arXiv:2305.03680v1 [cs.CY] 5 May 2023

“不平等的在线安全？”安全与隐私保护建议及行为模式的性别分析

Kovila P.L. Coopamootoo 伦敦国王学院，英国
kovila.coopamootoo@kcl.ac.uk

玛格达琳·吴英国威斯敏斯特大学
m.ng1@westminster.ac.uk

摘要

文献中有迹象表明，女性使用旨在保障其在线安全的信息安全与隐私（SP）技术的方式与男性不同。为了更好地理解这种性别差距，我们对 N=604 名英国参与者开展了一项在线调查，以了解他们对 SP 建议来源的偏好，以及对 SP 方法和技术的使用情况。我们发现了 SP 获取机会和参与程度不平等的证据。具体而言，女性更倾向于从亲密与社会关系（ISC）中获取建议，而男性则更偏好在线内容。ISC 与 SP 技术的使用之间不存在密切关联，也无法预测 SP 技术的使用情况；相比之下，在线来源（如在线论坛、评论、专业页面和技术广告）以及培训则与 SP 技术的使用密切相关。男性也更有可能使用多个建议来源，而这会提高其使用 SP 技术的可能性。女性倾向于向 ISC 寻求建议，主要是因为她们看重建议者的特征（如信息技术相关专业知识、经验和可信度）；而男性向 ISC 寻求建议，则是为了评估选项，并对自己的做法寻求 reassurance。本研究对在线安全机会的公平性提出了质疑，并给出了相关建议。

1 引言

数字技术是推动性别平等的重要力量，有望让女性和女孩获得信息、机会与资源。但性别鸿沟在全球范围内依然存在，这往往是由于社会规范和性别规范以及根深蒂固的性别刻板印象所致，进而导致人们对技术的使用呈现性别差异 [7]。然而，尽管据称发达国家的性别数字鸿沟正在缩小 [89],，相关文献中仅有少数实证研究表明，尽管女性比男性更关注安全与隐私（SP）问题 [20,64,66]，但她们在使用防火墙和垃圾邮件过滤器等保护性安全与隐私技术方面的参与度较低 [64],，例如追踪保护 [20],，或使用技术性隐私保护工具 [66]。与此同时，有报告指出，女性遭受在线伤害的风险更高比男性 [63],更多，国际和地方组织也呼吁采取行动，确保女性的在线人身安全。例如，联合国开发计划署（UNDP）倡导，仅让女性和女孩能够使用技术并掌握数字技能还不够——“她们还必须成为积极的变革推动者，共同创造更安全、更公平的数字未来”，并呼吁打造安全、负担得起且包容的互联网 [87]。在英国，通信监管机构 Ofcom 也敦促技术公司采取行动，保障女性的在线安全 [62]。

迄今为止，专门致力于理解性别差异的实用型 SP 研究还不多，尽管已有 [20,64,66]。本文报告了一项研究，揭示这种性别差异的特征（是什么）及其成因（为什么），进而展示技术刻板印象 [1] 和 SP 刻板印象 [91] 如何在实践中体现。研究的第一部分聚焦于 SP 获取和使用，并围绕以下研究问题展开：

- **研究问题1**：鉴于个体之间存在性别差异，他们会从哪些建议来源获取 SP保护建议？
- **研究问题2**：女性和男性分别使用哪些 SP 技术和方法？
- **研究问题3**：鉴于性别差异，建议来源与 SP 使用有何关联，又会如何影响 SP 使用？

第二部分探讨个体为何会向亲密与社会关系（ISC）寻求 SP 保护建议；这里的亲密与社会关系包括家人／伴侣、朋友、同事和社会熟人。我们也探讨他们通过以下途径获得何种建议：

- **研究问题 4**：女性和男性出于哪些原因会向 ISC 寻求 SP 保护建议？
- **RQ5**：女性和男性会从 ISC 获得哪类建议？

我们聚焦于 ISC 建议，因为尽管有迹象表明，ISC 的建议可能没有涵盖如何使用 SP 保护建议 [56,93],，ISC 仍然是一个易于获取且广受欢迎（因而很有价值）的信息来源 [93]，而且先前研究已经探讨过网络 SP 建议的质量 [80]。

贡献。 与以往关于SP建-

议 [72,78,80]或由社会支持的SP [56,60,93],保护的研究相比，本研究最主要的独特贡献在于，我们以相对大规模的样本，重点分析了SP保护获取方面的二元性别差异，尤其是来自ISC的差异，以及这些差异对SP 使用的影响，从而补充并拓展了SP研究中为数不多的性别分析 [20,64,66,91]；这些研究也考察了女性与男性的差异，但未涉及建议来源。总体而言，本研究：（1）提供证据表明，女性和男性获取SP及参与其中的模式各不相同，这可能加剧在线安全方面的不平等，并支持女性比男性面临更高在线风险的观点；（2）支持地方和国际层面为保障女性在线安全而采取行动的呼吁；（3）提出多利益相关方行动的推荐。

研究结果摘要。（1）女性获取SP保护的方式与男性不同。（**a**）我们发现，有证据表明，女性更倾向于寻求来自ISC的建议，而男性更偏好在线内容。（**b**）对于女性而言，家人（单独或与其他来源结合）是报告中最常见的建议来源；而对于男性，最常见的是一般性搜索。（**c**）女性更有可能报告不使用任何建议来源，而男性更有可能报告使用多个来源。

（2）女性使用SP技术的方式与男性不同。与男性相比，女性更熟悉简单或内置的SP功能（例如隐私设置、HTTPS、内置安全功能、安全软件更新或密码）以及用于SP保护的非技术方法；而男性则熟悉更广泛的SP保护手段，包括更复杂的方法（例如防火墙、VPN、反间谍软件、反恶意软件、反跟踪或多因素身份验证）。

（3）在线建议和建议来源的数量会影响SP技术的使用。（**a**）偏好来自ISC的建议并不能预测SP技术的使用，而在线建议显示出使用SP技术的可能性提高了3至11倍。（**b**）所使用的建议来源数量从1个增加到3个时，使用SP技术的可能性会逐步提高。

(4) 寻求 ISC 建议的动机不同。 女性寻求 ISC 的 SP保护建议的可能性是男性的 3 倍；她们的动机（对顾问专业知识的认知、经验和可信度）表明她们依赖 ISC，而男性则向 ISC 咨询选项，并寻求对自身做法的 reassurance。

(5) SP 建议的主题不同。 收到身份验证建议的女性比例较高，而收到有关恶意软件、欺诈以及沟通/网络隐私建议的男性比例较高。

注。 本文不对 SP 建议的来源作价值判断。ISC 建议并不必然比在线建议差。

2 背景

本节将探讨有关安全与隐私（SP）不平等的文献，并回顾以往关于 SP 建议的研究，以及与保护性安全与隐私相关的社会关系。

2.1（性别）安全与隐私方面的不平等

虽然数字鸿沟从广义上阐释了社会多样性如何导致技术获取、技能和结果方面的差异，进而加剧社会不平等 [89],但跨学科研究也探讨了隐私方面的不平等 [13, 76], 并特别提及性别 [4, 20, 50, 64, 66]。

首先，近期少数研究从概念层面探讨了隐私不平等，尤其借助数字鸿沟的概念研究，讨论隐私如何促使或再生产个体的社会地位，将隐私不公平视为数字参与不平等的成因或结果 [67],，并指出隐私分配不均是一个社会问题：在线隐私容易受到年龄、教育和性别相关社会不平等的影响 [13],；此外，信任他人处理个人数据、对负面或剥削性在线经验的担忧，以及对自身数据的掌控感，都会影响差异化网络使用 [76]。

其次，女性主义视角长期以来一直在质疑：对于女性而言，在线隐私是否与男性处于同一阵营 [4, 50]。具体而言，历史上女性拥有的往往是“错误类型的隐私”，例如隔离与禁闭；而她们在道德和政治层面应享有的，则是“正确类型的隐私”，即有意义的机会自主选择独处、亲密关系，以及对个人生活和健康作出决定的法律权利。在这种真正的女性隐私之下，平等将得以推进，并带来彻底的变革 [4, 5]。

第三，实证研究指出，尽管女性比男性更关注在线隐私，但她们使用防护技术的可能性较低 [8]。具体而言，与采用更多样化技术手段的男性相比，女性更常报告称，她们会使用技术性较弱、非技术性且简单的方法来保护自己在线安全 [20, 64, 66]。组织中员工自我报告的网络安全行为也因性别而异 [6]；一般而言，人们对安全与隐私（SP）抱有性别刻板印象，认为男性更愿意参与安全与隐私相关议题，或更可能采取有助于提升安全与隐私的行为，而女性则被认为对安全与隐私缺乏信心 [91]。

2.2 安全与隐私建议来源

以往研究表明，人们会从各种来源获取安全与隐私（SP）建议，这些建议通常涵盖 SP 的不同方面。个人了解 SP 的建议来源和方式可分为：（1）非正式来源，如家人、朋友 [23],同事 [70], 同伴 [60],或新闻文章；（2）半正式来源，指网页，

由第三方提供（包括政府在线网页、零售商、软件供应商，或专注于安全与隐私的组织，例如国际隐私组织）[34, 42, 72]；以及（3）更正式的来源，包括培训和教育。

虽然很大比例的互联网用户并不了解在线保护隐私与安全（SP）的技术，但他们可能会通过非正式渠道获取其他隐私与安全信息，例如威胁的来源、威胁的表现形式及其后果。具体而言，非专业人士（家人、朋友、同伴）的个人经历通常侧重于威胁来源是谁，而新闻文章则侧重于对值得关注的事件进行描述，以及提供与更广泛社会相关的建议。对于半正式渠道而言，网页被认为最具权威性，其目的是教育互联网用户，因此用户在在线寻求专业知识时会求助于这些网页。这些网页传达了组织或政府认为非专业人士应当了解的问题，例如国际隐私组织、电子前哨基金会、微软或英国国家网络安全中心。

总体而言， [77], 在家庭内部 [56],针对特定人口群体 [53, 56, 59, 61], 或在涉及个人信息共同所有权的技术情境中（例如社交媒体和智能家居） [24, 61], 家人、朋友或同事已被发现是 SP 建议的主要来源。在密码选择、身份验证、防病毒软件使用、软件更新等 SP 保护情境中，设备/软件提示已被视为建议的主要来源，其次是在线来源、印刷媒体、电视新闻或文章以及在线论坛 [77]。

2.3 社会关系与安全与隐私保护建议

保护行为的社会维度植根于个人的社会资本。社会科学家普遍认为，社会资本由嵌入社会关系和社会结构中的资源构成；当个人希望提高采取有目的行动的可能性时，这些资源便可被动员起来 [49]。具体而言，社会资本是个人通过其社会网络 [11], 能够获取的全部实际或潜在资源，其中包括物质、情感（体现为情感或社会支持）和信息（如建议或新信息）资源 [49]。研究者曾在安全与隐私领域探讨社会资本，尤其是在社交网站上协商隐私和信息披露的情境中 [14, 27, 86], 。近期研究则对社会群体（亲密关系、家庭与家庭成员、社会熟人及公众）如何影响他人的安全与隐私行为进行了概念化，尤其关注人们如何依赖这些社会关系获取建议和知识 [93]。

在家庭内部： 在家庭中为其他成员提供非正式支持的人，被称为*SP*管理者或自封的技术管理者 [23, 56], , 他们会帮助技术知识较少的家庭成员（如老年人），也可能为整个家庭制定技术使用指南——指南 [56]。不过，SP管理者本身并非SP专家，知识上可能有所欠缺，而且他们通常关注的不是SP技术（工具和设置），而是过往经验。他们也可能将自己的威胁与保护模型强加给家庭成员，并控制技术使用，从而体现出家长式作风并削弱他人的数字自主权。对于较年轻的群体，父母被认为会为子女提供建议和帮助 [47]。总的来说，人们认为互联网技能较低者会听取家人和朋友的建议，参与较少的SP实践，因此这些处于劣势的用户可能面临更高的脆弱性 [77]。

在家以外： 人们认为，老年人会向同伴寻求建议，例如*Cyberguardians*。他们是提供点对点SP支持的社区成员 [60],，并优先考虑信息提供者的可用性 [59, 61]。研究还发现，人们会通过向他人讲述自己的经历 [23],、从他人分享的故事中吸取教训 [73],、在发生安全事件后主动搜寻信息 [75],，或受到他人采用安全功能的影响（例如在社交媒体上） [24], 从社交圈获取保护性SP信息。此外，人们认为，互联网技能和社会经济地位较高的人会听取工作场所提供的建议，并具备从经验中学习所需的技术技能 [77]。

总体而言，包括年龄 [56, 60],、教育水平 [78],、技能和社会经济地位 [77]在内的用户特征会影响个人向谁寻求SP 建议，而建议来源又会影响个人收到的建议类型，进而影响其SP经验 [78], 。据我们所知，既有研究尚未关注女性与男性在接收、寻求或获取SP 建议方面有何差异，也未探讨这类行为如何影响其保护行为。

2.4 研究空白与贡献

首先，本文扩展了上文第2.1节所述的第三类研究，通过实证研究拓展了关于此前所识别的“性别差距”的认知 [20, 64, 66],，但与这些研究不同的是，本文聚焦于英国样本中参与者自己提及的寻求建议行为和广泛使用行为。相比之下，Wei等人使用美国样本，研究了人们对安全与隐私行为所持的偏见性假设和刻板印象 [91], ；Coopamootoo等人则使用英国和欧洲样本，仅关注与在线跟踪相关的感受和行为 [20],；Oomen与Leenes使用荷兰样本，考察风险感知如何与预先定义的安全与隐私策略（如匿名邮件转发器）相关联 [64],；Park则使用美国样本，研究隐私行为和信心如何因性别而异 [66]。此外，我们还考察了获取机会和结果方面的不平等，从而也为数字鸿沟文献作出贡献 [89]。

其次，本研究也补充了日益发展的可用性研究。

探讨建议来源 [80] 和社会性安全与隐私 [93],的安全与隐私文献，尤其是以下研究：（1）Rader 等人关于不同来源所提供的多种安全与隐私建议的研究 [72], 通过细致呈现安全与隐私建议来源的选择如何与保护相关；（2）Redmiles 等人关于社会人口特征对建议来源偏好的影响，以及不同技能水平间安全鸿沟普遍程度的研究 [78],以及 Geeng 等人关于安全与隐私建议对 LGBTQ 群体有效性的障碍的研究+ [35],通过深入的二元性别分析；（3）Redmiles 等人提出，个体可能认为信息安全社区是专家 [77],通过细致呈现选择或不选择信息安全社区建议的原因；以及（4）Murthy 等人 [56] 和 Nicholson 等人 [60] 关于社会联系如何支持安全与隐私保护的定性研究，并通过采用混合方法开展更大样本的研究。

3 方法

我们于2021年5月通过在线调查方法设计并开展了一项用户研究。

3.1 调查设计

调查首页包含一段信息说明，随后是自愿同意环节。之后是五部分必答题，具体如下。

部分 1： 我们通过一个开放式问题“您在线时最常使用哪些隐私和安全方法或工具？”了解参与者对安全与隐私的参与情况，并邀请他们列出三至五种。此前的研究也采用了类似方式，发现参与者在被询问时会提供三至五种隐私方法 [18]。

部分 2： 我们通过另一个开放式问题“您通常如何得知、了解或找到用于在线保护隐私和安全的技术/方法？”询问参与者如何了解安全与隐私方法和技术，并邀请他们列出所用的所有来源。

第 3 部分： 随后，我们通过“是/否”问题询问参与者，如果需要 SP 建议，他们是否会向 ISC 求助，并接着以开放式问题询问他们这样回答的原因。问题如下：“如果您在任何时候需要有关如何保护在线隐私和安全的建议/帮助，通常会向您的亲密与社会关系（例如家人、朋友、同事）寻求帮助吗？”以及“请说明您对上一个问题回答“是”或“否”的原因。”

第 4 部分： 我们进一步询问了他们此前收到过的建议实例和类型，问题如下：“如果您曾从亲密与社会关系中收到有关保护隐私/在线安全的技术/方法方面的建议/支持，请举例说明这些建议/支持。”

第 5 部分： 问卷的最后一部分包括：(1) 关于年龄、性别以及计算机/信息技术背景的人口统计学问题；随后是 (2) 通过 Van Deursen 等人的互联网/数字技能测量工具涵盖 5 种技能类型，如 [88], 所示。该工具包含 35 个条目，分为 5 种数字技能（操作、信息导航、社交、创造和移动技能），采用 5 点李克特量表进行测量，选项从“完全不符合我”到“非常符合我”。与以往关于技术技能（通过技术性网络技能 [40] 测量）对建议来源偏好 [77], 的影响的研究相比，我们选择数字技能测量工具 [88]，是基于 Helsper 关于数字鸿沟的理论模型 [41],，该模型关注数字技能与信息与通信技术使用之间的关系，且其开发过程中使用了英国样本 [41, 88]。(3) 我们还采用了 Franke 等人的技术交互亲和度（ATI）量表 [32]（据我们所知，这是该量表首次用于安全与隐私研究领域）。该量表包含 9 个条目，采用 6 点李克特量表进行测量，选项从“完全不同意”到“完全同意”。ATI 用于评估个人主动参与深度技术交互的倾向（即他们如何应对、回避或处理新的技术系统） [32],，将其视为应对技术的一项关键个人资源。在技术交互中，ATI 表现为一种倾向：为了问题解决，更积极地接触和探索新系统及其功能；与之相对的，是为了避免遭遇技术系统问题而回避与新系统交互。

我们注意到，Prolific 的筛选标准仅设为女性和男性，但性别调查问题的选项包括“女性、男性、非二元性别或其他”。只有 1 位参与者认同为非二元性别（未纳入分析）。

3.2 参与者

我们通过 Prolific Academic 的英国样本库招募了$N = 600+$ 名参与者。研究时长为 10 至 15 分钟。参与者按每小时 7.5 英镑的标准获得报酬。

剔除 14 份未完成的答卷和 1 份自我报告为非二元性别的答卷后，我们最终的样本包含$N = 604$ 名参与者，其中 89% 认同自己属于白人族裔。样本中的二元性别比例均衡，女性和男性各约占 50%（具体而言，女性$n = 303$ 名，男性$n = 301$ 名），以拓展关于此前所识别性别差距的知识；该差距专门比较了女性与男性 [20, 64, 66]。我们还按年龄均衡了样本，涵盖从 18 岁到 65+ 岁的 10 个年龄组，每组参与者约占 10%，因为先前研究表明，年龄会影响个人从何处获取安全与隐私建议，尤其会影响他们是否向家人和朋友寻求建议 [23, 56, 59, 60]。

该样本中大学毕业生的比例更高（为51.1%），而英国人口中的比例约为42% [22,31]），其中38.2%拥有本科层级大学学位，11.8%拥有硕士学位，1.5%拥有博士学位。不同性别的教育水平相近，如附录中的表5 所示，其中女性组的51.2%

相比之下，男性组为51.9%拥有大学学位（本科至博士合计）。这与英国人口的情况不同，在英国，女性比男性更有可能进入大学 [2, 12, 68]。

总体而言，16.5%的参与者（n=100）表示自己具有信息技术／计算机背景，即曾在信息技术、计算机科学或计算机工程领域接受教育或工作；这一比例在女性组中约为10%，在男性组中约为23%。我们样本中信息技术／计算机背景方面的性别差异，远小于英国人口中的差异 [92]。（请注意，在第4节报告的结果中，整个N=604 和无信息技术／计算机背景的n=504 所观察到的性别差异相同。）

我们还使用 Van Deursen 等人的互联网/数字技能测量工具 [88]（详见第3.1节）测量了参与者在5种技能类型上的数字技能。信息导航以及社交与移动数字技能方面没有差异，但不同性别在操作性（平均差异 = 1.7）和创造性（平均差异 = 3.5）数字技能方面略有差异。5种数字技能的量表信度 Cronbachα 介于.824至.910之间。此外，我们采用 Franke 等人的技术互动倾向（ATI）量表 [32]（详见第3.1节），发现女性参与者（$M = 3.37$，$SD = .92$）和男性参与者（$M = 3.86$，$SD = .97$）的 ATI 存在显著差异，男性的 ATI 得分更高（$p < .001$）。ATI 的 Cronbach α 为.825。

3.3 伦理

我们的研究方案在研究开始前已获得纽卡斯尔大学伦理委员会的批准。此外，在整个数据分析和论文撰写阶段，我们也遵循了伦敦国王学院的伦理准则，第一作者当时隶属于该校。

在参与者回答问卷之前，我们征得了参与者对数据收集的自愿同意，且未收集身份识别信息。参与研究是自愿且匿名的，参与者可以在任何阶段退出研究。

3.4 数据分析

我们采用了定性和定量两种分析方法，具体将在本节中进行介绍。

定性研究。通过归纳式内容分析对调查第 2 至第 4 部分收集的开放式回答进行了分析 [58, 83]，：针对每个问题，我们（1）阅读每份回答，提取主题并对各类别的回答进行综合；（2）制定编码手册，并通过迭代不断完善；（3）在 2 名编码员的协助下对所有回答进行编码；（4）计算评分者间信度（IRR）。第 1 部分的 SP 方法和技术的 elicitation 仅采用简单的识别方式，即确认回答中提及的 SP 方法。

我们的编码方法提供了代码存在的证据，但无法证明这些代码不存在。为了减轻其对研究结果可能产生的影响，我们专门询问参与者是否表示自己不使用或不了解（即不知道自己曾使用过任何安全与隐私技术或方法），对于建议来源，我们也采用了同样的询问方式，具体详见第3.1节以及附录中的问卷。

第 *1* 部分——*SP* 方法与技术使用：总体而言，我们汇总了参与者报告的 SP 使用情况，共计 26 种不同的工具和方法。我们根据技术类方法和非技术性方法对工具和方法进行了分类（汇总见附录中的表7）。我们将 *SP* 定义为依赖算法或软件编程的技术。换言之，这类技术本身具备保护个人隐私和安全的能力。我们将非技术性 *SP* 方法定义为由人类行为和策略构成。

第 *2* 部分——保护性 *SP* 的建议来源：我们发现，个人会通过一系列来源了解到、学习或找到保护其安全与隐私的技术／方法，这些来源包括先前研究中提及的 [72, 77–79, 93]。我们确定了以下类别：(i) 家人、朋友、同事及其他社会关系，这与 [56, 61, 93], 所述的类似，我们将其归为亲密关系和社会关系 [（家人包括伴侣、父母、子女或兄弟姐妹）]；(ii) 在线内容类别（类似于 [72,80]）；以及 (iii)“其他方法”类别，其中包括新闻和培训，汇总见表1。Cohen 评分者间信度$k = .950$。

第*3*部分——寻求 *ISC* 建议的动机：我们将参与者选择 ISC 建议的理由归类为：（i）对其 ISC 的技术技能和经验的认知；（ii）对其 ISC 所具备特质（如可信度、可获得性、助人性）的认知；（iii）对自身技能的认知；或（iv）其他原因。我们根据参与者提及自身技能（如自立和自信），或其他原因（如偏好其他来源），将参与者有意不选择 ISC 建议的回答进行归类。这与先前的研究相一致，即个人会根据自身的教育技能 [77],、对这些建议来源的信任和便利性认知 [77], 以及对 ISC 所具备技能的认知来使用 SP 建议来源，而这些 ISC 实际上可能并非 SP专家 [56]。Cohen 评分者间信度 $k = .861$。

第 *4* 部分——来自 *ISC* 的建议示例：我们将参与者报告从 ISC 收到的 SP 建议归类为 (i) 针对 SP 某一方面的建议，或 (ii) 一般性建议。具体的 SP 建议是指针对 SP保护某一方面的建议，例如身份验证、反恶意软件、通信 SP、电子邮件等，如附录表 11 所述。一般性建议类别中的回答没有提及具体的 SP 方面，而是包含一般性的 SP 内容，例如最佳实践、如何确保在线安全、警告、安装，或由他人代参与者完成（图 8）。Cohen 评分者间信度 $k = .907$。

定量分析。我们通过可视化呈现不同性别、建议来源和 SP 使用情况（方法/技术）下各主题的出现情况，以展示定量差异；χ^2检验和多变量分析用于呈现变量间的关联，逻辑回归则用于展示预测影响。我们检验了回归分析的假设，例如根据来源列表计算共线性统计量（回归结果见第 4.3.2 节），各来源的 VIF 介于 1.02 至 1.14 之间，表明来源之间相关性较弱。此外，鉴于此前缺乏关于性别对 SP 来源影响的估计，我们采用经验法则，要求 >500名参与者，且每个自变量至少有 10 个案例。此外，我们指出，内容分析也为实证研究作出了贡献 [10,43,46],，包括 SP 领域的大规模定量研究 [18–20,53]。

3.5 局限性

参与者特征：样本具备足够的数字技能，能够在 Prolific 平台上注册账户，且受教育程度高于英国人口的平均水平。不同的样本可能会呈现出安全与隐私使用及参与程度的差异。

数据收集：本研究依赖自我报告，而特定的安全与隐私情境可能充斥着关于信心的性别刻板印象 [91],，导致男性高估自身的技术参与度，女性则低估自身的技术参与度。此外，社会期许偏差对不同性别的影响可能有所不同：女性可能会更多承认自己曾从 ISC 获得建议，或更容易记得曾接受家人的帮助，从而符合不同性别的寻求帮助刻板印象。我们在讨论部分进一步考察了刻板印象对研究结果的影响5。

尽管如此，多年来，自我报告调查一直是收集安全与隐私经验见解的关键方法，其中包括有关安全与隐私建议的研究 [77] 以及安全与隐私使用的研究 [18],，这些研究与本研究相关；自我报告调查也被广泛用于安全与隐私研究，以深入了解人类的经验、认知或刻板印象 [18,77,78,91]。**分析：** 我们的编码方式可能存在一些局限性，具体讨论见第 3.4 节。不过，我们要指出的是，问题均为必答题，并提供了“不知道”、“没有”或“其他”选项。

4 结果

4.1 建议来源偏好

我们通过两个阶段研究RQ1，即考虑到个体之间的性别差异，他们会使用哪些建议来源来获取SP保护建议：（i）首先，我们描述参与者提及的来源类别和类型（我们将女性参与者的回答标记为W#，男性参与者的回答标记为M#）；（ii）随后，我们探讨建议来源类型偏好、所使用的建议来源数量方面的性别差异，包括其中的模式。

表1：类别与示例来源（N=604）

类别	建议来源	参与者百分比
亲密与社交 / 联系	家人	16.7
	朋友	16.1
	面对面／线下	5.8
	‘来自工作’	4.5
	同事	3.6
在线内容	一般研究，例如 Google	27.0
	专业页面，例如 TechCrunch	11.1
	在线评论和推荐	8.9
	科技广告、共享的公司信息	8.6
	社交媒体内容，例如 YouTube、Twitter	7.9
	在线论坛，例如 Reddit	7.6
其他方法	新闻、电视节目	10.8
	培训	5.0
	系统提示和设置	3.1
	消费者杂志	0.8
None	不知道	16.0

多源使用情况的。

4.1.1 所用建议来源的描述

我们在表1中总结了建议来源的类别和类型，并在下文对其进行说明，同时在附录9中提供示例回答。

亲密与社会联系／面对面 37。9% 的参与者报告了 ISC 类别的建议来源，其中最常提及的是家人和朋友，如表 1所示。“家人”包括向参与者的子女、伴侣、兄弟姐妹或父母征求或获得建议。“朋友”和“同事”的含义不言自明。“来自工作”包括参与者谈及从工作中了解 SP 方法和技术、提及其雇主以及工作场所实践／推荐；“面对面／线下”则指参与者获得家人、朋友或工作圈子以外熟人的支持。

在线内容 53。6% 的参与者表示，他们通过在线内容获取保护性 SP 建议，包括进行常规互联网搜索、访问专业页面、查阅在线评论和专家建议、从在线论坛获取建议，以及浏览社交媒体上分享的内容。

- 一般研究：(a) 使用互联网搜索（Google），或 (b) 从一般搜索入手，继而找到其他提供防护方法比较或评论的在线内容，或 (c) 表示自己在察觉到威胁时会研究 SP防护方法。
- 专业页面：提及使用技术网页和博客，或提供定向SP防护建议的网页。
- 在线评价或建议：提及专家评论或推荐。
- 技术广告和共享的公司信息：(a) 技术广告，(b) 技术公司或服务提供商发送的定向电子邮件／信息，(c) 知名品牌或零售商。
- 社交媒体内容：通常在社交媒体上分享的 SP 建议，或由他们可能并不认识的人非正式分享，或由警方等组织更正式地分享。

• 在线论坛：泛指在线论坛、技术相关论坛或特别提及 Reddit。

其他方法 18。8%的参与者表示，他们通过新闻、电视节目、培训、软件或设备推送的提示，或消费者杂志等其他媒体获取保护性的安全与隐私建议。

• 新闻和电视节目：指报纸、一般性或专注于技术的在线新闻/电视新闻，以及电视纪录片或节目。

• 培训：（a）在学校参加课程或培训，或作为其工作组织要求的一部分参加培训；或（b）具有计算机或安全与隐私（SP）相关背景；（c）由于其在工作中的信息技术（IT）/安全与隐私（SP）相关岗位而具备相关知识，这也意味着接受过培训。

• 系统提示和设置：（a）等待其使用的软件／设备发出提示或提供建议；或（b）直接查看其隐私／安全设置。

• 消费类杂志：面向消费者的非信息技术类杂志，例如英国的《Which?》杂志。

无：当参与者表示以下情况时，回答被归类为“无”：(a) 不知道 SP 工具和方法，或不主动寻求任何建议；以及 (b) 不主动寻求 SP 相关建议，而是使用其认为已集成在设备中的现有功能。

4.1.2 性别模式与差异

我们首先 可视化展示参与者对不同性别在 SP 建议来源偏好方面的整体回答，其次 通过二项逻辑回归描绘性别差异，最后 比较不同性别使用多种建议来源的情况。

性别模式可视化。图 1（附录表 6 提供了支持）显示女性和男性之间存在明显的差异模式，即

• 在报告信息共享与沟通（ISC）类别来源的人群中，也就是说，其来源是家人、朋友、线下建议（例如认识的计算机支持人员）、同事或工作实践的人群中，女性所占比例高于男性；

• 在报告通过在线内容类别了解 SP 方法和技术的人群中，例如通过一般研究、专业页面、在线论坛和评论、技术广告或共享在线内容，男性所占比例高于女性；并且

• 在报告从朋友那里获得建议的人群中，男性和女性所占比例大致相同。

在解读图1时，我们注意到，图中所示比例是根据报告各建议来源的参与者人数（即基准率）计算得出的，如表6所示。例如，报告会咨询家人（n=101）的参与者人数，是使用共享在线内容（n=48）或在线论坛（n=46）人数的两倍多。尽管报告使用共享在线内容而非咨询家人的男性人数仅多出 n=8 人，我们仍注意到，报告使用共享在线内容的男性人数是女性的两倍，而报告向家人寻求建议的女性人数是男性的三倍。

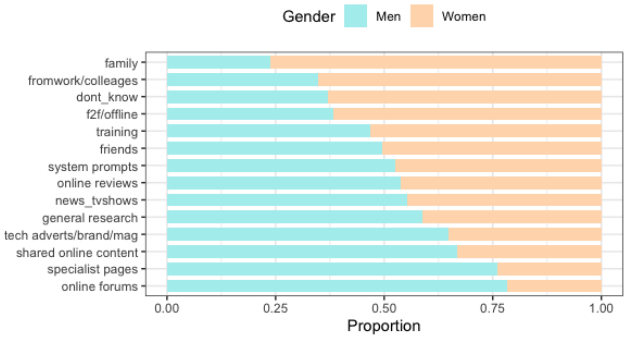


图 1：参与者提及的来源 按性别划分

回归模型。我们进行了二元逻辑回归，自变量（IV）为女性与男性（分类变量，以男性为基准组），因变量（DV）为各建议来源（分类变量；提及该建议来源时设为 1，未提及则设为 0）。以家人、工作场所/同事、一般研究、专业页面、在线论坛、共享在线内容和技术广告为因变量的模型均具有统计显著性（如表2所示），这意味着以性别为预测变量的模型比仅截距模型显著更好地拟合数据。与男性相比，女性报告将家人和工作场所/同事分别作为 SP 建议来源的可能性接近 4 倍（优势比 = 3.93，p<.001）和 2 倍（优势比 = 1.97，p=.029）。然而，与男性相比，女性报告从在线内容类别获取建议来源的可能性也低 40% 至 75%；具体而言，包括一般研究（p=.007）、专业页面（p<.001）、在线论坛（p<.001）、共享在线内容（p=.014）和技术广告（p=.018）（也就是说，男性报告这些建议来源的可能性是女性的 2 至 4 倍）。这些发现与以往的指示性研究大体一致 [53]，也与此前将教育水平较低和较少可能以同事或政府网站作为建议来源联系起来的研究相符 [78],；我们的不同性别群体教育水平相当。

计算机/信息技术背景。对于 没有 计算机/信息技术背景的子样本（n=504），性别对建议来源偏好的预测与表2类似，此外：女性从培训中获得建议的可能性显著高于男性。

对于具有计算机/信息技术背景的子样本（n=100），唯一显著的模型显示，女性从家人处获得 SP 保护建议的可能性是男性的 5.9 倍，而男性从在线论坛获得该建议的可能性是女性的 6.9 倍。

多重建议使用。表格3 显示，15.7%的参与者表示不了解或未使用任何 SP 建议来源，近 50% 表示仅使用 1 个来源，其余参与者表示使用了 1 个以上的 SP保护建议来源。更高的

表 2：回归结果，呈现女性（相较于男性）报告使用各建议来源的可能性。统计上显著的模型（p<.05）已突出显示。OR 指女性与男性（基准组）之间的优势比，CI 为置信区间，p值指性别的影响。

来源	OR	95% 置信区间	p值	
家人	**3.93**	**[2.41 - 6.42]**	**<.001**	***
朋友	1.07	[0.66 - 1.57]	.940	
来自工作/同事	**1.97**	**[1.07 - 3.63]**	**.029**	*
面对面／线下	1.65	[0.81 - 3.36]	.168	
一般研究	**0.61**	**[0.42 - 0.87]**	**.007**	**
专业页面	**0.27**	**[0.15 - 0.49]**	**<.001**	***
在线论坛	**0.25**	**[0.12 - 0.52]**	**<.001**	***
在线评论	0.84	[0.48 - 1.48]	.552	
共享在线内容	**0.47**	**[0.25 - 0.87]**	**.014**	*
科技广告 / 品牌 / 杂志	**0.50**	**[0.29 - 0.89]**	**.018**	*
新闻 / 电视节目	0.78	[0.46 - 1.30]	.344	
培训	1.14	[0.55 - 2.39]	.722	
系统提示	0.89	[0.36 - 2.22]	.804	

注：显著性代码：‘***’.001,‘**’.01,‘*’.05

表3：报告使用零个至多个 SP 保护建议来源的女性和男性百分比

建议来源数量	% 总体	% 女性	% 男性
不了解／未使用	15.7	19.8	11.6
仅有一个来源	47.7	47.9	47.5
多个来源	36.5	32.3	40.8

报告不了解或未使用任何安全与隐私建议来源的女性比例高于男性，而报告使用多个建议来源的男性比例更高。

我们在图 2 中直观呈现女性与男性使用多种建议来源的情况。再次可以看到性别差异，具体而言：(1) 相较于男性，更多女性仅从家人（13.9%）、朋友（4%）、线下来源（3.6%）、同事或工作（4.3%）获取 SP 建议；(2) 相较于女性，更多男性仅从“在线内容”或“其他方法”类别中的建议来源获取建议，在线评论除外——其中，13.3% 的人仅提及一般研究，5% 仅提及专业页面，4.7% 仅提及在线论坛；(3) 对男性和女性而言，一般研究都是最常与另一种建议来源搭配使用的建议来源；(4) 一般研究（单独使用或与其他来源搭配）是男性最常使用的建议来源，而家人（单独使用或与其他来源搭配）则是女性最常使用的建议来源，

4.2 不同性别间的安全与隐私

我们探讨研究问题2，即女性与男性分别使用哪些安全与隐私技术及方法。参与者提及的安全与隐私技术及方法完整列表见表7，附录C，以下总结男女在使用方面的差异：从图3可以看出，男性使用技术类安全与隐私措施的比例较高，而女性的安全与隐私行为则不那么成熟，她们更多使用内置类型的安全与隐私功能，以及比男性更多地采用非技术方法。

我们发现，男性使用技术型SP的可能性显著更高，$\chi^2(1) = 16.746$，$p < .001$；而女性报告未使用SP方法的可能性显著更高，$\chi^2(1) = 11.461$，$p = .001$。在非技术型SP方面，不同性别之间没有显著差异。附录8中的列联表C对此提供了支持，该表汇总了女性与男性使用SP方法的情况。

4.3 建议来源偏好的影响

我们研究研究问题3，即鉴于不同性别之间的差异，建议来源与安全与隐私使用有何关联及影响。

4.3.1 建议来源与安全与隐私使用的关联

我们通过对应分析（CA）考察不同性别中建议来源与安全与隐私技术及非技术方法使用之间的统计关联 [39]，并在图4的空间图中展示关联强度。

我们发现，SP 与建议来源之间存在显著关联，$\chi^2 = 551.203$，$p < .001$，其中第一维度（Dim1）解释了数据中 43.92% 的方差，而第二维度（Dim2）解释了 12.70%。这两个维度合计解释了 55.62% 的变异。图4中，同色点彼此接近表明它们具有相似性：地图上彼此靠近的建议来源（红点）具有相似的安全与隐私技术和方法使用情况，而距离较远的则不同；红蓝点彼此接近则表明两者存在关联。图4 直观地展示了建议来源从（1）左侧的“不知道”（以“don’t know”表示），到（2）社会关系网络中的建议来源（以“family”“friends”“from work and colleagues”以及“f2f_offline”表示），再到（3）最右侧可能涉及更复杂技能的建议来源（以“training”“specialist pages”和“online forums”表示）。空间图直观地显示，第一维度中“don’t know”一端（x 轴负向）与不使用任何安全与隐私技术和方法（以“donotremember-nothing”表示）关系更密切。相比之下，第一维度中社会关系网络里的建议来源与“other non tech”“other tech”、隐私和安全设置（通常为内置设置）、其他安全实践、密码、内置安全功能（以及限制参与和不打开可疑电子邮件）及女性性别组更为接近。“News and TV shows”与防火墙、双重身份验证/多重身份验证的关联更为密切。此外，第一维度中涉及更复杂技能的一端（以培训、专业页面和在线论坛为建议来源）与反恶意软件、VPN、反跟踪

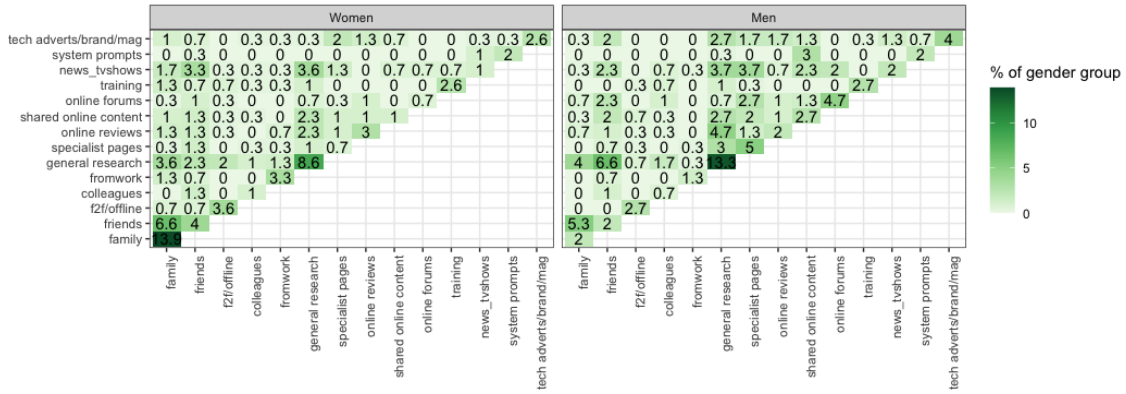


图2：不同性别使用多个建议来源的比例

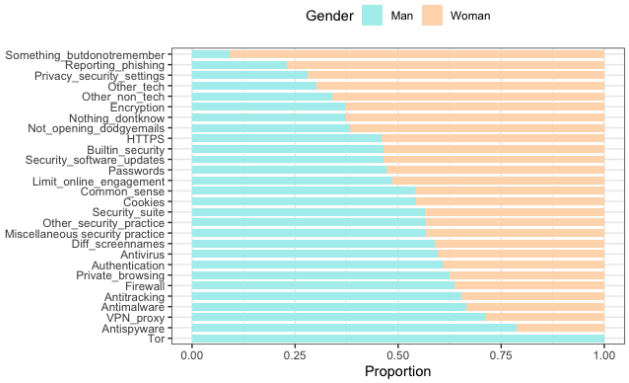


图3：列举特定安全与隐私技术及方法的女性和男性比例

或反间谍软件以及男性性别组密切相关。

4.3.2 建议来源对安全与隐私技术使用的影响

我们研究建议来源如何预测安全与隐私技术的使用情况，具体考察：（1）建议来源的类型；以及（2）所使用的建议来源数量。

建议来源类型。我们选择重点关注安全与隐私技术，而不是技术与方法的组合，以具体评估不同建议来源对技术使用的影响。

我们旨在进行二项逻辑回归分析，以“至少使用一种 SP 技术”与“未使用任何 SP 技术”为因变量，并以建议来源作为预测变量。我们在数据中观察到“准完全分离”现象 [51, 74, 94]，即解释变量几乎可以完美预测二元结果变量 [3]。具体而言，我们发现，培训、在线论坛、在线评论、专业页面和系统提示等建议来源中，只有 *1* 或 *2* 名参与者未使用 SP 技术；而共享在线内容的这一数字为“小于或等于 *5* 名”参与者未使用 SP 技术，如附录图 7所示，而大多数使用这些来源的参与者都报告称使用了 SP 技术。

在含有二元预测变量的应用逻辑回归中，分离是一个常见问题 [94], , 可通过贝叶斯 logit 回归 [36, 37] 加以解决。正如 Gelman 等人 [36]所建议的，可使用弱信息型 Cauchy (0, 2.5) 先验分布对系数进行正则化。我们使用 R [38]中 arm 软件包的 bayesglm 建立贝叶斯 logit 回归模型。该模型显著，$R^2 = 12.4$，AIC 为 538.29。表4显示，尽管社会关系类别下的建议来源（例如家人、朋友、同事、工作关系或其他线下联系人）对 SP 技术的使用没有显著影响，但“在线内容”和“其他方法”类别下的建议来源能够显著预测 SP 技术的使用。例如，与没有通过培训了解 SP 技术的人相比，通过培训了解 SP 技术的人使用该技术的可能性接近 10 倍，优势比为 $= 9.62$，$p = .007$；通过一般研究、专业页面、在线论坛和在线评论等在线内容了解 SP 技术的人，使用该技术的可能性分别约为未从这些来源获得建议者的 3 倍、8 倍、11 倍和 6 倍。我们还发现，与未从这些来源获得建议的人相比，从广告或知名技术公司、银行或消费者杂志提供的定向信息中获益的人，使用 SP 技术的可能性高出 5 倍，优势比为 $= 5.21$，$p = .004$。建议来源的数量。我们以所使用的 SP 建议来源数量为预测变量，以“至少使用一种 SP 技术”与“未使用任何 SP 技术”为目标变量，计算了二项逻辑回归模型。模型显著，χ^2 型拟合良好（$C = .678$），准确率为 80.8%，R^2 介于 9.0%（Cox & Snell）和 14.5%（Nagelkerke）之间。我们发现，与未使用任何 SP 建议来源的人相比，使用单一来源的人使用 SP 技术的可能性高出 5.4 倍，$p<.001$；使用 2 个来源的人高出 7.1 倍，$p<.001$；使用至少 3 个建议来源的人

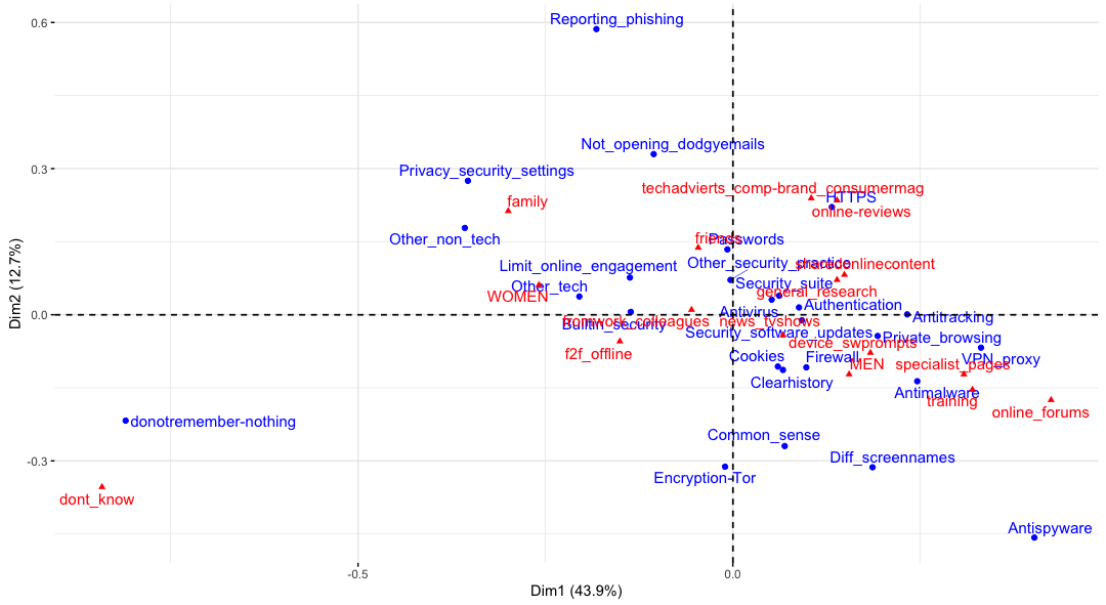


图4：关联　　安全与隐私技术和方法（蓝色）与建议来源之间的关联空间图（红　　*d)*

表4：使用防护性SP技术与不使用的贝叶斯逻辑回归。

预测变量	OR	p值	
家人（与非家人相比）	1.10	.734	
朋友（相较于没有）	1.43	.252	
工作_同事（相较于没有）	1.28	.530	
其他面对面_线下（相较于没有）	1.17	.717	
一般研究（相较于错误）	**2.99**	**<.001**	***
专业页面	**8.08**	**.002**	**
在线论坛	**11.13**	**.004**	**
在线评论	**5.61**	**.011**	*
共享在线内容	2.08	.139	
来自公司的广告/信息& 消费者杂志	**5.21**	**.004**	**
news	1.05	.909	
培训	**9.62**	**.007**	*
系统提示和设置	3.53	.076	

注：显著性代码为 '***' .001,'**' .01,'*' .05

使用 SP 技术的可能性高出 9.1 倍，p<.001。

4.4 寻求 ISC 建议的动机

我们探讨研究问题 4，即女性和男性出于什么原因向 ISC 寻求 SP 保护建议。总体而言，63%（n=382）的参与者回答是，表示曾向 ISC 寻求保护性SP信息和建议；37%（n=222）的参与者回答否。我们首先描述参与者给出的理由，其次考察这些理由中的性别模式。

4.4.1 理由描述

下面对参与者选择接触或不接触 ISC 的理由进行分类和描述，并提供示例附录中的表 10所列回答。

为安全与隐私接触 ISC。 参与者为保护安全与隐私而选择接触 ISC 的理由，按对 ISC 技能的认知、ISC 特质、参与者自身技能或"其他"进行分类。

ISC 技能。 39.3%的参与者提到了自己感知到的 ISC 技能，其中大多数谈及一般知识、技能、经验或 IT 工作，少数特别提到了 SP 技能。

- （一般性）信息系统与计算机（*ISC*）知识：（a）一般性知识；（b）认为自己的 ISC 知识比自己更丰富；或（c）以某种方式提及"专业领域"，但未具体指明安全与隐私（SP）。

- *ISC* 的技术技能：（a）大多是一般性技能，（b）少数是具名安全技能。
- *ISC* 从事*IT*工作：（a）笼统提及从事信息技术工作/在 IT 相关领域工作，（b）指出计算机的某个领域（但非安全），或（c）极少数回答提及从事安全工作。 [**（a-b）不保证具备 SP 专业知识**]

- *ISC*经验：(a) 广义上感知到的 ISC 经验，或 (b) 认为 ISC 过去曾有识别最佳工具／方法的经验。

- 最新动态：ISC 了解技术发展的最新进展。

ISC 特质。 16。2% 提到了对 ISC 特质的看法，包括：

- 可信赖：（a）总体上信任 ISC 或 ISC 建议，或（a）由于 ISC 被认为具备相应的技能和经验而信任 ISC。

- 易于接触：易于接触 ISC 建议或能够快速联系。

• 有帮助：(a) ISC 有帮助或能够帮助他们，或 (b) 提供良好／有帮助的建议。
• 可联系：(a) 有可寻求帮助的 ISC，或 (2) 他们的 ISC（随时）可以提供这类帮助。
• 可靠：具体而言，他们的 ISC 值得信赖。

参与者自身技能。 7.1% 的参与者提及了自身的技能水平，具体包括：(1) 他们需要帮助，或需要某些自己无法找到的建议或信息；(2) 他们缺乏 SP知识；或 (3) 信心不足。

其他原因。 10.6% 的参与者给出了与上述类别不同的原因，例如：

• 了解选项／相互交流：(a) 了解可用的选项，(b) 交流分享建议和经验。

• *reassurance*：联系 ISC，(a) 征求第二意见，(b) 获得 reassurance，或确认其 SP实践是否正确，或 (c) 避免犯错。

• 其他/无：少数参与者给出了各种陈述，这些陈述不属于上述原因。

尽管来自 ISC 的建议未必有风险，但遗憾的是，女性参与者提到的判断依据，例如从事IT工作、可信度或易于接触（与以往研究相辅相成 [79]），并不能保证 ISC 实际具备提供建议和促进学习所需的 SP 技能；以往研究也指出，家人未必是 SP专家 [56]。相比之下，男性给出的理由表明他们进行了更多分析性对话（例如评估选项）。

不向 ISC 寻求 SP 方面的帮助。 参与者不向自己的 ISC 获取保护性SP信息的理由，可归纳为对其技能的看法及其他原因，详述如下。

参与者自身技能。 17.5%的参与者给出的理由涉及他们更强的技能、自立或信心。

• 自力更生：(a)他们更愿意依靠自己；(b)他们能够自行摸索如何进行 SP保护。
• 更强的技能：(a) 他们认为自己的（技术）技能比 ISC 更先进；(b) 他们认为 ISC 知识不如自己／没有相关技能。
• 信心：有信心找到 SP 信息，或对自己的能力有信心。

其他理由。 19.5% 的参与者提到了不向 ISC 寻求 SP保护的其他理由，例如：(1) 更偏好其他来源（如在线来源）；(2) 不需要帮助，或有其他原因，例如没有遇到问题；(3) 自己是帮助他人的人。

4.4.2 性别模式与差异

75.9%的 n=303 女性参与者和50.5%的 n=301 男性参与者回答是 会寻求保护性SP信息和建议方面的ISC。我们通过 χ^2 检验，考察了性别与是否会寻求ISC之间的关联。结果发现，性别与个体通常是否会寻求ISC之间存在显著关联，$\chi^2(1) = 41.939$，$p < .001$，Cramer$V = .264$。

在报告 是 会向 ISC 求助的人中，相较于男性，更高比例的女性是受到以下对 ISC 的看法所驱动：ISC 具备一般知识、掌握最新技术、从事信息技术相关领域的工作、拥有技术／SP 技能或经验，以及可信度、易于接触和助人性，如图 5所示。然而，相较于女性，更高比例的男性表示，他们向 ISC 求助是为了了解各种 SP 选项、获得 reassurance、因为自己知识不足，或认为 ISC 可靠。相比之下，图 6 显示，相较于女性，在所有理由中，表示 否 不会向 ISC 求助的男性比例更高（理由包括信心、更强的技能、自立或偏好其他来源，以及自己是帮助他人的人）。

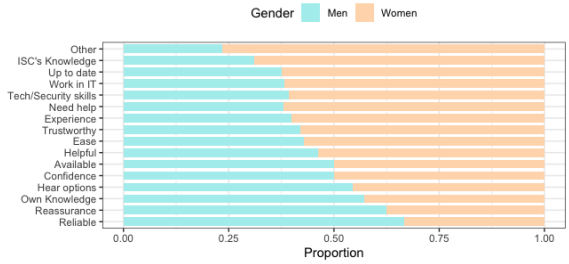


图5：在赞成接触 ISC 的理由中男性与女性的比例

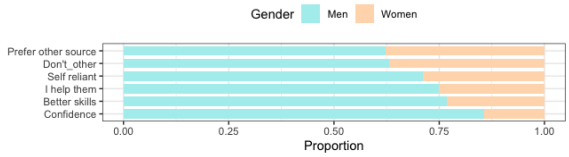


图6：在反对接触 ISC 的理由中男性与女性的比例

4.5 从 ISC 获得的建议

我们探讨 RQ5，即了解向 ISC 寻求安全与隐私保护建议的参与者中，63%（n=382）表示是的，他们收到了哪些建议。如第3.4节所述，建议分为具体建议（例如恶意软件保护或沟通隐私方面的建议）和一般建议（例如如何确保在线安全）。我们在附录的表11 中列出了具体建议及示例回答，并在图8中总结了女性与男性收到的建议。主要观察到的模式是：（i）男性收到有关“恶意软件／诈骗”的建议的比例高于女性，这类建议包括防病毒软件、病毒威胁、反恶意软件、恶意软件威胁、反间谍软件、欺诈，以及“沟通和网络隐私”；（ii）女性收到有关“身

份验证”的建议的比例较高，这类建议包括更改密码、使用多个密码、使用／设置强密码、使用密码管理器或启用多重身份验证；以及“隐私设置和社交网络服务”。

5 讨论

我们总结研究发现，并讨论这些发现如何拓展现有文献，以及它们对公平的网络安全有何启示。

要点。总体而言，研究发现如下：（1）女性与男性对 SP 获取和技术使用模式的报告各不相同，体现出 SP 性别鸿沟；（2）与来自 ISC 的建议相比，在线建议与 SP技术使用的关联更强，也更能预测 SP技术使用；（3）女性与男性报告了寻求 ISC 帮助的不同理由，也获得了不同的 SP 建议。

社会角色理论指出，社会角色的分化会催生性别化期望与刻板印象，例如女性被认为具有社群性／支持性特质，男性则被认为更有能动性／自信表达能力；这些期望与刻板印象进而导致人们习得不同的技能，并形成不同的行为方式 [25]。我们的研究发现可以被解释为源自性别刻板印象（无论是个人认同的，还是符合普遍持有的刻板印象）。具体而言，男性较少寻求 ISC 帮助，或可归因于不鼓励求助的男性气质态度 [45] 以及 SP刻板印象，即男性不太可能求助且过度自信（或者人们认为女性在 SP 方面能力不足，因此更愿意求助） [91]。此外，男性更常报告使用在线建议并参与 SP技术使用，这与 STEM 中的性别刻板印象有关：技术参与被视为一种 性别类型化活动 [52, 82], ；同时，人们还认为男性对整体防护更感兴趣、技能更强，或认为 SP 对女性而言过于复杂，因而女性会将其交由他人处理 [91]。男性参与者对新技术系统的亲和度高于女性参与者（如第 3.2 节所述），也支持这一观点。这种亲和度差异可能反映了社会因素，但也表明女性较少倾向于自主探索（技术层面的）SP。

除了性别之外，人们还具有种族、文化、性取向和社会经济身份，这些身份与其性别认同相互交织并彼此重叠 [17, 21]。这些因素会为 SP 获取、参与和网络安全结果带来某种特权或劣势（参见相关研究 [9, 90]），还会影响人们对 SP 的看法和态度 [48] 以及由此产生的 SP 经验（和需求） [35]。虽然我们没有控制这些因素，但不同性别之间的教育水平是均衡的。因此，观察到的明显 SP 性别鸿沟表明，对于与我们样本相似的用户群体而言，性别认同对于在线 SP 获取和参与具有相对重要的作用。不过，仍需进一步研究，以剖析交叉身份在 SP 情境下可能产生的影响。

对公平网络安全的启示。 我们补充了有关女性与男性之间存在性别差距和不平等的安全与隐私经验的证据 [20, 64, 66], , 并将性别分析引入安全与隐私建议文献 [72, 73, 77, 78]。这种保护方面的差距已表明存在网络安全鸿沟，并引发了对网络安全机会是否公平的质疑，也就是通过在线建议获取安全与隐私信息，以及安全与隐私技术可供性，是否经过适当配置并能满足女性的需求。关于安全与隐私是否适用的质疑，得到了“性别盲视”论点的支持：技术变革受到社会规范的影响 [7]，而这些技术的设计及其意义是在性别关系中形成的，因此反映了既存的性别不平等 [69],，例如，欧洲技术类工作中只有17%由女性担任 [28]。在线安全与隐私建议数量庞大、类型多样，众所周知，这些建议容易令人不知所措，且缺乏优先排序 [80],；这也可能比男性面临的障碍更严重地阻碍女性实现在线安全。

尽管发达国家（如英国）的女性拥有平等的技术获取机会和较高的教育水平 [2,12,68],，且据称发达国家中的性别数字鸿沟正在缩小 [89],，但这并不意味着她们能够获得同等的网络安全结果 [63]，也不意味着她们能够像本研究所示那样平等地获取和参与 SP 技术。数字鸿沟更大的国家，其 SP 差距可能会更加严重。总体而言，本研究支持“女性在网络环境中面临更高风险”的相关报告 [63]，前提是女性采用的获取方式和非技术策略无法带来与男性相同的在线安全结果。

6 项可行的推荐

我们为关注网络安全生态系统的利益相关方提出建议。

易于获取且有效的在线建议。我们的研究结果促使我们质疑在线安全建议的相关性、可及性和适用性，尤其是那些将 SP 技术作为保护手段、面向女性的建议。

首先，我们建议采取措施，确保在线建议生态系统能够满足广大女性群体的多样化需求，同时也提供针对特定威胁情境（如亲密伴侣暴力）的建议。在线安全建议的设计需要切合不同女性评估威胁和应对威胁的方式。鉴于 (a) SP 的情感维度 [19, 29, 85], 、(b) 女性更可能对在线威胁情境进行情绪化评估 [20],，以及 (c) 相关应对行动能够提供一种情绪应对方式 [16, 44, 65]，在设计 SP 和数字建议所提供的功能时，应融入可信度（如参与者所报告）和情感支持感。此前研究提出的建议也支持这一观点 [35]：以情感支持为先的沟通质量更高 [30]。例如，在实践中，在线安全建议所使用的语言应能代表其旨在服务的女性群体，而不应像先前报告所指出的那样，过度技术化 [80]。

第二，基于我们研究发现的补充，以及先前研究所提出的有关优先排序和.....的问题。

在线 SP 建议的可操作性 [80], 以及不同来源之间的碎片化问题 [78],鉴于当前影响女性的威胁形势，我们建议对一组核心在线来源及优先建议进行标准化，并持续修订。总体而言，当前关于在线 SP 建议体系对女性（以及不同性别群体）的有效性证据不足，这一问题亟待解决。

SP 技能。 与有关技术性网络技能 [40] 对建议来源偏好影响的研究相比， [77],我们的性别群体在信息导航、社交和移动技能各项量表上的数字技能相近，而在操作技能和创造性技能方面略有差异（通过互联网技能量表测量 [88]），这引发了关于在线安全所需数字技能组合的疑问。

首先，我们建议评估并明确理解和采取在线安全及 SP 技术建议所需的数字技能类型和水平，同时探索培养这些技能的方法，使人们得到支持，而不是只能自行弥补技能差距。鉴于我们注意到女性对技术系统的亲和力较低，这也关系到增强人们对 SP保护的信心。其次，为确保 SP 机会公平，我们建议设计建议和 SP 技术参与方式，使任何人无论技能水平如何，都能获得最佳保护。

获得社会支持的 SP。 正如我们的证据所示，ISC 建议为传统的个人主义 SP 设计提供了有价值的替代方案。与让个人用户独自承担解决问题的重任相比，它提供了一种协作、互助且有支持的方式，尤其有助于应对 SP 的复杂性，或攻击发生后的（心理和情绪）影响；这也包括用户可能尚无保护经验的新型攻击。我们提出建议，以支持有关社会化 SP 的研究 [84, 93]。

首先，我们建议 SP 技术提供由社群支持的版本，并根据用户偏好提供网络安全建议。其次，我们建议采用便于任何人寻求帮助或比较信息／选项的技术功能，无论是向熟人还是匿名求助。我们建议制定一份清单，明确应询问哪些问题以及应向谁寻求 SP 建议，因为女性参与者提供的启发式方法并不能保证 ISC 具备 SP 技能。第三，我们建议借鉴女性的策略，并开发能够维持面对面对话、使其有效支持学习的方法（例如简短易用的模板、多模态的传递方式、保护措施评估与反馈——在线／线下空间皆适用）；同时重新构想在线 SP，将女性采用的 SP 模式纳入其中，并促请设计者考虑技术中的刻板印象线索如何导致性别化的数字参与 [15, 55]。

性别议程。 我们距离解决性别差距还很遥远，许多未知问题仍然存在。我们强烈建议制定一项多视角研究议程，重点了解性别规范、刻板印象和交叉身份所发挥的作用发挥 SP 机会、获取途径和结果，以及性别理论在 SP 中的作用，例如 [33]。这需要：（1）共同努力并投入专门资源；（2）多学科研究人员与政策制定者、社区支持组织及 SP 倡导团体等利益相关者开展合作；（3）与地方及国际机构合作，这些机构一直呼吁采取行动，共创安全、公平的数字未来，并保障女性的在线安全 [62, 87]。

对公平的批判性反思。人们认为，发达国家的数字鸿沟正在缩小，在线建议也增加了获取 SP 的机会；然而，如何借此实现有助于维持 SP 使用并带来安全结果的有效且有意义的参与，仍有待探讨，正如本研究所示，女性尤其如此。此外，优质建议缺乏优先排序 [80] 与共识 [81]。

鉴于我们的研究结果显示，SP 机会与参与存在性别鸿沟，这一点体现在 SP 技术获取和使用方面的差距上，我们强烈建议更广泛的 SP 社群——包括研究人员、开发者、技术提供方、在线安全倡导者和政策制定者——采取批判性的反思行动，以回应以下问题：‘我们生产 *SP* 技术究竟是为了谁？’鉴于在线安全被视为一种社会公益，且国际人权组织倡导其公平性 [87], ‘就 *SP* 机会、获取、参与或结果而言，在线安全中的性别公平包含什么？’考虑到与男性相比，女性在个人、社会和经济方面的现实处境以及其社会文化角色，‘*SP* 平等（例如获取方式、分配和设计上的平等）能否带来公平的网络安全结果？’

公平保障。 鉴于基于性别的 SP 获取和参与可能使社会中的广大群体处于劣势，我们建议制定一套*SP* 公平保障框架及配套的技术政策，例如要求：(1) 在线 SP 提供方证明其在开发和分配过程中落实了公平保障，例如考虑女性的个人、社会和经济现实及其在线安全需求；(2) SP 倡导者、政策制定者和研究人员共同制定公平指标和标准。

7 结论

这项实证研究从保护性 SP 获取和保护结果两个层面对在线安全进行了性别分析，尤其表明，女性通过 ISC 表现出的独特 SP 获取偏好意味着她们无法享有广度和质量兼具的在线SP 建议，进而导致其 SP 技术参与程度较低，并可能影响保护结果（从而体现出 SP 性别差异），同时为此前关于 SP 性别鸿沟的少量证据增添了新的支持。因此，本研究（1）支持了与男性相比女性在网上面临更高风险的观点；（2）支持了国内外关于采取行动保障女性在线安全的呼吁；（3）并就多利益相关方行动提出建议，以确保女性受到保护。

参考文献

[1] Alison Adam。《性别、伦理与信息技术》。施普林格，2005年。[2] AdvanceHE。高等教育中的平等：2021年统计报告，2021年。[3] Adelin Albert和John A Anderson。逻辑回归模型中最大似然估计的存在性。《Biometrika》，71(1)：1–10，1984年。[4] Anita L Allen。《不安的访问：自由社会中的女性隐私》。Rowman & Littlefield，1988年。[5] Anita L Allen和Erin Mack。隐私如何具有性别。《N. Ill. UL Rev.》，10：441，1989年。[6] Mohd Anwar、Wu He、Ivan Ash、袁晓红、李玲和徐力。性别差异与员工的网络安全行为。《人类行为中的计算机》，69：437–443，2017年。[7] D Barbieri、J Caisl、M Karu、G Lanfredi、B Mollard、V Peciukonis和L Salanauskait˙e。2020年性别平等指数：数字化与工作的未来。《卢森堡：EIGE》，2020年。[8] Kim Bartel Sheehan。对在线隐私顾虑中的性别差异及由此产生的行为的调查。《互动营销期刊》，13(4)：24–38，1999年。[9] Catherine Barwulor、Allison McDonald、Eszter Hargittai和Elissa M Redmiles。“在美国主导的互联网上处于劣势”：性别、工作与技术。载于*2021*年计算机系统中的人为因素国际会议论文集，第1–16页，2021年。[10] Wilfried Bos和Christian Tarnai。实证社会研究中的内容分析。《国际教育研究期刊》，31(8)：659–671，1999年。[11] Pierre Bourdieu和John G Richardson。资本形式。1986年。[12] 英国广播公司。英国大学课程中女性比例创历史新高，2017年。[13] Moritz Büchi、Noemi Festic、Natascha Just和Michael Latzer。在线隐私保护中的数字不平等：年龄、教育和性别的影响。载于《数字不平等手册》。爱德华·埃尔加出版社，2021年。[14] 陈洪亮和Christopher E Beaudoin。社会网站的实证研究：探索社会资本和信息披露的影响。《远程信息处理与信息学》，33 435，2016 2 432( )：–。[15] Sapna Cheryan、Victoria C Plaut、Paul G Davies和Claude M Steele。环境归属感：刻板印象线索如何影响计算机科学中的性别参与。《人格与社会心理学期刊》，97(6)：1045，2009年。[16] Hichang Cho、李鹏翔和Zhang Hao Goh。隐私风险、情绪与社交媒体：在线隐私的应对模型。《ACM计算机与人类交互汇刊》，27 28，2020 6 1( )：–。[17] Patricia Hill Collins和Sirma Bilge。《交叉性》。约翰·威立父子出版公司，2020年。[18] Kovila PL Coopamootoo。隐私增强技术的使用模式。载于*2020*年*ACM SIGSAC*计算机与通信安全会议论文集，第1371–1390页，2020年。[19] Kovila PL Coopamootoo和Thomas Groß。为何隐私几乎被遗忘——一项关于隐私与分享态度的实证研究。《Proceedings on Privacy Enhancing Technologies》，4：39–60，2017年。[20] Kovila PL Coopamootoo、Maryam Mehrnezhad和Ehsan Toreini。“我感到被侵犯、恼怒、焦虑，而且可能会保护自己”：不同性别和国家的个体对在线跟踪的感受及其保护行为。《USENIX安全研讨会》，2022年。[21] Kimberle Crenshaw。《边缘制图：交叉性、身份政治与针对有色人种女性的暴力》。《斯坦福法律评论》，43 1241，1990：。[22] “Standout CV”。英国毕业生统计数据，2022。[23] Sauvik Das、Tiffany Hyun-Jin Kim、Laura A Dabbish 和 Jason I Hong。社会影响对安全敏感度的影响。载于第十届可用隐私与安全研讨会（{SOUPS} *2014*），第 143–157 页，2014。[24] Sauvik Das、Adam DI Kramer、Laura A Dabbish 和 Jason I Hong。社会影响在安全功能采用中的作用。载于第十八届 ACM 计算机支持的协同工作与社会计算会议，第 1416–1426 页，2015。[25] Alice H Eagly。《社会行为中的性别差异：一种社会角色解释》。心理学出版社，2013。[26] 电子前哨基金会。EFF 技术团队提供的工具，2022。[27] Nicole B Ellison、Jessica Vitak、Charles Steinfield、Rebecca Gray 和 Cliff Lampe。在社交媒体环境中协商隐私顾虑与社会资本需求。载于《在线隐私》，第 19–32 页。施普林格，2011。[28] 欧洲性别平等研究所。信息通信技术行业的工作与生活平衡，2022。[29] Fariborz Farahmand 和 Firoozeh Farahmand。隐私决策：脑科学方法。《计算机》，52(4):50–58，2019。[30] Bo Feng。对支持性交往中建议提供整合模型的检验。《人类传播研究》，35(1):115–129，2009。[31] 英国国家统计局。新冠肺炎（COVID-19）疫情期间毕业生劳动力市场结果：职业转换与技能错配，2021。[32] Thomas Franke、Christiane Attig 和 Daniel Wessel。技术交互的个人资源：技术交互亲和度（ATI）量表的开发与验证。《国际人机交互期刊》，35(6):456–467，2019。[33] Regine Frener 和 Sabine Trepte。在线隐私研究中的性别理论化。《媒体心理学杂志》，2022。[34] Steven Furnell 和 Liam Moore。安全素养：当今在线社会中缺失的一环？《计算机欺诈与安全》，2014 18，2014 5 12( ): – 。[35] Christine Geeng、Mike Harris、Elissa Redmiles 和 Franziska Roes-ner。“像女同性恋者一样沿着边缘行走”：{美国}.{LGBTQ+} 群体关于在线安全、人身安全和隐私建议的经验。载于第 31 届 USENIX 安全研讨会（USENIX Security 22），第 305–322 页，2022。[36] Andrew Gelman、Aleks Jakulin、Maria Grazia Pittau 和 Yu-Sung Su。逻辑回归及其他回归模型的弱信息默认先验分布。《应用统计年鉴》，2 1383，2008 4 1360( ): – 。[37] Andrew Gelman 和 Cosma Rohilla Shalizi。贝叶斯统计学的哲学与实践。《英国数学与统计心理学杂志》，66(1):8–38，2013。[38] Andrew Gelman、Yu-Sung Su、Masanao Yajima、Jennifer Hill、Maria Grazia Pittau、Jouni Kerman、Tian Zheng、Vincent Dorie 和维护者 Yu-Sung Su。“arm”软件包。《使用回归和多层级/层级模型进行数据分析》，2013。[39] Michael Greenacre。《对应分析实践》。Chapman and Hall/CRC，2017。[40] Eszter Hargittai 和 Yuli Patrick Hsieh。网络使用技能的简明调查测量指标。《社会科学计算机评论》，30(1):95–107，2012。[41] Ellen Johanna Helsper 和 Rebecca Eynon。通往数字参与的不同技能路径。《欧洲传播学杂志》，28(6):696–713，2013。

[42] Tabitha James、Quinton Nottingham 和 Byung Cho Kim。确定公众层面数字安全实践的前因。《Information Technology and Management》，14 89，2013 2 69( ): – 。[43] Michael John Jones 和 Paul A Shoemaker。会计叙事：内容与可读性实证研究综述。《Journal of Accounting Literature》，13:142，1994。[44] Yoonhyuk Jung 和 Jonghwa Park。基于位置的服务中隐私顾虑、情感反应与应对行为之间关系的调查。《International Journal of Information Management》，43:15–24，2018。[45] Joshua Juvrud 和 Jennifer L Rennels。“我不需要帮助”：性别刻板印象如何预测寻求帮助行为中的性别差异。《Sex Roles》，76:27–39，2017。[46] Richard H Kolbe 和 Melissa S Burnett。内容分析研究：应用考察及提升研究可靠性与客观性的指导。《Journal of Consumer Research》，18(2):243–250，1991。[47] Priya Kumar、Shalmali Milind Naik、Utkarsha Ramesh Devkar、Marshini Chetty、Tamara L Clegg 和 Jessica Vitak。“密码不能告诉别人，因为它们是私密的”：理解儿童对在线隐私与安全的心智模型。《Proceedings of the ACM on Human-Computer Interaction》，1(CSCW):1–21，2017。[48] Michelle Kwasny、Kelly Caine、Wendy A Rogers 和 Arthur D Fisk。隐私与技术：民间定义与观点。载于《CHI'08 Extended Abstracts on Human Factors in Computing Systems》，第 3291–3296 页。2008。[49] Nan Lin。《社会资本：社会结构与行动理论》。第 19 卷。剑桥大学出版社，2002。[50] Catharine A MacKinnon。《迈向女性主义国家理论》。哈佛大学出版社，1989。[51] Mohammad Ali Mansournia、Angelika Geroldinger、Sander Greenland 和 Georg Heinze。逻辑回归中的分离：成因、后果与控制。《American Journal of Epidemiology》，187(4):864–870，2018。

[52] Allison Master。性别刻板印象影响儿童对科学、技术、工程和数学的兴趣。*Child Development Perspectives*，15(3):203–210，2021。[53] Maryam Mehrnezhad、Kovila PL Coopamootoo 和 Ehsan Toreini。人们如何以及是否会保护自己免受在线跟踪？*Proceedings on PrivacyEnhancing Technologies*，1：105–125，2022。[54] 微软。拓展你的在线安全知识，2022。[55] Mary C Murphy、Claude M Steele 和 James J Gross。威胁信号：情境线索如何影响女性在数学、科学和工程领域的表现。*Psychological Science*，18(10)：879–885，2007。[56] Savanthi Murthy、Karthik Bhat、Sauvik Das 和 Neha Kumar。个体易受攻击，集体更安全：老年人家庭的安全与隐私实践。载于计算机支持的协同工作，2021。[57] 英国国家网络安全中心。建议与指导。[58] Kimberly A Neuendorf。内容分析指南。Sage，2002。[59] James Nicholson、Lynne Coventry 和 Pa mela Briggs。“如果很重要，就会上头条”：老年人如何搜寻网络安全信息。载于*Proceedings ofthe 2019 CHI Conference on Human Factors in Computing Systems*，第1–11页，2019。[60] James Nicholson 和 Jill McGlasson。Cyberguardians：通过嵌入式点对点支持提升社区网络韧性。载于*Companion Publication of the 2020 ACM Designing Interactive Systems Conference*，第117–121页，2020。[61] Norbert Nthala 和 Ivan Flechais。非正式支持网络：对家庭数据安全实践的调查。载于第十四届可用隐私与安全研讨会（{*SOUPS*} *2018*），第63–82页，2018年。

[62] 通信办公室。Ofcom敦促科技公司保障女性的在线安全，2022年6月。[63] 通信办公室。《在线国家》。技术报告，通信办公室，英国，2022年。[64] Isabelle Oomen 和 Ronald Leenes。隐私风险感知与隐私保护策略。载于身份管理政策与研究，第121–138页。施普林格，2008年。[65] Jonghwa Park、Hanbyul Choi 和 Yoonhyuk Jung。用户对智能音箱隐私风险的认知与情感反应。《国际人机交互期刊》，37 771，2021 8 759( ): – 。[66] Yong Jin Park。男性和女性在隐私方面是否存在差异？互联网中的性别化隐私与（不）平等。《人类行为中的计算机》，50：252–258，2015年。[67] Yong Jin Park。隐私为何对数字不平等至关重要。载于《数字不平等手册》。爱德华·埃尔加出版社，2021年。[68] 英国议会。英格兰高等教育中的机会与结果平等。技术报告，下议院图书馆，2021年。

[69] Caroline《Criado Perez女性：一个为男性设计的世界中的数据偏见》。Abrams，2019。

[70] Clay Posey、Tom L Roberts、Paul Benjamin Lowry 和 Ross T Hightower。弥合鸿沟：对信息安全专业人员与普通组织内部人员之间信息安全思维模式的定性比较。《信息与管理》，51(5):551–567，2014。

[71] Emilee Rader 和 Rick Wash。识别非正式安全信息来源中的模式。《网络安全杂志》，1(1)：121–144，2015。

[73] Emilee Rader、Rick Wash 和 Brandon Brooks。将故事作为有关安全的非正式课程。载于第八届可用隐私与安全研讨会论文集，第 1–17 页，2012。

[74] Carlisle Rainey 。处理逻辑回归模型中的分离 。政治分析，24(3)：339–355，2016。

[75] Elissa M Redmiles。《“我是否该担心？”账户安全事件响应的跨文化考察》。载于*2019*年*IEEE*安全与隐私研讨会（*SP*），第920–934页。IEEE，2019年。[76] Elissa M Redmiles和Cody LJ Buntain。《信任、担忧和个人在线数据控制感如何影响网络使用》。载于《数字不平等手册》。爱德华·埃尔加出版社，2021年。[77] Elissa M Redmiles、Sean Kross和Michelle L Mazurek。《我学会了如何保障安全：一项具有普查代表性的安全建议来源与行为调查》。载于*2016*年*ACM SIGSAC*计算机与通信安全会议论文集，第666–677页，2016年。[78] Elissa M Redmiles、Sean Kross和Michelle L Mazurek。《数字鸿沟在哪里？关于安全、隐私和社会经济状况的调查》。载于*2017*年计算机系统中的人为因素国际会议论文集，第931–936页，2017年。[79] Elissa M Redmiles、Amelia R Malone和Michelle L Mazurek。《我觉得他们是在试图告诉我什么：数字安全的建议来源与选择》。载于*2016*年*IEEE*安全与隐私研讨会（*SP*），第272–288页。IEEE，2016年。[80] Elissa M Redmiles、Noel Warford、Amritha Jayanti、Aravind Koneru、Sean Kross、Miraida Morales、Rock Stevens和Michelle L Mazurek。《对网络上的安全与隐私建议进行全面的质量评估》。载于第*29*届*USENIX*安全研讨会（*USENIX Security 20*），第89–108页，2020年。[81] Robert W Reeder、Iulia Ion和Sunny Consolvo。《在线保持安全的152个简单步骤：为不熟悉技术的用户提供的安全建议》。《*IEEE*安全与隐私》，15(5)：55–64，2017年。

[82] Catherine Riegle ‐Crumb、Chelsea Moore 和 Jenny Buontempo ‐ 转 ‐ 变科学、技术、工程和数学领域的刻板印象？考察同伴和教师性别所发挥的作用。《青少年研究杂志》，27(3):492–505，2017。[83] Daniel Riff、Stephen Lacy 和 Frederick Fico。《分析媒体信息：在研究中运用定量内容分析》。Routledge，2014。[84] Julia Slupska、Scarlet Dawson Dawson Duckworth、Linda Ma 和 Gina Neff。参与式威胁建模：探索重新配置网络安全的路径。载于*2021*年计算机系统中的人为因素国际会议扩展摘要，第1–6页，2021。[85] Luke Stark。信息隐私的情感背景。《信息社会》，32(1):14–27，2016。[86] Frederic Stutzman、Jessica Vitak、Nicole Ellison、Rebecca Gray 和 Cliff Lampe。互动中的隐私：探索 Facebook 上的信息披露与社会资本。载于国际人工智能促进会网络与社交媒体会议论文集，第6卷，2012。[87] 联合国开发计划基金。数字战略 2022–2025，2022。[88] Alexander JAM Van Deursen、Ellen J Helsper 和 Rebecca Eynon。衡量数字技能。《从数字技能到切实成果》项目报告。2014。[89] Jan Van Dijk。《数字鸿沟》。约翰·威立父子出版公司，2020。[90] Ashley Marie Walker 和 Michael A DeVito。“‘更 gay’更合适”：在线 LGBTQ+ 空间中的社群内部权力动态及其危害。载于*2020*年计算机系统中的人为因素国际会议论文集，第1–15页，2020。[91] Miranda Wei、Pardis Emami-Naeini、Franziska Roesner 和 Tadayoshi Kohno。技能娴熟还是轻信易骗？与计算机安全和隐私相关的性别刻板印象。*IEEE*安全与隐私研讨会，2023。[92] “STEM 女性”。科学、技术、工程和数学领域女性统计数据，2022年6月。[93] Yuxi Wu、W Keith Edwards 和 Sauvik Das。Sok：社交网络安全。载于*IEEE*安全与隐私研讨会（奥克兰），2022。[94] Christopher Zorn。二元响应模型中分离问题的一种解决方案。《政治分析》，13(2):157–170，2005。

A 性别视角下的教育

表 5：不同性别的教育水平占比

教育程度	% 女性	% 男性
学校教育未完成	5.9	4.0
高中	24.4	25.2
大学	18.5	18.9
本科	34.7	41.9
硕士	14.5	9.0
PhD	2.0	1.0

B 报告的建议来源

蓝色行表示男性人数较多，玫瑰色行表示女性人数较多。

表6：总体样本（N=604）的建议来源，女性和男性人数几乎相等。

来源（报告数）	女性占比（人数）	男性占比（人数）
一般研究（163）	41.1（67）	58.9（97）
家人（101）	76.2 (77)	23.8（24）
朋友 (97)	50.5（49）	49.5 (48)
专业页面（67）	23.9（16）	76.1（51）
新闻、电视节目（65）	44.6（29）	55.4（36）
科技广告/品牌/杂志 (57)	35.1 (20)	64.9 (37)
在线评论 (54)	46.3 (25)	53.7 (29)
来自工作/同事 (49)	65.3 (32)	34.7（17）
共享在线内容（48）	33.3 (16)	66.7（32）
在线论坛 (46)	21.7 (10)	78.3 (36)
面对面／线下 (34)	61.8 (21)	38.2 (13)
培训（30）	53.3（16）	46.7（14）
系统提示和设置（19）	47.4（9）	52.6（10）

C 安全与隐私技术和方法使用

表 7：安全与隐私技术／方法

类别	安全与隐私 方法	N=604 的百分比
技术类	防病毒软件	40.7
	密码	56.2
	防火墙	16.7
	VPN／代理	12.6
	反跟踪	11.1
	反恶意软件	10.9
	无痕浏览／隐身模式	11.4
	身份验证（双重身份验证、多重身份验证）	9.3
	隐私／安全设置	8.9
	安全套件/安全品牌	5.3
	Cookie	4.0
	安全和软件更新	2.1
	HTTPS（过滤）/网站安全	1.9
	反间谍软件	1.7
	加密	1.4
	Tor	0.5
	内置安全功能	6.1
	其他技术方式	2.1
非技术性	限制线上互动	5.8
	不打开或点击随机邮件和链接	4.3
	使用不同的屏幕名称	3.6
	“常识”	1.8
	举报钓鱼邮件	0.7
	其他非技术类	2.5
无 / 其他	无/“我不知道”	16.0
	‘某些事情，但不记得了’	1.7

我们注意到，“其他技术方式”指回答中提及使用 PayPal、通知、云存储或备份系统；而“其他非技术方式”指不在线存储信息、锁定屏幕、只使用一台设备、退出账户、避开可疑网站以及仅使用安全连接。

表8：报告至少使用 1 种 SP 方法的女性与男性比例（总体 *N=604*； 女性 *n=303*； 男性 *n=301*）

安全与隐私方法类型	% 总体	% 女性	% 男性
技术类安全与隐私	80.8	74.3	87.4
非技术类 SP	16.1	17.5	14.6
无	17.5	22.8	12.3

D 准分离示意图

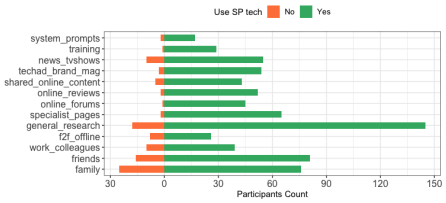


图 7：按建议来源偏好展示 SP 技术使用中的数据分离

E 示例回答与编码手册

表9：受访者提及的建议来源示例回答

建议来源	参与者回答示例
家人	“通过我的丈夫，这是他的工作" (W38)
朋友	“来自朋友 的建议， 他们更懂技术" (M18)
面对面／线下	“我只听帮我修笔记本电脑的男性” (W23)
来自工作	“来自我雇主的信息技术部门" (M9)
同事	“我阅读了从事网络安全工作的同事分享的文章， 并确保我关注与他们相同的安全公司" (W65)
一般研究	(a) “我通常会通过自己在线搜索他们来了解……" (M46) (b) “我在互联网上搜索最新、最可靠的系统" (M170)
专业页面，例如 TechCrunch	(a) “*IT* 杂志网站与博客" (M10) (b) “我从*TechCrunch*、*BuzzFeed*和一般的新闻媒体报道中学习……" (M48)
在线评论和推荐	“我会查看在线防护评论；如果过去一切顺利，就继续使用同一家公司" (M54)
科技广告，共享的公司信息， 知名品牌	(a) “我通常会在网上看到有关保护隐私的广告……" (M132) (b)“……此外，我也会让所使用的电子邮件公司（如 *ProtonMail*）将安全浏览信息和 *VPN* 信息发送到我的收件箱" (M60) (c) “来自微软 *[sic]*以及其他公司自身" (W160),“我倾向于使用知名品牌，例如 *Norton*" (M172)
社交媒体内容 例如 YouTube、Twitter	(a)“……例如在 *LinkedIn* 上 *[sic]*,他们会分享与安全相关的文章，我至少每周都会查看一次" (W65) (b)“我通常通过 *Twitter* 网络听说这些……" (M229) (c)“……警方和其他机构会在我关注的社交媒体上发布信息." (W362) (d)“我订阅了一些介绍保护方法的技术类 *YouTube* 博主"(M449)
在线论坛	(a) “……各种致力于技术和《计算机》使用的在线社区和论坛" (M578) (b)“我通常是在 *Reddit* 上听说它的" (W604)
新闻、电视节目	“偶尔会从报纸或网络上读到的文章中了解到" (W57),“通过在线阅读相关文章， 尤其是在 *BBC* 网站上" (W497),“看新闻" (M180),“通常通过 *BBC* 或 *Which* 等可靠网站 或消费者权益项目（例如 *Martin Lewis*）" (W16)
培训	(a) “……计算机系统和网络方面的 *A-level* 课程" (M394) (b) “我从小就受到教育，了解到在线保护信息的重要性" (M405) (c) “我研究软件工程和网络安全，这是我工作的一部分" (M239)
系统提示和设置	(a) “我拥有 *Apple*设备，并依赖它们定期更新电子设备上的隐私保护。我不 阅读这项保护措施的详细信息" (W39) (b) “我会使用特定应用程序或软件中的设置和常见问题”（M439），“……其他时候，我会查看隐私/安全” 设置，看看我需要做什么”（W412）
消费者杂志	“《*Which?*》杂志是一个很好的信息来源" (W24)

表 10：ISC 建议的理由及参与者回答示例

	类别	原因	参与者回答示例
Yes	ISC 技能	（一般）知识	(a) “因为她们通常知识丰富<*style id='3'>” (W41)*
		的 ISC	(b) “通常会问孩子们，因为他们知道的比我多得多”(M114)
			(c) “我的朋友和家人往往比我更早了解这些事情，所以我会向他们寻求建议”(M352)
		技术技能	(a) “我的女儿们更懂《计算机》，所以我问她们” (W94)
		ISC 的	(b) “因为我和一位非常了解信息技术安全的伴侣同住.....” (W37)
		ISC 从事IT工作	(a) “丈夫从事***IT***工作”(W28),“我丈夫在这些事情上都帮我。他是一名信息技术工程师”(W470)
			(b)“我有一些从事计算机程序员工作的朋友，所以我知道他们会告诉我该怎么做” (W29)
			(c) “我的大多数家人、朋友和同事都从事信息技术安全/网络相关工作” (W65)
		ISC经验	(a) “他们比我有更多经验”(M147)
			(b) “通常会有人曾经遇到过这种情况，而且不介意分享自己当时的做法”(W72)
		最新的	“/他们/ 是该主题方面最及时、最了解情况的人”(M150)
	ISC 特质	值得信任	(a) “因为朋友和家人都是值得信任的联系”(M137)
			(b) “我父亲对计算机非常有经验，而且我信任他的意见”(W560)
		易于访问	“因为我觉得向他人寻求建议更容易”(M112),“他们比我自己寻找更快就能知道答案”(W191)
		有帮助的	(a) “他们极大地帮助我改善了在线习惯”(M575)
			(b) “因为他们通常会提供很好的建议”(W283)
		可用	(a) “/他是个/ 计算机技术迷。他很容易联系到”(W230)
			(b) “因为我的朋友总是能联系到”(W209)
		可靠	“他们最值得信赖”（M12），“我可以依靠我的家人”（M140）
	其他	需要帮助	“我有时只需要支持”（M231），“如果我担心，我会问儿子该怎么做”（W225）
	技能	知识	“因为我对技术不太在行，而且对学习在线技术完全不感兴趣”(M18)
		信心	“没有足够的信心独自完成”(F102)
	其他	听取各种选项／相互交流	(a) “看看有哪些选项”(M572),“因为我可以从他们那里获得各种选项和建议”(M302)
			(b) “我和我的朋友总会彼此分享任何在线发生的事情的有用信息”(M152)
		reassurance	(a) “最好就这些事情征求第二意见，因为你可能遗漏了一些重要细节”(M186)
			(b) “我喜欢得到 *reassurance*，以确认自己做得正确，而且和他们的做法相同或相似”(M46)
			(c) “因为我想确保自己做的是正确的事”(W590)
No	Own 技能	自力更生	(a) “我可以依靠自己的研究” (M74)，“我可以自己完成” (M95)
			(b) “我往往相当自给自足，会自己查明情况” (M517)，“我可以自己想办法解决” (W555)
		更强的技能	(a) “我是*IT*专家” (M8)，“我对这方面的了解比大多数朋友、家人和同事都多” (M32)
			(b) “因为他们懂得没有我多” (M2)，“我不认为我的朋友／家人对任何与隐私相关的事情了解很多” (M131)
		信心	“我有信心能自己找到信息”(M107),“我有信心凭自己的能力找到所需的信息”(M127)
	其他	更喜欢其他来源	“通常，网上有大量专家信息，因此没必要咨询家人和朋友”(M35)
			“我更喜欢从政府网站获取信息”(M1), “我更愿意自己在网上查阅各种来源的信息”(M122)
		不需要帮助 / 其他	“因为我觉得自己不需要帮助”(M602),“我不常需要隐私/安全方面的帮助”(M268),“从未丢失过数据”(M490)
		帮助他人的那个人	“因为朋友/家人通常会来找我”(M178),“他们会指望我能告诉他们”(M10)

表 11：向 ISC 求助的参与者所收到的“具体”建议 / 支持（参与者百分比栏仅统计向 ISC 求助者）

建议主题	参与者百分比	参与者示例回答
防病毒、恶意软件和诈骗建议	19.1	“关于人们可能遭遇网络诱骗的不同方式”（M394）
身份验证	17.0	“.....合适的密码使用方式”（M62）；“.....一位家人向我推荐了 LastPass”（M162）
		“.....建议我为使用的每个网站设置不同的密码”（W81）
沟通，网络/隐私	11.2	“.....例如，设置 VPN”（M15）；“路由器安全设置”（M36）；“使用 HTTPS.....”（M64）
		“VPN 和代理方面的帮助”（M158）；“.....哪些防火墙最好，以及如何更新我的安全设置.....”（W427）
浏览器历史记录，跟踪防护	11.2	“协助我设置广告拦截器，并提醒我如何删除存储在笔记本电脑上的 Cookie”（W37）
		“清除历史记录和 Cookie”（M62）；“安装广告拦截器等”（W102）；“清除缓存，使用隐身模式”（M138）
		“如何启用隐私浏览并管理 Cookie”（M142）；“我最初是通过朋友了解到 Ghostery 的”（M268）
		“我爸提到 uBlock 是屏蔽广告的好选择”（W321）
隐私设置 / 社交网络服务	8.4	“如何设置在线隐私设置”（W543）；“关于如何访问和更改隐私设置的建议”（W501）
		“Facebook 和 Twitter 帖子”（M528）；“在 Facebook 上设置隐私”（M493）
其他具体事项	5.8	“我有一位亲密的朋友目前非常担心语音助手，例如 Alexa，所以尽可能关闭了
		他们所有设备上的麦克风”（W4）；“关于退出营销相关沟通的建议”（W39）
		“关于如何将零散的个人信息拼凑起来的建议”（W69）
		“.....关于如何尽量降低无意中将个人信息发布到在线平台上的风险”（M144）
		“关于欺诈案件，以及其他人遭遇的故事示例”（M150）
电子邮件安全	4.5	“他们还告诉我可以拥有多个电子邮件账户”（M180）；“使用别名电子邮件”（W226）
		“谨慎打开来自未知或可疑来源的电子邮件”（W210）；“使用虚假电子邮件”（M214）
网络安全	3.5	“使用熟悉的网站”；P396“检查网站，不要透露太多信息”（W382）
系统／操作系统	3.7	“如何安全地删除移动操作系统”（M10）；“我的伴侣帮我设置了计算机及其保护措施”（M73）
		“让我的笔记本电脑及时安装最新更新，并了解安全问题”（W41）
安全软件	3.4	“该使用哪些应用程序、如何使用，以及如何让它们保持最新”（W108）；“关于软件的说明和建议”（W282）
		“他们推荐了某些软件，并告诉我不同软件套装的优缺点”（W281）
		“我的朋友帮我设置了在线使用的安全措施”（W195）；“讨论了他们使用的应用程序”（M346）
安全支付	2.3	“家人会为我设置任何我需要的新技术。例如，PayPal”（M135）
		“关于如何安全地使用银行卡进行在线购物”（M351）；“考虑使用 PayPal 代替网上银行”（W550）

F 按性别划分的建议接收示例

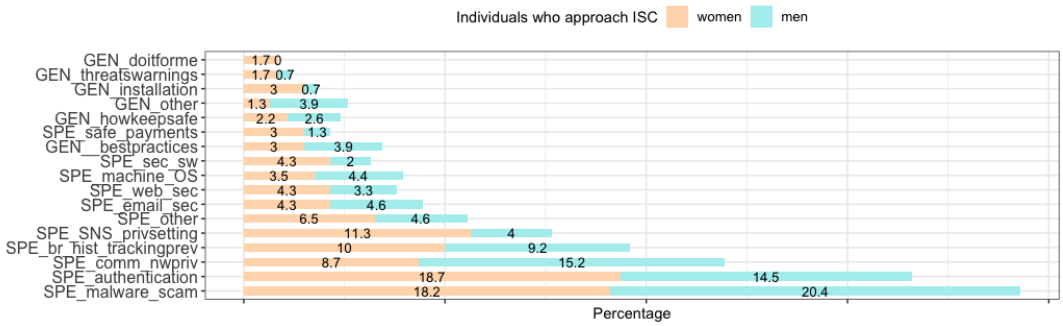


图 8：向 ISC 求助者中，女性和男性分别收到各类建议的百分比

G 问卷

第1部分：您在线上最常使用哪些隐私和安全方法或工具？ [如果您不了解或不使用任何方法或工具，请说明。]

第2部分：您通常如何了解、学习或找到用于保护在线隐私和安全的技术/方法？ [如果您不了解任何用于保护隐私/安全的技术/方法，请说明。]

第3部分：如果您在任何时候需要建议/帮助来保护在线隐私和安全，您通常会向亲密与社会关系（例如家人、朋友、同事）寻求帮助吗？请解释您对上一个问题回答“是”或“否”的原因。

第4部分：如果您曾从亲密与社会关系中获得过有关保护在线隐私/安全的技术/方法方面的建议/支持，请举例说明这些建议/支持。

第5部分：（i）您的性别是什么？ □ 女性 □ 男性 □ 非二元性别 □其他

(ii) 您的年龄是多少？

(iii) 您的族裔是什么？ □ 白人 □ 混合族裔 □ 亚裔：印度裔 □ 亚裔：华裔 □ 亚裔：其他 □ 黑人 □ 其他族裔

(iv) 您已完成的最高教育程度是什么？ □ 未上过学 □ 上过学但未毕业 □ 高中毕业 □ 大学毕业 □ 本科学位 □ 硕士学位 □博士

(v) 您是否接受过信息技术、计算机科学或计算机工程领域的教育，或在这些领域工作？ □ 否 □ 是（请说明您在计算机/信息技术方面的教育程度或工作领域。

(vi) 请根据以下陈述对您的符合程度作答，选项范围从 [完全不符合我] 到 [非常符合我]。 □ 完全不符合我 □ 大体符合我 □ 既不符合也不不符合我 □大体符合我 □ 非常符合我

我知道如何打开下载的文件
我知道如何下载/保存在网上找到的照片
我知道如何使用快捷键（例如，CTRL-C 复制，CTRL-S 保存）

我知道如何在浏览器中打开新标签页
我知道如何将网站添加为书签
我知道该点击哪里才能转到另一个网页
我知道如何填写在线表单
我知道如何上传文件
我知道如何调整隐私设置
我知道如何连接到 WIFI 网络
我觉得很难确定在线搜索时应该使用哪些最佳关键词。
我觉得很难找到以前访问过的网站。在线查找信息时，我会感到疲倦。有时，我最终会进入一些网站，却不知道自己是如何进入的。
我觉得许多网站的设计方式令人困惑。各种各样的网站布局让我很难使用互联网。我应该参加一门关于如何在线查找信息的课程。有时我觉得很难核实自己找到的信息。我知道哪些信息应该和不应该在线分享。我知道什么时候应该和不应该在线分享信息。我会谨慎地让自己的评论和行为符合我在网上所处的情境。我知道如何更改内容的分享对象（例如朋友、朋友的朋友或公众）。我知道如何从联系人列表中删除朋友。我觉得自己能够自在地决定在线关注谁（例如在 Twitter 等服务上）。

我知道如何利用现有的在线图片、音乐或视频创作新内容

我知道如何对他人创作的内容进行基本修改

我知道如何设计一个网络网站
我知道哪些不同类型的许可证适用于在线内容

我有信心将自己创作的视频内容发布到在线平台上。

我知道哪些应用程序/软件可以安全下载。
我有信心在博客、网站或论坛上发表评论。

我会有信心在网上写作和发表评论。
我知道如何在移动设备上安装应用程序
我知道如何将应用程序下载到移动设备上
我知道如何跟踪使用移动应用程序的费用

(vii) 本题将询问您与技术系统的互动情况。“技术系统”指应用程序或其他软件应用，以及完整的数字设备（例如手机、计算机、电视、汽车导航系统）。

请指出您在多大程度上同意或不同意以下陈述。 □ 完全不同意 □大体不同意 □略微不同意 □略微同意 □ 大体同意□完全同意

我喜欢更深入、详细地了解技术系统。

我喜欢测试新技术系统的功能。
我主要是因为不得不这样做，才会接触技术系统。

当我面前出现一个新的技术系统时，我会充分尝试使用它。我喜欢花时间熟悉新的技术系统。对我来说，技术系统能正常运行就足够了；我不在乎它如何运行或为什么这样运行。我会尝试弄清楚技术系统究竟是如何运行的。对我来说，了解技术系统的基本功能就足够了。我会尝试充分利用技术系统的各项功能。