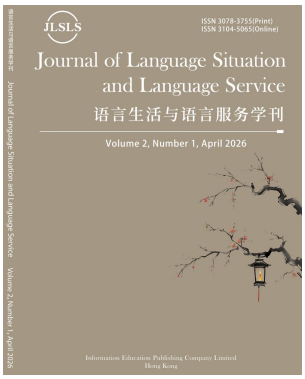

JLSLS

HIEP
Academic Publishing

Journal of Language Situation and Language Service

***JLSLS*, Vol. 1, No.1, 2026, pp.45-56**

Print ISSN: 3078-3755; Online ISSN: 3104-5065

Journal homepage: https://www.lslsjournal.com

DOI：https://doi.org/10.64058/jlsls260104calfi

基于语料分析的电信诈骗语言特征与识别防范研究

郭　杰（Guo Jie），马凤茹（Ma Fengru），岑　浩（Cen Hao）

摘要：以310起电信诈骗案件及五万余字的真实语料为基础，系统分析了电信诈骗在语言层面的表现特征、语义范畴的分类，并提出了相应的识别方法与防范策略。在语言层面，诈骗话语呈现出显著的“客服体”标准化特征，高频使用“您”“给”“有”“要”等词语，并常嵌入金融、互联网等领域的专业术语以增强欺骗性；在语义层面，诈骗行为可归纳为利益引诱型、财产保护型、紧急救助型、威胁恫吓型与博取同情型五类；在识别层面，公众可重点关注关键词分布、语音语调及行业用语等语言线索；在防范层面，建议通过理性判别预设、掌握对话主动权、抵御言语恐吓等策略，构建主动防御意识，从而系统提升社会公众的反诈骗能力。

关键词：电信诈骗；语言特征；语义类型；防范策略

作者介绍：郭杰，通讯作者，广州大学人文学院、广州大学荔湾研究院讲师，国家语言服务与粤港澳大湾区语言研究中心研究员，研究方向：理论语言学、现代汉语语法和语言服务，电邮：guangzhouguojie@163.com。**马凤茹**，云南大学文学院硕士研究生，研究方向：汉藏语，电邮：ma08252019@163.com。**岑浩**，广州大学人文学院硕士研究生，研究方向：现代汉语、语言服务，电邮：2407582138@qq.com。

Title: Corpus-Based Analysis of Linguistic Features and Identification-Prevention Strategies in Telecom Fraud

Abstract: Based on a corpus of 310 telecom fraud cases comprising over 50,000 words, this

Received: 22 Dec 2025 / Revised: 20 Mar 2026 / Accepted: 22 Apr 2026 / Published online: 30 May 2026 / Print published: 30 Jun 2026.

study conducts a systematic analysis of the linguistic features, semantic categories, and corresponding identification and prevention strategies associated with such fraud. At the linguistic level, fraudulent discourse exhibits a marked "customer-service style" characterized by standardized delivery, frequent use of terms such as "you"（您）, "give"（给）, "have"（有）, and "need"（要）, and the strategic incorporation of financial and internet-related jargon to enhance credibility. Semantically, fraudulent activities are categorized into five primary types: benefit inducement, asset protection, emergency assistance, intimidation and threat, and sympathy solicitation. For identification, the public is advised to focus on linguistic cues including keyword patterns, vocal tone, and industry-specific terminology. For prevention, strategies such as rational assessment of presuppositions, seizing conversational initiative, and resisting verbal intimidation are recommended to foster proactive defense awareness and systematically improve societal resilience against telecom fraud.

Keywords: telecom fraud; linguistic features; semantic types; prevention strategies

Author Biographies: Guo Jie, Corresponding Author, Lecturer, School of Humanities, Guangzhou University & Liwan Institute, Guangzhou University; Researcher, National Centre for Language Services and Language Studies in the Guangdong-Hong Kong-Macao Greater Bay Area. Research Interests: Theoretical Linguistics, Modern Chinese Grammar, Language Services. E-mail: guangzhouguojie@163.com. **Ma Fengru**, Master's Candidate, School of Literature, Yunnan University. Research Interest: Sino-Tibetan Languages. E-mail: ma08252019@163.com. **Cen Hao**, Master's Candidate, School of Humanities, Guangzhou University. Research Interests: Modern Chinese, Language Services. E-mail: 2407582138@qq.com.

一、引言

电信诈骗是指犯罪分子利用手机、固定电话、网络等现代通讯工具，通过编造虚假信息，骗取受害人信任，进而诱导其进行支付或转账的犯罪行为。近年来，此类犯罪活动在我国呈现高发态势。根据国务院新闻办公室新闻发布会披露的数据，在"十四五"规划期间（2021—2025 年），全国公安机关累计破获电信网络诈骗案件 173.9 万起，抓获犯罪嫌疑人 36.6 万名。同一时期，国家反诈中心共下发资金预警指令 2036.8 万条，各地公安机关成功进行见面劝阻 2821.5 万人次，有效维护了人民群众的合法权益。[1]

尽管治理成效显著，但电信诈骗的威胁依然严峻。诈骗手段持续迭代翻新，涉案金额巨大，且被骗资金往往难以全额追回，防范与打击工作面临复杂挑战。从行为模式看，此类犯罪的核心在于对"欺诈性语言"的操控，呈现出不同于传统诈骗的鲜明特征。诈骗分子不仅技术手段不断升级，其话术更具迷惑性，表现为熟练掌控对话进程、预设虚假情境、精准使用行业术语，从而使骗局极具伪装性和欺骗性。

近年来，学界从语用学、犯罪隐语分析、虚假身份建构及计算语言学等不同维度对电信诈骗话

[1] 光明网（2025 年 7 月）："'十四五'期间公安机关破获电诈案件 173.9 万起"，检索日期：2025 年 12 月 12 日，取自：https://m.gmw.cn/2025-07/23/content_1304091210.htm.

语展开研究，形成了各有侧重又相互补充的研究路径。

语用学视角聚焦于诈骗话语的话语模式与言语策略。袁瑛（2019）运用语用预设理论分析了电信诈骗案件中的话语模式，归纳出团伙型、设计型、菜单型和钓鱼型四种模式。钱永红（2019）从语言顺应论视角出发，分析了诈骗者建构的虚假身份类型及话语建构策略，揭示了诈骗者通过顺应受话人的社会心理倾向进行心理操控的机制。陈新仁（2013）提出的“语用身份”理论为理解诈骗身份操控提供了新视角，苏琪媛（2020）据此揭示诈骗人建构了“问题解决者”“威胁者”等五种语用身份，并通过话语特征实现身份转换。

犯罪隐语分析视角关注诈骗团伙内部的语言伪装。崔蒙（2021）系统搜集并分析了电信诈骗犯罪隐语，发现其在传统诈骗隐语基础上形成并不断发展，对应于诈骗犯罪的每一个环节，且受到方言和区域犯罪特点的显著影响；隐语的形成主要借助比喻、借代、谐音等修辞手法以及“饲养/诱捕—成长—宰杀”等隐喻模式。

计算语言学视角致力于涉诈文本的自动识别。周顶等（2025）引入大语言模型进行涉诈文本识别，通过形式还原与内容还原去除诈骗分子的伪装，综合运用反诈场景引导、涉诈样本启发和防诈知识支撑三种方式增强大模型的识别能力，在测试数据集上取得了 98.47%的召回率和 98.33%的精确率。

现有研究仍存在以下不足：一是各研究路径相对独立，缺乏对诈骗话语从词汇、句子、语义到结构的系统整合分析；二是话语结构研究多为定性描述或计算建模，基于大规模真实语料对诈骗话术的典型结构模式进行归纳的研究较少；三是理论分析向公众防范策略的转化不够充分，识别指标的可操作性有待加强。

鉴于此，本研究系统收集了由公安部网络安全保卫局、广州反诈服务号等权威平台发布的 2015-2025 年间的 310 起典型电信诈骗案件，整理出五万余字有效语料。在此基础之上，通过词频统计、句子分析、语义分类与话语结构模式的整合分析，揭示诈骗话语的语言特征，并据此提炼出可操作的语言识别指标与防范策略。

二、电信诈骗的语言特征

（一）语言载体与风格特征

1.以标准普通话为通用载体

语料分析显示，标准普通话是电信诈骗最主要的交流工具。无论是语音通话还是文字信息，诈骗分子均普遍采用，以最大限度覆盖潜在受害群体并消除沟通障碍。语料中仅发现 2 例（占比 0.6%）使用粤方言，且均为针对老年人的线下作案，这进一步印证了使用无地域差异的通用语是诈骗活动的普遍策略。

2.“客服体”的标准化伪装与心理操控

在语言风格上，“客服体”特征显著。在 310 条语料中，有 76 条（占比 24.5%）呈现出此类特征，具体表现为：语气刻意亲和、姿态主动迎合、发音异常标准、高频使用“您”“亲”“哦”等敬语或语气词。这种高度标准化、职业化的表达方式，旨在快速构建“专业”“可靠”的虚假形象，进而通过预设的语言逻辑，诱导受害人逐步陷入心理圈套，精准激发其不安、焦急或贪婪等目标情绪。

3.语言规范性的分化

从语言规范性来看，不同诈骗分子的表现存在明显差异，这直接反映了其组织化与专业化的程度。部分非专业团伙的诈骗材料会出现语法错误或错别字，手法相对粗糙，依赖“广撒网”式试探。而专业诈骗团伙的语料则通常语法规范、逻辑严密、用词准确，其成员往往经过系统训练，能够娴熟运用发音标准、口齿清晰且语气沉稳又不失亲切感的“客服式”语言，以此有效降低受害者的心理防备。

鉴于近四分之一（24.5%）的案件呈现出鲜明的“客服体”特征，公众在接到使用此类标准化、职业化话术的来电或信息时，应首先将其视为高风险信号，并立即对其身份真实性保持高度警惕，通过独立渠道进行主动核实，从源头上加强甄别，以有效规避诈骗风险。

（二）词汇特征

基于 310 条诈骗语料，本研究对出现频次≥3 的词汇进行了统计与分析，在剔除无实际意义的虚词（如“的”“了”）、专有名词（如人名）、无明显诈骗倾向的词汇后，最终得到有效词汇 1180 个。

1.超高频词

如表 1 所示，共有 19 个超高频词（频次≥100），占比 1.6%，累计出现 4630 次。

表 1 超高频词汇统计表（频次≥100）

Table 1 Statistics of high-frequency vocabulary (with frequency ≥ 100)

序号	词汇	词性	出现次数（次）
1	你	人称代词	851
2	我	人称代词	799
3	您	人称代词	558
4	是	动词	287
5	给	动词	205
6	好	形容词	198
7	吗	语气词	198
8	就	副词	172
9	在	副词	153
10	我们	人称代词	151
11	有	动词	140
12	钱	名词	136
13	可以	动词	128
14	现在	副词	120
15	要	动词	116
16	啊	语气词	110
17	需要	动词	105
18	会	动词	103
19	请	动词	100

首先，从词性来看，超高频词涵盖多种词类，其中人称代词（4 个）和动词（9 个）合计占比过半，是构成诈骗话语的核心词类。值得注意的是，人称代词“你”“我”“您”占据了频率前三，其中敬词“您”的高频使用显著印证了前文所述“客服体”所刻意营造的恭敬姿态，这是诈骗话术用以降低受害者防备的关键语言策略。在动词中，“是”“给”“有”“可以”“要”位列前五，共同构成一个完整的诈骗话术逻辑链：“是”（用以判断或冒充特定身份）→“有”（预设存现情境，如“有异常”或“有优惠”）→“可以”（探问虚实，提供所谓解决方案或权限）→“要”（基于情境提出具体要求）→“给”（发出最终指令，要求转账或提供验证码）。这一链条从建立身份到完成索求，环环相扣，高效驱动诈骗流程。

其次，从词汇构成看，基本词（990 个，占比 83.9%）占绝对主导，古语词、外来词及方言词极少。这表明诈骗分子刻意使用最通用、最易理解的词汇，旨在最大化潜在受害群体并最小化沟通障碍，从而提升诈骗效率。需要注意的是，行业词（186 个，占比 15.8%）的作用不容忽视。这些词汇高度集中于金融（51 个，如“流水”“冻结”）与互联网（48 个，如“网址”“下载”）两大领域。诈骗分子通过娴熟运用此类专业术语，伪造权威身份，有效增强了话语的欺骗性与威慑力。

综上分析，当通信中对方同时表现出使用敬语“您”的恭敬口吻与提及金融或互联网专业术语时，其性质高度可疑，公众应予以最高级别的警惕。

2.隐语（黑话）

语料分析显示，诈骗分子为规避网络平台审核与监管，常使用经过伪装的隐语。根据其构成原理与隐蔽性，可分为以下两类：

（1）谐音替代型隐语

此类隐语通常采用同音或近音汉字，对目标平台或服务名称进行替代性书写，以达到规避网络关键词屏蔽的目的。例如，以“收狗”指代“搜狗”“蚪音”指代“抖音”“姘多多”指代“拼多多”“竟东”指代“京东”。这类隐语基于公众熟知的日常词汇与平台名称，常伪装为“有偿收购账号”等广告，利用部分人群贪图小利的心理，诱骗其在虚假交易平台进行操作，继而以“提现失败”“需缴纳手续费”等为由实施诈骗。尽管其词汇形式具有隐蔽性，但所指含义相对直白，主要依托社会共有的认知基础（如知名应用或平台名称），公众稍加留意与辨识便可破解。

（2）意义转指型隐语

此类隐语的字面意思与实际含义完全剥离，通过建立隐秘的、约定俗成的内部代号来指代非法活动，具有极强的封闭性和欺骗性。比如“新茶已到，喝茶不？”“茶叶几百一斤？”“有五百的，有八百的，还有一千的极品哦！看您需要！”在此类诈骗话语中，“新茶”“茶叶”“喝茶”等词汇已脱离其本意，成为非法性服务的暗语。由于这类黑话的指代关系具有任意性和团伙专属性，局外人极难从字面推导其真实含义，隐蔽性极高，往往只有在深入接触或上当受骗后，才能意识到其诈骗本质。

综上所述，诈骗隐语是诈骗分子为适应网络监管而衍生的语言变体，谐音型隐语旨在绕过技术过滤，而转指型隐语则致力于构建隐秘的交流屏障，两者均增加了诈骗活动的识别与防范难度。

（三）句子特征

1.语气类型

从语气类型看，诈骗语料以祈使句和疑问句为主导。在 310 条语料中，含祈使句的语料有 143

条（占比 46.1%），含疑问句的语料有 158 条（占比 51.0%）。

（1）诈骗分子对祈使句的运用

诈骗分子大量使用祈使句，以建立权威、制造紧迫感，其典型句式结构可归纳为：“请+某人+快/赶紧/马上+V+某事”（如：请你马上点击链接进行验证；请各位家长尽快点击群收款交费）。此类句式语气强硬、直接，旨在短时间内对受害者形成心理威慑或诱导，使其在压力下丧失质疑能力，被动遵循指令。在冒充公检法或假冒老师收费等诈骗行为中，此类句式尤为常见。

（2）受害人对疑问句的使用

受害人的语言则主要由疑问句构成，其提问模式高度一致，通常遵循以下三步递进逻辑，这也反向揭示了诈骗的话术展开路径：

①认知启动（“是什么？”）：对诈骗分子抛出的新信息（如“刷单兼职”“账户异常”）产生疑问，标志着骗局介入的开始。

②操作探究（“怎么做？”）：在利益驱动或恐慌心理下，试图了解具体操作步骤，表明已产生初步信任。

③障碍求解（“怎么不行？”）：在操作遇阻（如“提现失败”“账户冻结”）时寻求帮助，此时已深陷圈套，当受害人意识到骗局时已经为时过晚。

2.句子长度

在不同类型的诈骗交互中，句式呈现显著的系统性差异。这种差异并非偶然，而是紧密对应并有效实现诈骗不同阶段的心理操控目标。

（1）诈骗分子单方主导：长句与书面语

在由诈骗分子单向发起、旨在建立权威的骗局（如冒充官方机构）中，语料普遍采用结构复杂的长句和正式的书面语体（占 50.96%）。长句的修辞功能在于承载密集信息，营造严肃、庄重的官方语境，从而提升欺骗性。例如，在假冒“最高检”或银行客服的骗局中，诈骗分子会使用包含大量修饰成分、逻辑关联词及专业术语的长句，以伪造公文效果，增强话语可信度。比如诈骗分子冒充金融客服时说：“尊敬的客户，根据国家金融监管政策与反洗钱相关规定，您尾号为 XXXX 的账户交易存在异常，为保障您的资金安全，现需您登录以下安全链接（……）完成身份核验与账户授权，否则将于 24 小时后实施临时管控。”

（2）双方交互主导：短句、否定句与口语

在诈骗分子与受害人存在多轮对话的骗局（如刷单返利、投资诈骗）中，诈骗分子的回应倾向于使用结构简短的散句、否定句，口语特征显著。这种句式选择旨在快速响应、降低理解门槛，同时通过频繁否定受害人的提议或质疑，牢牢掌控对话走向，打消其疑虑。比如下面对话：

诈骗分子：“小周，速转 97 万到 62XXXXXXXXX 这个账户。”
受害人：“胡总，是哪个项目的款？需要走审批吗？”
诈骗分子：“特急，投标保证金。先办，手续后补。”
受害人：“金额有点大，系统可能需要人脸识别……”
诈骗分子：“想办法克服。事关重大，下午必须到账。”

可见，电信诈骗在句子层面具有鲜明的策略性：诈骗分子通过具有威慑与指令功能的祈使句及书面化长句建立权威、制造心理压力；受害者则被动地以模式化的疑问句作出回应。当交互深入时，诈骗分子会策略性地转换为短促的否定句与口语化表达，以维持对话控制并消除对方疑虑。这种对不同句子类型的动态选择与转换，精准对应诈骗不同阶段的心理操控需要，是其语言操控的核心机制之一。

三、电信诈骗的语义类型和话语结构

电信诈骗种类繁多，下面结合实例，着重论述几种较为常见的、危害较大的诈骗类型。值得注意的是，各类诈骗在话语展开方式上均呈现出相对稳定的结构模式，这些模式化的“话术脚本”是识别电信诈骗的重要标记。

（一）利益引诱型

此类诈骗以提供实际或虚拟利益为诱饵，如退税、中奖、高薪兼职、投资分红等，诱使受害人上钩后，再以缴纳“保证金”“手续费”或“账户异常需资金验证”等借口骗取钱财。此类语料共59 条，占比 19.0%。

案例 1（诈骗分子冒充医护人员发放生育补贴）

诈骗人：李 XX 女士，您好！我是 XX 医院财务科的工作人员，您在我们医院刚办理完出院手续，现在有 2000 元生育补贴要返还给您。

受害人：啊，真的吗？这么好！为什么有补贴？

诈骗人：肯定是真的，医院不会造假。是这样的，现在国家实施二孩政策，您刚生下的是二孩，国家鼓励生育，所以有补贴。

受害人：哦，这样啊，那怎么给我呢？

诈骗人：需要您提供个人身份证编号和银行卡号。

受害人：好的，我马上给你说，你记一下。

……

诈骗人：李女士，刚才我按照您提供的工商银行账号给您转账，可是系统提示转账不成功，可能您这个账户有问题。

受害人：啊，不会吧，我一直在用这个号啊！

……

诈骗人：那这样吧，我帮您查证一下账户是否有问题吧，您这个账户的余额是多少？

受害人：记不清了，可能有 3000 元左右吧。

诈骗人：好，我把医院财务的账号发给您，您把余额先转到这个账户，如果能转账成功就说明账户没问题，我再把 2000 元补贴和您的余额一起返还给您。如果也无法转账，就说明账户有问题，我再想其他办法。

受害人：好的，你稍等。

诈骗分子通过精准的个人信息（如姓名、就医记录）与权威的身份伪装（医院财务人员）建立初步信任，再利用受害者对“政策红利”的期待心理，以“账户验证”等看似合理的借口诱导其操作。此类诈骗在话语结构上遵循“利益告知—身份确认—操作引导—障碍制造—资金骗取”的五步模式：诈骗分子首先以“您有一笔补贴/奖金待领取”等话术告知利益，随后通过核对个人信息强化

可信度，引导受害人进入“领取流程”，在操作环节人为制造“账户异常”“系统故障”等障碍，最终以“解冻费”“验证费”等名义完成资金骗取。此类话术高频词包括“退款”“退税”“中奖”“保证金”“账户”“验证”等。

（二）财产保护型

此类诈骗利用人们对财产安全的天然焦虑，虚构一个财产已遭受或即将遭受损失的紧急事件（如“信用卡境外盗刷”“涉嫌洗钱”），引发受害人恐慌。随后，诈骗分子伪装成银行、警察、检察院等权威机构，以“帮助保护资金”“配合调查以证清白”为名，诱导受害人将存款转入所谓“安全账户”或进行“资金核查”，从而完成诈骗。此类语料共 67 条，占比 21.6%，是发案率较高的类型之一。

案例 2（冒充“公检法”连环诈骗）

受害人：喂，你好，我刚刚收到短信说我的信用卡在境外消费了，这卡在我身上，没有在境外消费过。

诈骗人：小姐您别急，我们这里是广东肇庆邮政银行的工作人员，系统里确实能看到您的消费记录，而且我们也看到相关的短信提示。如果这笔钱不是您本人消费，那可能确实是您个人信息被盗用或者信用卡被盗刷。

受害人：啊，那我怎么办呢？

诈骗人：这样，你赶紧报警，为了节省时间，我直接把电话给您转到公安局。

受害人：您好，是警察吗，我信用卡被盗刷了。

诈骗人：银行已经把你的卡号和信息转过来了，这个问题挺严重的，我们看到这个银行卡涉嫌一起境外洗钱案件，我们已经通过电话定位了你的位置，马上将对你展开调查。

受害人：啊？我是被冤枉的，难道我的个人信息被盗用了？

诈骗人：不排除这个情况，我们也不会冤枉好人。这样吧，如果你想证明清白的话，现在把你银行卡内的剩余资金立刻转到公安的安全账户，接受我们的资金核查。现在你记一下安全账户的卡号，赶紧进行资金核查。

受害人：好的，我这就办。

此类骗局环环相扣，精准打击心理弱点。在话语结构上，遵循“危机预警—权威介入—恐慌强化—资金转移—消失收网”的五步模式：诈骗分子首先通过伪造的消费记录和“账户异常”“涉嫌犯罪”等话术制造危机感，随即以“银行客服”“办案民警”等权威身份介入，通过严厉的法律措辞在极短时间内制造出强烈的恐惧感与孤立感，反复强调“后果严重”“时间紧迫”以强化受害人恐慌心理，使受害人为求“自证清白”或“避免损失”而丧失理性判断，继而以“安全账户”“资金核查”为由诱导转账，待得手后迅速失联。整个过程通常由团伙分工扮演不同角色完成，仿真度极高。话术中充斥着“涉嫌犯罪”“安全账户”“资金核查”“加密保护”等具有威慑性与误导性的关键词。

（三）紧急救助型

此类诈骗精准利用人际信任与情感联结，通过冒充受害人的亲属、朋友、老师等亲密或权威关系人，虚构其遭遇疾病、车祸、被绑架等突发事件，制造紧张氛围。诈骗分子利用受害人急于救助亲人的慌乱心理，以“急需手术费”“支付赔偿金”“缴纳赎金”等借口，在极短时间内诱导其转

账。此类语料共 20 条，占比 6.5%。

案例 3（冒充学校老师谎称子女急病）

诈骗人：彭 XX 家长，您好！我是 XX 中学徐老师，您的女儿彭 XX 突然得了甲型 H1N1 流感，已经送到医院被隔离了，现在急需 1 万元治疗费用。

受害人：啊，真的吗？在哪个医院？

诈骗人：就在学校斜对面的 XX 医院。

受害人：那我马上过去，等我半个小时。

诈骗人：您可以马上过来，但现在赶紧给我治疗费，医院已经多次催促，只有先交治疗费才能抢救，我手头没那么多钱。

受害人：好，好，我让孩子妈妈打给你，账号给我。

诈骗分子通过预先获取的部分真实个人信息（如姓名、学校），迅速建立起可信的虚假身份，在话语结构上遵循“关系冒充—紧急求助—阻断核实—指令转账”的四步模式。他们首先冒充特定关系人直接切入，使用“突发”“隔离”“抢救”“马上”等词语制造不容置疑的紧迫感；当受害人产生核实时，立即以“手续后补”“救人要紧”“来不及了”等话术压制其核实念头或阻断联系渠道，最后直接提供账户指令转账，迫使受害人在情绪支配下做出非理性汇款决定。常见高频词包括“急救”“住院”“汇款”“账号”等。

（四）威胁恫吓型

此类诈骗直接利用人性中对人身安全与法律风险的深层恐惧。诈骗分子或冒充黑社会人员，以“绑架”亲属为由索要赎金；或伪装成警察、检察官等执法者，指控受害人“涉嫌重大刑事案件”（如洗钱、贩毒），并以“接受调查”“资产冻结”“逮捕”等话术相威胁，最终要求其将资金转入所谓“安全账户”以“证明清白”或“破财消灾”。此类语料共 20 条，占比 6.5%。

案例 4（冒充绑匪索要赎金）

诈骗人：妈妈，妈妈，我被三个叔叔抓走了，他们打我，我流血了……

受害人：怎么啦，儿子，谁打你？你说清楚。

诈骗人：你的孩子在我这里。

受害人：你是谁？为什么抓我儿子？

诈骗人：我是道上的，兄弟几个最近缺钱花了，你拿 2 万赎金，包你儿子没事。

受害人：你们胆子真大，光天化日敢绑架？

诈骗人：老子刚出狱，怕个鸟！最迟四点钟，不拿钱或者报警，你就等着撕票。

受害人：好好好，你别激动，千万不要伤害我孩子，你告诉我怎么给你钱。

骗术核心在于通过极具冲击力的声音效果（如模拟哭喊、殴打声）和极度暴力化的威胁语言，在最短时间内击溃受害人的心理防线。在话语结构上，此类诈骗呈现“恐吓切入—身份坐实—后果威胁—隔离受害—指令转账”的五步模式：诈骗分子以“你得罪人了”“你涉嫌洗钱”等恐吓话术开场，随即通过伪造证件、警号等手段坐实权威身份，接着以“撕票”“收尸”“抓捕”“判刑”等极端后果相威胁，同时警告“不许挂断”“不能告诉任何人”以隔离受害人与外界联系，使其陷

入巨大的情绪震荡与思维停滞，丧失核实真伪的基本能力，最终诱导其转账“消灾”。此类话术高频词包括“绑架”“撕票”“赎金”“涉嫌”“通缉”“安全账户”等。

（五）博取同情型

此类诈骗以长期情感经营为前提，诈骗分子在社交媒体上伪装成学生、打工者等弱势角色，通过日常聊天与受害人建立信任甚至情感依赖。在关系稳固后，再虚构自己或亲友遭遇重病、车祸等变故，以“急需用钱”为由唤起对方的同情心与保护欲，进而诱使其“借款”或“捐助”。此类语料共 8 条，占比 2.6%，虽数量较少，但因其基于信任关系，欺骗性极强。

案例 5（冒充贫困学生求助）

诈骗人：哥，我同学得了阑尾炎，急需住院，她没有那么多钱，我把自己的生活费借给她了。

受害人：真是好孩子！

诈骗人：可是我爸爸一个月就给我一次钱，今天才 6 号，我这一个月吃饭都成问题了！呜呜……

受害人：啊，这么惨啊，问你爸爸要啊！

诈骗人：我爸刚去美国了，我现在联系不上他，前面跟你说过，他经常出差。我还是自己想办法吧。

受害人：你能有什么办法啊？难不成抢银行啊！哈哈！

诈骗人：呜呜……

受害人：你一个月生活费多少钱？

诈骗人：我很节省的，一个月才 800 块。

……

受害人：好的，我微信转账给你吧。

诈骗人：哥真好，算你借我的，下个月我一定还给你，你放心！

此类骗局的核心在于“信任培育”与“时机选择”。在话语结构上，遵循“人设塑造—情感培育—危机虚构—求助触发—持续收割”的五步模式：诈骗分子首先通过长期、无经济目的的联系精心塑造“善良但不幸”的虚拟人设，逐步降低对方戒备并建立情感联结；待时机成熟后虚构突发危机（如生病、被盗），所述理由往往金额不大、合乎情理（如生活费、医药费），且以“借”“周转”“一定还”等温和话术触发小额求助，使受害人感到是在进行“低风险、高道德”的帮助，从而放松警惕；得手后可能编造新理由持续骗取。高频词包括“生病”“急救”“借款”“暂时周转”“一定还”等。

四、电信诈骗的语言识别和防范策略

（一）语言识别

基于前文对诈骗语料的分析，公众可通过以下语言特征进行快速识别与预警。

1.关键词/高频词识别

警惕包含“是”“给”“有”“可以”“要”动词的指令。这些词常构成一个完整的诈骗逻辑链条，紧随其后则常出现“转账”“下载”“点击链接”“提供验证码”等具体行为动词。识别此类词汇组合，可有效阻断诈骗情景的初始构建。

2.语音/语调识别

警惕过分标准的“客服体”语音。无论是冒充客服的“亲切版”，还是冒充公检法的“威严版”，其共同特征均为发音异常标准、语调刻意规范、用词极端礼貌。这种经过训练的“职业化”腔调，旨在快速建立虚假权威形象。

3.行业用语识别

警惕非官方场景中出现的金融、互联网行业术语。如“账户冻结”“征信修复”“平台清退”“激活额度”等。诈骗分子利用这些术语制造专业假象和紧迫情境，任何要求你进行“资金操作”来配合处理此类“业务”的，均应视为高风险信号。

4.人称与敬语识别

警惕高频、刻意的敬语使用，尤其是“您”字。在非亲密或非正式服务关系中，对方表现出超乎寻常的恭敬与耐心，往往是博取信任的话术策略，目的在于降低戒备、诱导服从。

5.固定句式识别

警惕高危开场句式，比如：“请+某人+立即/马上+V+某事”（“请你立即转账至安全账户”）、“某人/某物+已/被+动词”（“你的账户已被冻结”）。这些句式旨在用最简结构传递最强烈的权威断言或紧急指令，以压缩受害者的反应与核实时间。在通信伊始即出现此类句式，应立即中止交流并进行核实。

（二）防范策略

1.心态建设：树立理性屏障

防范诈骗的第一道防线是稳固的心理状态。面对诱惑（如“高薪”“退税”），需警惕非分之利，克制贪念；面对恐吓（如“涉案”“绑架”），必须克服恐惧，保持镇定。在任何涉及钱财的要求面前，坚持不轻信、不慌乱、不盲从。给自己预留冷静期与核实时间，避免在情绪支配下做出决定。

2.预设拆解：审视叙事起点

所有诈骗都始于一个虚构的叙事预设（如“您有一笔补贴待领取”“您的账户涉嫌洗钱”）。识破骗局的关键，在于主动质疑这个预设的真实性。无论对方如何用个人信息、伪造身份或紧急话术进行包装，都要牢记：权威机构绝不会通过电话、社交软件处理涉密案件或要求转账。遇到任何无法立刻证实的“好事”或“祸事”，务必通过官方渠道（如拨打 110、联系银行客服、直接询问亲友）进行多源头、交叉验证。

3.话轮掌控：夺回对话主导权

在交流中，避免被动应答，应主动提问并验证。例如，当对方自称“老同学”时，可反问具体姓名、共同经历细节；当对方自称“警察”时，可询问其警号、单位，并告知将主动拨打 110 核实。通过夺回提问权和话题控制权，能有效打乱诈骗分子的既定脚本，暴露其逻辑漏洞，从而化被动为主动。

4.情绪隔离：抵御恐吓话术

诈骗分子擅长使用“涉案”“抓捕”“绑架”“撕票”等极端词汇制造恐慌，目的是用情绪冲击替代理性思考。当接到此类信息时，要有意识地建立“情绪隔离”，认识到这只是一种话术，切勿在恐惧中做出任何转账或提供密码的决定。正确的做法是：立即挂断电话，与家人、朋友沟通，或直接拨打 110 报警，将专业问题交由专业机构处理。

基金项目：本文系广东省社科规划 2022 年度学科共建项目“粤港澳大湾区语言资源库建设研究”（项目编号：GD22XZY03）的成果之一。

Conflicts of Interest: The authors declare no conflict of interest.

ORCID

Guo Jie ID https://orcid.org/0009-0002-2933-2386

Ma Fengru ID https://orcid.org/0009-0007-4763-0906

Cen Hao ID https://orcid.org/0009-0007-8422-7462

References

陈新仁（2013）：《语用学视角下的身份与交际研究》。高等教育出版社。

[Chen Xinren (2013). *Studies on Identity and Communication from a Pragmatic Perspective*. Higher Education Press.]

崔蒙（2021）：“电信诈骗犯罪隐语分析”，《北京警察学院学报》（03）:102-105。

[Cui Meng (2021). “Analysis of Latent Language in Telecommunication Fraud Crimes.” *Journal of Beijing Police College* (03):102-105. DOI: https://doi.org/10.16478/j.cnki.jbjpc.20210510.002.]

钱永红（2019）：“网络电信诈骗话语中虚假身份建构的顺应性阐释”，《浙江外国语学院学报》(05):68-76+93。

[Qian Yonghong (2019). “An Adaptive Interpretation of False Identity Construction in the Discourse of Online Telecommunication Fraud.” *Journal of Zhejiang International Studies University* (05):68-76+93. DOI: https://doi.org/10.3969/j.issn.2095-2074.2019.05.010.]

苏琪媛（2020）：《顺应论视角下电信诈骗者语用身份的话语建构研究》，广东外语外贸大学，学位论文。

[Su Qiyuan (2020). *Discursive Construction of Telecom Fraudsters' Pragmatic Identity: From the Perspective of Adaptation Theory*. Guangdong University of Foreign Studies. Dissertation.]

袁瑛（2019）：“电信诈骗案件中的话语模式与言语策略研究”，《贵州警官职业学院学报》31(04):64-68。

[Yuan Ying (2019). “Research on Discourse Patterns and Speech Strategies in Telecommunication Fraud Cases.” *Journal of Guizhou Police College* 31(04):64-68. DOI: https://doi.org/10.13310/j.cnki.gzjy.2019.04.010.]

周顶、陈哲、叶蕴芳、李岩（2025）：“基于大语言模型的涉诈文本识别研究”，《电信工程技术与标准化》(8):7-13。

[Zhou Ding, Chen Zhe, Ye Yunfang, Li Yan (2025). “Fraudulent Text Identification Research Based on Large Language Models.” *Telecommunications Engineering Technology and Standardization* (8):7-13. DOI: https://doi.org/10.13992/j.cnki.tetas.2025.08.008.]