

消费者识别网络钓鱼欺诈的过度自信：紧迫性线索视觉显著性视角

尚璐瑶, 王志英*

江苏科技大学经济管理学院, 江苏 镇江

收稿日期: 2025年11月12日; 录用日期: 2025年11月24日; 发布日期: 2025年12月29日

摘要

电子商务领域是发生网络钓鱼欺诈的重灾区。在邮件中设置紧迫性线索是网络钓鱼欺诈常用的欺骗手段, 对消费者线上安全行为存在影响。作为影响消费者最终行为因素之一的过度自信是否受到网络钓鱼邮件中紧迫性线索特征的影响还不得而知。本研究结合S-O-R模型, 探究紧迫性线索的视觉显著性对消费者过度自信的影响。研究设计电子邮件合法性判断任务并应用眼动追踪技术, 将紧迫性线索视觉显著性分为高低两组, 进行组间实验。研究结果表明, 紧迫性线索的视觉显著性会显著降低消费者的过度自信水平, 即对消费者的不安全行为起到了抑制作用; 消费者对紧迫性线索的视觉注意在这种影响中起到了中介作用。本研究丰富了电子商务领域中信息安全的相关研究, 对消费者及电商平台的网络钓鱼欺诈防御工作的进行具有重要意义。

关键词

过度自信, 紧迫性线索, 视觉显著性, 网络钓鱼, 电子商务

Overconfidence in Consumers' Detection of Phishing Fraud: From the Perspective of the Visual Saliency of Urgency Cues

Luyao Shang, Zhiying Wang*

School of Economics and Management, Jiangsu University of Science and Technology, Zhenjiang Jiangsu

Received: November 12, 2025; accepted: November 24, 2025; published: December 29, 2025

*通讯作者。

Abstract

The e-commerce sector is a major hotspot for phishing. Creating a sense of urgency in emails is a common tactic used by phishing scammers, which significantly impacts consumers' online security behaviors. As one of the factors influencing consumers' final behavior, the effect of overconfidence, which is affected by characteristics of urgency cues in phishing emails remains unknown. This study combines the S-O-R model to investigate how the visual saliency of urgency cues affects consumers' overconfidence. Researchers designed an email legitimacy judgment task and applied eye-tracking technology, dividing visual saliency of urgency cues into high and low visual saliency groups for an intergroup experiment. Research findings indicate that the visual saliency of urgency cues significantly reduces consumers' overconfidence levels, thereby inhibiting unsafe consumer behaviors. Consumers' visual attention to urgency cues mediates this effect. This study enriches the literature on information security in the e-commerce domain and holds significant implications for enhancing phishing defense efforts among consumers and e-commerce platforms.

Keywords

Overconfidence, Urgency Cues, Visual Saliency, Phishing, E-Commerce

Copyright © 2025 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

随着电子商务的大范围应用，消费者享受到了便捷交易的体验，但与此同时个人信息等隐私与数据被大规模的采集与应用，为消费者的财产隐私安全埋下隐患[1]，更为网络钓鱼欺诈犯罪分子提供了机会。以电子邮件为载体的网络钓鱼本质上是利用人们心理弱点的一种社会工程攻击，是网络钓鱼者用来窃取消费者的敏感信息的惯用欺诈手段[2]，电子商务领域更是网络钓鱼欺诈的重灾区。反网络钓鱼工作小组(APWG, Anti-Phishing Working Group)的报告显示在2025年第一季度网络钓鱼攻击数量出现了自2023年第四季度观察到107万次以来最大的季度总数，共观察到1,003,924起网络钓鱼攻击[3]，其中电子商务领域遭受攻击次数占比更是高达15.3%。尽管电子邮件的筛选警告系统和用户培训等方面得到了大量关注，但消费者在线上进行购物支付等活动时仍难以避免落入网络钓鱼陷阱。尤其是电商消费者在面对网络钓鱼欺诈时的过度自信水平会对其不安全行为产生影响[4]，加剧了其落入网络钓鱼陷阱的可能性，因此，探究网络钓鱼线索特征对电商消费者过度自信的影响对于电商的良性可持续发展是一个迫在眉睫的问题。

消费者在处理邮件时会优先注意到紧迫性线索[5]，紧迫性线索经常被用在网络钓鱼邮件中催促收件人迅速回应遵从邮件指示以提高网络钓鱼攻击成功率。有研究表明超过25%的钓鱼电子邮件旨在诱导收件人产生紧迫感以敦促其做出不安全的反应[6]。在电子商务情境中，消费者常常会收到突出显著的“订单确认”、“限时优惠券”等提醒他们即刻点击确认的电子邮件，这些邮件天然地包含了紧迫性线索。而消费者每天可能要处理大量类似的电子邮件，对每封邮件均做出细致谨慎的检查判断是难以实现的。这种让消费者难以审慎分析的环境，可能使其对自身判断能力和判断准确性产生认知偏差导致过度自信。而紧迫性线索的特征如视觉显著性是否会对消费者识别网络钓鱼欺诈时的过度自信产生影响还不得而知。

综上所述，本文基于刺激 - 机体 - 反应(Stimulus-Organism-Response, S-O-R)模型构建了紧迫性线索

视觉显著性对消费者过度自信影响的研究模型，使用 STB (Saliency Toolbox) 视觉显著性计算模型对网络钓鱼邮件中紧迫性线索的视觉显著性进行测量，根据被试在判断后信心的自我评估结果计算其过度自信程度，结合眼动追踪实验获得被试对紧迫性线索的视觉注意。研究结果从视觉显著性视角出发探究了网络钓鱼邮件中紧迫性线索的影响，丰富了在电子商务领域中信息安全的相关研究，同时为网络钓鱼防御实践提供指导。

2. 文献综述

2.1. 网络钓鱼中的紧迫性线索

电子邮件是网络钓鱼攻击者常采用的攻击方法。攻击者会向收件人发送伪装成合法邮件的网络钓鱼邮件，意图骗取其信任[7]，因此有研究将网络钓鱼邮件定义为试图欺骗人们的电子邮件形式的诈骗[8]。作为网络钓鱼邮件中常用的欺骗线索之一，网络钓鱼的紧迫性线索对电子商务消费者的行为和决策存在重要影响，并且对消费者面对网络钓鱼邮件时的安全行为具有典型的双面作用，主要体现在对其安全行为积极提高和消极抑制等两个方面。

一方面，紧迫性线索降低了消费者对网络钓鱼邮件的信任，当他们面对网络钓鱼邮件时就不容易上当受骗，对安全行为具有积极影响。例如 Patel 等人通过对邮件中是否存在紧迫性线索和公司 logo 的不同情况影响的研究发现，当邮件中存在紧迫性线索时大大降低了收件人在处理网络钓鱼邮件时邮件的可信度[9]。同样 Baryshevtsev 等人通过两个实验考察网络钓鱼邮件中紧迫性等线索出现频率对邮件可信度的影响，发现邮件中紧迫性线索出现频率的增加会导致网络钓鱼邮件可信度的降低[10]。在电商情境下，当消费者面对来自电商平台或支付机构的、包含强烈紧迫性提示的邮件时，反而可能触发其风险意识，降低对邮件的信任，从而做出更安全的反应。

另一方面，当人们在处理任务时，需要面临高强度的时间紧迫感，也有可能使其无视安全要求，采取不安全的风险行为[11]。网络钓鱼邮件中的紧迫性线索意图威胁收件人、唤起恐惧或稀缺的感觉，从而缩短其评估过程并引发顺从行为[12]。在电子商务情境下，消费者接收到的“错过优惠”、“资金损失”等信息就旨在唤起这种心理，从而使其缩短决策流程，采取不安全行为。Vishwanath 的研究结论显示，面对网络钓鱼攻击时，对紧迫性线索投入更多关注的收件人会更容易陷入欺诈陷阱[12]。Williams 通过观察在工作场所中，网络钓鱼邮件是否包含紧迫性线索对员工网络钓鱼易感性的影响，发现当网络钓鱼邮件中包含紧迫性线索时，员工的网络钓鱼易感性会显著增加[13]。

2.2. 过度自信对行为影响的相关研究

过度自信是指个体在决策中的判断信心超过了他的实际表现，指个体的信心和实际表现之间的差异[4]。网络钓鱼相关研究表明人们在面对网络钓鱼邮件时的决策正确率与过度自信程度密切相关，过度自信常常会与一系列不安全的网络行为相关联，是一种典型的非理性行为表现。目前针对导致过度自信行为原因的研究已经在多个领域得到重视。贾心怡等人从人格特质、社会阶层以及认知层面等角度分析了国内投资者过度自信行为前因[14]。Ifcher 等人设计有激励的实验调查发现，男性群体的积极情绪对过度自信具有显著的提高作用[15]。Frank 等人利用机器学习方法，发现员工的职位、年龄等个体特质会增加其在信息安全方面表现出过度自信现象的风险[16]。Wang 等人探究了个体在识别网络钓鱼欺诈时形成过度自信的原因，发现个体的过度自信水平会被认知努力降低，但注意力分配的可变性对过度自信水平具有显著性提高作用[4]。以上可以发现，现有研究对过度自信成因的探讨，主要集中于个体层面的认知机制与人格特质等内在因素，而相对忽视了任务特征等外部因素的影响。因此，从网络钓鱼欺诈紧迫性线索视觉显著性特征这一外部维度切入，探索其对过度自信的影响作用，是当前值得深入拓展的研究方向。

2.3. 视觉显著性对行为影响的相关研究

在人们的视觉场景中,某些对象相对于场景中其他对象更加突出的程度被称为显著性[17]。作为信息的主要特征之一,已有研究发现视觉显著性对人们的行为具有一定影响。在网络钓鱼领域中,有研究探究了线索的视觉显著性对收件人行为的影响,如 Pan 的研究发现,含有高显著性线索的网络钓鱼邮件被收件人识别出的可能性更大[18]。同样,在电子商务领域中,李勋等人探究了电商网站上弹窗广告的视觉显著性对广告有效性的影响,结果证明了视觉显著性较高的弹窗广告会得到更好的注意效果[19]。

以上研究表明视觉显著性对人们的行为具有显著的影响作用,但现有研究中对视觉显著性采用的测量方式不尽相同。在网络钓鱼领域中 Pan [18]和 Jaeger [20]等人分别使用线索数量和文本图像作对比等手段测量线索的显著性。网络安全领域内, Ebert [17]使用文本大小进行信息视觉显著性的测量。市场营销中,视觉显著性也是获得关注的研究内容, Brüns [21]使用了对象外观颜色来进行测量。除以上经典的测量手段之外,杨强[22]使用了 STB 视觉显著性计算模型以客观数值对视觉显著性进行衡量,这种方法为本研究中视觉显著性的客观测量提供了方法基础。

2.4. 研究评述

综上可知,在目前对网络钓鱼邮件中的紧迫性线索对行为影响的相关研究中,其具体存在积极作用或消极影响,研究结论尚不统一,并且缺乏对紧迫性线索本身视觉呈现特征影响网络钓鱼过度自信的探索。现有研究主要通过直接控制文本大小或研究对象的颜色深浅等外观来定性地表达视觉显著性,特别是在网络钓鱼领域,缺乏使用视觉显著性计算模型这种更加客观的方式进行测量。综上,本研究从网络钓鱼邮件中紧迫性线索的视觉显著性入手,使用 STB 视觉显著性计算模型测量紧迫性线索的视觉显著性,探究紧迫性线索的视觉显著性如何影响消费者的过度自信,同时基于眼动追踪技术观察视觉注意在其中的中介作用。

3. 构建研究模型及提出假设

3.1. 研究模型

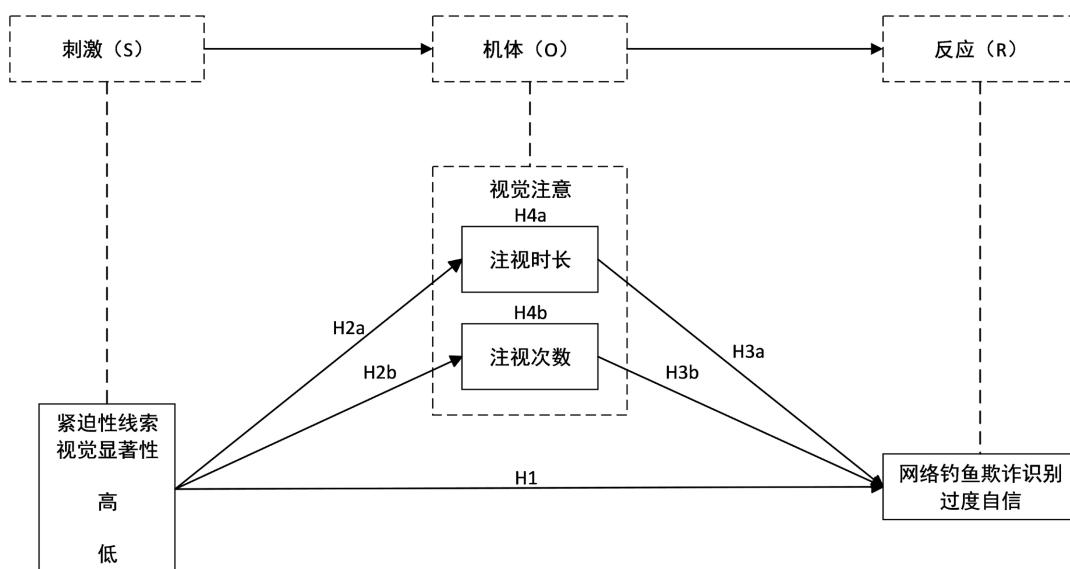


Figure 1. Research model

图 1. 研究模型

本研究的目的为探究网络钓鱼邮件中紧迫性线索的视觉显著性对过度自信的影响, 以及用户的视觉注意在其中产生的作用。S-O-R 模型为本研究提供了模型构建基础, 该模型用于解释人们接收到的刺激与情感状态变化以及最终产生的行为反应之间的关系[23], 其中 S 表示接收到的各种刺激, 包括实体对象、事件等; O 表示接收到这些刺激后, 人们的内部响应, 包括情感、认知变化等, 是行为产生的核心环节; R 表示人们对刺激产生的最终的行为反应。在本研究中, 将紧迫性线索视觉显著性视为外部刺激、视觉注意为被试接受外部刺激后产生的机体感知、过度自信为最终做出的行为反应, 构建的研究模型如图 1 所示。

3.2. 研究假设

(1) 紧迫性线索视觉显著性与过度自信

制造紧迫性是攻击者们基于说服策略的网络钓鱼攻击手段[24]。紧迫性线索的视觉显著性即其在网络钓鱼邮件中的明显程度[18]。显著性理论认为人们在做出决策时, 大脑会赋予高显著信息更多的主观权重, 更加关注这些显著信息的价值, 从而忽略低显著信息的价值[25], 如商家经常会用重点标注的“库存紧张”等标语促进用户消费, 各种电商平台也常会用“距双十一活动还有三天”等口号刺激消费者网购消费。同时, 当信息显著突出的时候也可能会对人的行为以及决策质量带来显著的积极影响, 如 Yeari 的研究显示, 学生会对标记出的显著信息内容进行更多的重读行为, 记忆效果也会更好[26]。Milutinović 等人的研究结果则显示更高的视觉显著性会对用户决策质量产生积极影响[27]。

过度自信是一种负面的行为反应。结合上文紧迫性线索对行为决策积极作用的描述可以推导, 如果网络钓鱼邮件中紧迫性线索的视觉显著性不同, 消费者在处理邮件时这个线索产生的影响可能也会存在差异。当紧迫性线索以视觉显著性更高的方式呈现时, 消费者在进行决策判断时可能会更倾向于怀疑邮件的真实性, 而非盲目顺从, 这样紧迫性线索的视觉显著性就产生了积极作用, 即降低了消费者的过度自信水平。综上, 本研究提出以下假设:

H1: 网络钓鱼邮件中紧迫性线索的视觉显著性负向影响消费者的过度自信。

(2) 紧迫性线索视觉显著性与视觉注意

视觉注意是一种信息选择和认知资源分配机制, 不仅是信息加工和认知功能的基础, 也是人们完成各种行为的重要条件[28]。自下而上的视觉注意机制认为信息的视觉显著性能够直接对人们的视觉注意资源的分配产生影响, 更加显著的信息或物体更能捕捉人们的注意[29], 视觉显著性理论同样认为人的注意力是由图像的颜色、亮度等低级特征控制的[30], 电商平台网站各种色彩丰富的广告正是利用了这一原理吸引消费者点击。生存信息偏见表明人会优先处理与他们的福祉有关的信息, 紧迫性线索会优先捕获他们的注意[31], 这一点与紧迫效应相似, 即在任务中, 人们会优先处理更加紧迫的信息, 完成更加紧急的任务[32], 消费者在进行购买行为时也会优先注意到折扣活动快到期的商品。McAlaney 等人的研究结果也证明了这一点, 相较于网络钓鱼邮件中存在的拼写错误等线索, 紧迫性线索会更快被注意到[5], 并劫持人们的注意力[12]。因此当消费者面对网络钓鱼欺诈时, 邮件中高视觉显著性的紧迫性线索相对于其他显著性更低的信息而言, 触发了消费者自下而上的注意捕获机制, 使其对高显著性的紧迫性线索可能会分配到更多的视觉注意。因此, 本研究提出以下结论:

H2a: 网络钓鱼邮件中紧迫性线索的视觉显著性正向影响消费者的注视时长。

H2b: 网络钓鱼邮件中紧迫性线索的视觉显著性正向影响消费者的注视次数。

(3) 视觉注意的中介作用

利用眼动追踪技术获得的人们的注视时长和注视次数可以推断出他们在这些信息上消耗多少认知资源[5]。当消费者分配更多的视觉注意资源在网络钓鱼邮件中的紧迫性线索上时, 这种认知资源分配促进

了消费者的认知系统对其盲目点击邮件等自动的顺从行为的控制。根据说服的精细加工可能性模型可知,系统性加工的中央路径更加依赖信息的深度处理结果,启发式加工的边缘路径更多依赖直觉决策[33]。对紧迫性线索分配的更多的注意使其更加容易获得消费者的信息加工资源并引起中央路径的精细加工[34]。在网络钓鱼领域中,同样有研究表明,对相关线索更关注、投入更多认知努力的个体,其网络钓鱼易感性更低[35],即更容易做出安全行为。当消费者对紧迫性线索投入更多的视觉注意资源时,大量的认知资源使认知系统更可能激活信息处理的中央路径,从而使其对信息进行深度加工进而做出理性决策,而非单纯依据信息表面特征等启发式线索凭直觉做出决策,这种视觉注意增加带来的认知努力就削弱了紧迫性线索的欺骗能力,从而降低了消费者在面对网络钓鱼邮件做出判断时的过度自信水平。

综上,本研究提出以下假设:

H3a: 消费者对网络钓鱼邮件中紧迫性线索的注视时长负向影响过度自信。

H3b: 消费者对网络钓鱼邮件中紧迫性线索的注视次数负向影响过度自信。

H4a: 消费者对网络钓鱼邮件中紧迫性线索的注视时长在视觉显著性与过度自信之间起中介作用。

H4b: 消费者对网络钓鱼邮件中紧迫性线索的注视次数在视觉显著性与过度自信之间起中介作用。

4. 研究设计

4.1. 实验设计

研究采用组间实验设计。参考先前视觉显著性相关研究设计[36],实验的组间变量为紧迫性线索的视觉显著性,按高或低分为两组。眼动追踪技术被用来获得被试在进行判断时的眼动数据,本研究使用邮件合法性判断任务,获得被试的过度自信水平。

(1) 实验设备及材料



Figure 2. Examples of visual saliency of urgency cues in email

图 2. 邮件紧迫性线索视觉显著性示例

实验使用 E-Prime 软件进行实验程序的编写以及行为数据的采集工作。实验中眼动数据的采集工作依靠 Tobii 公司研究制造的 Tobii Pro Glasses 3 戴式眼动仪记录。眼动数据收集后的处理工作采用与眼动仪配套的 Tobii Pro Lab 数据分析软件进行。实验中所用电子邮件均为真实电子邮件或根据已有研究改编自真实电子邮件,包括修改发件人和发件地址、改编邮件附加链接等[37]。实验共设计 24 封电子邮件,其中包括合法邮件 12 封,钓鱼邮件 12 封。邮件中紧迫性线索通过改变字体颜色、是否加粗、是否高亮以及改变字体大小等方法进行设计,保证同一封邮件除了紧迫性线索视觉显著性之外,其余信息和视觉呈现均相同。实验中使用的两组邮件大小一致以避免在后续处理眼动数据时因线索 AOI 区域大小不同造

成误差。邮件设计完成后使用 STB 视觉显著性计算模型以客观数据分析出紧迫性线索的高和低视觉显著性。如图 2 所示。

(2) 被试

研究通过发布自愿报名链接方式招募实验被试。要求被试均无色盲色弱, 视力或矫正视力正常, 无精神病史。实验开始前, 每名被试均阅读并签署实验知情同意书。实验结束后给予被试一定的现金报酬。实验共招募 92 名被试, 在数据处理阶段, 因眼动轨迹长时间未移动剔除 4 人[38], 因实验中注意力不集中, 频繁关注屏幕外剔除 4 人[39]。最终收集并纳入分析被试共 84 人, 其中高视觉显著性组 42 人, 低视觉显著性组 42 人。

(3) 实验流程

在正式实验开始之前, 预实验被用来检验实验设计中是否存在不合理以及设备是否可用, 如电子邮件设计、观察时间等是否不合理, 显示设备是否能正常显示等, 并及时进行修改完善以保证正式实验的顺利进行。

正式实验开始前被试需要填写实验知情同意书, 填写完毕后告知被试实验流程。被试需坐在显示器前约 50 cm 处, 将下巴放在下巴架上以保持头部稳定。随后被试佩戴 Tobii pro glasses 3 眼动仪进行眼动校准, 如果多次校准失败, 则剔除被试。校准完成后, 正式进行实验。被试首先阅读所呈现的实验指导语, 接着判断显示屏中呈现的电子邮件图片。每封邮件展示时间参考先前电子邮件判断任务的展示时间设定为 20 秒[40]。20 s 后页面将自动跳转到判断选择界面, 要求被试判断此封电子邮件是否为网络钓鱼邮件。判断后被试选择自己对这封邮件的信心程度, 即对判断正误的主观概率。全部判断完毕后, 要求被试估计自己正确判断出多少封邮件, 实验全程约 15 分钟。

4.2. 研究变量

本研究中, 研究变量包括紧迫性线索的视觉显著性、视觉注意以及过度自信, 各变量具体描述及计算方式如表 1 所示:

Table 1. Research variables

表 1. 研究变量

维度	变量名称	变量描述	公式
因变量	过度自信	由过精度和高估共同表达[4]	过精度:
		\bar{f} 表示被试对每次判断的主观概率的平均值	$Overprecision = \bar{f} - \bar{d}$
		\bar{d} 表示每个判断的正确率(正确为 0, 错误为 1)的平均值	高估:
自变量	紧迫性线索 视觉显著性	\tilde{d} 表示被试估计正确数在 24 封邮件中所占比例	$Overestimation = \tilde{d} - \bar{d}$
		由 STB 视觉显著性计算模型获得[41]	
中介变量	视觉注意	VS 表示邮件中紧迫性线索的视觉显著性得分	$VS = 1 - (p - 1)/x$ [42]
		p 表示紧迫性线索的扫描顺序	
		x 表示扫描对象的总数	
		由注视时长和注视次数共同表达[43]	使用眼动追踪技术获得

其中, 过度自信表示被试对自己表现的主观估计与实际表现情况之间的差异。当得出的值为正数时, 表示被试对自己的估计大于自己的实际表现, 呈现过度自信情况[44]。视觉显著性得分在 0 到 1 之间。视觉显著性的扫描图使用 STB 视觉显著性计算模型并结合 MATLAB 算法模拟仿真获得。在视觉显著性的

相关研究中, 扫描图中的前 5 个表示对象的仿真效果被认为较好[45]。因此, 本研究只考虑扫描图中的前 5 个标识对象以度量紧迫性线索的视觉显著性, p 值为 1 到 5。在过往研究中, 视觉显著性的高或低变量被认为是最合适的衡量指标[42]。因此在本研究中按照紧迫性线索的显著性得分将视觉显著性水平设置为高、低分类变量。图 3 为紧迫性线索高视觉显著性扫描路径。

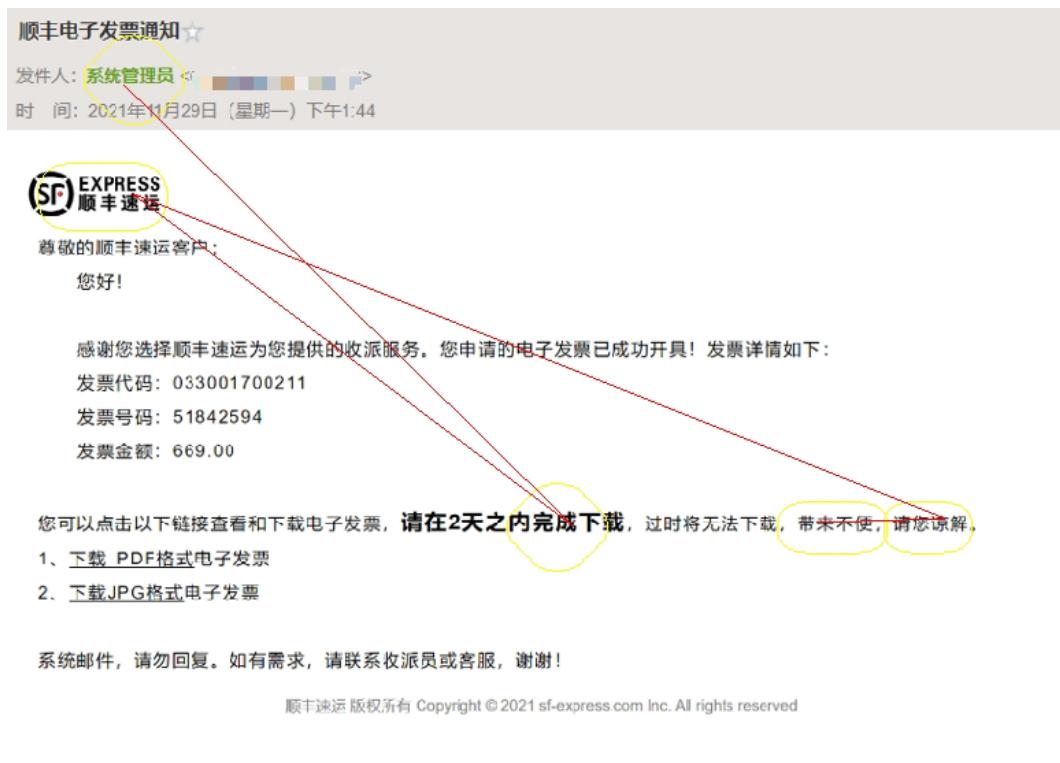


Figure 3. Visual saliency scanning path map of urgency cue

图 3. 紧迫性线索视觉显著性扫描路径图

5. 数据分析结果

5.1. 描述性统计

本研究按照紧迫性线索视觉显著性分为高视觉显著性和低视觉显著性两组。首先对两组被试在邮件判断任务时获得的眼动指标和过度自信进行描述性统计和分析。视觉显著性水平为分类变量, 将高视觉显著性编码为 1, 低视觉显著性编码为 0。研究使用 SPSS26.0 软件进行数据分析来验证假设。被试的过度自信、注视时长与注视次数的描述性统计分析如表 2 所示。

Table 2. Results of descriptive statistical analysis

表 2. 描述性统计分析结果

组别	过度自信						注视时长(秒)	注视次数(个数)
	过精度		高估		均值	标准差		
视觉显著性	组别	均值	标准差	均值	标准差	均值	标准差	均值
高	1	-0.595	0.115	-0.058	0.220	15.112	7.123	64.381
	2	0.214	0.126	0.046	0.207	9.603	4.554	44.357
								13.974

5.2. 假设检验

(1) 紧迫性线索的视觉显著性与过度自信的关系分析

研究使用过精度和高估共同代表被试的过度自信。独立样本 t 检验的分析结果如表 3 所示。

Table 3. The relationship between the visual saliency of urgency cues and overconfidence
表 3. 紧迫性线索的视觉显著性与过度自信的关系

	t 值	p 值	差值 95% 置信区间	
			下限	上限
过精度	-30.722	0.000	-0.861	-0.756
高估	-2.217	0.029	-0.196	-0.011

结果表明, 当钓鱼邮件中紧迫性线索的视觉显著性水平不同时, 被试在判断过程中的过度自信水平有显著差异。具体表现为高视觉显著性组的被试过精度水平和高估水平低于低视觉显著性组($t = -30.722$, $p < 0.05$; $t = -2.217$, $p < 0.05$)。即紧迫性线索的视觉显著性能够负向影响被试的过度自信水平, 假设 H1 得到支持。图 4 为不同视觉显著性下的过度自信情况。

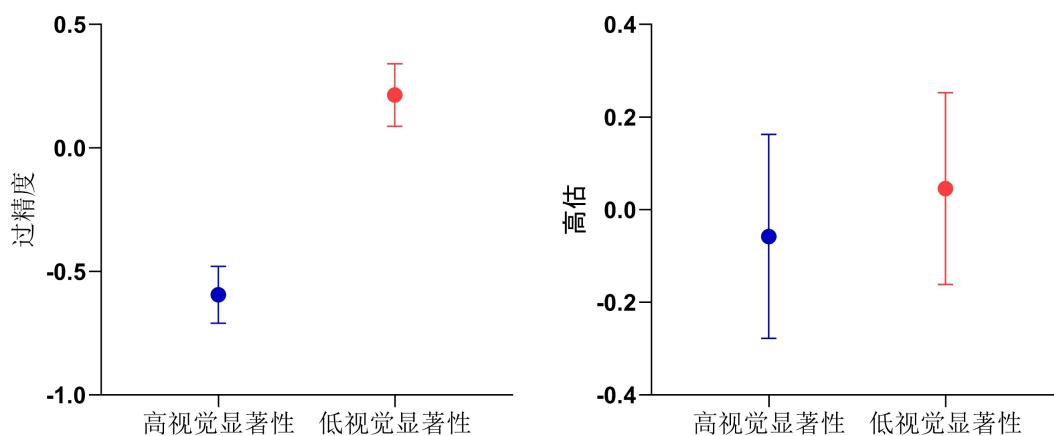


Figure 4. Overconfidence under different visual saliency

图 4. 不同视觉显著性下的过度自信

(2) 紧迫性线索视觉显著性与视觉注意的关系分析

独立样本 t 检验被用来探究紧迫性线索不同视觉显著性条件下被试的视觉注意的差别, 结果如表 4 所示。

Table 4. The relationship between the visual saliency of urgency cues and visual attention
表 4. 紧迫性线索的视觉显著性与视觉注意的关系

	t 值	p 值	差值 95% 置信区间	
			下限	上限
注视时长	4.223	0.000	2.914	8.104
注视次数	5.169	0.000	12.318	27.730

结果表明, 当钓鱼邮件中紧迫性线索的视觉显著性水平不同时, 被试在判断过程中的对线索的注视

时长有显著差异。具体表现为高视觉显著性组被试的注视时长和注视次数均高于低视觉显著性组($t = 4.223, p < 0.05$; $t = 5.169, p < 0.05$)。即紧迫性线索的视觉显著性能够正向影响被试对紧迫性线索的视觉注意, 假设 H2a, H2b 得到支持。图 5 为不同视觉显著性下的视觉注意情况。

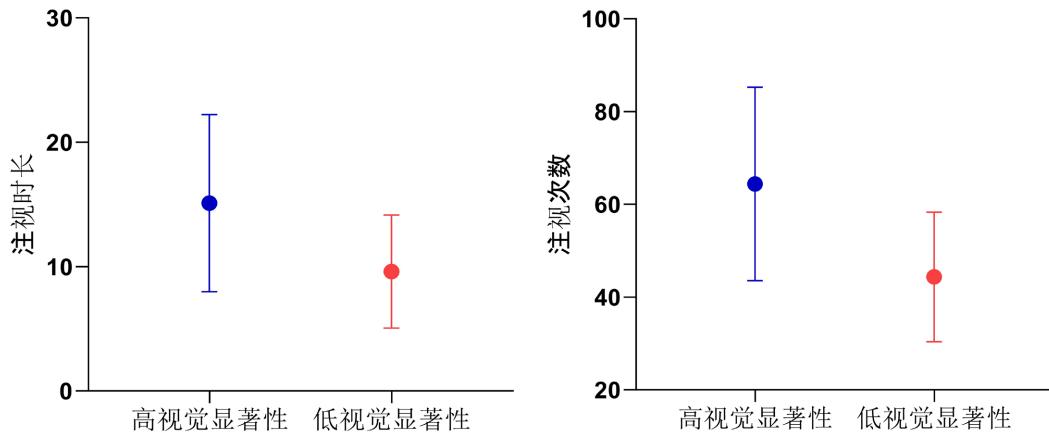


Figure 5. Visual attention under different visual saliency
图 5. 不同视觉显著性下的视觉注意

图 6 为不同视觉显著性水平的紧迫性线索的网络钓鱼邮件的注视热图。在热图中区域颜色越深表示用户对该区域的关注程度越高。通过对比可以看出, 与视觉显著性水平较低的紧迫性线索相比, 在热图中视觉显著性水平较高的紧迫性线索区域的颜色更深。说明了被试对其分配更多的视觉注意资源。



Figure 6. Gaze heatmap
图 6. 注视热图

(3) 视觉注意与过度自信的关系分析

线性回归分析被用来对被试在紧迫性线索上的视觉注意(注视时长和注视次数)与过度自信(过精度和高估)关系进行分析。结果如表 5 所示。模型 1 到模型 4 分别为被试的注视时长、注视次数对其判断时的过精度和高估水平的线性回归结果。结果显示被试在面对网络钓鱼邮件时对紧迫性线索的视觉注意能显著预测其过度自信水平($t = -4.811, p < 0.05$; $t = -2.477, p < 0.05$; $t = -5.684, p < 0.05$; $t = -2.880, p < 0.05$)。即被试对紧迫性线索的视觉注意(注视时长和注视次数)会降低被试的过度自信(过精度和高估), 回归图如图 7 和图 8 所示。假设 H3a、H3b 得到支持。

Table 5. Linear regression analysis of visual attention and overconfidence
表 5. 视觉注意与过度自信的线性回归分析

	自变量	因变量	未标准化系数		标准化系数 Beta	t 值	p 值
			B	标准误差			
模型 1	注视时长	过精度	-0.030	0.006	-0.469	-4.811	0.000
模型 2	注视时长	高估	-0.009	0.004	-0.264	-2.477	0.015
模型 3	注视次数	过精度	-0.011	0.002	-0.532	-5.684	0.000
模型 4	注视次数	高估	-0.003	0.001	-0.303	-2.880	0.005

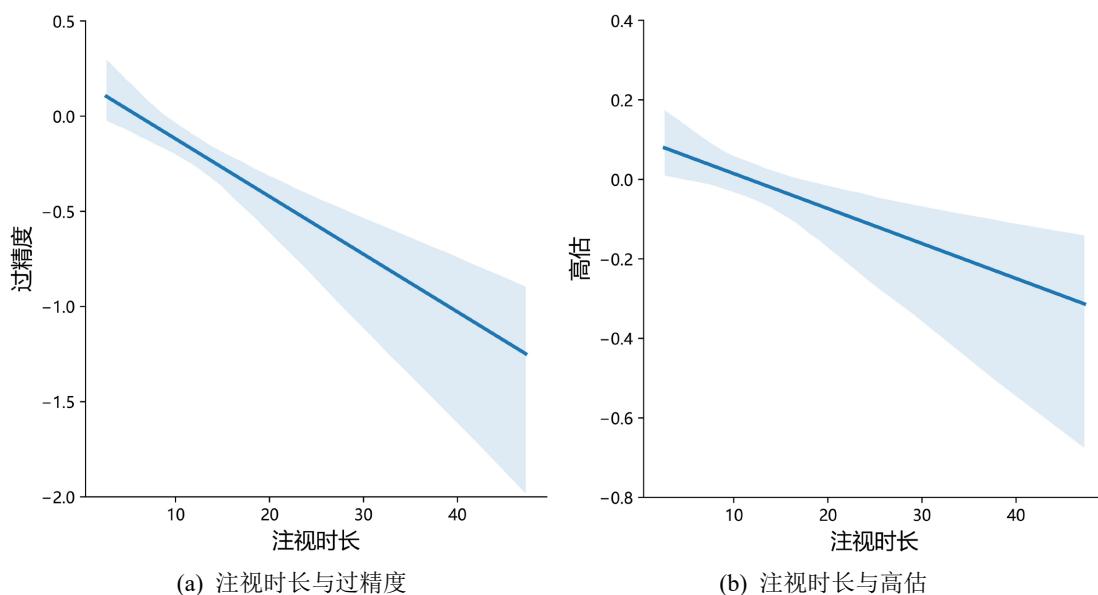


Figure 7. Regression plot of fixation duration and overconfidence
图 7. 注视时长与过度自信回归图

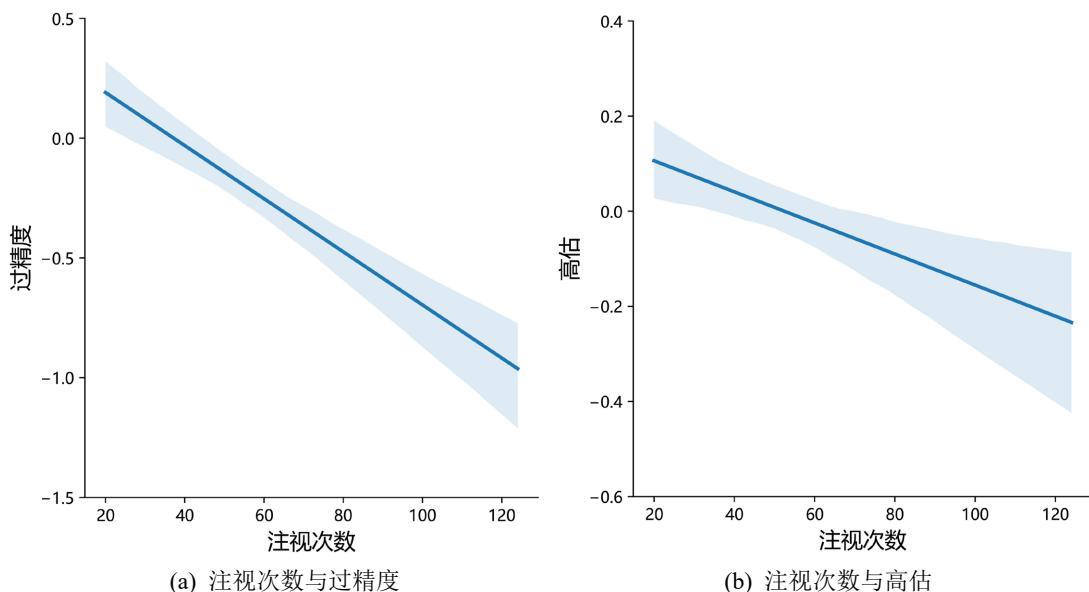


Figure 8. Regression plot of fixation count and overconfidence
图 8. 注视次数与过度自信回归图

(4) 视觉注意的中介效应检验

为检验被试的视觉注意在紧迫性线索视觉显著性和过度自信关系之间的中介效应。研究以紧迫性线索的视觉显著性为自变量, 以被试在判断过程中的过度自信水平为因变量, 以视觉注意为中介变量, 使用 Bootstrap 法进行中介效应检验。研究采用 Hayes [46] 编制的 SPSS 宏程序 Process3.5 中的 Model4 完成中介效应分析, 设定样本量为 5000, 置信区间为 95%。结果如表 6 所示。

Table 6. Tests for mediating effects of visual attention

表 6. 视觉注意的中介效应检验

路径	效应	效应值	标准误	95%置信区间	
				下限	上限
视觉显著性→注视时长→过精度	总效应	-0.810	0.026	-0.861	-0.757
	直接效应	-0.781	0.028	-0.838	-0.725
	间接效应	-0.028	0.011	-0.051	-0.008
视觉显著性→注视时长→高估	总效应	-0.103	0.047	-0.196	-0.011
	直接效应	-0.067	0.051	-0.168	0.034
	间接效应	-0.037	0.022	-0.092	-0.006
视觉显著性→注视次数→过精度	总效应	-0.810	0.026	-0.861	-0.757
	直接效应	-0.778	0.030	-0.840	-0.719
	间接效应	-0.031	0.015	-0.064	-0.005
视觉显著性→注视次数→高估	总效应	-0.103	0.047	-0.196	-0.011
	直接效应	-0.050	0.053	-0.155	0.054
	间接效应	-0.053	0.026	-0.107	-0.004

结果显示, 注视时长作为中介变量时, 对视觉显著性对过精度的影响具有部分中介效应, 对视觉显著性对高估的影响具有完全中介效应。具体而言, 其中间接效应分别为 -0.028 和 -0.037, 总效应分别为 -0.810 和 -0.103, 间接效应占比分别为 3.4% 和 36%。注视次数作为中介变量时, 对视觉显著性对过精度的影响具有部分中介效应, 对视觉显著性对高估的影响具有完全中介效应。其中间接效应分别为 -0.031 和 -0.053, 总效应分别为 -0.810 和 -0.103, 间接效应占比分别为 3.8% 和 51%。以上表明中介效应模型与数据拟合良好, 网络钓鱼邮件中紧迫性线索的视觉显著性通过影响用户的视觉注意在一定程度上降低了用户在面对网络钓鱼邮件时的过度自信。假设 H4a、H4b 得到支持。

6. 结论与启示

6.1. 结论

本研究针对电子商务领域中面对的日益严峻的网络钓鱼欺诈行为, 探究了网络钓鱼邮件中紧迫性线索的视觉显著性对消费者辨别欺诈时过度自信行为的影响, 并探究了视觉注意在其中产生的中介作用。研究结果对电子商务领域中网络钓鱼欺诈行为研究与防御具有理论与实践意义。主要获得以下结论:

首先, 紧迫性线索的视觉显著性对消费者在面对网络钓鱼欺诈时的过度自信行为具有显著的抑制作用。

其次, 消费者对紧迫性线索的视觉注意在视觉显著性对过度自信的影响中表现出中介效应。需要指出的是, 对于过精度的间接效应占比相对较小, 而对高估的间接效应占比更为显著, 说明视觉注意在解

释高估维度上具有更重要的实际意义。

6.2. 研究意义

(1) 理论意义

本研究对电子商务领域中网络钓鱼欺诈相关研究存在重要的理论意义，具体如下：

- ① 研究结果从视觉显著性视角丰富了网络钓鱼欺诈中紧迫性线索影响的相关研究。

网络钓鱼欺诈在电子商务平台日益猖獗，消费者在使用过程中的各种行为(频繁交易、物流信息处理、接收促销通知)不可避免地会收到各种邮件，为攻击者提供了绝佳机会。在网络钓鱼攻击中，攻击者的手段层出不穷，其中在网络钓鱼邮件中添加紧迫性信息，应用时间紧迫性催促消费者尽快做出决策，顺从邮件要求，从而落入网络钓鱼陷阱，是网络钓鱼攻击者经典手段。电子商务环境中，消费者收到的大部分邮件包含紧迫性相关信息，消费者处理信息的高频率与情感化使其受到这些信息影响的可能性大大增加。在网络钓鱼领域中对紧迫性线索的相关研究也多数从线索是否存在[13]以及与其他线索相对比[5]出发进行探讨，缺乏对紧迫性线索本身视觉呈现等特征影响的探索。区别于先前对使用文本大小等视觉显著性测量手段，本研究利用 STB 视觉显著性计算模型对紧迫性线索的视觉显著性进行衡量。研究结果验证了紧迫性线索视觉显著性对消费者面对网络钓鱼邮件时的过度自信水平的负向影响。研究结果表明，当消费者面对网络钓鱼邮件时，若紧迫性线索的视觉显著性较高，其在进行判断时的过度自信水平会降低。与先前研究显示视觉显著性的积极效用相似[18]，网络钓鱼邮件中高视觉显著性的紧迫性线索并没有强化消费者的不安全行为倾向，反而触发了个体对邮件更高程度的审慎，降低了其在判断自身识别能力时的过度自信程度，研究从视觉显著性视角丰富了紧迫性线索影响的相关研究。

- ② 揭示了视觉注意在紧迫性线索视觉显著性与过度自信关系之间的中介作用

本研究结合吸收先前相关研究经验，使用了眼动追踪方法实时捕获被试的注视行为，收集被试对不同视觉显著性水平的紧迫性线索的视觉注意情况。随后分析了被试的视觉注意与过度自信的关系。眼动数据分析表明，视觉显著性更高的紧迫性线索能够有效捕获被试的注意力，从而延长他们对线索的加工时间，以促使其对信息做出更加深入的审视。当被试对紧迫性线索投入更多的视觉注意时，这种认知投入的增加使他们发现异常的可能性会增加，从而降低了原本会存在的过度自信倾向。中介效应结果表明紧迫性线索视觉显著性对过度自信的影响可以通过用户对线索的视觉注意来产生作用。研究结果验证了紧迫性线索视觉显著性对过度自信影响中，视觉注意的中介作用。证明高视觉显著性的紧迫性线索不仅能够让消费者“看到”潜在危险，更可以让他们“更谨慎”地思考，降低盲目自信，从而降低做出不安全行为的可能性。证明了紧迫性线索视觉显著性能够通过引发消费者视觉注意从而影响其过度自信。

综上，研究结果表明网络钓鱼邮件中存在的紧迫性线索的视觉显著性对消费者的过度自信存在抑制作用。这种影响可以通过影响消费者对线索的视觉注意产生，即消费者对线索的视觉注意在其中产生中介作用。

(2) 实践意义

本文研究对电子商务领域中消费者面对网络钓鱼欺诈时的识别技巧及电商平台的反网络钓鱼工作进行具有重要的实践意义，具体如下：

- ① 研究结果为减少消费者识别网络钓鱼的过度自信提供实践指导

传统的电商安全防御措施多集中于技术层面(信息加密、反网络钓鱼自动识别工具等)，但人是安全链条中重要的一环，也是网络钓鱼攻击最薄弱的环节[47]，因此反网络钓鱼工作最为重要的是用户本身，在面对网络钓鱼攻击时，消费者自身能否正确识别网络钓鱼陷阱至关重要。当他们面对可疑的电子邮件时，要能找到关键显著的欺骗线索。意识到邮件中醒目、突兀的紧迫性线索本身就是一个“危险信号”，适

当地分配更多注意进行识别观察。其次消费者在注意到显著性明显的危险信号后，要避免产生识破骗局的得意，而应该是继续谨慎地寻找观察其他线索，降低自己的过度自信程度。越是看到显著的紧迫性线索的敦促要求，越要进行彻底的检查，给自己留出“冷静期”以避免冲动回复，在回复之前先核实，最大程度降低成为网络钓鱼受害者的可能。

② 研究结果为电商平台的反网络钓鱼手段的完善提供了实践指导

虽然目前反网络钓鱼自动识别工具已经相对完善，但攻击者的手段与时俱进是不能忽略的问题。研究结果为电商平台反网络钓鱼工具的改善与优化提供了一定的启示，可以适当优化安全界面，增加能够主动识别并增强紧迫性线索视觉显著性的功能，比如延迟响应设计：在邮件客户端强制显示“冷静倒计时(如30秒倒计时后才能点击链接)”，打断消费者的冲动反应，直接吸引消费者注意以让其进行深度处理。当检测到消费者可能接触到了邮件中欺骗线索，如光标长时间停留等，及时跳出警告，做出提醒。

6.3. 不足及展望

本研究仍然存在一定的局限性。首先，本研究中的被试均为在校本科生或研究生，覆盖范围有限。考虑到社会中不同年龄阶层或行业的人对电子邮件使用以及网络钓鱼诈骗的认识及接触并不相同。未来可以进一步扩大被试群体，进行更大范围的研究；其次，本研究中仅将过度自信作为消费者面对网络钓鱼攻击时的不安全行为，但现有研究中用户的网络钓鱼易感性等也是常用指标。未来研究可以考虑探究紧迫性线索除对消费者的过度自信影响之外，对消费者其他行为如是否点击邮件链接等是否具有影响作用。

基金项目

本工作得到了国家自然科学基金项目(项目批准号：72074101、72474089)和江苏省研究生科研与创新实践计划项目(项目批准号：KYCX25_4309)的资助。

参考文献

- [1] 唐宇悦. 电子商务中消费者个人信息法律保护的困境及规制[J]. 电子商务评论, 2025, 14(10): 1645-1650.
- [2] Wang, P. and Lutchkus, P. (2023) Psychological Tactics of Phishing Emails. *Issues in Information Systems*, **24**, 71-83.
- [3] APWG (2025) Phishing Activity Trends Report, 1st Quarter 2025. <https://apwg.org/>
- [4] Wang, J., Li, Y. and Rao, H.R. (2016) Overconfidence in Phishing Email Detection. *Journal of the Association for Information Systems*, **17**, 759-783. <https://doi.org/10.17705/1jais.00442>
- [5] McAlaney, J. and Hills, P.J. (2020) Understanding Phishing Email Processing and Perceived Trustworthiness through Eye Tracking. *Frontiers in Psychology*, **11**, Article No. 1756. <https://doi.org/10.3389/fpsyg.2020.01756>
- [6] Chowdhury, N.H., Adam, M.T.P. and Skinner, G. (2019) The Impact of Time Pressure on Cybersecurity Behaviour: A Systematic Literature Review. *Behaviour & Information Technology*, **38**, 1290-1308. <https://doi.org/10.1080/0144929x.2019.1583769>
- [7] 周寒, 肖益. 文档型恶意软件攻击的原理分析与防御策略研究[J]. 网络安全技术与应用, 2025(10): 42-44.
- [8] Sarno, D.M. and Neider, M.B. (2021) So Many Phish, So Little Time: Exploring Email Task Factors and Phishing Susceptibility. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, **64**, 1379-1403. <https://doi.org/10.1177/0018720821999174>
- [9] Patel, P., Sarno, D.M., Lewis, J.E., Shoss, M., Neider, M.B. and Bohil, C.J. (2019) Perceptual Representation of Spam and Phishing Emails. *Applied Cognitive Psychology*, **33**, 1296-1304. <https://doi.org/10.1002/acp.3594>
- [10] Baryshevtsev, M. and McGlynn, J. (2020) Persuasive Appeals Predict Credibility Judgments of Phishing Messages. *Cyberpsychology, Behavior, and Social Networking*, **23**, 297-302. <https://doi.org/10.1089/cyber.2019.0592>
- [11] Hu, Q., West, R. and Smarandescu, L. (2015) The Role of Self-Control in Information Security Violations: Insights from a Cognitive Neuroscience Perspective. *Journal of Management Information Systems*, **31**, 6-48. <https://doi.org/10.1080/07421222.2014.1001255>

- [12] Vishwanath, A., Herath, T., Chen, R., Wang, J. and Rao, H.R. (2011) Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model. *Decision Support Systems*, **51**, 576-586. <https://doi.org/10.1016/j.dss.2011.03.002>
- [13] Williams, E.J., Hinds, J. and Joinson, A.N. (2018) Exploring Susceptibility to Phishing in the Workplace. *International Journal of Human-Computer Studies*, **120**, 1-13. <https://doi.org/10.1016/j.ijhcs.2018.06.004>
- [14] 贾心怡, 刘伟. 国内个人投资者过度自信的前因分析——人格特质、社会阶层及认知能力[J]. 科技创业月刊, 2024, 37(12): 159-166.
- [15] Ifcher, J. and Zarghami, H. (2014) Affect and Overconfidence: A Laboratory Investigation. *Journal of Neuroscience, Psychology, and Economics*, **7**, 125-150. <https://doi.org/10.1037/npe0000022>
- [16] Frank, M., Jaeger, L. and Manuel Ranft, L. (2023) Using Contextual Factors to Predict Information Security Overconfidence: A Machine Learning Approach. *Computers & Security*, **125**, Article ID: 103046. <https://doi.org/10.1016/j.cose.2022.103046>
- [17] Ebert, N., Ackermann, K.A. and Bearth, A. (2022) When Information Security Depends on Font Size: How the Saliency of Warnings Affects Protection Behavior. *Journal of Risk Research*, **26**, 233-255. <https://doi.org/10.1080/13669877.2022.2142952>
- [18] Pan, S., Kwak, D., Kuem, J. and Kim, S.S. (2024) Roles of Feedback and Phishing Characteristics in Anti-Phishing Training Performance: Perspectives of Goal Setting and Skill Acquisition. *Journal of the Association for Information Systems*, **25**, 1037-1078. <https://doi.org/10.17705/1jais.00854>
- [19] 李勋, 孙林辉, 朱鹏烨. 弹窗广告的视觉显著性对消费者注意的影响研究[J]. 人类工效学, 2021, 27(6): 33-40.
- [20] Jaeger, L. and Eckhardt, A. (2020) Eyes Wide Open: The Role of Situational Information Security Awareness for Security-Related Behaviour. *Information Systems Journal*, **31**, 429-472. <https://doi.org/10.1111/isj.12317>
- [21] Brüns, J.D. and Meißner, M. (2023) Show Me That You Are Advertising: Visual Salience of Products Attenuates Detrimental Effects of Persuasion Knowledge Activation in Influencer Advertising. *Computers in Human Behavior*, **148**, Article ID: 107891. <https://doi.org/10.1016/j.chb.2023.107891>
- [22] 杨强, 蒋玉石, 申黎华, 等. 隐喻修辞对网络横幅广告注意效果的影响研究[J]. 管理工程学报, 2023, 37(2): 48-59.
- [23] Wang, Z., Li, G., Diao, Y. and Wang, N. (2024) Warning Deterrence or Knowledge Guidance? Research on Triggering Mechanism of Phishing Sensitivity. *Computers & Security*, **142**, Article ID: 103875. <https://doi.org/10.1016/j.cose.2024.103875>
- [24] Williams, E.J. and Polage, D. (2018) How Persuasive Is Phishing Email? The Role of Authentic Design, Influence and Current Events in Email Judgements. *Behaviour & Information Technology*, **38**, 184-197. <https://doi.org/10.1080/0144929x.2018.1519599>
- [25] Cakici, N. and Zaremba, A. (2022) Salience Theory and the Cross-Section of Stock Returns: International and Further Evidence. *Journal of Financial Economics*, **146**, 689-725. <https://doi.org/10.1016/j.jfineco.2021.10.010>
- [26] Yeari, M., Oudega, M. and van den Broek, P. (2016) The Effect of Highlighting on Processing and Memory of Central and Peripheral Text Information: Evidence from Eye Movements. *Journal of Research in Reading*, **40**, 365-383. <https://doi.org/10.1111/1467-9817.12072>
- [27] Milutinović, G., Ahonen-Jonnarth, U. and Seipel, S. (2021) Does Visual Saliency Affect Decision-Making? *Journal of Visualization*, **24**, 1267-1285. <https://doi.org/10.1007/s12650-021-00760-4>
- [28] Chun, M.M., Golomb, J.D. and Turk-Browne, N.B. (2011) A Taxonomy of External and Internal Attention. *Annual Review of Psychology*, **62**, 73-101. <https://doi.org/10.1146/annurev.psych.093008.100427>
- [29] Connor, C.E., Eggerth, H.E. and Yantis, S. (2004) Visual Attention: Bottom-Up versus Top-Down. *Current Biology*, **14**, R850-R852. <https://doi.org/10.1016/j.cub.2004.09.041>
- [30] Li, W., Guan, J. and Shi, W. (2021) Increasing the Load on Executive Working Memory Reduces the Search Performance in the Natural Scenes: Evidence from Eye Movements. *Current Psychology*, **42**, 10234-10247. <https://doi.org/10.1007/s12144-021-02270-w>
- [31] Hussein, N. (2023) Eye-Tracking in Association with Phishing Cyber Attacks: A Comprehensive Literature Review. *10th International Conference on Computer Networks & Communications (CCNET 2023)*, Vancouver, 25-26 February 2023, 71-85. <https://doi.org/10.5121/csit.2023.130406>
- [32] Zhu, M., Yang, Y. and Hsee, C.K. (2018) The Mere Urgency Effect. *Journal of Consumer Research*, **45**, 673-690. <https://doi.org/10.1093/jcr/ucy008>
- [33] Wagner, B.C. and Petty, R.E. (2022) The Elaboration Likelihood Model of Persuasion: Thoughtful and Non-Thoughtful social Influence. In: *Theories in Social Psychology*, 2nd Edition, Wiley, 120-142.
- [34] Shah, D.V., Kwak, N., Schmierbach, M. and Zubric, J. (2004) The Interplay of News Frames on Cognitive Complexity.

- Human Communication Research*, **30**, 102-120. <https://doi.org/10.1111/j.1468-2958.2004.tb00726.x>
- [35] Canfield, C.I., Fischhoff, B. and Davis, A. (2016) Quantifying Phishing Susceptibility for Detection and Behavior Decisions. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, **58**, 1158-1172. <https://doi.org/10.1177/0018720816665025>
- [36] Sheng, X., Felix, R., Saravade, S., Siguaw, J.A., Ketron, S.C., Krejtz, K., et al. (2020) Sight Unseen: The Role of Online Security Indicators in Visual Attention to Online Privacy Information. *Journal of Business Research*, **111**, 218-240. <https://doi.org/10.1016/j.jbusres.2019.11.084>
- [37] Rajab, M. (2019) Visualisation Model Based on Phishing Features. *Journal of Information & Knowledge Management*, **18**, Article ID: 1950010. <https://doi.org/10.1142/s0219649219500102>
- [38] Porta, M., Ravarelli, A. and Spaghi, F. (2013) Online Newspapers and Ad Banners: An Eye Tracking Study on the Effects of Congruity. *Online Information Review*, **37**, 405-423. <https://doi.org/10.1108/oir-01-2012-0001>
- [39] Frank, M.C., Vul, E. and Johnson, S.P. (2009) Development of Infants' Attention to Faces during the First Year. *Cognition*, **110**, 160-170. <https://doi.org/10.1016/j.cognition.2008.11.010>
- [40] Pietrantonio, F., Botta, A., Zinno, S., Ventre, G., Gallo, L., Mancuso, L., et al. (2024) A Gaze-Based Analysis of Human Detection of Email Phishing. 2024 Silicon Valley Cybersecurity Conference (SVCC), Seoul, 17-19 June 2024, 1-8. <https://doi.org/10.1109/svcc61185.2024.10637355>
- [41] Walther, D. and Koch, C. (2006) Modeling Attention to Salient Proto-Objects. *Neural Networks*, **19**, 1395-1407. <https://doi.org/10.1016/j.neunet.2006.10.001>
- [42] Wilson, R.T., Baack, D.W. and Till, B.D. (2015) Creativity, Attention and the Memory for Brands: An Outdoor Advertising Field Study. *International Journal of Advertising*, **34**, 232-261. <https://doi.org/10.1080/02650487.2014.996117>
- [43] Menzel, T., Teubner, T., Adam, M.T.P. and Toreini, P. (2022) Home Is Where Your Gaze Is—Evaluating Effects of Embedding Regional Cues in User Interfaces. *Computers in Human Behavior*, **136**, Article ID: 107369. <https://doi.org/10.1016/j.chb.2022.107369>
- [44] Lawson, P., Pearson, C.J., Crowson, A. and Mayhorn, C.B. (2020) Email Phishing and Signal Detection: How Persuasion Principles and Personality Influence Response Patterns and Accuracy. *Applied Ergonomics*, **86**, Article ID: 103084. <https://doi.org/10.1016/j.apergo.2020.103084>
- [45] Elazary, L. and Itti, L. (2008) Interesting Objects Are Visually Salient. *Journal of Vision*, **8**, 1-15. <https://doi.org/10.1167/8.3.3>
- [46] Klompstra, L., Deka, P., Almenar, L., Pathak, D., Muñoz-Gómez, E., López-Vilella, R., et al. (2022) Physical Activity Enjoyment, Exercise Motivation, and Physical Activity in Patients with Heart Failure: A Mediation Analysis. *Clinical Rehabilitation*, **36**, 1324-1331. <https://doi.org/10.1177/02692155211103696>
- [47] Proctor, R.W. and Chen, J. (2015) The Role of Human Factors/Ergonomics in the Science of Security: Decision Making and Action Selection in Cyberspace. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, **57**, 721-727. <https://doi.org/10.1177/0018720815585906>