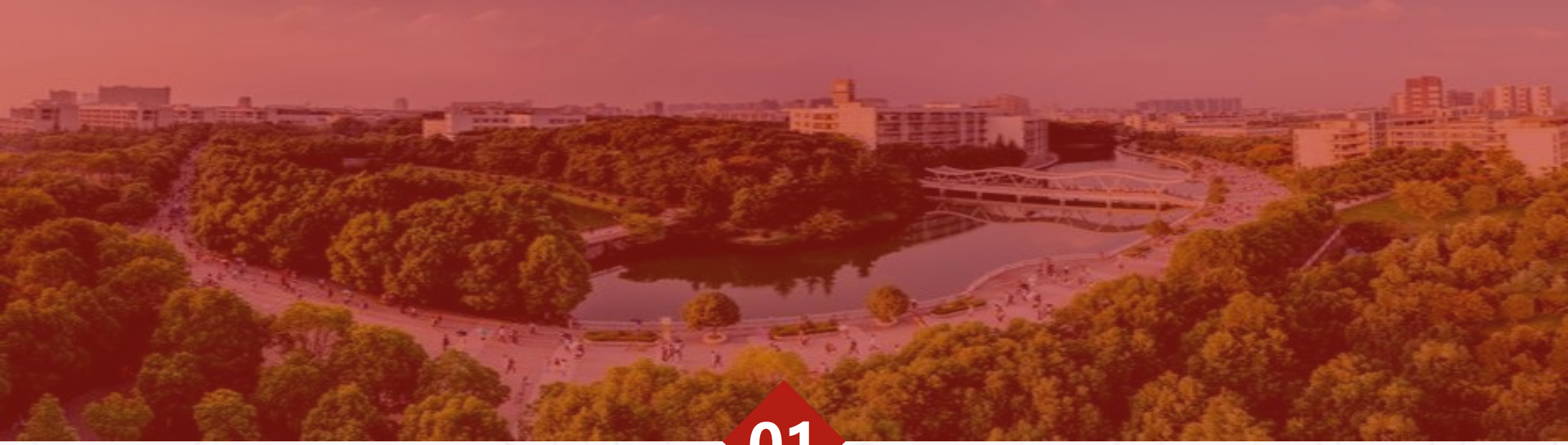
洞察诈骗套路，夯实资金安全

目录 CONTENTS



01

电信网络诈骗

电信网络诈骗是什么？

电信网络诈骗是指通过电话、网络和短信方式，编造虚假信息，设置骗局，对受害人实施远程、非接触式诈骗，诱使受害人打款或转账的犯罪行为。

手法特点

1.全程通过电话、微信、APP 等远程沟通，诈骗分子隐匿身份（跨地域、用虚拟号码），事后难以追踪。
2.要么用 “高收益” 勾起贪念（刷单、投资），要么用 “涉案、紧急” 制造恐惧 / 焦虑（冒充公检法、亲友借钱），打乱判断节奏。
3.借助伪基站（伪造官方号码）、AI 技术（换脸克隆）、虚假网站 / APP（仿冒正规平台），提升 “可信度”，降低识别难度。
4.通过非法渠道获取人群标签（学生、老年人、投资者、网购用户），针对性推送诈骗信息，避免 “广撒网” 的低效。

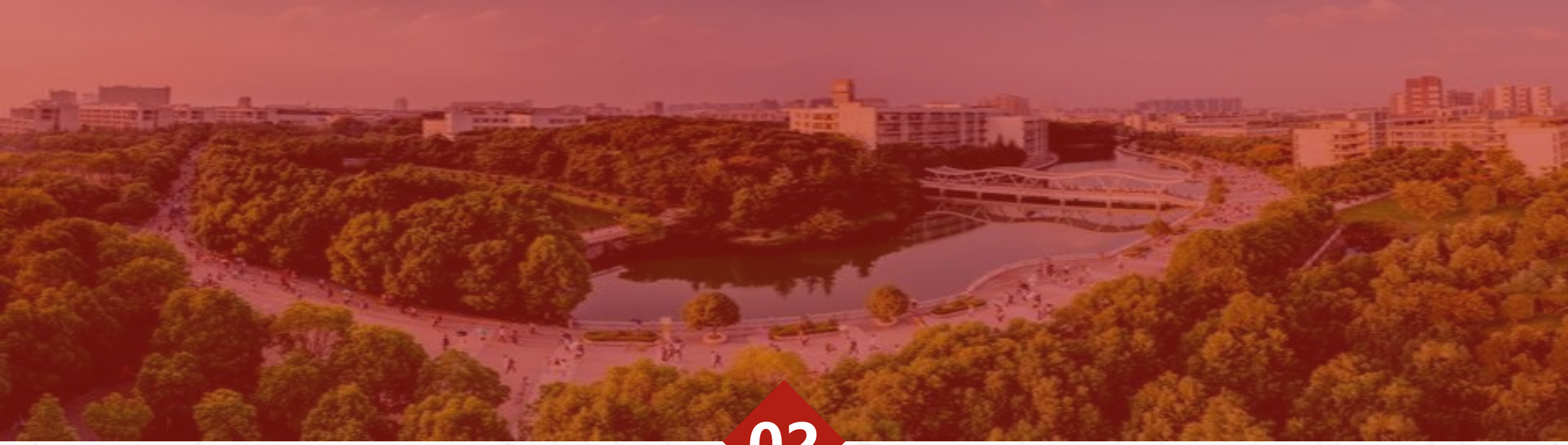
现实案例

2025 年 8 月，太原某高校大三学生小张接到冒充邮政人员电话，称其名下手机号欠费 2680 元并转接到“天津大港公安分局”。“民警”以“涉密案件”为由要求保密，发送伪造逮捕令后，诱导小张购买新手机、办理新电话卡，并拍摄“被绑架”视频发送给父母索要100万元赎金。警方通过家属报警拦截资金，成功解救小张。

https://society.huanqiu.com/article/9CaKrnJXxzf

遇到此类事件，如和防范呢？

1.不轻信（高息、“公检法涉案” 等陌生信息）、不透露（银行卡号、验证码、密码）、不转账（未当面核实的 “借钱” “安全账户” 需求）
2.遇 “亲友 / 领导 / 客服” 提转账，通过官方电话、当面沟通二次确认，警惕 AI 换脸、克隆语音
3.不随意填写问卷、扫码领礼，不向陌生平台提供身份证、手机号等隐私
4.若疑似被骗或收到可疑信息，立即拨打110或全国反诈专线96110咨询，不拖延



02

新型AI语音克隆诈骗

新型AI语音克隆诈骗是什么？

随着人工智能技术的发展，诈骗分子开始利用AI语音克隆进行精准诈骗。他们通过非法获取受害人的声音样本（如社交媒体的视频、语音消息），使用AI软件克隆声音，然后冒充亲友、同事或领导，通过电话紧急求助（如车祸、被抓、急需用钱），诱骗受害人转账。

手法特点

1.仅需 3 秒以上目标语音样本（如社交平台发言、电话录音），通过低成本 AI 工具即可克隆，生成的声音在语调、情绪甚至背景音上高度还原，肉眼耳力难辨真假，多从公开社交内容、骚扰电话诱导应答等渠道偷取语音素材，无需与受害者直接接触，不易被察觉；
2.专挑亲友、领导、子女等受害者高度信任的角色，利用情感或职场信任突破心理防线；
3.常伪造 “车祸赔偿” “手术缴费” “工作急款” 等紧急事件，制造恐慌感，以 “手机没电” “别联系本人” 为由切断核实渠道，催促立刻转账；

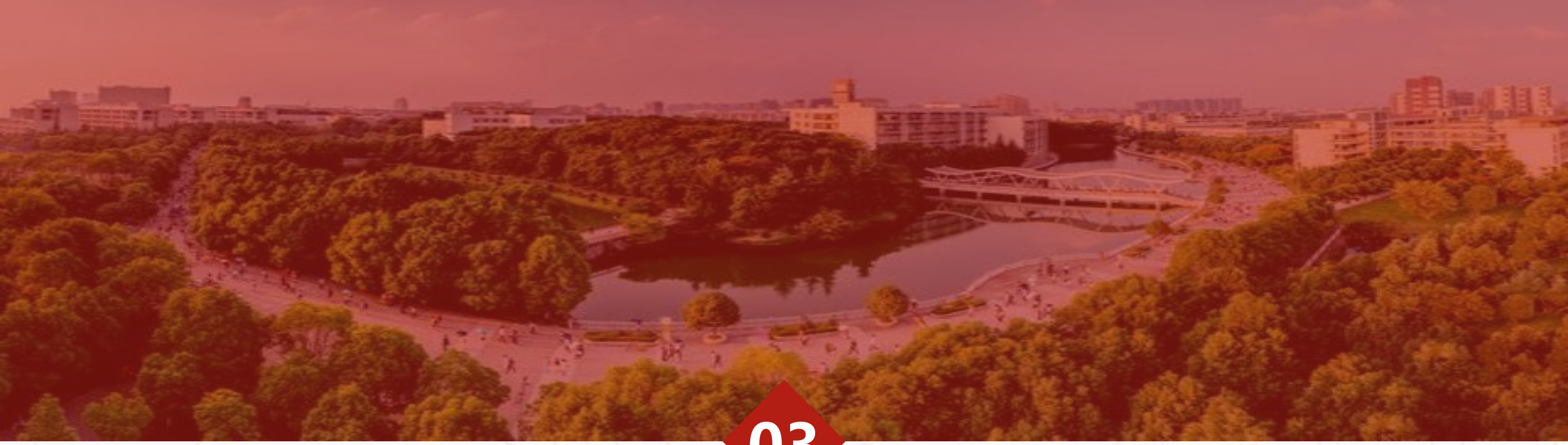
现实案例

2024年3月诈骗团伙使用 Telegram 等加密软件接收“上线”提供的语音模型，通过实时语音合成技术克隆张婆婆孙子的声音，称“摔手机伤人需赔偿”，并安排同伙冒充“孙子朋友”上门取钱。法院以诈骗罪判处主犯有期徒刑一年

https://xg.hbjc.gov.cn/xjdt/mtbb_71030/202411/t20241112_1837270.shtml

遇到此类事件，如和防范呢？

1. 无论对方声音多像，务必通过 “视频通话” “当面确认” 或 “拨打常用手机号（而非对方提供的新号码）” 验证身份，AI 可克隆语音，但暂难同步克隆实时视频动作。
2. 涉及转账、借钱，尤其是 “领导指令” “亲友求助”，务必走正常验证流程（如向领导发微信文字确认、联系其他亲友核实情况），不要因 “紧急” 跳过关键步骤。
3. 不随意在社交平台发布自己的语音、通话片段，不轻易将亲友关系、工作细节透露给陌生人，从源头减少语音样本和个人信息泄露的可能。



03

“校园贷”诈骗

“校园贷”诈骗是什么？

“校园贷”诈骗是指不法分子针对在校学生（无稳定收入、金融认知较弱、易有消费/应急资金需求），以“低利息、无抵押、快速放款”为诱饵，通过非法借贷、虚假合同、套路计息等手段实施的诈骗行为，本质是利用学生弱点设计的“高利贷陷阱”与“资金掠夺”

手法特点

1.以“低利息、无抵押、秒放款”为噱头，伪装成“校园应急贷”“创业贷”，隐瞒高额手续费、管理费，甚至签空白合同；
2.放款时扣“砍头息”，逾期后利滚利，债务快速翻倍；
3.逼学生抵押身份证、学生证，甚至拍“裸照”“手持身份证视频”作担保，后续用泄露隐私威胁还款，以“帮办贷款”为由骗走学生身份、银行卡信息，私下伪造签名办贷款，让学生莫名背债；
5.逾期后用电话轰炸、短信辱骂、校园堵人施压，还诱导“以贷养贷”，让学生陷入多重陷阱。

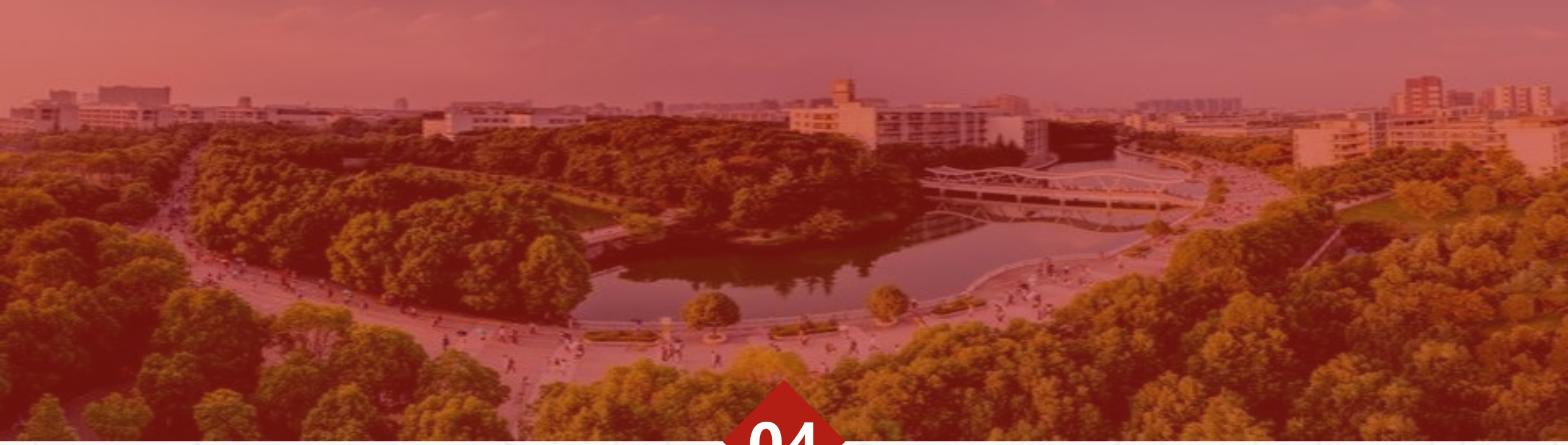
现实案例

张某等 11 人针对大学生发放 “无抵押高息贷”，通过 “借新还旧” “转单平账” 将 4000 元借款滚至 45 万元，并以裸体视频威胁、破坏门锁等方式催收。主犯张某获刑 10 年。

https://m.gmw.cn/2023-12/18/content_1303603982.htm

遇到此类事件，如和防范呢？

1.不盲目追求高消费，避免超前消费、攀比消费，缺钱优先向家长、学校求助，从源头减少借贷需求；
2.如需贷款，仅通过银行校园贷、国家开发银行助学贷款等官方途径，警惕 “无抵押、低利息、秒放款” 的非正规推销；
3.不向陌生人泄露身份证号、银行卡号、手机号及验证码，不随意签订空白合同，不轻易抵押证件或拍摄私密照片；
4.对“校园创业贷”等推销保持警惕，不相信 “先交钱再放款” “手续费抵扣本金” 等说辞，遇可疑情况及时向学校保卫处或老师反映；
5.若不慎陷入陷阱，绝不 “以贷养贷”，第一时间告知家长、老师，保留合同、转账记录等证据，必要时拨打 110 或向市场监管部门投诉，用法律维护权益。



04

“培训贷”诈骗

“培训贷”诈骗是什么？

诈骗机构以“包就业”、“高薪保障”为名，诱骗学生参加高价培训班（如编程、设计、短视频运营），并承诺“培训后分期付款”或“就业后还款”。实则通过伪造合同、隐形高息、暴力催收等方式实施诈骗，甚至骗取学生个人信息办理网络贷款。

手法特点

1.以 “包就业、月薪过万、100% 推荐岗位” 为噱头，瞄准想提升技能找工作的毕业生、职场新人，用 “先培训后赚钱” 画饼，降低警惕
2.不提 “贷款”，只说 “分期付学费” “先学后付”，甚至趁受害者不注意，引导签署第三方金融平台的借贷合同，事后才发现背负贷款
3.宣称 “名师授课、精品课程”，实际师资造假、内容劣质（多为网上拼凑的基础内容），甚至没上完课机构就 “失联跑路”，受害者既没学到东西，还得还贷款
4.中途以 “基础班不够就业，需报高级班” 为由，诱骗受害者再签一笔贷款；若受害者质疑，就推卸责任，称 “贷款是你自己签的，与机构无关”

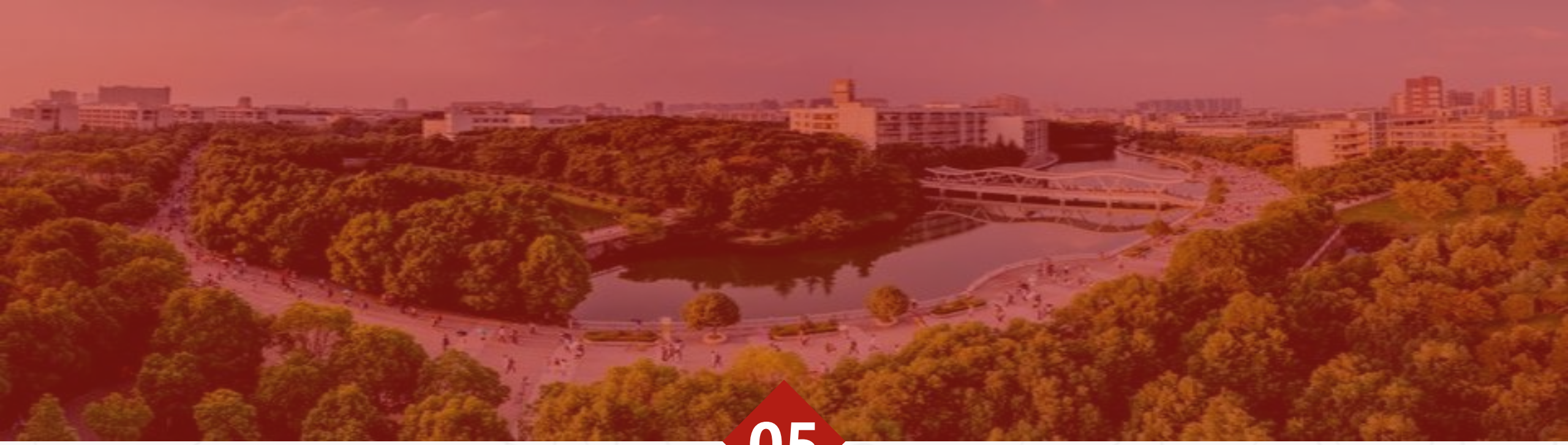
现实案例

广东某科技有限公司以“媒体运营岗位”招聘应届毕业生小唐，以“技术能力不足”为由要求参加2.6万元培训，并引导其通过网贷平台贷款支付。课程内容为网上公开的基础操作，学员要求退课时被告知“贷款需继续偿还”。经法院调解，14名学员最终分批拿回部分学费并解除借贷记录。

https://news.dayoo.com/guangzhou/202407/24/139995_54691053.htm

遇到此类事件，如和防范呢？

1. 通过 “国家企业信用信息公示系统” 查培训机构是否有 “教育培训” 经营范围，避开仅标注 “技术推广” “咨询服务” 的无资质机构；
2.对 “高薪就业” “边学边赚” “0 元入学” 等宣传保持警惕，此类话术多隐藏贷款陷阱，可要求出具真实就业案例或课程大纲；
3. 重点核对费用、还款责任、退课规则，拒绝 “未明确贷款性质” “无论就业与否均需还款” 的霸王条款，签前可找学校就业办或律师帮忙把关；
4. 任何以 “培训” 为由要求签贷款 / 分期协议的，直接拒绝，警惕 “教育分期” “消费分期” 等包装话术，避免不知情背负债务；
5. 保存宣传截图、合同、沟通记录，若发现被骗，立即向 12315、地方金融监管局投诉，或联系学校协助维权。



05

AI代写刷单诈骗

AI代写刷单诈骗是什么？

以"AI论文代写""作业代做"为诱饵吸引大学生，初期完成小额"代做任务"后及时结算佣金建立信任。随后引导参与"刷单返利"，要求垫付资金购买虚拟商品（如游戏点卡、影视会员），声称完成多单后返还本金和高额佣金，实则以"任务未完成""卡单"为由不断要求追加垫付资金。

手法特点

1.以“AI 自动代写论文 / 文案 / 简历，无需手动操作，接单即赚佣金”为噱头，主打“低门槛、高收益、靠技术躺赚”，吸引学生等想轻松兼职的人群；
2.首单推“低垫付、短周期”任务，完成后立即返现，让受害者放松警惕，误以为“靠谱”；
3.后续以“AI 代写需先付素材版权费”“大额订单佣金更高”为由，要求垫付数百至数千元；或诱导“充值开通AI会员才能接更多单”，充值后要么无单可接，要么垫付后失联；
4.部分会签“虚假协议”，称“不完成指定订单量需赔违约金”，或谎称“AI 代写出错需补缴‘修正费’”，逼迫受害者持续掏钱；
5.注册或接单时要求提交身份证、银行卡号“绑定提现”，实则非法收集个人信息，甚至用信息冒名贷款。

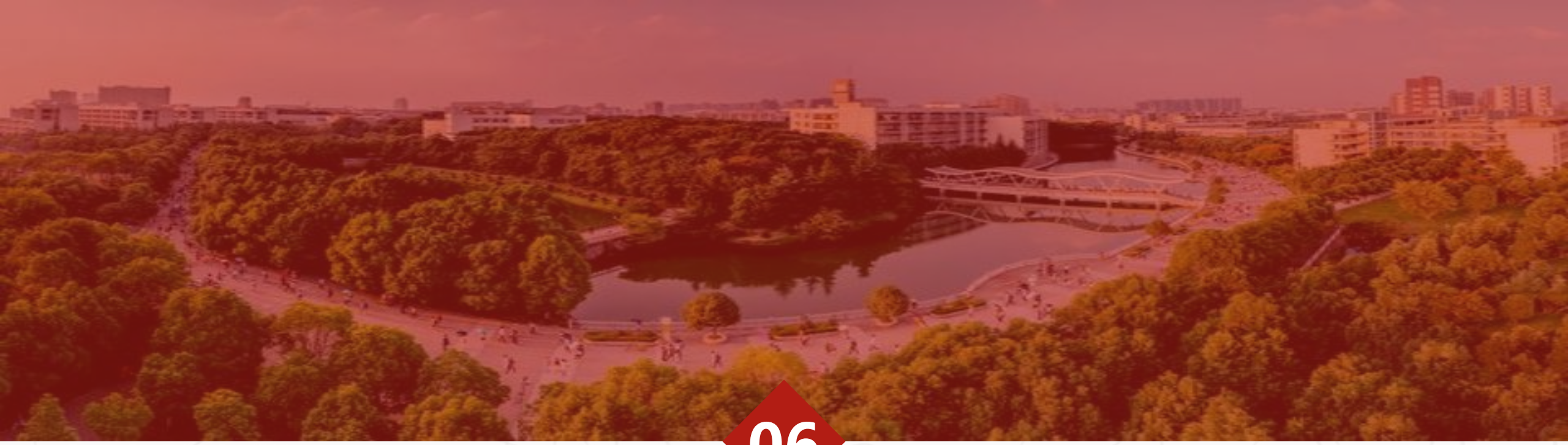
现实案例

南京某大学学生小李加入某 "论文代写交流群" 后，看到群内发布 "刷单返利" 广告，称 "每单返现 15%，日赚 300 元"。小李尝试刷单 3 次（垫付金额分别为 200 元、500 元、1000 元），均收到返利。随后，对方以 "高额任务需连续完成 5 单" 为由，诱导其垫付 8000 元。转账后，平台提示 "操作超时需重新激活"，小李意识到被骗时已损失 1.2 万元，且此前代写的论文也未通过学校查重。

https://m.gmw.cn/2024-12/19/content_1303926808.htm

遇到此类事件，如和防范呢？

1.拒绝论文代写等违规兼职，通过学校勤工助学中心、正规招聘平台寻找合法岗位
2.牢记"刷单就是诈骗"，凡是要求"先垫付资金"的兼职均不可信
3.遭遇疑似诈骗及时保存聊天记录、转账凭证，向学校保卫处或110报案



06

游戏装备金融化诈骗

游戏装备金融化诈骗是什么？

在游戏社群、交易平台发布"游戏装备增值理财"广告，声称"购买稀有装备托管给平台，每月可获得8%-15%收益，随时可赎回"。初期展示虚假收益截图吸引投资，待大量学生投入资金后，关闭平台卷款跑路。

手法特点

1.将普通游戏装备 / 皮肤吹成 “稀缺资产”，用虚假盈利截图、“内部消息” 营造 “能升值、稳赚钱” 假象，诱骗玩家跟风投入；
2.搭建仿官方的假交易平台，或引导 “线下转账 + 线上赠装备” 的场外交易，收了钱却不发装备，甚至卷款跑路；
3.联合非法渠道推 “借钱买装备投资”，用高利息套牢玩家，让其既亏本金又背债务；
4.借游戏交易冷却期、确认期等规则，或冒用他人账号租装备转卖，让玩家想买的买不到、想卖的卖不出，最终血本无归；
5.靠 “托儿” 晒 “暴富单”、群内煽动，利用玩家想快速赚钱的心理，等大量投入后突然抛售砸价，完成收割。

现实案例

一群专业操盘手通过批量注册账号哄抬《CS:GO》虚拟贴纸"黑蛋"的价格，在玩家群散布"绝版升值""内幕消息"，雇佣"托儿"晒出虚假盈利截图。两个月内，该贴纸价格从 5 元暴涨至 3000 元，吸引大量玩家（超六成是大学生）借贷入场。庄家在 9 月 13 日集中抛售，价格三天内暴跌至不足 200 元，受害者总损失超亿元。

https://www.toutiao.com/article/7553055297758118419/?upstream_biz=doubao&source=m_redirect

遇到此类事件，如和防范呢？

1.认清游戏装备的虚拟商品属性，不存在稳定增值的理财功能
2.通过官方认可的交易平台进行装备交易，拒绝第三方托管
3.不相信"低风险高收益"的游戏相关投资，切勿向陌生平台充值。

谢谢观看