安全提示是静态的吗？重新思考人生转变中的警告与信任指标

Sarah Tabassum

北卡罗来纳大学夏洛特分校，stabass2@charlotte.edu

警告和信任信号等安全提示通常被设计为稳定的界面元素，然而人们的生活、所处情境和脆弱性会随时间变化。迁移、老龄化或制度环境的变化等人生转变，会重塑人们对风险与信任的理解及其应对方式。然而，当前系统很少根据这些不断变化的条件调整安全提示，从而将解读这些提示的负担转嫁给用户。在这篇进行中研究论文中，我们认为，安全提示的静态特性与不断变化的人生经历之间存在设计错配。我们以先前关于教育迁移的实证研究洞见为出发案例，并将讨论拓展至其他人生转变。在这些洞见的基础上，我们提出过渡感知安全线索（TASeC）框架，并展示思辨设计概念，说明安全提示如何随过渡阶段演变。我们邀请人机交互领域重新思考安全提示，将其视为具有纵向视角、以生活为中心的设计元素，并共同参与设计。

CCS 概念 • 安全与隐私 → 安全与隐私的社会层面；• 以人为中心的计算 → 交互设计的系统与工具。

补充关键词与短语： 安全提示、可用安全、信任指标、人生转变、风险沟通、以人为中心的设计

1 引言

在日常生活中，人们越来越依赖数字设备来完成日常及影响重大的任务，涵盖沟通、理财、工作和公民参与等方面。在这些系统中，警告、指示器、信任信号和提示等安全提示，是向用户传达风险、安全性和可信度的关键界面机制 [4, 11]。浏览器警告、权限对话框、挂锁图标和确认消息会影响人们对点击什么、分享什么以及信任谁的决策 [1, 10]。因此，许多人机交互和可用安全研究都致力于提升这些提示的清晰度、可见性和有效性，以支持更安全的决策。与此同时，人们的生活很少一成不变。许多人会经历迁移或流离失所、老龄化、患病或康复、进入新的机构，或数字素养发生变化等人生转变。在这些人生转变期间，用户的知识、信心和脆弱性可能迅速变化，从而改变他们对安全、风险或可信度的感受。然而，安全提示通常被设计为保持不变，不受这些变化的影响。

这造成了静态界面设计与动态人生之间的不匹配。当前的安全提示隐含地假设用户、情境和解读方式都是稳定的，因此将意义建构的负担交给用户，而用户恰恰可能在此时最感到不确定。对于正在经历人生转变的人来说，这种假设会让安全提示难以理解、容易被忽略，或产生误导。本文认为，安全提示的设计仿佛人生是静止不变的，然而人生

本质上处于不断转变之中。为弥合这一差距，我们提出一个针对过渡感知安全线索的设计框架，将人生转变视为首要设计条件，而非边缘案例。该框架将警告、指示器和信任信号重新构想为纵向的、以生活为中心的设计元素，并使其随着用户熟悉度和信心的变化而演进。我们通过思辨设计概念展示这一方法，说明提示策略如何在转变的不同阶段进行调整。

2 背景与问题界定：过渡性生活中的安全提示

安全提示和提示语是广泛使用的界面机制，用于向用户传达风险、信任与安全[4, 6]。其中包括关于不安全网站的浏览器警告、请求访问敏感数据的权限对话框，以及挂锁图标等视觉指示器。此前的人机交互和可用安全研究考察了这些提示如何影响用户的理解、信任判断和决策，通常侧重于提升清晰度、可见性和感知控制力[1, 11]。从本质上说，安全提示是风险沟通的一种形式，旨在引导用户在涉及不确定性或潜在危害的情境下采取行动。

尽管安全提示发挥着核心作用，但大多数安全提示的设计都建立在一种隐含的稳定性假设之上。通常，所有用户都会以相同形式看到相同的提示，并且这些提示被期待在一段时间内传达一致的含义。关于信任指标和网络钓鱼的研究表明，用户会根据经验和情境，以不同方式解读徽标、图标或视觉合法性标记等提示，但系统很少考虑这种差异性[4]。同样，权限界面的研究表明，即使提供了解释和视觉线索，用户仍可能感到不知所措，或误解其含义，这对“信息越多就越有助于做出更好决策”的假设提出了挑战[6]。这些设计预设了稳定的知识、稳定的情境和稳定的用户，而这一假设在现实使用中很容易变得脆弱。

人生转变使这种脆弱性尤为明显，并可被理解为对安全提示的一种设计压力测试。诸如迁移、流离失所、老龄化、疾病或开始接入数字世界等转变，往往涉及知识、信心、权力和信任关系的变化[3, 7, 8]。在这些时期，用户可能更加依赖机构、合法性表象或熟悉的模式，同时也面临新形式的风险。然而，安全提示通常保持静态，随着用户所处情境的变化，将解读负担完全置于用户身上。这造成了一个核心错位：生活的变化快于界面。当解读情境发生变化而线索保持不变时，其含义和有效性会发生漂移，这促使我们需要这样的设计方法：将人生转变视为安全线索设计的核心条件，而非边缘情形。

3 过渡感知安全线索（TASeC）框架

为了解决静态安全提示与动态人类生活之间的不匹配问题，我们提出了过渡感知安全线索（*TASeC*）框架。TASeC 是一个面向设计的框架，用于思考安全警告、指示器和信任信号应如何随着人们经历人生转变而不断演变。TASeC 不将安全提示视为普适且持久存在的界面元素，而是将其界定为以人生为中心的纵向组成部分，其形式、显著性和功能会随用户所处的情境而变化。迁移 [8], 流离失所、老龄化 [5], 或数字素养的变化 [2]等人生转变，会带来熟悉程度、信心和脆弱性的变化，使同一安全提示在不同时间具有不同含义。TASeC 将人生阶段、用户状态和线索策略联系起来，以支持在这些

变化过程中进行更恰当的安全沟通。该框架具有概念性和生成性，旨在支持设计推理，而非规定或验证某个特定系统。

3.1 设计原则

TASeC 遵循四项设计原则。**时间性**强调安全提示应随时间变化，而非一成不变。**脚手架支持**主张在不确定时期提供更多解释和指导，并在信心增强后逐步减少支持。**可逆性**着重于调整操作阻力和指导，使用户能够安全地暂停、重新评估或改变操作方向，而非依赖不可逆的警告。**校准**强调提示应与用户当前的信心和能力相匹配，并认识到同一提示在某种情境下可能有所帮助，而在另一种情境下可能显得多余或不足。

3.2 框架模型

TASeC 围绕三个维度组织安全线索设计：人生阶段、用户状态和线索策略（图 1 ）

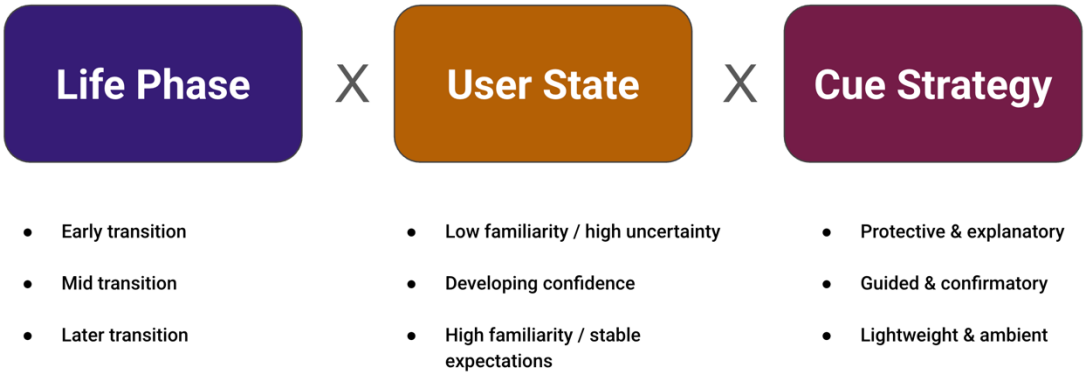
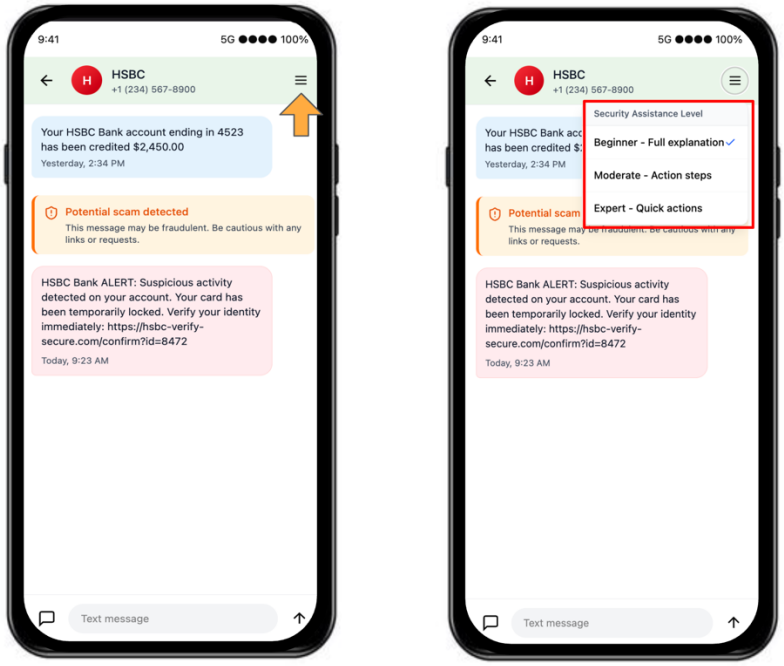


图 1：该图说明，如何根据不断变化的人生情境和用户信心选择不同的线索策略，而不是将其设计为固定或确定性的流程。

人生阶段刻画一个人在转变过程中所处的位置，用户状态反映情境知识与信心，线索策略则描述风险与信任如何被传达。该框架鼓励在早期、中期和后期阶段选择不同的线索策略，从而明确一个可随时间与情境调整安全提示的设计空间。

4 面向 TASeC 框架的示例性设计概念

我们通过一个具体且常见的高风险场景来说明 TASeC 框架：收到一条可能存在欺诈风险的短信。这个示例展示了安全提示如何随着人生过渡阶段的变化而调整，而不是始终保持不变。



(a) Potential scam text and initial state of the interaction

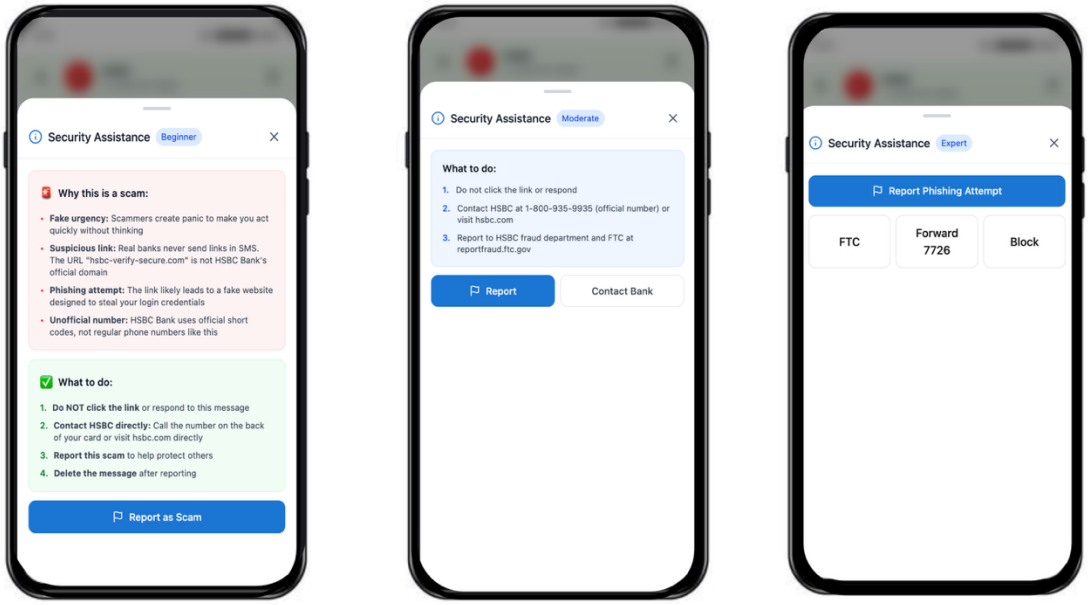
(b) Our proposed extension to the warning interface

图2：初始状态，显示针对收到的短信的标准潜在诈骗警告

图2 (a) 展示了移动平台上常见的标准潜在诈骗警告。这类警告通常以简短提醒的形式出现，提示用户存在风险，但几乎不提供背景说明。虽然这种方式在某些情况下有效，但它假设所有用户都会以相同的方式理解并响应这一提示。为解决这一局限，我们提出对警告界面进行扩展。如图2 (b) 所示，选择汉堡菜单后会显示三个分别适用于不同过渡阶段的支持选项：**初学者**（完整说明）、**中级**（包含确认步骤的行动步骤）和**专家**（干扰极少的快捷操作）。

4.1 初学者：完整说明

初学者选项适用于过渡早期阶段，此时用户对相关情况不够熟悉，且存在较高的不确定性。如图3（a）所示，该界面包含三个部分：说明消息为何可疑、清晰地分步指导用户接下来该怎么做，以及提供举报该消息的选项。这种模式会提供更多解释，并增加操作步骤，帮助用户暂停下来并做出明智的决定。



(a) Full Explanation for Beginner Option

(b) Action Steps for Moderate Option

(c) Quick Actions for Expert Option

图3：TASeC 的三种交互选项：(a) 初学者模式，提供完整说明；(b) 中级模式，提供行动步骤；(c) 专家模式，提供快捷操作。

4.2 中级：行动步骤

中级选项面向过渡中期阶段，此时用户已能识别常见的诈骗线索，但仍需要确认。如图3（b）所示，该界面侧重于简明的行动步骤，保留举报功能，并提供联系可信机构进行核实的选项。这种模式在提供指导的同时，也兼顾了用户逐渐增强的信心。

4.3 专家：快捷行动步骤

专家选项适用于后期过渡阶段，此时用户已熟悉诈骗模式并对此充满信心。如图3(c)所示，该界面尽量减少打扰，并提供快速操作，例如举报、屏蔽发件人，或将消息转发至举报服务。此模式优先考虑低操作阻力、自主性和不显眼的安全提示。

5 反思与启示

本文提出的过渡感知方法引发了一些值得认真思考的开放性问题和设计张力。首先，一个核心挑战在于如何识别人生转变。自动检测转变可能导致错误分类，并引发对推断和监控的担忧；而完全依赖用户自我识别，则可能增加负担，或使那些不了解现有支持的人无法获得帮助。未来需要进一步探讨如何以透明、可选且尊重用户自主权的方式激活过渡感知安全线索。第二个张力涉及适应与控制之间的平衡。尽管自适应安全提示能够在脆弱性时期提供有价值的支持，但过度适应可能会削弱用户能动性，或使用户对系统引导产生依赖。

因此，设计者必须考虑适应何时有益，以及何时可能变得具有侵扰性或适得其反。此外，并非所有情境都需要适应。即使处于变化时期，一些用户也可能更偏好稳定且可预测的界面，这凸显了可逆性和用户选择的重要性。

除了这些挑战之外，本文提出的框架对人机交互和可用安全研究也具有更广泛的意义。在可用安全以及信任与安全设计领域，该框架促使人们摆脱一刀切警告，转而采用能够考虑用户状态变化和长期生活经验的设计[8, 9]。更广泛地说，对于人机交互而言，它有助于推进相关讨论：设计不应只面向孤立的交互，还应关注那些跨越时间、生活事件和变化中的情境逐步展开的过程。这项工作所提出的关键转变，是从将安全提示设计为静态界面元素，转向将其设计为与用户共同演变的**以生活为中心的过程**。将人生转变视为首要设计条件，为重新思考系统如何在不确定、变化和学习的时刻传达风险并支持决策开辟了新的可能。

6 结论

尽管人们的生活、情境和脆弱性会随时间变化，安全警告、指示器和信任信号通常仍被设计成静态且普适的形式。本文指出，这种不匹配在人生转变期间尤为明显；此时，用户必须在不确定性和信心变化的情况下解读安全提示。为弥补这一缺口，我们提出了过渡感知安全线索 *(TASeC)*框架，将安全提示重新定义为纵向的、以生活为中心的设计元素，而非固定的界面组件。通过关联人生阶段、用户状态和线索策略，TASeC 开辟了一个设计空间，用于开发能够更好地契合不断变化的生活经验（即用户所处情境）的自适应支持性安全线索。我们希望这一框架能促使可用安全、信任与安全以及人机交互领域的未来研究，将人生转变视为设计系统如何传达风险与信任的核心条件，而非边缘情况。

参考文献

[1] Sarah Delgado Rodriguez、Anh Dao Phuong、Franziska Bumiller、Lukas Mecke、Felix Dietz、Florian Alt 和 Mariam Hassib。2023。Padlock，这个通用安全符号？——探索隐私与安全的符号和隐喻。载于《第22届国际移动与泛在多媒体会议论文集》。10–24。[2] Yoram Eshet-Alkalai 和 Eran Chajut。2009。数字素养的变化。CyberPsychology & Behavior 12, 6（2009），713–715。[3] Alisa Frik、Leysan Nurgalieva、Julia Bernd、Joyce Lee、Florian Schaub 和 Serge Egelman。2019。老年人的隐私与安全威胁模型及缓解策略。载于《第十五届可用隐私与安全研讨会》（SOUPS 2019）。21–40。[4] Markus Jakobsson、Alex Tsow、Ankur Shah、Eli Blevis 和 Youn-Kyung Lim。2007。什么能建立信任？一项关于网络钓鱼的定性研究。载于《国际金融密码学与数据安全会议》。Springer，356–361。[5] Benjamin Morrison、Lynne Coventry 和 Pam Briggs。2021。老年人如何看待参与网络安全？Human behavior and emerging technologies 3, 5（2021），1033–1049。[6] Vera Schmitt、Maija Poikela 和 Sebastian Möller。2022。Android 权限管理器、视觉线索及其对隐私意识和隐私素养的影响。载于《第17届国际可用性、可靠性与安全会议论文集》。1–12。[7] Sarah Tabassum、Cori Faklaris 和 Heather Richter Lipford。2024。是什么导致人们容易受到短信钓鱼攻击？一项针对美国手机用户如何以及为何判断短信真伪的访谈研究。载于《第二十届可用隐私与安全研讨会》（SOUPS 2024）。393–411。[8] Sarah Tabassum、Nishka Mathew 和 Cori Faklaris。2025。《移动中的隐私：从传播隐私管理理论视角理解教育移民的社交媒体实践》。载于《ACM SIGCAS/SIGCHI计算与可持续社会会议论文集》。1–18。[9] Warda Usman、John Sadik、Ran Elgedawy、Scott Ruoti、Daniel Zappala 等。2024。美国第一代和第二代巴基斯坦移民的安全与隐私体验：认知、实践、挑战及亲子互动。载于《2025 IEEE安全与隐私研讨会》（SP）。IEEE计算机学会，31–31。[10] Rei Yamagishi 和 Shota Fujii。2024。用户对安全图标认知的调查与分析。载于《2024年欧洲跨学科网络安全会议论文集》。202–209。

[11] Narges Zare, Co ri Faklaris、Sarah Tabassum 和 Heather Richter Lipford。2025。《通过视觉信任指标提升短信钓鱼的移动安全》检测》。载于 20 25 IEEE 世界人工智能物联网大会（AIIoT）。IEEE。doi:10.1109/AIIoT65859.2025.11105314