件提供商进行端到端测量并通过真实世界的欺骗/网络钓鱼测试检查用户对欺骗的反应来回答这些问题。我们的主要发现有三方面。首先，我们观察到大多数电子邮件提供商都有必要的协议来检测欺骗，但仍然允许伪造的电子邮件到达用户收件箱（例如 Yahoo Mail、iCloud、Gmail）。其次，一旦收到伪造的电子邮件，大多数电子邮件提供商都不会向用户发出警告，尤其是对于移动电子邮件应用程序。一些提供商（例如 Gmail 收件箱）甚至具有误导性的 UI，使伪造的电子邮件看起来是真实的。第三，一些电子邮件提供商 (9/35) 在未经验证的电子邮件上实施了视觉安全指示器。我们的网络钓鱼实验表明，安全指标对减少有风险的用户操作有积极影响，但不能消除风险。我们的研究揭示了电子邮件提供商和最终用户之间的主要误解。 需要在两端（服务器端协议和 UI）进行改进以弥合差距。

1 简介

尽管最近系统和网络安全得到了发展，但人为因素仍然是一个薄弱环节。
因此，攻击者越来越依赖网络钓鱼策略——
抽动破坏各种目标网络[62]. 例如，电子邮件网络钓鱼涉及近两年报告的 2000 多起安全漏洞中的近一半，导致数十亿用户记录泄露[4].

电子邮件欺骗是网络钓鱼的关键步骤，攻击者冒充受信任的实体以获得受害者的信任。根据反网络钓鱼工作组（APWG）的最新报告，电子邮件欺骗在鱼叉式网络钓鱼攻击中广泛使用，以针对各种企业的员工[2]. 不幸的是，tos 电子邮件传输协议（SMTP）没有内置机制来防止欺骗[56]. 它依赖于电子邮件提供商来实现 SMTP 扩展，例如 SPF[40]，金[19] 和 DMARC[50] 以验证发件人。由于实施这些扩展是自愿的，因此它们的采用率远不能令人满意。2015 年进行的真实世界测量显示，在 Alexa 前 100 万个域中，40% 具有 SPF，1% 具有 DMARC，正确/严格配置的更少[23, 27].

有限的服务器端保护可能会使用户处于易受攻击的位置。由于并非每个发件人域都采用了 SPF/DKIM/DMARC，电子邮件提供商仍然面临着可靠地验证所有传入电子邮件的关键挑战。当电子邮件未通过身份验证时，就电子邮件提供商如何处理该电子邮件而言，这是一个“黑盒”过程。伪造的电子邮件是否仍会发送给用户？如果是这样，用户怎么知道电子邮件有问题？以 Gmail 为例，Gmail 将某些伪造的邮件发送到收件箱，并在发件人图标上放置一个安全指示器（红色问号，如图6(a)). 我们很好奇更广泛的电子邮件提供商如何处理伪造的电子邮件，以及安全指标实际上有助于保护用户的程度。

在本文中，我们描述了我们在评估针对电子邮件欺骗的真实防御措施方面所做的努力和经验[1]. 我们通过经验性的端到端欺骗测量和用户研究来回答上述问题。

[1]我们的研究已获得当地 IRB（IRB-17-397）的批准。

首先，我们对流行的电子邮件提供商如何检测和处理伪造的电子邮件进行测量。关键思想是将每个电子邮件提供商视为一个黑盒，并改变输入（伪造的电子邮件）以监控输出（res 收件箱）。我们的目标是了解伪造/网络钓鱼电子邮件在什么条件下能够到达用户收件箱，以及使用什么安全指标（如果有）来警告用户。其次，为了检查用户对欺骗电子邮件的反应以及安全指标的影响，我们在用户研究中进行了真实世界的网络钓鱼测试。我们已仔细应用“欺骗”来检查用户对欺骗电子邮件的自然反应。

测量。我们首先扫描 Alexa 从 2017 年 2 月到 2018 年 1 月的前 100 万主机。我们确认 SMTP 安全扩展的整体采用率仍然很低（SPF 44.9%，DMARC 5.1%）。这促使我们研究电子邮件提供商如何处理未通过身份验证的传入电子邮件。

我们对数十亿用户使用的 35 个流行电子邮件提供商进行端到端欺骗实验。我们发现，在适当的条件下，伪造的电子邮件可以渗透大多数电子邮件提供商（34/35），包括 Gmail、Yahoo Mail 和 Apple iCloud。即使收件人执行了所有身份验证检查（SPF、DKIM、DMARC），欺骗未受保护的域或具有“宽松”DMARC 策略的域也可以帮助伪造的电子邮件到达收件箱。此外，欺骗受害者的“现有联系人”也有助于攻击者渗透电子邮件提供商（例如，Hotmail）。

更令人惊讶的是，虽然大多数供应商允许伪造的电子邮件进入，但他们很少警告用户注意未经验证的发件人。 35 家供应商中只有 9 家实施了一些安全指标：8 家供应商在其网络界面（例如 Gmail）上有安全指标，只有 4 家供应商（例如 Naver）的移动应用程序具有一致的安全指标。如果用户使用 Microsoft Outlook 等第三方电子邮件客户端，则不会出现安全警告。更糟糕的是，某些电子邮件提供商具有误导性的 UI 元素，这些元素可以帮助攻击者使伪造的电子邮件看起来真实。例如，当攻击者欺骗现有联系人（或来自同一提供商的用户）时，35 家提供商中的 25 家将自动加载被欺骗的发件人的照片、名片或电子邮件历史记录以及伪造的电子邮件。这些 UI 设计本应提高电子邮件的可用性，但反过来又会帮助攻击者在发件人地址实际被欺骗时进行欺骗。

网络钓鱼实验。虽然少数电子邮件提供商已经实施了安全指标，但真正的问题是它们的有效性。我们使用用户研究（N = 488）来回答这个问题，参与者在界面上检查带有或不带有安全指示器的欺骗性网络钓鱼电子邮件。这是一个真实世界的网络钓鱼-在测试中仔细应用欺骗，以便用户在不知道电子邮件是实验的一部分（经 IRB 批准）的情况下检查欺骗性电子邮件。我们在实验后向用户汇报并征得他们的同意。

我们的结果表明，安全指标对减少有风险的用户操作有积极影响，但不能消除风险。当未显示安全指示器（受控组）时，在打开欺骗性电子邮件的所有用户中，48.9% 的用户最终点击了电子邮件中的钓鱼 URL。对于我们向其提供安全指标的另一组用户，相应的点击率略低（37.2%）。对于不同人口统计特征（年龄、性别、教育水平）的用户，这种影响始终是积极的。另一方面，鉴于 37.2% 的点击率，我们认为安全指标不能消除网络钓鱼风险。服务器端安全协议和用户端安全指标都应该得到改进，以最大限度地发挥影响。

贡献。我们有 3 个主要贡献：

- 首先，我们的端到端测量提供了有关电子邮件提供商如何处理伪造电子邮件的新见解。我们揭示了不同电子邮件提供商在电子邮件可用性和安全性之间的权衡
- 其次，我们是第一个根据经验分析安全指标在欺骗性电子邮件上的使用情况的公司。我们表明，大多数电子邮件提供商不仅缺乏必要的安全指标（尤其是在移动应用程序上），而且还具有帮助攻击者的误导性 UI。
- 第三，我们进行了真实世界的网络钓鱼测试，以评估安全指标的有效性。我们展示了安全指标的积极影响（和潜在问题），并提供了初步的改进指南。

本文中的定量结果提供了关于欺骗性电子邮件如何渗透主要电子邮件提供商并一路影响最终用户的端到端视图。我们希望这些结果可以引起社区更多的关注，以促进 SMTP 安全扩展的采用。此外，我们还寻求提高电子邮件提供商对设计和部署更有效的 UI 安全指标的关注，特别是针对保护较少的移动电子邮件应用程序。我们已经与Gmail团队沟通了结果，并提出了改进安全指标的建议。

2 背景和方法论

今天的电子邮件系统是建立在 SMTP 协议之上的，该协议最初设计时并没有考虑到安全性。

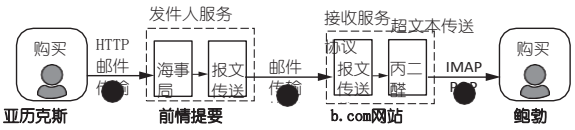


图 1：从 Alex 到 Bob 的电子邮件传输。

后来引入了安全扩展以提供机密性、完整性和真实性。下面，我们简单介绍一下 SMTP 和相关的安全扩展。然后我们介绍我们的研究问题和方法。

2.1 SMTP 和电子邮件欺骗

简单邮件传输协议（SMTP）是用于电子邮件传输的 Internet 标准[56]. 数字1 显示了传递电子邮件的三个主要步骤。（0）从发件人的邮件用户代理（MUA）开始，首先通过STMP或HTTP/HTTPS将消息传输到发件人服务提供商的邮件提交代理（MSA）。（@）然后发件人的邮件传输代理（MTA）使用 SMTP 将邮件发送到收件人的电子邮件提供商。（@）然后邮件传递代理（MDA）通过 Internet 消息访问协议（IMAP）、邮局协议（POP）或 HTTP/HTTPS 将邮件传递给接收用户。

最初设计时，SMTP 没有任何安全机制来验证发件人身份。因此，攻击者可以通过修改 SMTP 中的“MAIL FROM”字段轻松制作伪造的电子邮件来冒充/欺骗任意发件人地址。电子邮件欺骗是网络钓鱼攻击的关键步骤——通过将受信任的实体冒充为电子邮件发件人，攻击者更有可能获得受害者的信任。实际上，攻击者通常通过设置自己的 MTA 服务器来利用步骤（@）中的 SMTP。

或者，如果未仔细配置合法电子邮件服务，攻击者也可能利用步骤（0）。例如，如果 a.com 配置为开放中继，则攻击者可以使用 a.com 的服务器和 IP 发送冒充任何电子邮件地址的伪造电子邮件。

2.2 电子邮件认证

为了抵御电子邮件欺骗攻击，已经提出并标准化了各种安全扩展，包括 SPF、DKIM 和 DMARC。 BIMI 和 ARC 等新协议建立在 SPF、DKIM 和 DMARC 之上。在本文中，我们主要关注 SPF、DKIM 和 DMARC，因为它们在实践中已被电子邮件服务采用了一定程度。BIMI 和 ARC 还没有完全标准化，我们稍后再讨论 §7.

防晒系数。发件人策略框架（SPF）允许电子邮件服务（或组织）发布 IP 列表有权为其域发送电子邮件（RFC7208[40]). 例如，如果域“a.com”在 DNS 中发布了其 SPF 记录，则接收电子邮件服务可以检查此记录以将发件人 IP 与发件人电子邮件地址相匹配。这样只有授权的IP才能发送
电子邮件为“a.com”。此外，SPF 允许组织指定有关收件人应如何处理未通过身份验证的电子邮件的策略。

DKIM。 DomainKeys Identified Mail（DKIM）使用基于公钥的方法来验证电子邮件发件人（RFC6376[19]). 发件人的电子邮件服务将在电子邮件标头中放置一个数字签名，该数字签名由与发件人域关联的私钥签名。接收服务可以从 DNS 中检索发送方的公钥以验证签名。为了从 DNS 查询 DKIM 公钥，不仅需要域名，还需要一个选择器（DKIM 签名中的一个属性）。选择器用于允许同一域下的多个密钥，以实现更细粒度的签名控制。 DKIM 没有指定如果身份验证失败接收方应该采取什么操作。

DMARC。基于域的消息身份验证、报告和一致性（DMARC）建立在 SPF 和 DKIM（RFC7489[50]），它不是一个独立的协议。 DMARC 允许域管理所有者发布策略以指定接收方在传入电子邮件未通过 SPF 和 DKIM 检查时应采取的操作。此外，DMARC 支持从收件人到发件人的更系统的报告。域的 DMARC 记录在 DNS 中的 dmarc.domain.com 下可用。

2.3 研究问题与方法

尽管有可用的安全机制，但如果这些机制在实践中没有正确部署，那么重大挑战仍然存在。 2015 年进行的测量表明，SMTP 安全扩展的采用率远未令人满意[23, 27]. 在 Alexa 前 100 万个域中，只有 40% 发布了 SPF 记录，只有 1% 有 DMARC 政策。这些结果表明保护用户免受电子邮件欺骗是一项真正的挑战。首先，由于大量域未发布 SPF/DKIM 记录，电子邮件提供商无法可靠地检测到欺骗未受保护域的传入电子邮件。其次，即使域受 SPF/DKIM 保护，缺乏（严格的）DMARC 策略也会使接收服务器处于困难的境地。目前尚不清楚接收端的电子邮件提供商将如何处理未经验证的电子邮件。现有作品[23, 27] 主要关注服务器端的身份验证协议。但是服务端的检测和实际对用户的影响还有很大的差距。

地位	所有域# (%)	MX 域 # (%)
总域名	1,000,000 (100%)	792,556 (100%)
含防晒指数	492,300 (49.2%)	473,457
(59.7%) 有效 SPF	**448,741 (44.9%)**	430,504
(54.3%) 策略：软故障	272,642 (27.3%)	268,317
(33.9%) 政策：硬失败	**125,245 (12.5%)**	112,415
(14.2%) 政策：中性	49,798 (5.0%)	48,736 (6.1%)
政策：通过	1,056 (0.1%)	1,036
(0.1%) 有 DMARC	51,222 (5.1%)	47,737
(6.0%)		
有有效的 DMARC	**50,619 (5.1%)**	**47,159 (6.0%)**
政策：无	39,559 (4.0%)	36,984 (4.7%)
政策：拒绝	**6,016 (0.6%)**	**5,225 (0.7%)**
政策：检疫	5,044 (0.5%)	4,950 (0.6%)

表 1：Alexa 100 万个域的 SPF/DMARC 统计数据。数据收集于 2018 年 1 月。

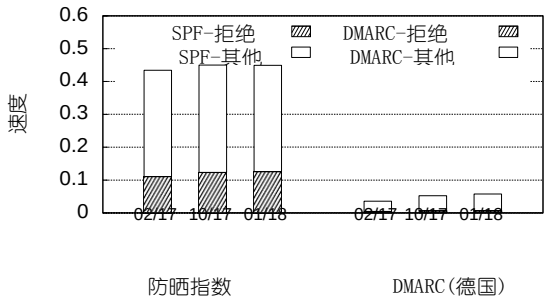


图 2：SPF 和 DMARC 的采用率三个快照中的 Alexa 100 万个域。

我们的问题。我们的研究旨在通过回答三个关键问题来重新审视电子邮件欺骗问题。（1）当电子邮件提供商在验证传入电子邮件时面临不确定性时，他们将如何处理这种情况？在什么情况下会向用户发送伪造的电子邮件？（2）一旦伪造的电子邮件到达收件箱，使用什么类型的警告机制（如果有的话）来通知用户未验证的发件人地址？（3）预警机制的有效性如何？回答这些问题对于了解欺骗攻击给用户带来的实际风险至关重要。

我们通过端到端欺骗实验回答问题（1）-（2）(§3, §4 和§5). 对于给定的电子邮件提供商，我们将其视为“黑匣子”。通过控制输入（例如，伪造的电子邮件）和监控输出（res inbox），我们推断出黑盒内的决策过程。我们通过进行大量用户研究来回答问题（3)(§6). 这个想法是让用户阅读带有和不带有安全指示器的欺骗/网络钓鱼电子邮件。伦理。我们已采取积极措施确保研究伦理。我们的衡量研究仅使用作者拥有的专用电子邮件帐户，没有真正的用户参与。此外，为了尽量减少对目标电子邮件服务的影响，我们仔细控制了邮件发送速率（每 10 分钟一封邮件），这与普通电子邮件用户没有什么不同。对于涉及“欺骗”的用户研究，我们与 IRB 密切合作进行实验设计。稍后将提供更详细的伦理讨论。

3 采用 SMTP 扩展

我们测量的高级目标是提供针对流行电子邮件提供商的电子邮件欺骗攻击的端到端视图。在此之前，我们首先检查 SMTP 安全扩展的近期采用率与三年前相比[23, 27]. 这有助于为电子邮件提供商在验证传入电子邮件时面临的挑战提供背景信息。

扫描 Alexa 排名前 100 万的域名。电子邮件身份验证要求发件人域将其 SPF/DKIM/DMARC 记录发布到 DNS。为了检查 SPF 和 DMARC 最近的采用率，我们抓取了 Alexa 前 100 万主机的 DNS 记录的 3 个快照[1] 2017 年 2 月、2017 年 10 月和 2018 年 1 月。类似于[23, 27], 此度量不适用于 DKIM，因为查询 DKIM 记录需要了解每个域的选择器信息。选择器信息仅在电子邮件标头中的 DKIM 签名中可用，这不是公开信息。我们稍后将在端到端测量中测量 DKIM 使用情况。

最近的采用率。桌子1 显示 2018 年 1 月最新快照的统计数据。 SPF 和 DMARC 的采用率都有一定的提高，但不是很显着。大约 44.9% 的域在 2018 年发布了有效的 SPF 记录（2015 年为 40%[27]), 5.1% 在 2018 年拥有有效的 DMARC 记录（2015 年为 1.1%[27]). 无效记录通常是由域管理员使用错误的 SPF/DMARC 记录格式引起的。另一个常见错误是 SPF（或 DMARC）有多个记录，根据 RFC7489，这相当于“无记录”[50]. 数字2 显示所有三个快照的采用率。同样，采用率一直在缓慢增长。

在 100 万个域中，有 792,556 个域是 MX 域（即托管电子邮件服务的邮件交换器域）。 MX 域之间的采用率略高（SPF 54.3%，DMARC 6.0%）。对于非 MX 域，我们认为发布 SPF/DMARC 记录也很重要。例如，office.com 不是 MX 域，但它托管 Microsoft Office 的网站。攻击者可以欺骗 office.com 来钓鱼 Microsoft Office 用户甚至员工。

失败的政策。 SPF 和 DMARC 都指定了有关接收方在身份验证失败后应采取的操作的策略。桌子1 显示只有一小部分域指定了严格的“拒绝”策略：12.5% 的域为 SPF 设置了“硬失败”，并且

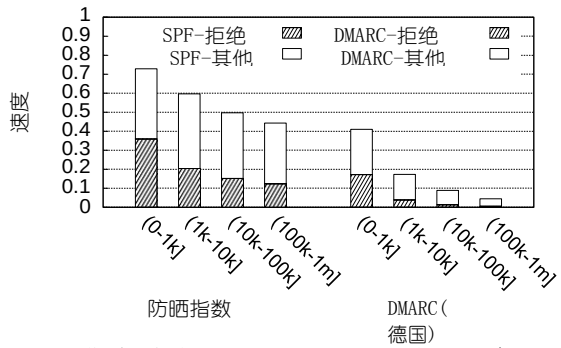


图 3：作为域的 Alexa 排名函数的采用率（2018 年 1 月）。

0.6% 为 DMARC 设置“拒绝”。其余域只需将决定留给电子邮件接收者。 “软失败”/“隔离”意味着电子邮件接收者应谨慎处理电子邮件。 “中性”/“无”表示未指定政策。 SPF的“pass”是指收件人应该让邮件通过。如果域同时具有 SPF 和 DMARC 策略，只要 DMARC 策略不是“无”，DMARC 就会覆盖 SPF。

使用 DKIM 的域还需要通过 DMARC 发布其策略。事实上，只有 5.1% 的域具有有效的 DMARC 记录，而 0.6% 的域具有“拒绝”策略，这表明大多数 DKIM 采纳者也没有指定严格的拒绝策略。

热门域名。毫不奇怪，如图所示，流行的采用率更高3.我们将前 100 万个域划分为对数大小的容器。对于 SPF，前 1,000 个域的采用率为 73%。对于 DMARC，前 1000 个域的采用率为 41%。这表明流行域的管理员更有动力防止他们的域被欺骗。尽管如此，仍有大量（流行的）域未受到保护。

4 端到端欺骗实验

鉴于目前 SMTP 扩展协议的采用率，电子邮件提供商要可靠地验证所有传入电子邮件仍然具有挑战性。当遇到有问题的电子邮件时，我们很好奇电子邮件提供商是如何做出此类决定的。在下文中，我们详细描述了我们的测量方法和程序。

4.1 实验设置

我们对数十亿用户使用的流行电子邮件提供商进行端到端欺骗实验。如图4，对于给定的电子邮件提供商 (B.com)，我们在 B.com 下设置一个用户帐户作为电子邮件接收者 (test@B.com)。然后我们建立一个实验

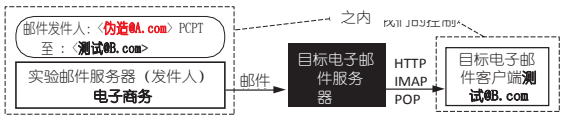


图 4：端到端欺骗实验设置。我们使用我们的服务器 E.com 通过欺骗 A.com 向目标电子邮件服务 B.com 发送伪造的电子邮件。

服务器 (E.com) 将伪造的电子邮件发送到接收者帐户。我们的服务器运行 Postfix 邮件服务[3] 迪-

使用 SMTP 直接与目标邮件服务器交互。通过控制输入（伪造的电子邮件）和观察输出（接收者帐户），我们推断出目标电子邮件服务内部的决策过程。

选择目标电子邮件提供商。本研究着重于流行和公共电子邮件服务，有两个考虑因素。首先，超过 10 亿用户使用 Yahoo Mail 和 Gmail 等流行的电子邮件服务[46, 55]. 他们的安全政策和设计选择可能会影响更多的人。其次，要进行端到端的实验，我们需要从接收端收集数据。公共电子邮件服务允许我们创建一个帐户作为收件人。我们的实验方法适用于私人电子邮件服务，但需要内部用户的协作。

为了获得流行的公共电子邮件服务列表，我们参考了 Adobe 泄露的用户数据库（1.52 亿个电子邮件地址，930 万个唯一电子邮件域）[41]. 我们根据受欢迎程度对电子邮件域进行排名，并手动检查了前 200 个域（占所有电子邮件地址的 77.7%）。合并来自同一服务（例如 hotmail.com 和 outlook.com）的域并排除不允许我们创建帐户的服务后，我们获得了 28 个电子邮件域的简短列表。为了包括最近的公共电子邮件服务，我们在 Google 上搜索并添加了 6 个服务（yeah.net 、protonmail.com 、 tutanota.com 、 zoho.com 、fastmail.com 和 runbox.com）。我们注意到 Google 的 Gmail 和 Inbox 具有非常不同的电子邮件界面，我们将它们视为两种服务。

我们总共有 35 种流行的电子邮件服务，覆盖 Adobe 数据库中的 9980 万个电子邮件地址 (65.7%)。作为附加参考，我们还分析了 Myspace 数据库（1.314 亿个电子邮件地址）[54]. 我们发现 1.018 亿个电子邮件地址（77.5%）来自 35 个电子邮件服务，证实了它们的受欢迎程度。电子邮件提供商的列表显示在表中2

4.2 实验参数

为了检查不同的因素如何影响电子邮件欺骗的结果，我们对实验应用了不同的配置。我们主要关注那些参数

可能会影响欺骗结果，包括欺骗的发件人地址、电子邮件内容、发件人 IP 和收件人的电子邮件客户端（用户界面）。

欺骗性发件人地址。发件人地址是身份验证的关键部分。例如，如果欺骗域 (A.com) 具有有效的 SPF/DKIM/D-MARC 记录，则接收方（理论上）能够检测到欺骗。我们为欺骗的发件人域配置三个配置文件：（1）无：没有 SPF/DKIM/D-MARC 记录（例如，thepiratebay.org）；（2）Relaxed：具有"无"政策的 SPF/DKIM（例如，tumblr.com）；（3）严格：具有严格"拒绝"政策的 SPF/DKIM（例如，facebook.com）。对于每个配置文件，我们从 Alexa 前 5000 个域中随机选择 10 个域（总共 30 个域）（详细列表在附录 A 中）。

电子邮件内容。电子邮件内容会影响垃圾邮件过滤器处理传入电子邮件的方式[11]. 请注意，我们的实验并不是要对垃圾邮件过滤器如何对不同的关键字进行加权进行逆向工程，这几乎是一个无限的搜索空间。相反，我们专注于欺骗（伪造发件人地址）。我们希望将垃圾邮件过滤器的影响降到最低，并检查地址伪造（欺骗）单独如何影响接收者的决定。

为此，我们为研究配置了 5 种不同类型的电子邮件内容：(1) 一封空白电子邮件，(2) 一封带有良性 URL (http://google.com) 的空白电子邮件，(3) 一封带有良性附件（空文本文件）。然后我们有 (4) 一封包含实际内容的良性电子邮件。这封电子邮件是一封真实世界的合法电子邮件，用于通知同事会议时间的变更。使用"良性"内容的原因是要测试单独的"欺骗"因素对电子邮件提供商的决定有多大影响。此外，为了测试钓鱼邮件是否可以渗透目标服务，我们还包括 (5) 一封带有钓鱼内容的邮件。这封钓鱼邮件是最近针对我们机构的一次钓鱼攻击的真实样本。该电子邮件冒充技术支持人员通知受害者她的内部帐户已被暂停，并要求她使用 URL（到 Amazon EC2 服务器）重新激活该帐户。

发件人IP。发件人邮件服务器的 IP 地址也可能影响欺骗成功。我们配置一个静态IP地址和一个动态IP地址。通常，邮件服务器需要托管在静态 IP 上。实际上，攻击者可能会使用动态 IP 来降低成本。

电子邮件客户端。 我们检查不同的电子邮件客户端如何警告用户伪造的电子邮件。我们考虑 3 种常见的电子邮件客户端：(1) 网络客户端，(2) 移动应用程序，以及 (3) 第三方电子邮件客户端。所有 35 项选定的服务都有网络界面，28 项服务有专门的移动应用程序。第三方客户端是指电子邮件应用程序-

允许用户检查来自任何电子邮件提供商的电子邮件的应用程序（例如，Microsoft Outlook 和 Apple Mail）。

5 欺骗实验结果

在本节中，我们将描述我们的实验结果。首先，为了提供上下文，我们测量了目标电子邮件提供商用来检测伪造电子邮件的身份验证协议。然后，我们检查电子邮件提供商如何处理伪造的电子邮件并确定决策制定中的关键因素。对于到达收件箱的电子邮件，我们检查电子邮件提供商是否以及如何警告用户他们的潜在风险。请注意，在本节中，所有实验结果都反映了截至 2018 年 1 月目标电子邮件服务的状态。

5.1 认证机制

为了更好地解释结果，我们首先检查 35 个电子邮件提供商如何验证传入的电子邮件。了解他们的身份验证协议的一种方法是分析电子邮件标头并查找 SPF/DKIM/D-MARC 身份验证结果。然而，并非所有的电子邮件提供商都将身份验证结果添加到标题中（例如，qq.com）相反，我们遵循更可靠的方法[27]通过为我们自己的域设置权威 DNS 服务器并从我们的域发送电子邮件。同时，权威DNS服务器会观望目标邮件服务是否查询SPF/DKIM/DMARC记录。我们将 SPF、DKIM 和 DMARC 记录的 TTL 设置为 1（秒），以强制目标电子邮件服务始终查询我们的权威 DNS 服务器。结果见表2 （左 4 列）。 35 个电子邮件提供商可根据其协议分为 3 类：

- 完全身份验证 (16)：执行所有三种身份验证检查（SPF、DKIM 和 DMARC）的电子邮件服务。此类别包括最流行的电子邮件服务，例如 Gmail、Hotmail 和 iCloud。
- SPF/DKIM 但没有 DMARC (15)：检查 SPF/DKIM 但不检查发件人的 DMARC 策略的电子邮件服务。这些电子邮件服务可能会自行做出决定。
- 无身份验证 (4)：不执行三种身份验证协议中的任何一种的电子邮件服务。

5.2 关于伪造电子邮件的决定

接下来，我们检查伪造电子邮件的决策过程。对于 35 个目标电子邮件服务中的每一个，我们测试所有可能的参数设置组合

（30个欺骗地址×5种邮件内容×2个IP

电子邮件供应商	支持的协议 防晒指数 金 DMARC(德国)	全面的速度 n=1500	知识产权 静止的 750	知识产权 动态的 750	欺骗地址配置文件 没有任何的 500	欺骗地址配置文件 严格的 500	欺骗地址配置文件 有关 500	电子邮件内容 大块 300	电子邮件内容 网址 300	电子邮件内容 阿塔。 300	电子邮件内容 良性 300	电子邮件内容 网络钓鱼。 300
邮件. ru		0.69	0.69	0.69	1.00	0.99	0.07	0.70	0.69	0.69	0.68	0.68
fastmail.com网站		0.66	1.00	0.32	0.70	0.65	0.64	0.67	0.66	0.67	0.67	0.65
163.com		0.58	0.66	0.50	0.73	0.54	0.47	0.53	0.60	0.45	0.66	0.66
126.com		0.57	0.66	0.48	0.74	0.54	0.43	0.54	0.56	0.46	0.65	0.64
gmail.com		0.53	0.56	0.51	0.93	0.66	0.00	0.58	0.58	0.50	0.60	0.40
gmail收件箱		0.53	0.56	0.51	0.93	0.66	0.00	0.58	0.58	0.50	0.60	0.40
naver.com(浏览网站)		0.50	0.50	0.51	0.95	0.56	0.00	0.51	0.50	0.50	0.50	0.50
是的.net		0.36	0.51	0.21	0.44	0.38	0.26	0.23	0.35	0.34	0.61	0.28
图塔诺塔网		0.36	0.41	0.30	0.90	0.17	0.00	0.39	0.39	0.20	0.39	0.39
雅虎网		0.35	0.67	0.03	0.52	0.52	0.00	0.33	0.34	0.33	0.38	0.35
收件箱.lv		0.32	0.63	0.00	0.50	0.45	0.00	0.32	0.32	0.32	0.32	0.32
质子号航空母舰		0.30	0.60	0.00	0.45	0.45	0.00	0.32	0.26	0.29	0.31	0.32
seznam.cz网站		0.24	0.48	0.00	0.35	0.25	0.13	0.35	0.35	0.35	0.08	0.08
美国在线		0.18	0.16	0.19	0.29	0.25	0.00	0.24	0.20	0.22	0.23	0.00
icloud.com网站		0.07	0.10	0.04	0.11	0.09	0.00	0.01	0.01	0.01	0.17	0.14
hotmail.com		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
君诺网		1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
新浪网		0.79	0.79	0.79	1.00	0.60	0.76	0.80	0.79	0.78	0.79	0.78
op.pl		0.71	0.71	0.71	1.00	0.72	0.40	0.71	0.71	0.71	0.71	0.71
SAP.pt		0.59	0.67	0.50	0.91	0.54	0.31	0.64	0.53	0.49	0.63	0.64
zoho.com		0.58	0.57	0.58	0.99	0.54	0.21	0.59	0.54	0.59	0.59	0.59
腾讯网		0.43	0.80	0.06	0.57	0.42	0.29	0.43	0.44	0.43	0.41	0.43
我的网		0.35	0.63	0.07	0.04	0.28	0.37	0.47	0.35	0.07	0.43	0.43
gmx.com网站		0.27	0.54	0.00	0.38	0.27	0.17	0.30	0.06	0.30	0.35	0.35
邮件.com		0.27	0.54	0.00	0.37	0.27	0.17	0.29	0.06	0.30	0.35	0.35
daum.net		0.27	0.52	0.01	0.33	0.29	0.18	0.28	0.26	0.27	0.27	0.25
runbox.com		0.24	0.48	0.00	0.28	0.26	0.19	0.25	0.00	0.00	0.48	0.48
interia.pl		0.14	0.28	0.00	0.20	0.14	0.08	0.01	0.00	0.00	0.36	0.34
o2.pl		0.12	0.20	0.04	0.22	0.12	0.02	0.23	0.03	0.23	0.07	0.03
wp.pl		0.11	0.20	0.04	0.20	0.12	0.02	0.23	0.03	0.23	0.04	0.03
搜狐网		0.03	0.03	0.03	0.02	0.03	0.03	0.04	0.04	0.01	0.03	0.03
在线测试		1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
excite.com网站		1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
免费邮箱.hu		0.99	0.99	0.99	1.00	1.00	0.96	0.97	1.00	0.97	1.00	1.00
rediffmail.com		0.78	0.79	0.78	0.74	0.80	0.80	0.76	0.79	0.76	0.79	0.79

表 2：到达收件箱的电子邮件比率（收件箱率）。我们分解了具有不同配置参数（发件人 IP、发件人地址的 SPF/DKIM/DMARC 配置文件和电子邮件内容）的电子邮件的收件箱率。

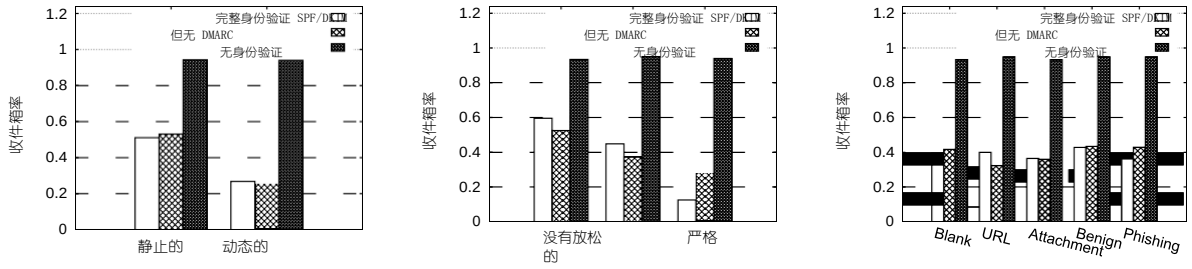
地址），然后重复实验 5 次。每个电子邮件服务接收 300 5 = 1,500 封电子邮件（总共 52,500 封电子邮件）。我们打乱了所有电子邮件并以随机顺序发送它们。我们还设置了 10 分钟的发送时间间隔（每个电子邮件服务），以尽量减少对目标邮件服务器的影响。该实验于 2017 年 12 月至 2018 年 1 月进行。请注意，与每天通过互联网发送的数千亿封电子邮件相比，实验中的电子邮件数量被认为非常低[5]. 我们有意限制我们的实验规模，以便实验电子邮件不会以任何重大方式影响目标服务（及其电子邮件过滤器）。随机顺序和较慢的发送速度有助于减少较早的电子邮件对实验中较晚的电子邮件的影响。

实验结束后，我们依靠 IMAP/POP 从目标电子邮件提供商处检索电子邮件。对于一些不支持 IMAP 或 POP 的提供商，我们使用基于浏览器的爬虫直接通过 Web 界面检索电子邮件。如表所示2,我们根据支持的身份验证协议对电子邮件提供商进行分组。在每个组中，我们根据收件箱率对电子邮件提供商进行排名，收件箱率是到达收件箱的电子邮件与已发送电子邮件总数的比率。未到达收件箱的电子邮件是 ei-

它们被放入垃圾邮件文件夹或被电子邮件提供商完全阻止。

收件箱中电子邮件的比例。桌子2 表明可以成功渗透绝大多数电子邮件服务。 35 个电子邮件服务中的 34 个允许至少一封伪造的电子邮件到达收件箱。唯一的例外是 Hotmail，它阻止了所有伪造的电子邮件。 35 项服务中有 33 项允许至少一封网络钓鱼电子邮件进入收件箱。特别是，网络钓鱼电子邮件已经渗透到执行完全身份验证的电子邮件提供商（例如 Gmail、iCloud、Yahoo Mail），这些电子邮件提供商在欺骗没有严格拒绝 DMARC 策略的发件人域时。 此外， juno.com 、 t-online.de 和 excite.com 等提供商根本没有阻止收件箱率为 100% 的伪造电子邮件。 juno.com 实际上检查了 SPF 和 DKIM。这表明即使电子邮件提供商可能已经检测到电子邮件伪造，他们仍然会将电子邮件发送到用户收件箱。

接收方身份验证的影响。桌子2 显示电子邮件提供商的身份验证方法会影响欺骗结果。对于不执行身份验证的电子邮件提供商，聚合收件箱率为 94.2%。相比之下，执行完全身份验证的电子邮件提供商的总收件箱率要低得多



(a) 发件人IP (b) 发件人地址 SPF/DK./DMA。轮廓 (c) 电子邮件内容

图 5：到达用户收件箱的电子邮件的总比率（收件箱率）。图例显示接收者的 3 个身份验证组。每个子图显示具有特定配置的电子邮件的细分结果。

(39.0%) 和仅执行 SPF/D-KIM (39.3%) 的电子邮件提供商。为了检查差异的统计显着性，我们对发送给三种电子邮件提供商的电子邮件应用了卡方检验。结果证实，与具有统计显着性的其他两组相比，电子邮件更有可能到达“无身份验证”提供者的收件箱（均 $p < 0.01$）。

然而，“完全认证”电子邮件提供商和“仅 SPF/DKIM”电子邮件提供商之间的差异在统计上并不显着 ($p = 0.495$)。这表明 DMARC 检查的影响相对较小。桌子2 显示 DMARC 检查主要影响欺骗域具有“严格”拒绝策略的电子邮件。然而，即使经过完全验证，这些邮件的收件箱率也不总是 0.00（例如 mail.ru 、 fastmail.com 、 163.com 、 126.com 、 yeah.net、seznam.cz）。这是因为某些电子邮件提供商会将 DMARC 政策视为“建议的行动”，但并不总是执行该政策。

发件人 IP 的影响。为了更好地说明不同电子邮件配置的影响，我们绘制了图5.我们首先根据身份验证方法（3 组）对目标电子邮件提供商进行分组，然后计算特定配置设置的聚合收件箱率。如图5(a), 与来自动态 IP 的电子邮件 (33.9%) 相比，从静态 IP 发送的电子邮件更有可能到达收件箱 (56.9%)。卡方统计分析显示差异具有统计学意义 ($p < 0.0001$)。然而在实践中，动态 IP 仍然是攻击者的一个可行选择，因为它们更便宜。

为确保结果的有效性，我们进行了额外的分析以确保我们的 IP 在实验期间未被列入黑名单。更具体地说，我们分析我们的实验痕迹以监控整个实验过程的收件箱率。在我们的实验中，每个电子邮件服务都会收到 1500 封电子邮件，并且我们检查了一段时间内每 100 封电子邮件的收件箱率。如果我们的 IP
在实验过程中被列入黑名单，应该有
收件箱率在某个时候急剧下降。我们做了在任何经过测试的电子邮件服务中都没有观察到这一点。我们还检查了 94 个公共黑名单[2]，而我们的 IP 不在其中任何一个上。

欺骗性发件人域的影响。数字5(b) 演示了欺骗性发件人地址的影响。总体而言，欺骗没有 SPF/DKIM/DMARC 记录的发件人域会产生更高的收件箱率 (60.5%)。使用 SPF/DKIM 和“宽松”失败策略欺骗发件人域具有较低的收件箱率 (47.3%)。毫不奇怪，具有 SPF/D-KIM 记录和“严格”拒绝政策的域是最难欺骗的（收件箱率为 28.4%）。卡方统计分析显示差异显着 ($p < 0.00001$)。结果证实了发布 SPF/DKIM/DMARC 记录的好处。但是，发布这些记录并不能完全防止被欺骗，因为电子邮件提供商可能仍会发送未通过 SPF/DKIM 身份验证的电子邮件。

电子邮件内容的影响。数字5(c) 显示不同电子邮件内容的收件箱率差别不大。差异很小但并非偶然（卡方检验 $p < 0.00001$）。这表明我们的结果不依赖于为研究选择的特定电子邮件内容。回想一下，我们专门使用看似良性的内容来最大限度地减少垃圾邮件过滤器的影响，以便我们可以测试“欺骗”因素对电子邮件提供商的决定有多大影响。这并不意味着电子邮件内容对决策制定没有影响。相反，如果一封电子邮件有一个列入黑名单的 URL 或一个已知的恶意软件作为附件，我们预计会有更多的电子邮件被阻止（这不是我们的研究目的）。我们的结果简单地表明，当今的攻击者可以轻松地应用欺骗来进行有针对性的鱼叉式网络钓鱼。在鱼叉式网络钓鱼的背景下，攻击者将使用尚未列入黑名单的 URL 制作看似良性的内容是一个合理的假设[33].

对因素进行排名。为了确定哪些因素对成功渗透的贡献更大，我们执行

[2]https://mxtoolbox.com/blacklists.aspx

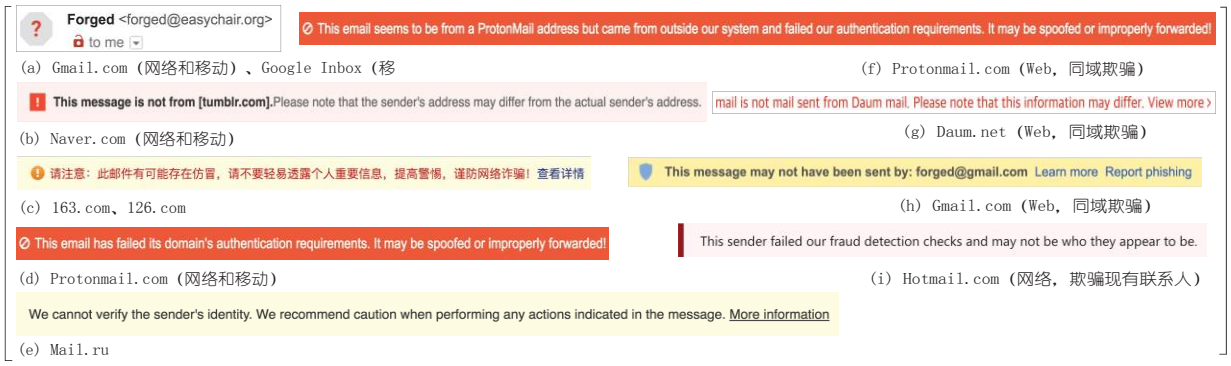


图 6：来自 9 个电子邮件提供商的伪造电子邮件的安全指标。 (a)–(e) 适用于常规的伪造电子邮件。(f)–(h) 只有当被欺骗的发送者和接收者属于同一个提供者时才会出现。 (i) 仅在欺骗现有联系人时显示。

特征	志^2	相互信息
收件人认证方式	6497.93	0.0707
欺骗性发件人地址	3658.72	0.0356
发件人IP	2799.51	0.0269
邮件内容	115.27	0.0011

表 3：特征排名。

“特征排名”分析。我们将所有电子邮件分为两类：正面（收件箱）和负面（垃圾邮件文件夹或已阻止）。对于每封电子邮件，我们计算四个特征：电子邮件内容（F_1）、发件人地址配置文件（F_2）、收件人身份验证组（F_3）和发件人IP（F_4），所有这是分类变量。然后我们根据特征的区分能力对特征进行排名，使用标准指标将电子邮件分为两类：卡方统计[45]和互信息[17]. 如表所示3, 一致地，“接收方身份验证方法”是最重要的因素，其次是“欺骗性发件人地址”。请注意，此分析仅比较我们实验中因素的相对重要性。我们并不是要对完整的防御系统进行逆向工程，这需要分析更多的特性。

讨论。发件人和收件人都需要进行可靠的电子邮件身份验证。当其中之一未能完成工作时，伪造的电子邮件更有可能到达收件箱。此外，电子邮件提供商倾向于优先考虑电子邮件交付而不是安全。当电子邮件未通过身份验证时，只要欺骗域的策略不是“拒绝”，大多数电子邮件提供商（包括 Gmail 和 iCloud）仍会发送电子邮件。根据之前的测量结果(§3), 100 万个域中只有 13% 设置了“拒绝”或“硬失败”策略，这为攻击者执行欺骗留下了充足的空间。

我们的分析还揭示了两个电子邮件服务（sapo.p 和 runbox.com）中的漏洞，这将允许攻击者通过电子邮件发送欺骗性电子邮件提供商的 IP。由于这是一个不同的威胁模型，我们在附录 B 中讨论了此漏洞的详细信息。

5.3 电子邮件客户端和安全指示器 对于到达用户收件箱的电子邮件，我们接下来检查电子邮件界面上的安全指示器以警告用户。结果再次代表了截至 2018 年 1 月的电子邮件服务状态。

网络客户端。我们发现只有 6 个电子邮件服务在伪造的电子邮件上显示了安全指示器，包括 Gmail、protonmail 、 naver 、 mail.ru 、 163.com 和 126.com（图6 (a)–(e)）。其他电子邮件服务会在没有任何视觉警告的情况下显示伪造的电子邮件（例如 Yahoo Mail、iCloud）。特别是Gmail和Google Inbox是同一家公司的，但是网页版的Google Inbox没有安全提示。 Gmail 的指示器是发件人图标上的一个“问号”。只有当用户将鼠标移到图像上时，它才会显示以下消息：“Gmail 无法验证 <sender> 是否确实发送了此邮件（而不是垃圾邮件发送者）”。红色锁图标与欺骗无关，但表示 MX 服务器之间的通信未加密。另一方面，naver、163.com 和 protonmail 等服务使用露骨的短信来警告用户。

移动客户端。更少的移动电子邮件应用程序采用了安全指标。在具有专用移动应用程序的 28 种电子邮件服务中，只有 4 种服务具有移动安全指标，包括 naver、protonmail、Gmail 和 google inbox。其他服务删除了移动用户的安全指标。与网络界面相比，移动应用程序的屏幕尺寸非常有限。开发人员经常删除“不太重要”的信息以保持界面简洁。不幸的是，安全指示器是被删除的元素之一。

误导性用户界面	电子邮件提供商（35 家中的 25 家）
发件人照片（6）	G-收件箱、Gmail、zoho、icloud*、gmx†、mail.com†
名片（17）	雅虎，hotmail，tutanota，seznam.cz，fastmail，gmx，mail.com，Gmail*，新浪*，君诺*，美国在线*，163.com†，126.com†，yes.net†，搜狐†，导航†，佐禾†
电子邮件历史（17）	hotmail，163.com，126.com，yes.net，qq，zoho，mail.ru，雅虎*，Gmail*，

表 4：攻击者欺骗现有联系人时的误导性 UI 元素。（）仅表示网页界面。（†）*表示仅限移动设备。

第三方客户端。最后，我们使用第三方客户端检查电子邮件，包括 Microsoft Outlook、Apple Mail 和 Yahoo Web Mail。我们测试了桌面版和移动版，发现它们都没有为伪造的电子邮件提供安全指标。

5.4 误导性的 UI 元素

我们发现攻击者可以触发误导性的 UI 元素，使伪造的电子邮件看起来很逼真。

欺骗现有联系人。 当攻击者欺骗收件人的现有联系人时，伪造的电子邮件可以自动加载误导性的 UI 元素，例如联系人的照片、名片或以前的电子邮件对话。我们进行如下快速实验：首先，我们为 35 个电子邮件服务中的每个接收者帐户创建一个“现有联系人”(contact@vt.edu)，并添加姓名、个人资料照片和电话号码（如果允许）。然后我们伪造此联系人的地址（contact@vt.edu）以发送伪造的电子邮件。桌子4 显示了具有误导性 UI 的 25 个电子邮件提供商。示例屏幕截图显示在附录 C 中。我们认为这些设计旨在通过为发件人提供上下文来提高电子邮件服务的可用性。然而，当发件人地址实际被欺骗时，这些 UI 元素将帮助攻击者使伪造的电子邮件看起来更真实。

此外，欺骗现有联系人可以让伪造的电子邮件渗透到新的电子邮件提供商。例如，Hotmail 阻止了表中的所有伪造电子邮件2. 然而，当我们欺骗现有联系人时，Hotmail 会将伪造的电子邮件发送到收件箱并添加一个特殊的警告标志，如图所示6(i).

同域欺骗。 触发误导性 UI 元素的另一种方法是伪造与收件人属于同一电子邮件提供商的电子邮件地址。例如，当欺骗<伪造@seznam.cz>发送电子邮件至<test@eznam.cz>，将自动加载欺骗发件人的个人资料照片。自从

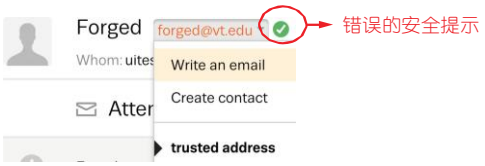


图 7：Seznam.cz 在伪造地址上显示“可信地址”标志。

欺骗性发件人来自同一电子邮件提供商，电子邮件提供商可以直接从自己的数据库中加载发件人的照片。这种现象也适用于 Google Inbox 和 Gmail（移动）。但是，电子邮件提供商还会使用特殊的安全指示器提醒用户。如图6(f)-(h), 相关的电子邮件提供商包括 protonmail、Gmail 和 daum.net。加上之前观察到的安全指标，总共有 9 家电子邮件提供商至少提供了一种类型的安全指标。

错误的安全指标。 一家电子邮件提供商 seznam.cz 向用户显示虚假的安全指示器。seznam.cz 执行完全身份验证，但仍将欺骗性电子邮件发送到收件箱。数字7 显示 seznam.cz 在发件人地址上显示绿色复选标记，即使该地址是伪造的。当用户点击该图标时，它会显示“可信地址”，这很可能会给用户一种安全的错觉。

6 安全指标的有效性

作为一项端到端的研究，我们接下来检查最后一跳——用户对欺骗电子邮件的反应。到目前为止，我们的结果表明，一些电子邮件提供商已经在电子邮件界面上实施了可视化安全指示器，以警告用户伪造电子邮件。在下文中，我们试图了解这些安全指标如何有效地提高用户检测欺骗性网络钓鱼电子邮件的效率。

6.1 实验方法

为了评估安全指标的有效性，我们设计了一个实验，参与者会收到一封带有伪造发件人地址的网络钓鱼电子邮件。通过控制界面上的安全指标，我们评估安全指标如何帮助用户安全地处理钓鱼邮件。

实施这个想法面临一个关键挑战，即捕捉用户对电子邮件的真实反应。理想情况下，参与者应该在不知道自己正在进行实验的情况下检查网络钓鱼电子邮件。但是，这会导致实际困难，无法进行用户研究并事先获得知情用户同意。到

为此，我们将欺骗引入研究方法。在高层次上，我们在研究之前和期间使用分散注意力的任务来隐藏研究的真正目的。然后在研究完成后，我们向用户汇报以获得知情同意。我们与我们的 IRB 密切合作，遵循道德规范进行网络钓鱼测试。

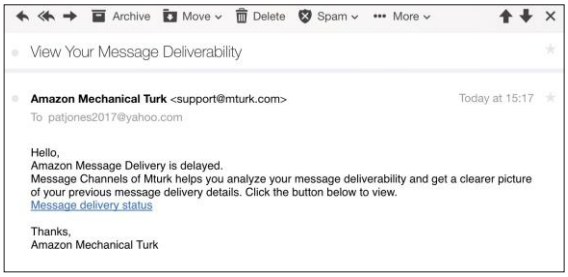
程序。我们将这项研究作为一项调查来了解用户的电子邮件习惯。真正的目的对参与者是隐藏的。本研究包含两个阶段。阶段 1 是设置欺骗，阶段 2 进行网络钓鱼实验。

Phase1： 参与者首先输入他们自己的电子邮件地址。然后我们立即向参与者发送一封电子邮件，并指示参与者从他们的电子邮件帐户中查看这封电子邮件。电子邮件包含一个跟踪像素（一个 1 1 透明图像）来衡量电子邮件是否已被打开。之后，我们会询问有关电子邮件的几个问题（以确保他们确实打开了电子邮件）。然后我们会询问其他关于他们的电子邮件使用习惯的分散注意力的调查问题。Phase1 有三个目的：(1) 确保参与者实际拥有电子邮件地址；(2) 测试跟踪像素是否有效，考虑到一些用户可能将他们的电子邮件服务配置为阻止图像和 HTML；(3)设置欺骗。在 phase1 之后，我们给参与者的印象是调查已经完成（参与者在 phase1 之后得到报酬）。这样，参与者就不会期望收到第二封钓鱼邮件。

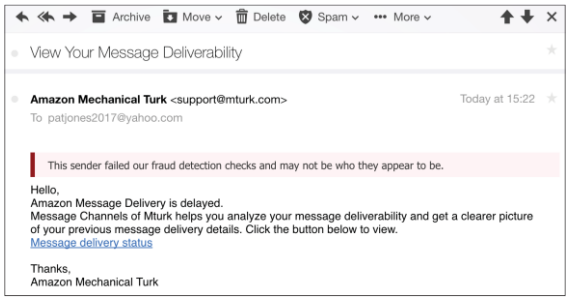
阶段 2： 我们等待 10 天并发送钓鱼邮件。钓鱼邮件包含指向我们自己服务器的良性URL，以衡量该URL是否被点击。此外，电子邮件正文包含一个跟踪像素，用于衡量电子邮件是否已被打开。如图8，我们冒充 Amazon Mechanical Turk 的技术支持 (support@mturk.com) 发送网络钓鱼电子邮件，告知一些技术问题。这封邮件之前其实是针对我们自己的机构的。网络钓鱼电子邮件仅发送给电子邮件服务未配置为阻止 HTML 或跟踪像素（基于阶段 1）的用户。

我们再等 20 天来监控用户点击。研究结束后，我们发送一封汇报电子邮件，解释实验的真正目的并获得知情同意。参与者可以随时撤回他们的数据。在我们提交时，没有用户要求撤回他们的数据。

安全指标。根据我们之前的测量结果，大多数电子邮件服务都采用了基于文本的指标（图6(b)-(i)）. 就连Gmail的特殊指标（图6(a)）当用户将鼠标移到上方时将显示一条文本消息。为此，我们使用基于文本的指示器并进行两项设置，即与安全性



(a) 不带安全指示灯



(b) 带安全指示灯

图 8：网络钓鱼电子邮件屏幕截图。

指示器和不带安全指示器。对于没有安全指标的群体，我们从雅虎邮箱中招募用户。我们选择 Yahoo Mail 用户是因为 Yahoo Mail 是最大的电子邮件服务，没有实施任何安全指标。对于有安全指标的对照组，为了保持一致性，我们仍然招募了雅虎邮箱用户，并在界面中添加了我们自己的安全指标。更具体地说，在发送电子邮件时，我们可以在电子邮件正文中嵌入一段 HTML 代码，以显示基于文本的指示器。这正是大多数电子邮件提供商在电子邮件正文中插入视觉指示符的方式（Gmail 除外）。

在 phase2 中，我们无法控制用户是否会使用移动应用程序或网站来阅读电子邮件。这对雅虎邮箱用户来说不是什么大问题。雅虎的网络和移动客户端都默认呈现 HTML。基于文本的指示器由我们嵌入到电子邮件正文中，它将为网络和移动用户一致显示（通过我们自己的测试确认）。

招募参与者。为了从阶段 2 收集足够的数据点，我们需要招募大量用户，因为许多用户可能不会打开我们的电子邮件。我们选择最受欢迎的众包平台 Amazon Mechanical Turk (MTurk) 来招募参与者。MTurk 用户比其他 Internet 样本和大学生样本稍微多样化一些。使用 Amazon Mechanical Turk 可能会在用户群体方面引入偏见。然而，据报道，多样性比调查大学生更好[9]. 为了避免不认真的用户，我们应用筛选标准

阶段	用户	没有起诉书。	带起诉书。
阶段1	所有参与者	243	245
	不块像素	176	179
阶段2	打开的电子邮件	94	86
	点击网址	46	32
点击率	全面的	26.1%	17.9%
	打开电子邮件后	48.9%	37.2%

表 5：用户研究统计数据。

用户	无指示器		带指示灯	
	桌面	移动的	桌面	移动的
打开的电子邮件	45	49	41	45
点击网址	21	25	15	17
点击率	46.7%	51.0%	36.6%	37.8%

表 6：不同用户代理的用户研究统计数据。

在 MTurk 中常用的[10, 28]. 我们从美国招募用户，这些用户的最低人类智能任务（HIT）支持率为 90%，并且批准的 HIT 超过 50 个。

总的来说，我们从 MTurk 招募了 N = 488 名用户：243 名用户用于“无安全指标”设置，另外 245 名用户用于“有安全指标”设置。每个用户只能参与一次设置，仅可获得 0.5 美元。在招聘信中，我们明确告知用户我们需要收集他们的电子邮件地址。这可能会引入自我选择偏差：我们可能会招募愿意与我们的研究团队分享电子邮件地址的人。尽管存在潜在的偏见，但由此产生的用户人口统计数据非常多样化：49% 是男性，51% 是女性。大多数参与者年龄在 30-39 岁（39.1%），其次是 29 岁以下（31.8%）、50 岁以上（14.5%）和 40-49 岁（14.5%）的用户。大多数参与者具有本科学历（35.0%）或大专学历（33.8%），其次是研究生学历（20.7%）和高中学历（10.5%）。

道德准则。我们的研究获得了 IRB 的批准，我们已采取积极措施保护参与者。首先，只有良性 URL 被放置在指向我们自己的服务器的电子邮件中。单击 URL 不会给参与者或其计算机带来实际风险。虽然我们可以看到参与者的 IP，但我们选择不将 IP 信息存储在我们的数据集中。此外，我们按照 IRB 的推荐做法进行了欺骗性实验。在实验说明中，我们仅在绝对必要时才省略信息（例如，研究的目的和第二封电子邮件的详细信息）。提前披露此类信息将使我们的结果无效。实验结束后，我们立即与参与者联系，解释我们的真正目的和详细过程。我们为参与者提供选择退出的机会。选择退出的用户仍会获得全额付款。

6.2 实验结果

我们分析实验结果以回答以下问题。一、安全指标的有效性如何保护用户？其次，安全指标的影响在不同的用户人口统计数据中有何不同？点击率。桌子5 显示网络钓鱼结果的统计信息。对于阶段 2，我们计算两个点击率。首先，在所有收到钓鱼邮件的参与者中，带有安全指标的点击率是32/179=17.9%。没有安全指标的点击率更高：46/176=26.1%。然而，这种比较并不完全公平，因为许多用户并没有打开邮件，因此根本没有看到安全标志。

为了检验安全指标的影响，我们还根据打开邮件的用户计算点击率。更具体地说，我们向未屏蔽跟踪像素的 176 和 179 名用户发送了钓鱼邮件，其中 94 名和 86 名用户打开了邮件。这将返回 53.4% 和 48.9% 的电子邮件打开率。在这些用户中，相应的点击率分别为48.9%（无安全标志）和37.2%（有安全标志）。结果表明，安全指标对减少有风险的用户操作具有积极影响。当出现安全指示器时，与没有安全指示器的情况相比，点击率在数值上较低。然而，差异不是很显着（Fisher 精确检验 p = 0.1329）。由于样本量相对较小，我们使用 Fisher 精确检验而不是卡方检验。结果表明，安全指标具有适度的积极影响。

用户代理。在我们的实验中，我们记录了用户打开电子邮件时的“User-Agent”，这有助于推断用户用来查看电子邮件的设备类型。回想一下，无论用户使用什么设备，我们的安全指示器（嵌入在电子邮件正文中）都会显示。桌子6 显示移动端用户比桌面端用户更容易点击钓鱼链接，但差异并不显着。

人口因素。 在图中9，我们交叉检查了有关人口因素的结果。为确保每个人口统计组包含足够的用户，我们为每个因素创建二元组。对于“教育程度”，我们将用户分为High-Edu（本科及以上学历）和Low-Edu（无本科学历）。对于“年龄”，我们将用户分为年轻（年龄<40）

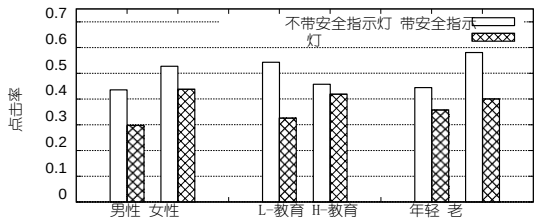


图 9：人口因素和安全指标对点击率的联合影响。

和老（年龄> = 40）。选择阈值以使两组的大小相对均匀。如图9，当为所有人口群体提供安全指标时，点击率始终较低。差异仍然很小。 Fisher 精确检验显示最小的 p = 0.06，这是低教育组产生的。总体而言，我们的结果证实了安全指标对不同用户人口统计数据的积极影响，但也表明影响有限。安全指标本身不足以降低风险。

7 讨论

在本节中，我们总结了我们的结果并讨论了它们对防御电子邮件欺骗和广泛的鱼叉式网络钓鱼攻击的影响。此外，我们讨论了电子邮件服务在我们的实验之后所做的新变化，以及我们未来的研究方向。

7.1 我们结果的意义

电子邮件可用性与安全性。我们的研究表明，即使电子邮件未通过身份验证，许多电子邮件提供商也会选择将伪造的电子邮件发送到收件箱。这是安全性和电子邮件可用性之间的艰难权衡。如果电子邮件提供商阻止所有未经验证的电子邮件，用户可能会丢失他们的电子邮件（例如，来自未发布 SPF、DKIM 或 DMARC 记录的域）。丢失合法电子邮件对于电子邮件服务来说是不可接受的，这很容易将用户赶走。

挑战在于加速采用 SPF、DKIM 和 DMARC。尽管互联网工程任务组（IETF）做出了努力，但这些协议在处理邮件转发和邮件列表等特殊电子邮件场景方面仍然存在局限性，从而进一步阻碍了广泛采用[40, 19, 37]. 我们的测量显示互联网主机中 SPF（44.9%）和 DMARC（5.1%）的采用率较低。从电子邮件提供商的角度来看，未经验证的入站电子邮件的比例可能会更低，因为大量的电子邮件发送域很可能会采用这些协议。根据谷歌2015年的统计[23]，大多数 Gmail 的入站电子邮件都有 SPF（92%）或 DKIM（83.0%），但只有一小部分（26.1%）有 DMARC 政策。这带来了持续的挑战，因为鱼叉式网络钓鱼不需要大量电子邮件即可进入。有时一封电子邮件足以破坏目标网络。**对策与建议。首先——**

大多数情况下，电子邮件提供商应考虑采用 SPF、DKIM 和 DMARC。尽管他们无法验证所有传入的电子邮件，但这些协议允许电子邮件提供商做出更明智的决定。需要进一步研究以简化部署过程并帮助避免现有电子邮件操作中断[15].

此外，如果电子邮件提供商决定向收件箱发送未经验证的电子邮件，我们认为有必要根据我们的用户研究结果放置一个安全指示器来警告用户。一个潜在的好处是安全指示器可以作为发件人域正确配置其 SPF/DKIM/DMARC 的强制函数。

第三，我们认为电子邮件提供商应该为不同的接口制定一致的安全指标。目前，由于缺乏安全指标，移动用户面临更高级别的风险。另一个例子是，与使用 Gmail 界面的用户相比，Google Inbox（网络）用户受到的保护较少。

最后，对于具有未经验证的发件人地址的电子邮件，应禁用误导性的 UI 元素，例如“个人资料照片”和“电子邮件历史记录”。这应该适用于欺骗现有联系人和欺骗同一电子邮件提供商的用户。目前，我们已经与Gmail团队沟通了我们的结果，并提出了改进当前安全指标的建议。我们正在与研究中涵盖的其他电子邮件提供商进行沟通。

新协议 BIMI 和 ARC。最近，开发了新的协议来增强欺骗检测。例如，BIMI（用于消息识别的品牌指标）是建立在 DMARC 之上的协议。通过 DMARC 确认电子邮件发件人的真实性后，电子邮件客户端可以显示 BIMI 徽标作为发件人品牌的安全标志。这意味着带有 BIMI 徽标的电子邮件已通过验证，但没有 BIMI 徽标的电子邮件不一定是恶意的。

ARC（Authenticated Received Chain）是一个未开发的协议，它在 SPF、DKIM 和 DMARC 之上运行。ARC 旨在解决由邮件转发和邮件列表引起的问题。例如，当通过邮件列表发送电子邮件时，电子邮件发送 IP 和电子邮件内容可能会更改（例如，添加页脚），这将破坏 SPF 或 DKIM。 ARC 提议通过不同的方式来保存电子邮件认证结果——

图 10：Gmail 针对同域欺骗的新警告消息。

耳鼻喉科发送方案。对于 ARC 和 BIMI，它们很可能面临与 DMARC（2015 年标准化）一样被广泛采用的相同挑战。

7.2 来自电子邮件服务的 UI 更新

一些电子邮件服务在 2018 年 1 月至 6 月期间更新了他们的用户界面。特别是，在我们将结果传达给 Gmail 团队后，我们注意到一些重大改进。首先，当我们执行同域欺骗（即欺骗 Gmail 地址）时，除了问号之外，还会在电子邮件正文中添加一条新的警告消息，如图所示10. 其次，新的移动 Gmail 应用程序不再在未经验证的邮件中显示“误导性”的个人资料照片（无论是欺骗现有联系人还是同域帐户）。同样的更改也适用于新的 Google Inbox 应用程序。然而，移动客户端的信息量仍然不如网络版。例如，移动应用程序上的问号标志没有解释信息。此外，新的警告消息（图10) 也没有始终如一地添加到移动应用程序中。

Inbox.lv 最近推出了其移动应用程序。与其网络版本一样，移动应用程序不提供安全指示器。但是，移动应用程序的用户界面得到了简化，不再为未经验证的电子邮件加载误导性元素（例如，个人资料照片）。雅虎邮箱和 Zoho 也更新了他们的网络界面，但这些更新与安全功能无关。

7.3 未决问题和局限性

打开问题。鉴于身份验证协议的采用率很低，电子邮件欺骗问题不太可能很快消失。需要进一步研究以设计更有效的指标，以最大限度地提高其对用户的影响。另一个相关问题是如何保持安全指标的长期有效性，克服“预警疲劳”[8]. 最后，需要对用户进行培训/教育，教用户如何解读警告信息，并安全地处理有问题的电子邮件。对于安全关键用户（例如，记者、政府代理人、军事人员），另一种方法是使用 PGP 来防止电子邮件欺骗[29]. 仍需做大量工作使 PGP 为广大互联网用户广泛访问和使用[30, 48].

研究局限性。 我们的研究有一些局限性。首先，我们的衡量仅涵盖公共电子邮件服务。未来的工作将探索结论是否也适用于非公共电子邮件服务。其次，虽然我们已付出巨大努力来维持网络钓鱼测试的有效性，但我们所能控制的仍然有限。出于伦理考虑，我们无法将实验完全扩大到 488 名用户之外，这限制了我们可以测试的变量数量。我们的实验只测试了一封电子邮件内容的二元条件（有或没有安全指示符）。未来的工作需要涵盖更多变量以探索设计空间，例如警告消息的措辞、安全指示器的颜色和字体、网络钓鱼电子邮件内容和用户群体（例如，除了 MTurk 和 Yahoo Mail用户）。最后，我们将“点击钓鱼网址”作为风险行为的衡量标准，这仍然不是钓鱼攻击的最后一步。然而， 欺骗用户让出他们的实际密码会产生重大的道德影响，因此我们决定不采取这一步。

8 相关工作

电子邮件机密性、完整性和真实性。 SPF、DKIM、DMARC 和 STARTTLS 等 SMTP 扩展用于为电子邮件传输提供安全属性。最近，研究人员对这些协议的服务器端使用情况进行了详细测量[23, 27, 34, 36]. 与之前的工作不同，我们的工作展示了一个端到端的视图，并展示了服务器端欺骗检测和用户端通知之间的差距。我们的研究是对现有工作的补充，以描绘更完整的画面。

电子邮件网络钓鱼。先前的工作已经开发了基于从电子邮件内容和标题中提取的特征的网络钓鱼检测方法[20, 22, 26, 35, 51, 57].网络钓鱼检测不同于垃圾邮件过滤[58] 因为钓鱼邮件不一定是批量发送的[65] 但可以具有很强的针对性[33]. 除了欺骗之外，攻击者还可以应用域名仿冒或 unicode 字符[6] 使发件人地址看起来与他们想要模拟的地址相似（但不相同）。这样的发件人地址是网络钓鱼的有力指标，已被用于检测网络钓鱼电子邮件[42, 44]. 另一条研究重点是钓鱼网站，通常是钓鱼邮件中 URL 的登陆页面[18, 32, 63, 68, 71, 72].

人为因素（人口统计、个性、认知偏见、疲劳）会影响用户对网络钓鱼的反应[52, 31, 38, 53, 60, 64, 66, 69, 16, 47]. 这

研究结果已被用于促进网络钓鱼培训[67]. 虽然这些研究大多使用“角色扮演”方法，但用户在模拟环境中阅读网络钓鱼电子邮件。有罕见的例外[38, 52] 研究人员在其中进行了真实世界的网络钓鱼实验。研究人员在与现实的角色扮演实验中证明了行为差异[59]. 我们的工作首次使用真实的网络钓鱼测试来检查安全指标对网络钓鱼电子邮件的影响。

视觉安全指示器。安全指示器通常用于网络或移动浏览器，以警告用户未加密的网络会话[25, 39, 61, 49], 网络钓鱼网页[21, 24, 69, 70], 和恶意软件网站[7]. 现有工作表明，由于对攻击缺乏了解，用户往往会忽略安全指标[69] 或频繁暴露于误报[43]. 研究人员已经探索了各种方法来使安全 UI 更难被忽视，例如使用吸引子[13, 12, 14]. 我们的工作是第一个衡量伪造电子邮件安全指标的使用和有效性的工作。

9 结论

通过广泛的端到端测量和真实世界的网络钓鱼测试，我们的工作揭示了服务器端欺骗检测与对用户的实际保护之间存在令人担忧的差距。我们证明大多数电子邮件提供商允许伪造的电子邮件进入用户收件箱，同时缺乏必要的警告机制来通知用户（特别是在移动应用程序上）。对于少数实施安全指标的电子邮件服务，我们表明安全指标对减少网络钓鱼攻击下的风险用户操作有积极影响，但不能消除风险。我们希望这些结果可以帮助吸引更多社区关注促进 SMTP 安全扩展的采用，并为 Web 和移动电子邮件界面开发有效的安全指标。

致谢

我们要感谢匿名审稿人提供的有益反馈。该项目部分得到了 NSF 赠款 CNS-1750101 和 CNS-1717028 的支持。本材料中表达的任何意见、调查结果、结论或建议均为作者的意见，不一定反映任何资助机构的意见。

参考文献

[1] 亚历克莎。http://www.alexa.com.

[2] 网络钓鱼活动趋势报告，2015 年第一、三季度。http://docs.apwg.org/reports/ 2015 年第一季度至第三季度-APWG 趋势报告.pdf.

[3] 后缀。http://www.postfix.org.

[4] 数据泄露调查报告。威瑞森公司，2017 年。http://www.verizonenterprise.com/verizon- 洞察实验室/dbir/2017/.

[5] 电子邮件统计报告。 Radicati 集团，2017 年。http://www.radicati.com/wp/wp-content/uploads/2017/01/Email-统计-报告- 2017-2021-执行摘要.pdf.

[6] AGTEN, P., JOOSEN, W., PIESSENS, F., AND NIKIFORAKIS, N. 七个月的错误：域名滥用滥用的纵向研究。在过程中。 NDSS (2015)。

[7] AKHAWE, D., AND FELT, A. P. Alice in warningland：浏览器安全警告有效性的大规模实地研究。在过程中。 USENIX 安全 (2013)。

[8] ANDERSON, B. B., VANCE, T., KIRWAN, C. B., EARGLE, D., AND HOWARD, S. Users are n't (necessarily) lazy: Using neurois to explain habituation to security warnings.在过程中。安迅思 (2014)。

[9] ANTIN, J., AND SHAW, A. 社会期望偏差和动机的自我报告：美国和印度的亚马逊机械土耳其人研究。在过程中。 CHI（2012 年）。

[10] BILOGREVIC, I.、HUGUENIN, K.、MIHAILA, S.、SHOKRI, R. 和 HUBAUX, J.-P.预测位置签到背后的用户动机和隐私保护机制的效用影响。在过程中。 NDSS (2015)。

[11] BLANZIERI, E., AND BRYL, A. 基于学习的垃圾邮件过滤技术调查。人工智能评论 29, 1 (2008), 63–92。

[12] BRAVO-LILLO, C., CRANOR, L., 和 KOMANDURI, S. 更难被忽视？重新审视弹出窗口疲劳和防止它的方法。在过程中。汤 (2014)。

[13] BRAVO-LILLO, C.、CRANOR, L. F.、DOWNS, J. 和 KOMANDURI, S. Bridging the gap in computer security warnings: A mental model approach.在过程中。 IEEE 标准普尔 (2011)。

[14] BRAVO-LILLO, C., KOMANDURI, S., CRANOR, L. F., REEDER, R. W., SLEEPER, M., DOWNS, J., AND SCHECHTER, S. 请注意：Designing security-decision uis to make true risks hard to to忽略。在过程中。汤 (2013)。

[15] 康斯坦丁， L. 雅虎电子邮件反欺骗政策破坏了邮件列表。 电脑世界，2014 年。https://www.pcworld.com/article/2141120/ 雅虎电子邮件-反欺骗-政策-中断- 邮件列表.html.

[16] CONWAY, D.、TAIB, R.、HARRIS, M.、YU, K.、BERKOVSKY, S. 和 CHEN, F. 对银行员工信息安全和网络钓鱼体验的定性调查。在过程中。汤 (2017)。

[17] COVER, T. M., AND THOMAS, J. A. 信息论要素。约翰·威利父子公司，2012 年。

[18] CUI, Q.、JOURDAN, G.-V.、BOCHMANN, G. V.、COUTURIER, R. 和 ONUT, I.-V.随着时间的推移跟踪网络钓鱼攻击。在过程中。万维网 (2017)。

[19] D. CROCKER、T. HANSEN、M. K. Domainkeys 确定的邮件 (dkim) 签名，2011 年。https://tools.ietf.org/html/rfc6376.

[20] DEWAN, P.、KASHYAP, A. 和 KUMARAGURU, P. 分析社交和文体特征以识别鱼叉式网络钓鱼电子邮件。在过程中。电子犯罪 (2014)。

[21] DHAMIJA, R.、TYGAR, J. D. 和 HEARST, M. 为什么网络钓鱼有效。在过程中。 CHI (2006 年)。

[22] DUMAN, S., KALKAN-CAKMAKCI, K., EGELE, M., ROBERTSON, W. K., AND KIRDA, E. Emailprofiler: 带有电子邮件标题和样式特征的鱼叉式网络钓鱼过滤。在过程中。 COMPSAC (2016 年)。

[23] DURUMERIC, Z., ADRIAN, D., MIRIAN, A., KASTEN, J., BURSZTEIN, E., LIDZBORSKI, N., THOMAS, K., ERANTI, V., BAILEY, M., AND HALDERMAN, J. A. 都不是snow nor rain nor mitm: 电子邮件传递安全性的实证分析。在过程中。 IMC (2015 年)。

[24] EGELMAN, S., CRANOR, L. F., AND HONG, J. 你已被警告：网络浏览器网络钓鱼警告有效性的实证研究。在过程中。 CHI (2008)。

[25] FELT, A. P., 等人。重新思考连接安全指标。在过程中。汤 (2016)。

[26] FETTE, I.、SADEH, N. 和 TOMASIC, A. 学习检测网络钓鱼电子邮件。在过程中。万维网 (2007)。

[27] 福斯特，I.D.，拉尔森，J.，马西奇，M.，斯诺伦，A. C.、SAVAGE, S. 和 LEVCHENKO, K. 任何其他名称的安全性：关于基于提供商的电子邮件安全性的有效性。在过程中。中国船级社 (2015)。

[28] GADIRAJU, U.、KAWASE, R.、DIETZE, S. 和 DEMARTINI, G. 了解众包平台中的恶意行为：在线调查案例。在过程中。 CHI (2015 年)。

[29] GARFINKEL, S. PGP：很好的隐私，第 1 版。 O'Reilly & Associates, Inc., 1996。

[30] GAW, S., FELTEN, E.W., AND FERNANDEZ-KELLY, P. Secrecy, flagging, and paranoia: Adoption criteria in encryption email.在过程中。 CHI (2006 年)。

[31] GREITZER, F. L., STROZER, J. R., COHEN, S., MOORE, A. P., MUNDIE, D., AND COWLEY, J. 分析源自社会工程漏洞的无意内部威胁。在过程中。 IEEE S&P 研讨会 (2014)。

[32] HAN, X., KHEIR, N., AND BALZAROTTI, D. Phisheye：沙盒网络钓鱼工具包的实时监控。在过程中。中国船级社 (2016)。

[33] HO, G., SHARMA, A., JAVED, M., PAXSON, V., AND WAGNER, D. 在企业环境中检测凭据鱼叉式网络钓鱼。在过程中。 USENIX 安全 (2017)。

[34] HOLZ, R., AMANN, J., MEHANI, O., WACHS, M., AND KAAFAR, M. A. Tls in the wild: An internet-wide analysis of tls-based protocols for electronic communication.在过程中。 NDSS (2016 年)。

[35] HONG, J. 网络钓鱼攻击的状态。 ACM 通讯 55, 1 (2012)。

[36] HU, H., PENG, P. 和 WANG, G. 致力于采用反欺骗协议。 CoRR abs/1711.06654 (2017)。

[37] HU, H., PENG, P. 和 WANG, G. 了解在电子邮件系统中采用反欺骗协议。在过程中。 SecDev (2018)。

[38] JAGATIC, T. N.、JOHNSON, N. A.、JAKOBSSON, M. 和 MENCZER, F. 社交网络钓鱼。 ACM 通讯 50, 10 (2007)。

[39] JOEL WEINBERGER, A. P. F. 一周记住浏览器警告存储策略的影响。在过程中。汤 (2016)。

[40] KITTERMAN, S. 发件人政策框架 (spf)，2014 年。https://tools.ietf.org/html/rfc7208.

[41] KOCIENIEWSKI, D. Adobe 宣布存在安全漏洞。纽约时报，2013 年。网址：www.nytimes.com/2013/10/04/technology/Adobe 宣布安全漏洞.html.

[42] KRAMMER, V. 针对 idn 地址欺骗攻击的网络钓鱼防御。在过程中。太平洋标准时间 (2006)。

[43] KROL, K.、MOROZ, M. 和 SASSE, M. A. 不工作。不能工作？为什么是时候重新考虑安全警告了。在过程中。危机 (2012)。

[44] KUMARAGURU, P., RHEE, Y., ACQUISTI, A., CRA- NOR, L. F., HONG, J., AND NUNGE, E. 保护人们免受网络钓鱼：嵌入式培训电子邮件系统的设计和评估。在过程中。 CHI (2007)。

[45] LANCASTER, H. O., AND SENETA, E. 卡方分布。威利在线图书馆，1969 年。

[46] 拉迪诺瓦，F. Gmail 现在每月有超过 1b 的活跃用户。技术紧缩，2016 年。https://techcrunch.com/2016/02/01/gmail-现在有超过 1b 个每月活跃用户/.

[47] LASTDRAGER, E., GALLARDO, I. C., HARTEL, P., AND JUNGER, M. 针对儿童的反网络钓鱼培训效果如何？在过程中。汤 (2017)。

[48] LUBAR, K. 和 IMAGES, G. 3 年后，为什么 gmail 的端到端加密仍然不为人所知。连线，2017 年。https://www.wired.com/2017/02/3-years-gmails端-端-加密-静止-蒸汽/.

[49] LUO, M.、STAROV, O.、HONARMAND, N. 和 NIKIFORAKIS, N. 后见之明：了解移动浏览器中 ui 漏洞的演变。在过程中。中国船级社 (2017)。

[50] M. KUCHERAWY, E. Z. 基于域的消息认证、报告和一致性 (dmarc)，2015 年。https://tools.ietf.org/html/rfc7489.

[51] MCGRATH, D. K. 和 GUPTA, M. 网络钓鱼背后：网络钓鱼作案手法检查。在过程中。 LEET（2008）。

[52] OLIVEIRA, D., ROCHA, H., YANG, H., ELLIS, D., DOMMARAJU, S., MURADOGLU, M., WEIR, D., SOLIMAN, A., LIN, T., AND EBNER, N.剖析老年人和年轻人的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。在过程中。 CHI（2017 年）。

[53] PATTINSON, M. R., JERRAM, C., PARSONS, K., MCCORMAC, A., AND BUTAVICIUS, M. A. 为什么有些人比其他人更好地管理网络钓鱼电子邮件？信息。管理。电脑。安全，1（2012），18–28。

[54] 佩雷斯，S。 最近确认的 myspace 黑客攻击可能是迄今为止规模最大的一次。 科技危机，2016 年。 https://techcrunch.com/2016/05/31/recently- 确认-myspace-hack-可能是- 最大/.

[55] PERLROTH, V. G. 雅虎称有 10 亿个用户帐户遭到黑客攻击。纽约时报，2016 年。 https://www.nytimes.com/2016/12/14/ 技术/yahoo-hack.html.

[56] POSTEL, J. B. 简单邮件传输协议，1982 年。 https://tools.ietf.org/html/rfc821.

[57] PRAKASH, P.、KUMAR, M.、KOMPELLA, R. R. 和 GUPTA, M. Phishnet：用于检测网络钓鱼攻击的预测性黑名单。在过程中。 INFOCOM（2010）。

[58] RAMACHANDRAN, A.、FEAMSTER, N. 和 VEMPALA, S. 使用行为黑名单过滤垃圾邮件。在过程中。中国船级社（2007）。

[59] SCHECHTER, S. E., DHAMIJA, R., OZMENT, A., AND FISCHER, I. 皇帝的新安全指标：网站认证评估和角色扮演对可用性研究的影响。在过程中。 IEEE 标准普尔（2007）。

[60] SHENG, S., HOLBROOK, M., KUMARAGURU, P., CRANOR, L. F., AND DOWNS, J. Who falls for phish?：网络钓鱼敏感性和干预有效性的人口统计分析。在过程中。气（2010）。

[61] SUNSHINE, J.、EGELMAN, S.、ALMUHIMEDI, H.、ATRI, N. 和 CRANOR, L. F. Crying wolf：ssl 警告有效性的实证研究。在过程中。 USENIX 安全（2009）。

[62] THOMAS, K., LI, F., ZAND, A., BARRETT, J., RANIERI, J., INVERNIZZI, L., MARKOV, Y., CO- MANESCU, O., ERANTI, V., MOSCICKI, A ., MARGOLIS, D., PAXSON, V., AND BURSZTEIN, E. 数据泄露、网络钓鱼或恶意软件？了解凭证被盗的风险。在过程中。中国船级社（2017）。

[63] VARGAS, J. 、BAHNSEN, A. C. 、VILLEGAS, S. 和 INGEVALDSON, D. 了解你的敌人：利用数据分析揭露针对美国主要金融机构的网络钓鱼模式。在过程中。电子犯罪（2016）。

[64] VISHWANATH, A., HERATH, T., CHEN, R., WANG, J., AND RAO, H. R. 人们为什么会被网络钓鱼？测试集成信息处理模型中网络钓鱼漏洞的个体差异。决定。支持系统。 51，3（2011）。

[65] WANG, J., HERATH, T., CHEN, R., VISHWANATH, A., AND RAO, H. R. 研究文章网络钓鱼敏感性：对有针对性的鱼叉式网络钓鱼电子邮件处理的调查。 IEEE 专业交流汇刊 55，4（2012），345–362。

[66] WANG, J., LI, Y., AND RAO, H. R. 网络钓鱼电子邮件检测中的过度自信。信息系统协会杂志 17，1（2016）。

[67] WASH, R., AND COOPER, M. M. 谁提供网络钓鱼培训？事实、故事和像我这样的人。在过程中。 CHI'18（2018）。

[68] WHITTAKER, C.、RYNER, B. 和 NAZIF, M. 网络钓鱼页面的大规模自动分类。在过程中。 NDSS（2010）。

[69] WU, M., MILLER, R. C., AND GARFINKEL, S. L. 安全工具栏真的可以防止网络钓鱼攻击吗？在过程中。 CHI（2006 年）。

[70] ZHANG, B., WU, M., KANG, H., GO, E., AND SUNDAR, S. S. 安全警告和即时满足线索对移动网站态度的影响。在过程中。气（2014）。

[71] ZHANG, Y., EGELMAN, S., CRANOR, L., AND HONG, J. Phinding Phish：评估反网络钓鱼工具。在过程中。 NDSS（2007）。

[72] ZHANG, Y., HONG, J. I., AND CRANOR, L. F. Cantina：基于内容的网络钓鱼网站检测方法。在过程中。万维网（2007）。

附录 A – 欺骗目标域

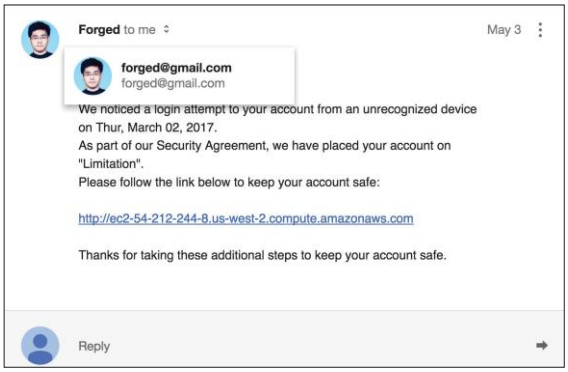
桌子7 列出了端到端欺骗实验使用的 30 个域作为欺骗性发件人地址。每个类别的域是从 Alexa 前 5000 个域中随机选择的。

无： 无 SPF/DKIM/DMARC（10）
thepiratebay.org, torrent-baza.net, frdic.com, chinafloor.cn, onlinesbi.com,4dsply.com, peliculasflv.tv, sh.st, contw.com anyanime.com
宽松： SPF/DKIM；DMARC=无（10）
tumblr.com、wikipedia.org、ebay.com、microsoftonline.com、msn.com、apple.com、vt.edu、github.com、qq.com、live.com
严格： SPF/DKIM；DMARC=拒绝（10）
google.com、youtube.com、yahoo.com、vk.com、reddit.com、facebook.com、twitter.com、instagram.com、linkedin.com、blogspot.com

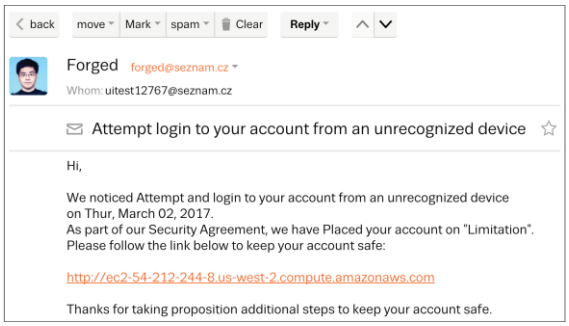
表 7：欺骗性发件人域列表。

附录 B – 其他漏洞

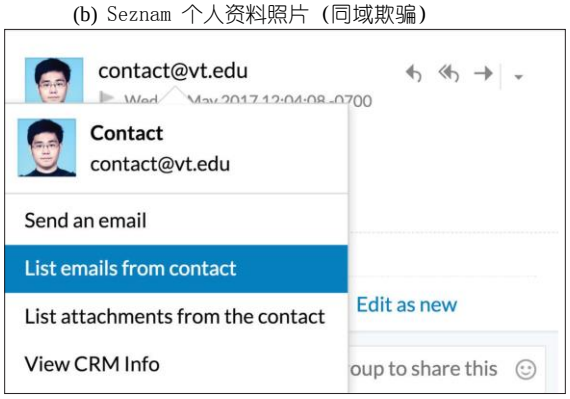
我们发现 2 个电子邮件服务“sapo.pt”和“runbox.com”没有仔细配置，允许



(a) Google 收件箱个人资料照片（同域欺骗）



(b) Seznam 个人资料照片（同域欺骗）



(c) Zoho 个人资料照片和电子邮件历史记录（欺骗联系人）

图 11：误导性 UI 示例（个人资料照片、电子邮件历史记录、名片）。

攻击者搭载他们的邮件服务器来发送伪造的电子邮件。这种威胁模型与我们上面的实验有很大的不同，我们用图简单描述一下1. 在这里，攻击者是发送者 MUA，易受攻击的服务器（例如 runbox.com）是发送者服务。通常，Runbox 应该只允许其用户发送电子邮件，发件人地址为“someone @runbox.com”。然而，Runbox 的服务器允许用户（攻击者）在步骤中自由设置“MAIL FROM”（无需验证）
{ }
0 发送伪造的电子邮件。这种攻击无助于伪造电子邮件以绕过 SPF/DKIM 检查。但是，它为攻击者提供了一个静态且信誉良好的 IP 地址。如果攻击者通过易受攻击的邮件服务器主动发送恶意电子邮件，则可能会损害 IP 的声誉。我们已将漏洞报告给服务管理员。

附录 C – 误导性用户界面

数字11 显示了三个误导性 UI 元素的示例。数字11(a) 和11(b) 显示当攻击者欺骗来自与接收者相同的电子邮件提供商的用户时，电子邮件提供商将自动从其内部数据库加载被欺骗的发件人的个人资料照片。在谷歌收件箱和 Seznam 中，伪造的电子邮件看起来像是用户“伪造”发送的，照片图标使伪造的电子邮件看起来更真实。数字11(c) 演示了当攻击者欺骗接收者的现有联系人时的误导性 UI。同样，尽管发件人地址（contact@vt.edu）是伪造的，Zoho 仍会从其内部数据库中加载缺点照片。此外，用户可以通过单击突出显示的链接来查看最近与此联系人的电子邮件对话。这些元素使伪造的电子邮件看起来很真实。