Advances in Psychology 心理学进展, 2023, 13(10), 4389-4402
Published Online October 2023 in Hans. https://www.hanspub.org/journal/ap
https://doi.org/10.12677/ap.2023.1310553

Hans汉斯

电信网络诈骗易感性的理论模型综述：心理学视角

王浩宇

中国人民公安大学犯罪学学院，北京

收稿日期：2023年8月24日；录用日期：2023年10月7日；发布日期：2023年10月18日

摘　要

电信网络诈骗易感性是指个体在面临特定电信网络诈骗情境下成为受害者的倾向性。目前国内外学者已经针对电信网络诈骗易感性的影响因素开展了一定的研究和探索，并构建了相应的理论模型。本文对前人发展的理论模型和研究结果进行梳理和比较，并对未来研究进行展望。未来研究有必要立足我国电信网络诈骗的现实状况，开展系统化、精细化、本土化研究，并加强研究成果向公安实践的反诈宣传、预警、监测等方面工作的转化。

关键词

电信网络诈骗，诈骗易感性，影响因素

A Review of Telecom and Online Fraud Susceptibility Theories: A Psychological Perspective

Haoyu Wang

Department of Criminology, People's Public Security University of China, Beijing

Received: Aug. 24th, 2023; accepted: Oct. 7th, 2023; published: Oct. 18th, 2023

Abstract

Telecom and online fraud susceptibility refers to the tendency of being victimized in the context of the telecom and online fraud. Domestic and foreign studies have investigated the influencing factors of telecom and online fraud susceptibility. The article sorted out and compared previous

文章引用: 王浩宇(2023). 电信网络诈骗易感性的理论模型综述: 心理学视角. *心理学进展, 13(10),* 4389-4402.
DOI: 10.12677/ap.2023.1310553

theoretical models, and discussed the future research directions. Grounded in the Chinese context, future research is needed to develop a measurement system of the telecom and online fraud susceptibility, and to conduct systematic, refined and localized research, aiming at helping Public Security Authority to screen and educate potential victims, and construct early warning system.

Keywords

Telecom and Online Fraud, Fraud Susceptibility, Influencing Factors

Copyright © 2023 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

电信网络诈骗，是指以非法占有为目的，利用电信网络技术手段，通过远程、非接触等方式，诈骗公私财物的行为。[1]作为目前最为高发的新型网络犯罪，电信网络诈骗对人民群众的生命财产安全、心理安全感和社会公信力带来了极大威胁。近年来，我国采取一系列强有力的举措，遏止了电信网络诈骗犯罪的高发势头。但随着网络技术的发展，诈骗团伙隐匿性进一步增强，诈骗手法不断升级，诈骗模式持续更新，整体治理形势依然复杂严峻。

目前在理论研究和公安实战中，多运用网络技术手段对电信网络诈骗的来源进行拦截、在诈骗过程中进行预警和阻断、诈骗结束后对钱款进行追踪等方式预防和治理电信网络诈骗犯罪。虽然上述技术手段在保护人民财产安全方面取得了巨大成效，但并没有从根本上减少电信网络诈骗犯罪的发生。随着信息科技的飞速发展，阻碍电信诈骗陷阱的外部防护体系已经趋于成熟，但人们的内在心理“弱点”依然让诈骗犯屡屡得手。在面临电信网络诈骗时，人们的自身特质、心理过程与决策行为对其是否成为受害者起到重要影响，上述因素被统称为电信网络诈骗易感性。

电信网络诈骗易感性是指个体在面临特定电信网络诈骗情境下成为受害者(即出现经济损失)的倾向性。被骗易感性包含了一系列个体特征(包括心理、行为和社会特征等)，这些特征在诈骗情境下被激活，促使其做出错误判断或危险行为。研究表明，在网络安全中，人是最脆弱、风险最高的环节，而非技术系统(Yan et al., 2018)。因此，对电信网络诈骗被害易感性的研究十分重要，有助于开展针对民众和受害者的宣传、预警、监测和救助等工作。本文将从心理学视角，对电信网络诈骗易感性的相关理论和研究现状进行梳理和总结，并提出后续研究的新视角。

2. 电信网络诈骗易感性理论模型

目前，已经有一些学者提出了与电信网络诈骗易感性相关的理论模型。这些模型大多是心理学和社会学中更加经典的底层理论的延伸。电信网络诈骗犯罪往往是在特定的人际互动场景中实施的，是诈骗者说服受害者相信自己的过程。因此，可以从更加广泛的人际欺骗或说服理论视角理解电信网络诈骗。本部分将首先阐述与欺骗或说服相关的经典理论，这些理论对于电信网络诈骗易感性的研究具有重要的借鉴意义。此后，本研究将对目前已有的电信网络诈骗易感性理论进行梳理。

(一) 与欺骗或说服相关的理论

[1]《中华人民共和国反电信网络诈骗法》第二条。

1) 人际欺骗理论

Buller 和 Burgoon (1996)提出的人际欺骗理论(Interpersonal Deception Theory, IDT)基于人际沟通和社会心理学视角，强调欺骗过程发生在人际互动场景中，受到欺骗者和接收者的认知、情感和行为方式的共同影响(如图 1)。欺骗过程包含了目标导向的策略性行为和欺骗诱发的非策略性行为。前者是指双方为了达到欺骗或探测欺骗的目标，进而出现的一系列形象管理、自我保护等策略性行为；后者是指欺骗本身诱发的生理唤醒、情绪激活或认知负荷带来的外在表现，这些表现往往违背了欺骗者的目标。因此，识别出欺骗者的非策略性行为是识别欺骗的关键。最后，IDT 模型认为欺骗是一个随时间变化的动态过程，当欺骗者和接收者适应对方的言语和非言语信息的反馈时，行为模式会随着时间而波动。

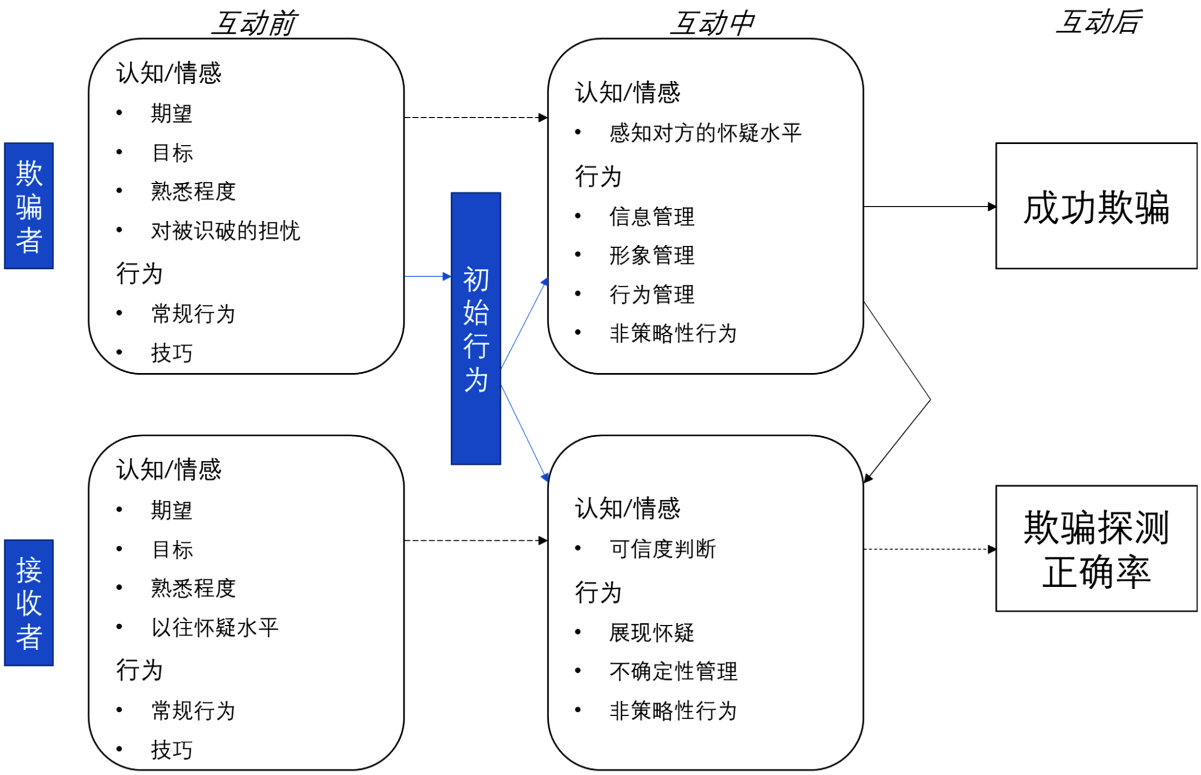


Figure 1. The interpersonal deception theory model
图 1. 人际欺骗理论模型

2) 欺骗探测模型

Grazioli 基于信息加工理论的视角提出了欺骗探测模型(the Deception Detection Model)，以探究个体在加工欺骗信息时的认知过程。该模型将欺骗探测过程分为四个认知阶段：激活、生成假设、评价假设、总体评估，并根据评估结果做出相应的回应或不回应行为(如图 2) (Grazioli, 2004)。

激活是指个体识别出当前环境中呈现的信息与期待的不一致(如个体发现某平台的理财利润过高，超出了经验中的一般水平)；生成假设是指个体对上述不一致的解释性假设；第三步是对上述假设进行评估；最后一步是整合当前假设，得出是否为欺骗的综合结论。之后有研究者将这一模型进一步整合，认为探测网络欺骗主要分为：对诈骗信息的怀疑水平、确认和反应三个行为阶段。其中，确认包含了对诈骗信息产生假设并进行验证(如通过查阅资料、电话询问等方式)的过程。与人际欺骗理论不同，该模型主要用于解释钓鱼邮件等互动性低的诈骗形式，且更关注诈骗信息的内容，而非与诈骗者的互动过程。

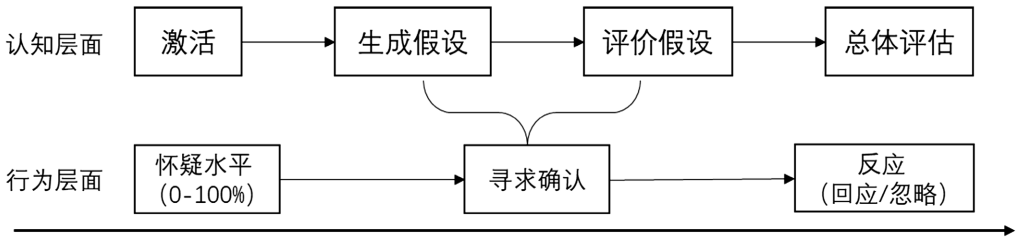


Figure 2. The deception detection model
图 2. 欺骗探测模型

3) 双过程模型

诈骗者说服受害者相信自己是实施电信网络诈骗的关键步骤，因此可借鉴社会心理学中的说服理论解释被害的心理过程，如详尽可能性模型(Elaboration Likelihood Model, ELM) (Petty & Cacioppo, 1986)和启发式－分析式模型(Heuristic-Systematic Model, HSM) (Khalifa, 2022)。上述两种模型均为双过程模型，阐释了人们对信息的认知加工和态度改变的过程。HSM 模型将信息加工分为分析式加工和启发式加工，前者是指个体使用较高的认知资源，花费更多的时间对信息进行充分的思考和加工，进而做出决策；后者则是指使用启发式的思维，对与事件不相关的信息进行低水平的认知加工，简单快速做出决策。ELM 模型则将信息加工分为中心路径和外周路径，其含义与分析式和启发式加工是相似的。上述模型认为，个体使用何种认知模式既取决于信息本身的特点，也取决于接收者对信息加工的动机和能力。使用启发式/外周路径进行认知加工更加节省认知资源，但也更容易出现非理性的决策错误，低估环境中的风险(Trumbo, 2002)。

有研究者将上述模型应用于电信网络诈骗情景，诈骗者的诈骗策略需要尽可能诱发潜在受害对象的启发式加工，抑制其分析式加工模式，以增加诈骗成功概率(Luo et al., 2013)。例如，大多数钓鱼邮件都通过各种线索(如强调时间的紧急性或事件的严重性)诱发个体进行启发式加工，关注信息的外周线索，忽视其他提示风险的线索，无法对信息的内容进行充分细致的加工，进而影响个体的认知选择(Vishwanath et al., 2011)。某些典型的说服策略被认为具有上述功能，如表 1 所示。

Table 1. Common persuasion techniques in telecom and online fraud
表 1. 电信诈骗中常见的说服技术

说服技术	用于电信诈骗场景
权威性(Authority)	冒充公检法诈骗(塑造公职人员形象，提升可信度)
喜爱水平(Liking)	情感类诈骗(在实施诈骗前先与受害者建立关系)
遵从性(Conformity)	理财类诈骗(将受害者拉入群，群内成员均为“托儿”，营造投资获利的假象)
急迫性(Urgency) & 稀有性(Scarcity)	刷单返利类诈骗(“限时优惠”制造时间压力)
奖赏(Reward)	中奖类诈骗(金钱诱惑)
损失(Loss)	冒充公检法诈骗(如不“配合”会被认定犯罪)

上述三个理论分别从不同角度阐述了欺骗或说服的过程。其中，IDT 理论最为全面，它从人际互动的角度分析了欺骗的动态变化过程，比较符合电信网络诈骗的现实场景。但其缺点也较为明显，即理论较为宽泛模糊，阐述的欺骗机制中没有包含方向(即某变量对识别欺骗的影响是积极的还是消极的)。欺骗探测模型则仅从接收者的视角分析了个体加工和探测欺骗信息的内在心理过程，与 IDT 理论相比，欺骗者变成了静态的信息，缺少互动过程，因此比较适合解释钓鱼邮件等互动性较低的电信网络诈骗类型。

双过程模型是目前应用最多、解释范围最广的理论之一，阐述了个体在人际沟通或信息加工中的认知选择和态度改变，也指出可能影响这一过程的说服策略，比较适合分析电信网络诈骗的话术或套路。

上述理论对网络诈骗易感性模型的提出具有重要的参考意义。例如，IDT 理论中强调接收者对信息的熟悉度和知识水平，欺骗探测模型中强调个体寻求确认的过程，双过程模型指出认知能力和资源对态度改变的影响，均被不同学者借鉴和吸收，形成了针对性的诈骗易感性模型。

(二) 诈骗或网络诈骗易感性模型

1) Langenderfer 的诈骗易感性模型

根据双过程模型，除了诈骗者策略以外，接收者的认知能力和加工动机也会影响被骗可能性。个体对信息加工的动机越强，越容易使用分析式加工/中心路径进行决策，越不容易被骗。然而，有研究者对此提出异议，认为个体在极强的动机水平下，注意资源反而被环境中的外周路径因素所吸引(如诈骗环境下的金钱奖赏)，使其难以进行精细化加工。这被研究者称为本能因素的影响(visceral influences) (Loewenstein, 1996)，本能因素是指一种原始驱动的状态，例如恐惧、饥饿、渴望金钱、性冲动等。当处于这一状态下，个体会产生想要获得满足的强烈冲动。

为了解决双过程模型和本能因素影响之间的矛盾，Langenderfer 和 Shimp (2001)发展出针对诈骗场景的诈骗易感性模型，如图 3 所示(以奖赏类诈骗为例)。在模型中，接收者的诈骗易感性评估可分为两个阶段，第一阶段为接收者自身的动机水平，第二阶段为环境中本能因素的影响程度，两阶段因素之间的相互作用共同影响个体的诈骗易感性水平。

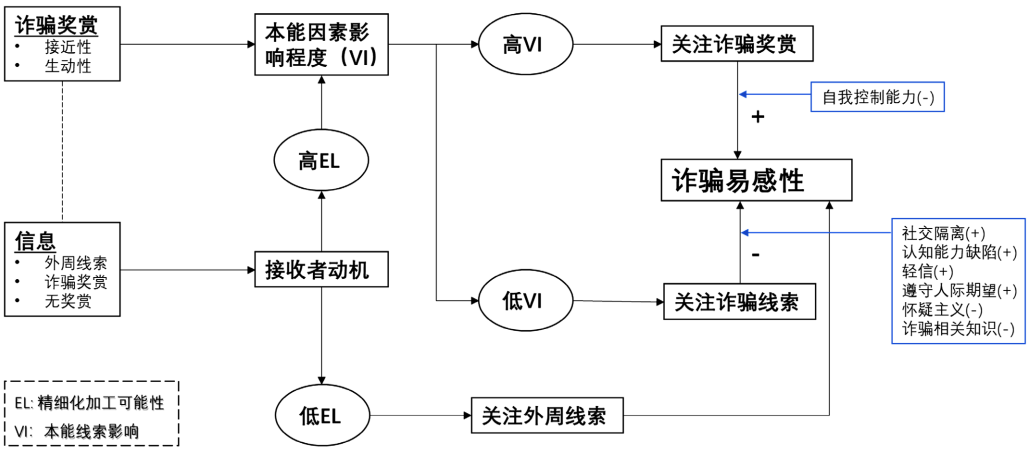


Figure 3. Langenderfer's model of scamming vulnerability
图 3. Langenderfer 的诈骗易感性模型

2) 基于人格的诈骗易感性框架

有研究者更加注重诈骗易感性的个体差异。Parrish 等以诈骗受害者的个体因素为中心发展出基于人格的诈骗易感性框架，如图 4 所示(Parrish, Bailey, & Courtney, 2009)。该框架分为五个模块：个人因素、经验因素、人格因素和攻击因素共同预测个体的被骗易感性，且不同因素之间存在复杂的交互作用。人格特质是该理论的核心，对诈骗易感性具有直接作用。例如，尽责性较高的个体更容易遵守网络规则，因此不容易掉入诈骗陷阱；宜人性较高的个体具有更强的信任倾向，依从性较强，因此在面对诈骗邮件时也更容易放松警惕。

上述理论是 Parrish 等人基于文献综述和理论分析得到的，但并没有进行系统验证。此后有研究者通过问卷调查和模型验证的方式分析了不同人格特质对诈骗易感性的影响(Modic & Lea, 2011)。

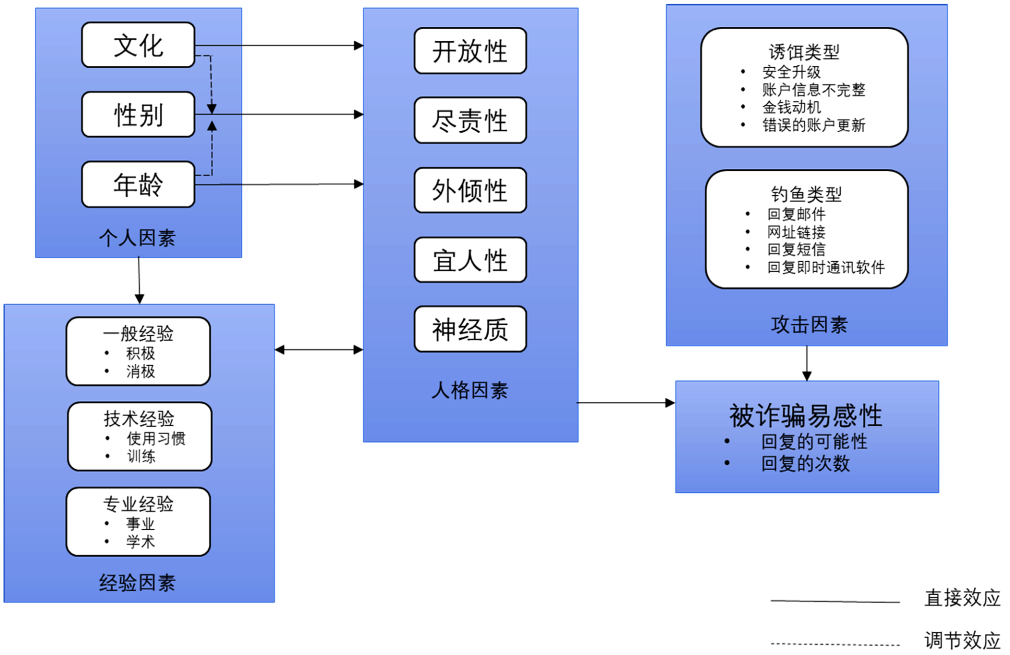
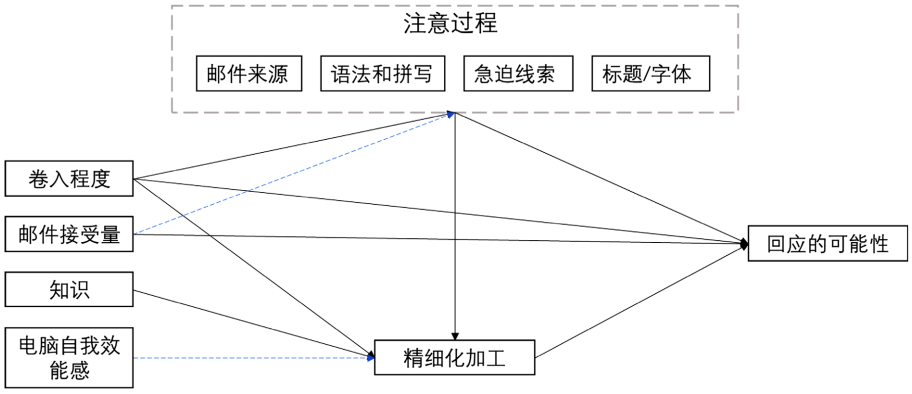


Figure 4. Personality based phishing susceptibility framework
图 4. 基于人格的诈骗易感性框架

3) 整合信息加工模型(IIPM)

基于前人提出的理论模型，Vishwanath 等(2011)提出了基于钓鱼邮件的整合信息加工模型(Integrated Information Processing Model, IIPM)，如图 5 所示。该模型将个体对钓鱼邮件的信息加工分为注意和精细化加工两个阶段，均会影响个体的欺骗探测能力。其中，注意是信息加工的第一个阶段，包括对邮件来源、文法、字体、急迫性等信息的注意；精细化加工是指个体在观察到的线索和先验知识之间建立有意识联系的过程。与欺骗探测模型相比，IIPM 的注意和精细化加工共同参与了激活过程，此外，精细化加工还包含了欺骗探测模型中的生成假设、评价假设和总体评估阶段。此外，该模型还引入并验证了个人因素和情境因素对个体的注意、精细化加工过程和欺骗探测结果的影响，如对钓鱼邮件的卷入程度、诈骗邮件相关知识、邮件数量等。

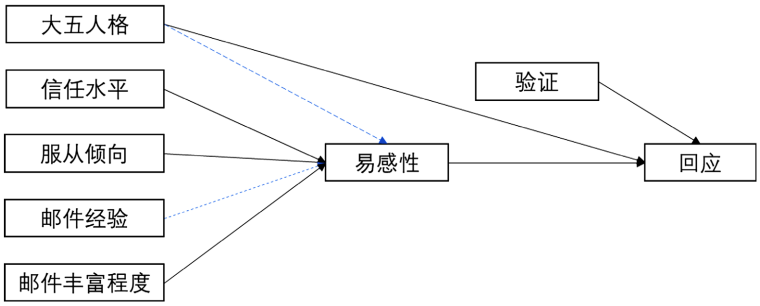


(注：蓝色虚线为研究结果未证实)

Figure 5. The Integrated Information Processing Model
图 5. IIPM 理论框架

4) 钓鱼邮件被骗易感性模型

根据欺骗探测模型，个体对欺骗信息的探测需要检验各类线索，做出判断，若无法成功识别出欺骗信息，则可能成为受害者。在此基础上，Alseadoon 进一步探究了无法成功识别诈骗信息的原因，提出了个体识别钓鱼邮件的易感性模型(如图 6)，并使用调查、实验和访谈的方法对模型进行验证(Alseadoon, Othman, & Chan, 2015)。结果发现，个体的信任倾向、服从倾向和邮件丰富程度均预测了更强的被骗易感性，而易感性水平能积极预测个体回复邮件的可能性(即成为受害者的可能性)。此外，外向性、宜人性、开放性人格特质均能积极预测个体对钓鱼邮件的回应行为；个体在欺骗探测过程中进行验证的途径的丰富程度(从面对面、电话、邮件的验证方式的丰富程度递减)对个体的回应行为有消极预测作用：验证的途径越丰富，个体越不容易回应钓鱼邮件，越不容易成为受害者。



(注：蓝色虚线为研究结果未证实)

Figure 6. The model of phishing susceptibility
图 6. 钓鱼邮件被骗易感性模型

5) 怀疑、认知和自动性模型(SCAM)

上述模型主要通过信息加工的角度分析网络诈骗中个体的认知加工过程。因此，不少干预研究致力于通过改变个体的认知加工方式，以提升其对风险线索的识别能力。然而，有研究发现这一干预方式只在短时间内有效，被试会随着时间恢复原本的加工模式(Ferguson, 2005)。这说明信息加工可能并非诈骗易感性的唯一决定因素。除了有意识的认知加工外，个体自动化的网络使用行为也可能影响诈骗易感性，如长期形成的邮件使用习惯。Vishwanath 等(2018)就此发展出了怀疑、认知和自动性模型(Suspicion, Cognition and Automaticity Model, SCAM)，如图 7 所示，并进行了实验验证。该模型认为，个体对网络风险的信念决定了在加工网络信息时的动机和投入程度，通过双通路信息加工作用于信息怀疑水平。此外，自动化的网络行为习惯(如邮件使用习惯)会绕过有意识的认知加工，直接影响个体的怀疑水平。而这一过程受到自我管理机制的影响，即自我管理水平较高的个体对习惯性行为的控制力更强。

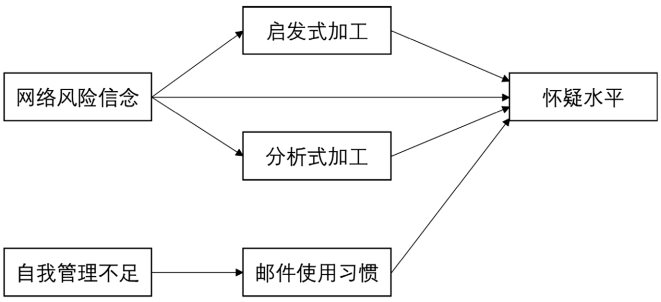


Figure 7. Suspicion, cognition and automaticity model
图 7. SCAM 理论模型

6) 网络诈骗易感性模型

Dove (2018)通过质性访谈和实证研究的方法发展了诈骗易感性模型，并进行了验证，如图 8 所示。该模型基于时间顺序展开，当潜在受害者接触到诈骗信息时，是否进一步深入了解取决于前驱因素，如是否有足够的时间进行思考、参与动机等。例如，有找工作需求的个体更容易被招聘相关的诈骗信息所吸引。进一步接触诈骗场景后，诈骗易感性取决于诈骗场景与个体因素两个方面。就前者来说，诈骗信息中的权威性、可信度、稀有性均能提升诈骗易感性；个体因素包括了服从性、冲动性、警觉性和决策时间。Dove 认为，仅仅是推迟做决定也能显著降低诈骗易感性，因为这会削弱本能线索的影响，促使个体做出更加理性的决策。此外，当个体遭受电信诈骗之后，会采取一系列回避行为使自己免于再次受骗，例如增强对自身易感性的觉察并采取相应的补偿策略。最后，受害者的某些信念也会增加被骗易感性。例如认为诈骗只会发生在别人身上，不会发生在自己身上。这一信念会降低个体面临诈骗情境下的警觉性，进而提升被骗易感性。

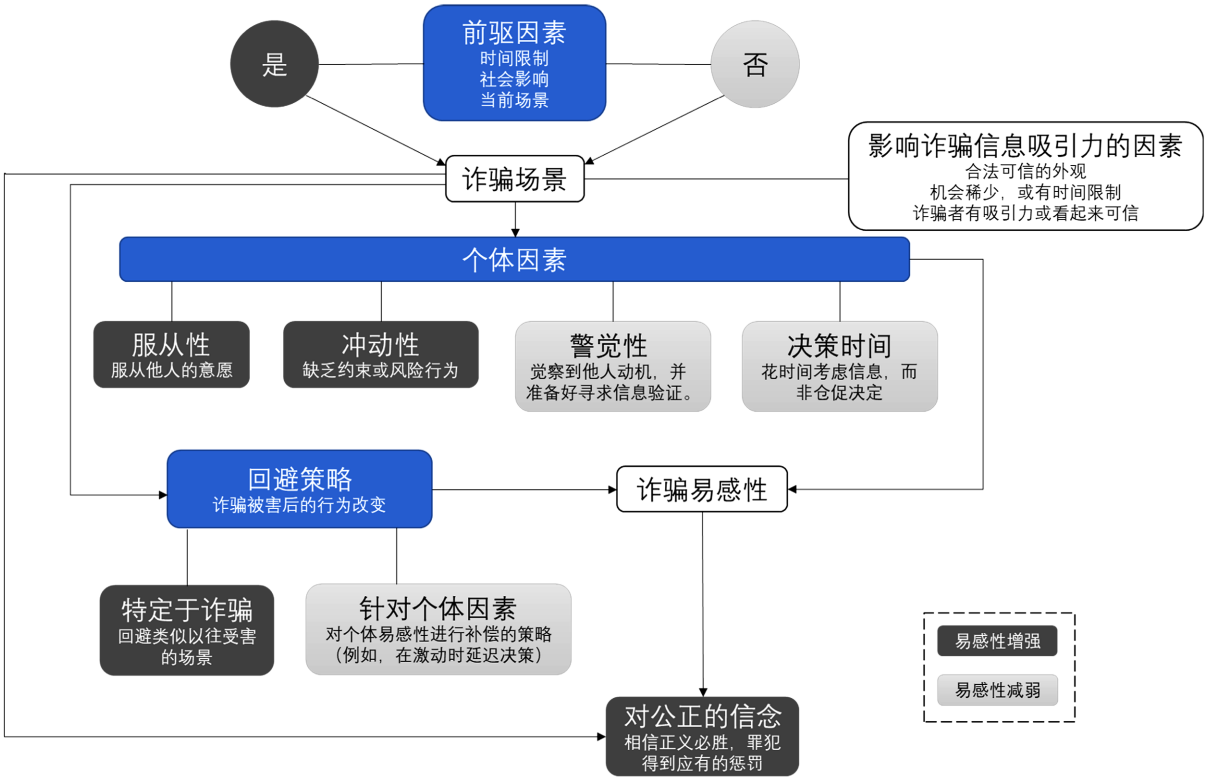


Figure 8. Dove's model of fraud susceptibility
图 8. Dove 的网络诈骗易感性模型

7) 诈骗互动识别易感性模型

在电信诈骗易感性的理论构建上，前人研究主要将电信诈骗被害过程中的易感性因素分为情境因素(诈骗剧本所包含的因素)和个人因素(被害者的个人特质)。Norris 等人通过元分析的方法进一步总结，认为电信网络诈骗过程中影响受害者决策的因素主要包括诈骗者呈现的信息因素和受害者因素，后者可以进一步划分为经验因素和特质因素，理论模型如图 9 所示(Norris, Brookes, & Dowell, 2019)。然而，电信网络诈骗是一个复杂的社会情境，情境因素与个人因素往往相互影响，或隐含着共同的心理过程，难以清晰区分。

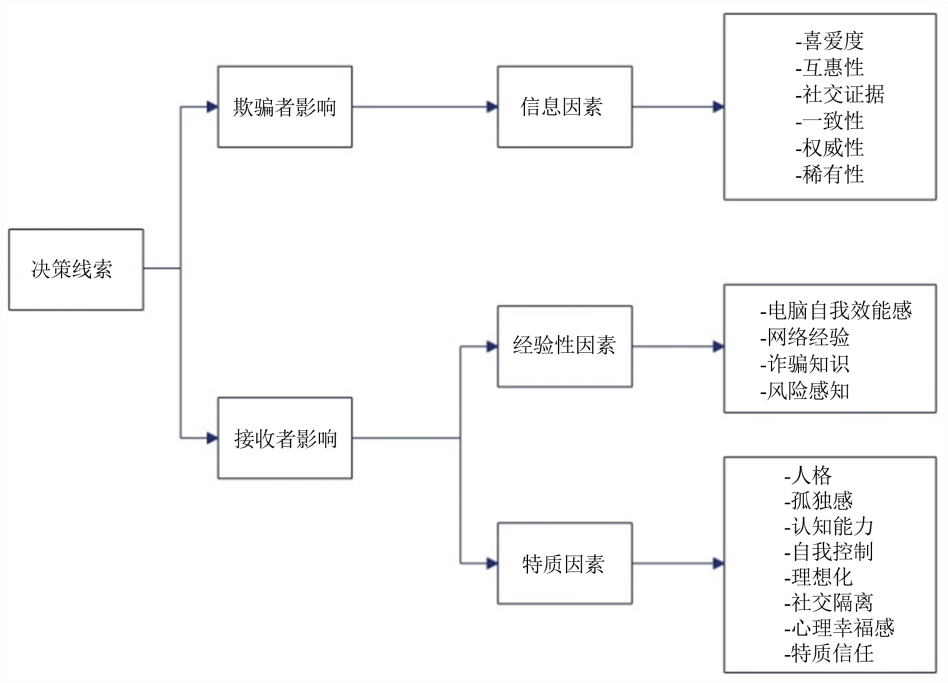


Figure 9. Fraudulent communication's identification model
图 9. 诈骗互动识别易感性模型

8) 网络诈骗易感性因素模型

近年来，我国学者也开始对电信网络诈骗易感性开展系统性研究，并提出了相应的理论模型。高原使用质性访谈的方法构建出电信网络诈骗易感性模型，并通过实验对模型进行验证，如图 10 所示(高原，2021)。根据这一模型，个体对诈骗相关的知识和网络经验、信任、风险感知、对风险线索的注意和疑虑水平均能显著预测个体的诈骗易感性。同时，线索注意水平可以中介经验因素与诈骗易感性的关系；线索疑虑水平可以中介信任和风险感知两种心理特质与诈骗易感性之间的关系。与前人相比，高原将电信网络诈骗看作动态变化的过程，首次分析了个体因素与过程性因素(信息加工过程)的相互作用对诈骗易感性的影响。

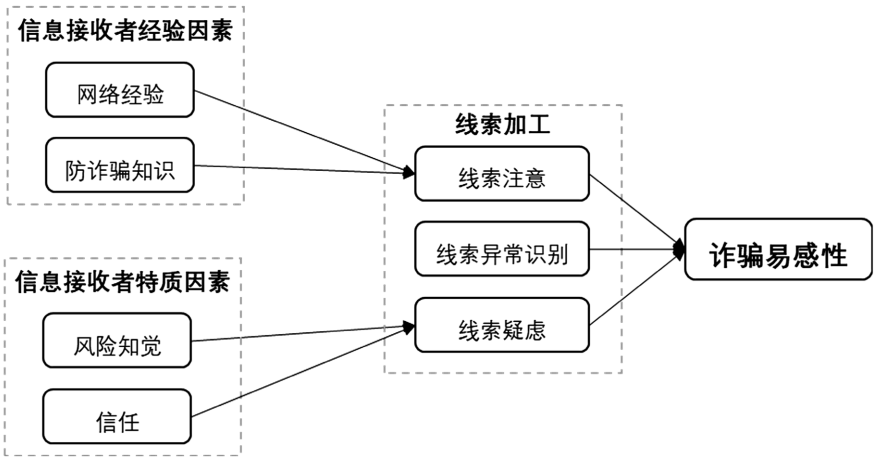


Figure 10. The influencing model of fraud susceptibility
图 10. 电信网络诈骗易感性因素模型

Table 2. Summary table of the telecom and online fraud susceptibility models
表 2. 电信网络诈骗易感性理论模型梳理

	模型名称	Langenderfer 易感性模型	基于人格的诈骗易感性模型	IIPM	Alseadoon 易感性模型	SCAM	Dove 诈骗易感性模型	Norris 诈骗互动识别模型	高原诈骗易感性模型
	诈骗类型	诈骗	钓鱼邮件	钓鱼邮件	钓鱼邮件	钓鱼邮件	网络诈骗	网络诈骗	电信网络诈骗
	理论来源	双过程模型	前人研究构建	人际欺骗理论、双过程模型、欺骗探测模型	欺骗探测模型	双过程模型	基于质性分析	前人研究构建	基于质性分析
	是否验证	否	否	实证验证	实证验证	实证验证	实证验证	否	实证验证
信息加工因素	注意 注意过程			√					√
	注意 风险感知	√					√	√	√
	认知 认知加工	√ (ELM)				√ (HSM)			√ (疑虑)
	认知 自动化加工					√ (邮件习惯)			
	动机/卷入	√		√					
	自我觉察						√		
	信念					√ (网络风险信念)	√ (公正信念)	√ (理想化)	
个体稳定因素	人口统计学变量		√ (性别、年龄、文化)						
	人格特质	√ (自控力、信任、服从性)	√ (大五)		√ (大五、信任、服从性)	√ (自控力)	√ (冲动性、服从性)	√ (人格、自控力、信任)	√ (信任)
	社交特质	√ (社交隔离)						√ (社交隔离，孤独感)	
	认知能力缺陷	√						√	
	幸福感							√	
	知识/经验	√ (诈骗)	√ (网络、诈骗)	√ (网络、诈骗)			√ (诈骗)	√ (网络、诈骗)	√ (网络、诈骗)
	自我效能感							√ (电脑使用自我效能感)	
情境因素	其他因素				√ (邮件的丰富程度)		√ (时间限制、社会影响、当前情景)		
	诈骗信息因素	√ (本能线索)	√ (钓鱼类型)				√ (外观可信度、稀有性、喜爱)	√ (喜爱、互惠、社会证据、一致性、权威性、稀有性)	

注：表格中“√”表示理论模型支持该因素对电信网络诈骗易感性存在影响。

3. 电信网络诈骗易感性的影响因素

综合前人研究，本文对已有的诈骗易感性模型进行了梳理和比较，结果如表 2 所示。本研究发现，诈骗易感性的影响因素可以归纳为个体稳定因素、情境因素和信息加工因素三大类。个体稳定因素是指个人自身心理特质或社会属性，具有较强的稳定性；情境因素是指在电信网络诈骗情景下诈骗者及诈骗环境中的相关因素；信息加工因素是指在诈骗互动过程中潜在被害人的信息加工和决策过程，具有情景依赖性。每一类因素都可再进一步划分。

由此可知，电信网络诈骗易感性是一个较为复杂的变量，会受到个体和环境等不同因素的共同影响。这与前人的研究结果是一致的，但前人研究往往单独探讨某一特定类别的易感性因素。例如，Neupane等(2014)的研究主要探讨信息加工因素的影响。实验要求被试对一系列网页是否为虚假网站进行判断，同时用核磁共振记录大脑的活动。结果发现，被试在执行任务时呈现出与注意、决策、问题解决、语言阅读和理解等认知过程相关的一系列脑区激活。这说明个体对网络信息的真伪判断涉及一系列复杂的信息加工过程。Wen 等研究者对电信网络诈骗的受害者进行质性访谈，提取出诈骗易感性的五个主要范畴：心理特质、经验因素、动机、认知偏差和不平衡的情绪状态。其中，前三者是与诈骗情景无关的个体因素(个体稳定因素)；认知和情绪则是在诈骗情景下的状态依赖性因素(信息加工因素)，这些因素共同作用于诈骗情景下个体的内部心理状态，影响其对诈骗情景的判断。Shadel (2012)则从诈骗过程出发，探究个体诈骗易感性的情境因素，包括四个阶段：提升潜在受害者的参与动机、发展关系、获取钱财、重复实施骗局。

此外，在前人研究中，对其中一些诈骗易感性因素的研究得到了一致的结果，另一些因素则存在矛盾。这可能与不同研究关注的电信网络诈骗类型和使用的研究方法的差异有关。例如，大多数理论是国外学者针对钓鱼邮件构建的诈骗易感性模型；而我国学者高原提出的理论是基于我国电信网络诈骗犯罪的实际情况，针对刷单返利和冒充类诈骗构建的易感性模型。此外，在前文提到的 8 种理论模型中，只有 5 种得到了实证研究的修正或验证(见表 2)，且使用了不同的诈骗易感性指标，因此也可能导致结果的差异。

同时，已有理论模型均更重视诈骗易感性中认知加工因素的影响。但电信网络诈骗作为复杂的社会情景，往往会诱发个体强烈的情绪体验，进而影响其对诈骗情境的感知和判断(赵雷，陈红敏，2022；Norris & Brookes, 2021)。尽管 Langenderfer 和 Shimp 的诈骗易感性模型认为本能线索与情绪密切相关，但前人的理论模型均未直接指出情绪因素对诈骗易感性的影响。由此可知，目前的电信网络诈骗易感性模型中包含的因素还不全面，未来应进一步探究情绪在电信网络诈骗过程中的作用，以及情绪与其他因素的交互作用，并将其纳入电信网络诈骗易感性的理论模型中。

4. 总结与展望

(一) 进一步加强电信网络诈骗易感性的研究

前人研究已经对电信网络诈骗易感性的影响因素进行了深入探讨，并构建了相应的理论模型，但仍存在一定的问题。首先，电信网络诈骗是一个复杂的犯罪现象。当诈骗类型、互动方式不同时，个体的被骗易感性水平及其影响因素也可能会发生变化。因此，研究者无法找到一个“万能”的模型以解释全部电信网络诈骗犯罪，需要进行更加细致的划分。部分前人研究区分了钓鱼邮件类诈骗与其他类型的诈骗，认为前者是技术层面、缺乏社交互动的诈骗类型，其影响因素也更为单纯。未来研究应进一步区分不同性质的诈骗类型，并对不同类型诈骗情境的易感性因素开展针对性的研究。

同时，目前大多数关于电信网络诈骗易感性的研究都来自西方国家，国内对相关领域的理论和实证

研究较少。然而，从现实层面，我国电信网络诈骗犯罪的特点与国外相比有所差异，存在互动性强、类型广泛的特征。因此，目前已有的理论模型可能并不适用于我国的情况，需要进一步开展适合我国犯罪特点的相关研究。

综上所述，不同个体、不同诈骗类型下的易感性水平均会发生变化，且受害者因素和诈骗类型因素之间也可能存在交互作用。未来研究还需进一步开展针对电信网络诈骗易感性的本土化、系统化、精细化研究，增强对电信网络诈骗易感性的理论构建和风险机制的理解。

(二) 构建电信网络诈骗被害心理动态模型

电信网络诈骗易感性并非“全或无”的概念，而是在一个从低到高的连续轴上滑动，每个人都存在被骗的可能性。英国国家诈骗管理局(NFA)发布的关于诈骗类型和受害者的报告中指出：“诈骗被害人的画像几乎涵盖了所有人。因此，几乎所有人都可能成为诈骗的受害者”(Button, Lewis, & Tapley, 2009)。国外对钓鱼邮件诈骗的实证研究也表明，设计精妙的钓鱼邮件可以骗过 90%以上的被试(Zhang et al., 2007)。因此，并不仅仅只有诈骗易感性高的群体会遭受诈骗，在合适的情境诱导下，任何人都有可能被骗。前人研究发现，通过增强诈骗信息的权威性、稀有性、吸引力和社会影响，诱导个体使用外周路径或启发式的加工模式，可增强其被骗易感性。因此，有必要探究影响个体被骗易感性的诈骗情境因素和被害心理过程。

然而，被骗易感性是一个动态的变量。同一个体的电信网络诈骗易感性水平会随着时间、经验和状态的变化而发生改变。目前的研究仅将易感性看作静态因素，未考虑时间维度下个体的被骗易感性随情境和互动的动态变化过程。未来研究应借鉴人际欺骗理论模型中的动态视角，研究诈骗互动下不同阶段被害易感性水平和影响因素的变化，构建电信网络诈骗被害心理动态模型，并将其应用于电信网络诈骗的被害预防体系。

(三) 加强研究成果向公安实战的转化

在前人研究的基础上，未来应注重电信网络诈骗易感性研究向应用的转化，将研究成果服务于公安实战中的宣传、预警、监测和救助等措施。

在宣传和预警层面，应针对不同潜在被害群体或诈骗类型，开发针对性强、易被接受的反诈宣传和预警措施，降低民众的被骗易感性水平。目前已有研究者开发了效果良好的干预措施，但也有研究表明，针对受害者识别诈骗邮件能力的训练在短期内有效，但不具备长期效果(Vishwanath, Harrison, & Ng, 2018)。因此，如何设计效果最优的宣传或训练方法还需要未来研究进一步的探索。

在监测层面，有研究尝试使用技术手段分析网络诈骗的情境特征，并通过机器学习识别出具有诈骗高风险的网站或用户。例如，有研究使用深度学习方法分析了线上相亲网站中不同用户的个人简介信息，提取出识别诈骗用户的关键特征，并发展出诈骗用户风险检测系统(Suarez-Tangil et al., 2019)。未来研究应进一步发掘电信网络诈骗的情境因素，并将其应用于涉诈风险网络平台的动态监测和预警工作中。

最后，研究者也需要关注电信诈骗被害人的心理救助和去污名化问题。大量研究均证实，任何人都可能成为电信网络诈骗的受害者。但事实上，国内外针对电信诈骗被害人的偏见、歧视和污名化从未停息，这不仅阻碍了他们的求助动机，甚至可能对被害人的心理造成二次伤害。因此，未来研究也应致力于降低民众对被害群体的偏见，并构建被害人心理健康服务系统。

5. 结语

随着网络技术的不断发展，电信网络诈骗犯罪问题日渐凸显，对人们的信息和财产安全造成了极大威胁。在此背景下，对电信网络诈骗犯罪预防和治理的研究十分迫切。其中，电信网络诈骗易感性是与人的因素相关的重要研究领域。基于心理学中的信息加工视角，这一概念可被看作是个体加工诈骗信息

过程中所有心理因素的组合。《中华人民共和国反电信网络诈骗法》第 8 条明确规定：“应当结合电信网络诈骗受害群体的分布等特征，加强对老年人、青少年等群体的宣传教育，增强反电信网络诈骗宣传教育的针对性、精准性。”这要求将电信网络诈骗犯罪的治理链条向前延伸，注重事前的宣传教育和风险预防工作。因此，有必要开展电信网络诈骗易感性的系统化、精细化研究，以增强对不同受害群体易感因素的理解，绘制出不同诈骗类型下不同群体易感因素的风险图谱，进而开发针对性的干预和训练措施，协助公安机关开展反诈宣传和预警等工作，从源头减少电信网络诈骗犯罪的发生。

基金项目

本文是《中国人民公安大学新任教师科研启动基金项目社科类：电信诈骗被害者的心理过程研究》的阶段性成果之一，项目编号：2022JKF408。

参考文献

高原(2021). *大学生网络诈骗易感性的影响因素：心理特质、经验因素与线索加工*. 硕士学位论文, 杭州: 浙江大学.

赵雷, 陈红敏(2022). 电信诈骗中青年受骗的影响因素和形成机制研究. *中国青年社会科学, 41(3)*, 102-112.

Alseadoon, I., Othman, M. F. I., & Chan, T. (2015). What Is the Influence of Users' Characteristics on Their Ability to Detect Phishing Emails? In H. A. Sulaiman, M. A. Othman, M. F. I. Othman, Y. Abd Rahim, & N. C. Pee (Eds.), *Advanced Computer and Communication Engineering Technology* (pp. 949-962). Springer International Publishing. https://doi.org/10.1007/978-3-319-07674-4_89

Buller, D. B., & Burgoon, J. K. (1996). Interpersonal Deception Theory. *Communication Theory, 6*, 203-242. https://doi.org/10.1111/j.1468-2885.1996.tb00127.x

Button, M., Lewis, C., & Tapley, J. (2009). *Fraud Typologies and the Victims of Fraud: Literature Review*. National Fraud Authority.

Dove, M. (2018). *Predicting Individual Differences in Vulnerability to Fraud*. Doctoral Dissertation, University of Portsmouth.

Ferguson, A. J. (2005). Fostering Email Security Awareness: The West Point Carronade. *EDUCAUSE Quarterly, 28*, 54-57.

Grazioli, S. (2004). Where Did They Go Wrong? An Analysis of the Failure of Knowledgeable Internet Consumers to Detect Deception over the Internet. *Group Decision and Negotiation, 13*, 149-172. https://doi.org/10.1023/B:GRUP.0000021839.04093.5d

Khalifa, H. K. H. (2022). A Conceptual Review on Heuristic Systematic Model in Mass Communication Studies. *International Journal of Media and Mass Communication, 4*, 164-175. https://doi.org/10.46988/IJMMC.04.02.2022.007

Langenderfer, J., & Shimp, T. A. (2001). Consumer Vulnerability to Scams, Swindles, and Fraud: A New Theory of Visceral Influences on Persuasion. *Psychology and Marketing, 18*, 763-783. https://doi.org/10.1002/mar.1029

Loewenstein, G. (1996). Out of Control: Visceral Influences on Behavior. *Organizational Behavior and Human Decision Processes, 65*, 272-292. https://doi.org/10.1006/obhd.1996.0028

Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating Phishing Victimization with the Heuristic-Systematic Model: A Theoretical Framework and an Exploration. *Computers and Security, 38*, 28-38. https://doi.org/10.1016/j.cose.2012.12.003

Modic, D., & Lea, S. E. (2011). How Neurotic Are Scam Victims, Really? The Big Five and Internet Scams. In *2011 Conference of the International Confederation for the Advancement of Behavioral Economics and Economic Psychology* (pp. 1-24). https://ucilnica.fri.uni-lj.si/pluginfile.php/160506/mod_resource/content/1/Modic%2C%20D.%2C%20%20Lea%2C%20S.%20E.%20G.%20%282011%29.%20How%20neurotic%20%5BRevised%5D.pdf

Neupane, A., Saxena, N., Kuruvilla, K., Georgescu, M., & Kana, R. K. (2014). Neural Signatures of User-Centered Security: An fMRI Study of Phishing, and Malware Warnings. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)* (pp. 1-16). https://doi.org/10.14722/ndss.2014.23056

Norris, G., & Brookes, A. (2021). Personality, Emotion and Individual Differences in Response to Online Fraud. *Personality and Individual Differences, 169*, Article 109847. https://doi.org/10.1016/j.paid.2020.109847

Norris, G., Brookes, A., & Dowell, D. (2019). The Psychology of Internet Fraud Victimisation: A Systematic Review. *Journal of Police and Criminal Psychology, 34*, 231-245. https://doi.org/10.1007/s11896-019-09334-5

Parrish, J. L., Bailey, J. L., & Courtney, J. F. (2009). A Personality-Based Model for Determining Susceptibility to Phishing Attacks. In *Proceedings of the Southwest Decision Sciences Institute Annual Meeting (SDSI'09)* (pp. 285-296). University of Arkansas.

Petty, R. E., & Cacioppo, J. T. (1986). The Elaboration Likelihood Model of Persuasion. In *Communication and Persuasion* (pp. 1-24). Springer. https://doi.org/10.1007/978-1-4612-4964-1_1

Shadel, D. M. (2012). *Outsmarting the Scam Artists: How to Protect Yourself from the Most Clever Cons*. John Wiley and Sons.

Suarez-Tangil, G., Edwards, M., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M. (2019). Automatically Dismantling Online Dating Fraud. *IEEE Transactions on Information Forensics and Security, 15*, 1128-1137. https://doi.org/10.1109/TIFS.2019.2930479

Trumbo, C. W. (2002). Information Processing and Risk Perception: An Adaptation of the Heuristic-Systematic Model. *Journal of Communication, 52*, 367-382. https://doi.org/10.1111/j.1460-2466.2002.tb02550.x

Vishwanath, A., Harrison, B., & Ng, Y. (2018). Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility. *Communication Research, 45*, 1146-1166. https://doi.org/10.1177/0093650215627483

Vishwanath, A., Herath, T., Chen, R., Wang, J., & 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

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the Weakest Links in the Weakest Link: How Well Do Undergraduate Students Make Cybersecurity Judgment? *Computers in Human Behavior, 84*, 375-382. https://doi.org/10.1016/j.chb.2018.02.019

Zhang, Y., Egelman, S., Cranor, L., & Hong, J. (2007). *Phinding Phish: Evaluating Anti-Phishing Tools*. ISOC.