

基于置换检验的高校学生防诈骗认知与需求实证研究

陈依勤, 黄惠婷*

广东技术师范大学 数学与系统科学学院, 广东 广州 510665

DOI:10.61369/ASDS.2026070014

摘 要 : 电信网络诈骗的持续蔓延加剧了高校学生的受害风险。深入了解高校学生的防诈骗认知与需求, 能够有效推动校园安全措施的优化。本研究基于实证调查数据, 运用结构方程模型与非参数组合置换检验, 系统地分析了高校学生防诈骗意识对防范需求的影响路径及群体差异。研究发现, 提高防诈骗意识能够显著增强学生主动获取防诈骗知识的内在需求; 高校学生的防骗意识水平随年级增长呈现单调递增趋势; 防诈骗应用程式的使用能够增强个人防诈骗意识。研究结果揭示了高校学生防骗认知与需求之间的内在联系, 验证了非参数组合置换检验在序数数据分析中的稳健性, 为改进校园安全防诈措施提供了实证参考。

关 键 词 : 电信诈骗; 高校学生; 结构方程模型; 置换检验; 序数数据

Empirical Study on Anti-Fraud Cognition and Prevention Needs Among University Students Based on Permutation Tests

Chen Yiqin, Huang Huiting*

College of Mathematics and Systems Science, Guangdong Polytechnic Normal University, Guangzhou, Guangdong 510665

Abstract : The widespread adoption of telecommunications and the rise of online fraud are increasing the risk of university students falling victim. Understanding the connection between students' awareness of fraud prevention and their needs can help the university to design appropriate security measures to deal with actual risks. This study adopted the Structural Equation Modeling (SEM) and the Nonparametric Combination (NPC) permutation tests to analyse the relationship between fraud prevention awareness and their fraud prevention needs, as well as the differences among groups. Our findings show that when students' fraud prevention awareness increases, their need for fraud prevention also grows. Furthermore, we also found that their fraud prevention awareness rises with grade level or the intensity of anti-fraud app usage. In summary, this paper not only identifies the relationship between students' preventive awareness and their preventive needs but also further confirms the reliability of the NPC permutation test for ordinal data. The results of this study could provide a workable, practical foundation for optimising campus anti-fraud prevention systems.

Keywords : telecommunications fraud; university students; structural equation modeling; permutation test; ordinal data

引言

电信诈骗伴随信息技术的发展呈全球蔓延态势。三六零手机卫士发布的《2023年度中国手机安全状况报告》中显示, 在2023年度电信诈骗受害者中, 90后占比最高, 达38.2%, 其次是80后和00后, 比例分别为33.3%、19.8%, 50后占比最低, 为0.6%。显然, 80后、90后、00后均为受骗高发人群^[1]。新型诈骗手段促使案件数量于2016年与2022年形成双峰, 2022年我国电信诈骗犯罪立案总数首次超越盗窃案件数^[2]。大学生群体受害现象凸显其巨大社会危害性, 已引起各高校和社会的高度重视。

高校学生作为青年主要群体, 已成为电信网络诈骗侵害的高危对象。其高度的互联网参与度与相对薄弱的风险防范意识之间存在显著错位, 导致其在面对复杂诈骗情境时辨识能力不足, 进而造成严重的经济损失与心理压力^[3-4]。本研究通过实证分析高校学生遭遇电信诈骗的行为规律与认知特征, 探究其内在机制以增强信息安全防范能力, 为校园反诈防控体系的科学构建提供实证依据。

基金项目: 2023年度广东省普通高校青年创新人才类项目(2023KQNCX038)。

作者简介: 陈依勤(第一作者), 广东技术师范大学数学与系统科学学院, 本科生, 专业为应用统计学。

通讯作者: 黄惠婷, 广东技术师范大学, 讲师, 研究方向为非参数统计。

一、文献综述

（一）国内研究现状

1. 关于电信诈骗的相关研究文献分析

本文通过中国知网以“电信诈骗”主题词进行检索，显示2009至2026期间，该领域的年度发文量如图1（左）所示，2009–2015年发文量缓慢上升，2016年因政策强化与社会关注度提升，研究量显著增长，2018–2020年文献数量有所下降，2022年达峰值436篇，整体呈现上升的趋势。以“大学生电信诈骗”为主题词进行搜索，如图1（右）所示，其研究数量随时间变化的趋势与“电信诈骗”整体研究基本同步，但发文量相对较少，这表明针对高校学生群体的电信诈骗研究尚不充分。因此，对高校学生电信诈骗问题的行为规律分析研究具有必要性。

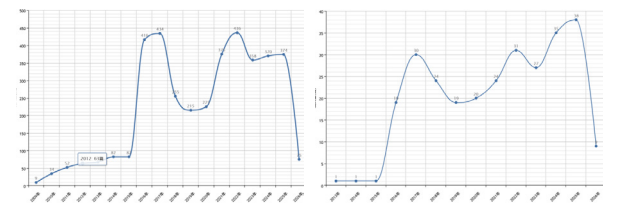


图1：CNKI 分别以“电信诈骗”（左）和“大学生电信诈骗”（右）为主题发文量

2. 关于高校学生电信诈骗问题研究的基本观点

（1）关于电信诈骗的界定

近年来，电信诈骗犯罪案件剧增，伴随着一系列新兴技术的崛起，犯罪分子作案手段不断翻新，从一定程度上加大了电信诈骗犯罪认定问题的难度。文献梳理表明，学界对电信诈骗的界定存在一定的差异^[5-7]，但总的来说可以总结为犯罪分子以非法占有他人财物为目的，利用网络平台或者通信设备，通过隐瞒真相或虚构事实，采取非接触的手段来骗取他人一定数额钱财的行为。

（2）电信诈骗的特点分析

关于电信诈骗的特点，很多学者进行了总结。丁红军、尚欣认为电信诈骗具有隐蔽性强、诈骗手段精准、诈骗过程科技化、洗钱快、追赃难、犯罪分工细化、犯罪组织去中心化凸显、犯罪链条长的特点^[8]。张启飞和虞纯纯在其研究中将电信网络诈骗的特点总结为以下三点：一是非接触式犯罪；二是隐蔽性强、被害人不确定；三是组织性、专业性^[9]。大数据时代背景下，电信诈骗及关联犯罪与传统诈骗犯罪存在一定的差异性，电信诈骗本质上是传统诈骗罪在信息技术条件下的演进形态。

（3）关于高校学生电信诈骗现状及防范措施分析

在关于高校学生遭遇电信诈骗问题的现状分析中，席东升列举了4种主要的犯罪类型，有冒充类、利诱类、威胁类、交友类，犯罪分子根据不同作案理由对受害者实施诈骗，让人防不胜防^[10]。在分析大学生遭遇电信诈骗问题的过程中可以看到，电信诈骗对大学生心理健康、对高校校园安全有着极大的危害性，应加强对其的防范举措。赵雷和陈红敏研究了青年受骗的影响因素以及形成机制，并有针对性地提出了施策建议，如转变治理思路，由打击为主转向预防和打击统筹治理、重点提升青年群体的预防电信诈骗能力、加强对个人信息犯罪的源头治理等^[11]。

（二）国外研究现状

电信诈骗具有跨国界特征，全球协同治理已成为国际社会的共同挑战。尽管各国法律文化与司法制度存在差异，但诈骗手

段的跨国渗透使各国均面临严峻的治理压力。全球反诈联盟（GASA）的最新调查显示^[12]，电信诈骗已成为全球性的治理痛点：巴西约41%的受访者表示每天都会遭遇诈骗，香港（33%）与韩国（26%）的比例亦居高不下。随着生成式人工智能技术的进步，技术赋能型诈骗日益猖獗，而公众的认知水平尚未同步跟进。调查显示，日本（15%）、泰国（12%）与马来西亚（11%）等国公民普遍承认对诈骗者利用AI技术的能力缺乏足够了解。这种全球范围内的认知滞后与技术代差，进一步凸显了提升个体防骗意识与行为干预能力的紧迫性。

二、研究设计

（一）数据来源及样本介绍

本研究选取多所高校学生为研究对象，通过问卷星平台实施线上调查，共收集345份问卷。采用筛查题进行质量控制，经数据核查排除4份无效样本，最终获得有效问卷341份，问卷有效回收率为98.84%。样本性别分布总体平衡，性别比例差异处于合理区间。涵盖高校本科各年级及研究生群体，年级分布呈梯度特征：大四年级占比最高达34.6%，研究生占比最低为7%。月生活费分布方面，74.2%受访者处于1000–2000元区间；3000元以上占比7%；1000元以下与2001–3000元两区间群体规模相近，各占9.4%与10%。

（二）信效度检验

1. 信度检验

本研究对核心变量采用李克特5点量表测量，具体题项分布见表1。

表1：量表设计

维度	题项	标签
防骗意识	当收到可以信息时，我能辨别其真伪	Q1
	若不慎遭受诈骗，我会主动采取措施以免上当或再次受骗	Q2
	我经常关注和学习电信诈骗的案例	Q3
	我了解并掌握与电信诈骗相关法律知识	Q4
	我有很强的防范电信诈骗意识	Q5
防骗需求	提供并加强防诈骗相关教育课程和培训	Q6
	提供并加强实际案例分析和警示	Q7
	提供并加强网络电信诈骗举报渠道	Q8
	提供并加强网络安全知识宣传和教育	Q9
	提供并加强网络电信诈骗防范经验分享	Q10

信度检验结果显示，防骗意识和防骗需求维度的克隆巴赫Alpha系数分别为0.830和0.901，表明该维度5个题项的内部一致性符合测量标准，整个量表的信度比较好。删除任一题项后克隆巴赫Alpha系数均低于总量表系数0.903，故保留全部题项，此时量表信度良好。

2. 效度检验

在信度检验达标的基础上，本研究采用探索性因子分析检验量表的结构效度。结果显示，KMO值为0.905，巴特利特球形度检验近似卡方值为1877.621，自由度为45， $P=0.000$ ，表明测量题项间存在显著相关性，数据适合进行因子分析。综合检验结

果，量表效度符合测量要求。

（三）结构方程模型

本研究以认知行为理论为基础，应用结构方程模型（SEM）探讨高校学生防骗意识与防骗需求的影响路径。

1. 研究假设

通常情况下，具备较高防骗意识的高校学生能更敏锐地识别潜在的诈骗风险，进而激发其主动获取防骗知识、提升自我保护能力的内在需求。基于此，本研究提出如下假设：H1：防骗意识对防骗需求具有显著的正向影响。

2. 测量模型检验与结构方程构建

本研究首先运用验证性因子分析（CFA）检验测量模型的效度，确保观测变量能够准确反映预设的潜变量^[13]。随后，基于理论假设构建以防骗意识为自变量、防骗需求为因变量的结构方程模型，通过最大似然估计法考察变量间的因果路径。

（四）置换检验

为进一步探究防骗意识在不同群体间的分布特征，本研究引入基于置换检验的非参数组合（Non-Parametric Combination, NPC）方法进行差异性分析。由于年级、反诈 App 使用深度等变量具有显著的自然顺序特征，本研究构建有序约束检验，用以验证防骗意识是否随上述变量呈现单调增长趋势。相较于传统参数检验，NPC 方法不要求数据服从正态分布，能够更稳健地识别序数数据中的群体差异规律^[14-15]。

三、实证研究结果

（一）高校学生电信诈骗问题的现状分析

1. 高校学生遭受电信诈骗的现状分析

调查结果显示，高校学生电信诈骗的遭遇率较高，整体形势严峻（见表2）。在受访群体中，67.5% 的学生曾遭遇过电信诈骗，其中22.0% 的学生遭受了实际经济损失。这表明，在新型网络犯罪手段日益复杂多变的形势下，尽管高校持续开展反诈宣传，社会阅历尚浅的学生群体仍表现出较高的受害风险。

表2：被调查者遭遇电信诈骗情况分析表

变量	选项	人数	百分比
您或您周围的同学是否遭遇过电信诈骗	遇到过且被骗了	75	22.0%
	遇到过但未被骗	155	45.5%
	从未遇到过	111	32.6%

对上述75名受骗学生的进一步调查显示，经济损失呈现明显的梯度分布特征。40.0% 的学生损失在2000元以内，损失在5000元以上的高额损失占比29.3%，甚至出现5万元以上的极端案例。在财产追偿方面，受害者表现出较高的报警意愿，但追回效果不尽人意。仅有9.3% 的受害者实现了全额追回，而高达37.3% 的受害者未能追回任何损失。此外，21.3% 的受害者因各种原因选择放弃报警，这反映出学生在面对电信诈骗时，不仅面临取证难和追回率低的现实困境，还存在维权成本考量导致的沉默化倾向。

从遭遇频次来看，44.9% 的学生在近三年内至少遭遇过一次诈骗，其中11.1% 的群体属于高频受扰人群（遭遇4次及以上）。

这说明电信诈骗对校园群体的渗透具有持续性与反复性。在诈骗发生时间的认知上，32.6% 的学生认为其发生无明显规律，体现了电信诈骗行为的随机性与隐蔽性。在有明确倾向的受访者中，选择白天（19.1%）与夜晚（17.4%）的比例相近，说明诈骗分子善于利用学生在工作学习时的心理防范空隙或休闲娱乐时的网络活跃期实施犯罪。

2. 高校学生遭受诈骗类型与欺骗性认知分析

调查数据显示，受访学生遭遇的电信诈骗类型分布呈现显著的集中性。社交账号盗用冒充是受访学生最常遇到的诈骗形式，占比达51.9%；其次为高薪招聘诈骗，占比达24.0%；投资理财诈骗与奖助学金等诈骗的遭遇比例较低。然而，学生对诈骗手法的欺骗性认知却呈现出不同的分布特征。网络购物诈骗被认为最具欺骗性，占比为26.4%，而遭遇率最高的社交类诈骗在欺骗性排名中仅位列第三，如表3所示。

通过对比遭遇频率与欺骗性认知发现，虽然社交媒体诈骗在校内频繁发生，但学生并未将其视为最大的威胁。这种认知错位说明了高校常态化反诈宣传活动的有效性。高校通过持续宣讲典型案例，增强了学生对常见社交类诈骗手段的心理防御能力。相比之下，网络购物和兼职招聘类诈骗利用复杂的商业流程来掩盖欺诈行为，而高度的信息不对称使得学生极难识别。这种隐蔽性导致学生认为这些手段更难防范，即使它们出现的频率较低，这也反映出利益诱导类诈骗是当前校园反欺诈工作面临的核心挑战。

表3：诈骗类型遭遇情况与欺骗性认知对比表

诈骗维度	第一位	第二位	第三位	第四位
遭遇类型	社交账号盗用 51.9%	高薪招聘 24.0%	投资理财 15.8%	奖助学金等 8.3%
最具欺骗性 认知	网络购物 26.4%	兼职招聘 25.9%	社交媒体 25.5%	学业考试 22.0%

3. 高校学生遭受电信诈骗的特点分析

受访学生对电信诈骗特征的认知呈现多元化分布。排名前三的特征分别为作案方式信息化、手段更新迅速以及团伙化作案，选择比例分别为23.7%、22.5%和19.8%。表明学生群体对诈骗行为的技术化与组织化特征有较为清醒的认识。此外，分别有18.4%和15.5% 的学生关注到诈骗行为的社会危害性与调查取证难度。少量补充案例显示，诈骗分子常利用避害心理设计渐进式陷阱（如招聘诈骗），通过成本沉没效应加剧受害者的财产损失风险。

（二）测量模型与结构模型分析

1. 测量模型检验与修正

本研究首先采用验证性因子分析（CFA）检验测量模型的适配度。初始模型拟合指标显示 χ^2 值为147.25，且 χ^2/df 、RMSEA和AGFI等指标未达理想标准。通过修正指数发现，对误差项e3与e4等建立共变关系。修正后的CFA模型拟合显著改善（ $\chi^2/df=2.253$ ，RMSEA=0.061，AGFI=0.934），各项关键拟合指数均达到模型适配标准，表明测量模型具有良好的建构效度。

2. 信效度分析

如表4所示，各题项的标准化因子载荷介于0.590至0.832之间。除Q4载荷（0.59）略低于0.6外，其余均在0.6以上且在0.001水平上显著。潜变量防骗意识F1与防骗需求F2的组合信度

分别为0.816和0.902；平均方差抽取量分别为0.472和0.649。尽管F1的AVE值略低于0.5，主要原因是测量“法律知识掌握”的Q4题项载荷为0.59。考虑到法律知识获取的专业性与普通防骗认知存在客观差异，且该题项是法律维度的唯一指标，为保证理论框架的完整性，本研究予以保留。综合来看，模型整体收敛效度处于可接受范围。

表4：信效度检验结果

潜变量	题项	组合信度（CR）	平均方差抽取量（AVE）	因子载荷范围
F1	Q1-Q5	0.816	0.472	0.59~0.783
F2	Q6-Q10	0.902	0.649	0.781~0.832

3. 潜变量关联与残差分析

潜变量关联分析显示，防骗意识与防骗需求的相关系数为0.754， $p < 0.001$ ，表明二者存在显著的正相关关系，初步证实了意识对需求的驱动关系。修正后的模型引入了Q3和Q4等残差协方差，反映了案例学习与法律认知之间的经验迁移效应，这与实际行为逻辑相符。所有残差相关系数的绝对值均小于0.5，有效改善了模型拟合，且不影响区分效度。

4. 结构方程模型构建与整体拟合效果

（1）结构模型拟合评价

基于理论假设与模型适配度，本研究构建了以防骗意识为自变量、防骗需求为因变量的结构方程模型（见图2）。由于该结构模型采用了修正的验证性因子分析（CFA）模型的测量关系和残差协方差设置，其整体适配度指标与CFA模型一致，且各项指标均达优秀标准，表明该理论模型与实际数据高度契合。

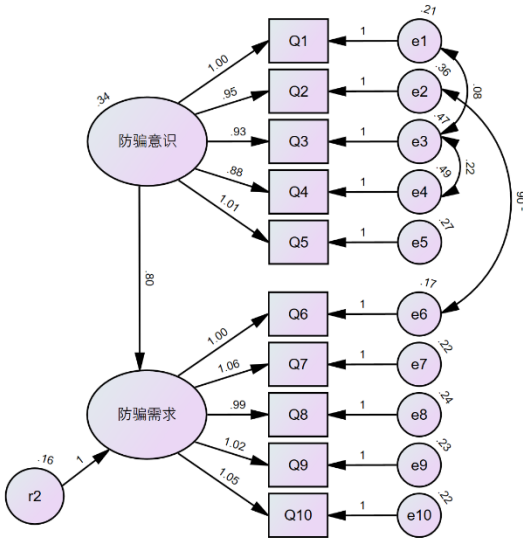


图2：SEM模型的拟合结果

（2）路径估计与结果讨论

结构路径估计结果如表5所示。防骗意识（F1）显著正向促进防骗需求（F2），未标准化路径系数为0.800。该结果支持认知驱动需求的理论假设，即防骗意识每提高1个单位，防骗需求将相应增加0.800个单位，且防骗意识能够解释防骗需求56.9%的变量。

从实践角度来看，上述结果支持提高防骗意识能有效增加相关教育资源需求的观点。例如，提高学生识别诈骗的能力（Q1）

与防范意识（Q5）可以增加对其他教育资源的需求，如案例警示（Q7）和经验分享（Q10）等。这为校园反诈资源的优化配置提供了实证依据，将意识培养作为前置环节，可以更有效地引导学生主动掌握防骗技能。

表5：结构路径系数与假设检验结果

	未标准化载荷	S.E.	C.R.	P	标准化载荷
F2←F1	0.800	0.069	11.629	***	0.754

（三）基于非参数组合置换检验的群体差异分析

本研究引入基于置换检验的非参数组合方法，考察年级与反诈App使用深度对防骗意识的影响。将年级划分为大一至研究生的五个类别，反诈App使用情况分为未下载、下载后未开启及下载并开启三个类别。这两类变量均具有显著的序数特征且数据呈现非正态分布，采用置换检验能有效克服参数检验的局限，确保群体差异推断的稳健性。

1. 统计检验设计

针对序数变量下的有序约束假设，构建如下检验模型：

$$H_0: X_1 =_d \cdots =_d X_K \quad \text{vs.} \quad H_1: X_1 \leq_d \cdots \leq_d X_K$$

将全局假设分解为 $K-1$ 个成对的子假设：

$$H_0: \left\{ \bigcap_{k=1}^{K-1} (X_{1(k)} =_d X_{2(k)}) \right\} \quad \text{vs.} \quad H_1: \left\{ \bigcup_{k=1}^{K-1} (X_{1(k)} \leq_d X_{2(k)}) \right\}$$

采用蒙特卡洛随机置换技术，设置置换次数为10000次，选择样本均值作为局部检验统计量，并通过Direct、Fisher和Liptak三种组合函数对局部P值进行全局整合，以确保推断结论的稳健性。

2. 年级对防骗意识的影响分析

针对不同年级群体的有序约束检验结果如表6所示。实证结果显示，在三种组合函数下，全局P值均显著小于0.05，这表明高校学生的电信诈骗防范意识在年级维度上存在显著的阶梯式差异。随着年级的增长，学生的社会阅历和受教育程度提升，其防范意识呈现出显著的单调递增趋势。

3. 反诈App使用深度对防骗意识的影响分析

针对反诈App的三种使用状态进行有序约束检验，结果如表6所示。三种组合函数下的全局P值均达到显著性水平，这表明反诈App的使用深度与防骗意识之间存在显著的有序约束关系。随着App使用程度的加深，学生的防骗意识整体呈现上升趋势，说明了技术干预手段在提升个体自我保护能力方面的有效性。

表6：个人特征对防骗意识影响的置换检验结果

	T_D^*	T_F^*	T_L^*
年级	0.021	0	0.025
反诈App使用深度	0.0154	0.0197	0.0155

四、研究结论与对策建议

（一）研究结论

本研究采用结构方程模型和置换检验相结合的方法，系统地分析了高校学生电信诈骗的防诈骗意识对防骗需求的影响路径及群体差异。主要结论如下：（1）基于结构方程模型路径分析表

明, 提高防骗意识能够有效激发学生对防骗知识的内在需求, 说明意识培养是促进主动学习的关键。(2) 基于置换检验发现, 防骗意识随年级增长呈现显著的单调有序特征。高年级学生由于积累了更多社会经验, 在面对潜在诈骗风险时表现出比低年级学生更强的防范素质。(3) 反诈 App 的使用深度与防骗意识显著正相关, 深度使用反诈 App 的学生通常拥有更高的警觉性。技术防控手段的有效介入, 为筑牢校园安全防线提供了重要技术支持。

(二) 对策建议

基于上述实证结果, 应对电信诈骗的有效途径是构建多层次

的防护体系: (1) 在个体层面, 学生应养成保护个人信息的好习惯, 避免随意泄露身份证号和银行卡等信息, 提高网络交互风险识别能力。(2) 在学校层面, 应加强教育宣传, 重点通过法律讲座、案例分析等防诈骗教育, 讲解正确的防范诈骗方法, 提高学生的防诈骗意识。(3) 在技术层面, 公安机关可利用社交媒体发布新型诈骗预警, 并加强反诈 App 的覆盖率与活跃度。(4) 在法律层面, 应加强反诈法律法规宣传普及, 引导学生提高法律意识, 在遭遇侵害时能够及时采取法律武器维护自身合法权益。

参考文献

[1]360手机卫士. 2023年度中国手机安全状况报告[R/OL]. (2024-03)[2026-03-20]. https://pop.shouji.360.cn/safe_report/Mobile-Security-Report-202312.pdf.
[2] 单勇. 数字平台与犯罪治理转型[J]. 社会学研究, 2022, 37(04): 45-68+227.
[3] 北京师范大学法学院课题组. 2022年电信网络诈骗治理报告: 以短视频平台为样本的研究[R/OL]. (2022-12-01)[2026-03-20]. <https://law.bnu.edu.cn/xsyj/xsdt/db33e1c2d69b46f3a5888122e09008cd.htm>.
[4] 谭秀娟, 鹿子佳, 聂永飞, 白学军. 大学生电信网络受骗易感性量表的编制[J]. 心理与行为研究, 2025, 23(02): 280-288.
[5] 李学军, 贺娇. 推定在电信网络诈骗及其关联犯罪案件证明中的适用与规制完善[J]. 法学论坛, 2024, 39(02): 119-130.
[6] 陆雪, 徐睿. 电信网络诈骗犯罪定性的实证研究——以某市147份刑事判决书为样本[J]. 上海公安学院学报, 2021, 31(04): 37-44.
[7] 中华人民共和国最高人民检察院. 电信网络诈骗的治罪与治理[EB/OL]. (2024-01-16)[2026-03-20]. https://www.spp.gov.cn/spp/llyj/202207/t20220706_562146.shtml.
[8] 丁红军, 尚欣. 电信网络诈骗犯罪治理研究[J]. 中国人民警察大学学报, 2023, 39(12): 5-10.
[9] 张启飞, 虞纯纯. 论电信网络诈骗犯罪的刑法规制[J]. 法律适用, 2023(08): 74-82.
[10] 席东升. 电信诈骗犯罪的经济学思考[D]. 广西大学, 2022.
[11] 赵雷, 陈红敏. 电信诈骗中青年受骗的影响因素和形成机制研究[J]. 中国青年社会科学, 2022, 41(03): 102-112.
[12] GASA. The global state of scams[R/OL]. (2025-12)[2026-03-20]. <https://gasa.org/knowledge-base/reports/global-state-of-scams-2025>.
[13] 张伟豪, 徐茂洲, 苏荣海. 与结构方程模型共舞[M]. 厦门: 厦门大学出版社, 2020.
[14] Huang, H., Barzizza, E., Ceccato, R., & Pesarin, F. Permutation tests for multivariate order-constrained testing problems[J]. Communications in Statistics-Simulation and Computation, 2025, 54(1), 267-282.
[15] Pesarin F., Salmaso L. Permutation tests for complex data: theory, applications and software[M]. Chichester: John Wiley & Sons, 2010.