防范电信网路诈骗之网络涉黄诈骗

底层逻辑 + 衍生陷阱专题宣讲

校园反诈形势严峻，警钟长鸣

本学期校内诈骗案件整体态势

26起

26.7万元

诈骗案件频发，涉案资金规模触目惊心，已成为威胁校园财产安全的首要隐患。

网络涉黄类诈骗：小数量，大危害

76%

20.3万元

仅5起案件却占据总损失近八成，单笔金额巨大，是当前校园诈骗中破坏力最强的类型。

套路隐蔽瞄准大学生，防范教育刻不容缓

此类诈骗手段经过精心包装，专门针对大学生群体的心理特点设计，隐蔽性极强，极易诱导学生落入圈套。目前校园反诈形势已极为严峻，单纯的提醒已不足以应对风险，亟需开展全员、全覆盖、沉浸式的防范教育工作，提升学生的识骗、防骗能力，筑牢校园财产安全防线。

本次宣讲核心内容

01 核心底层逻辑

揭秘所有诈骗套路的根源，深度剖析骗子如何精准拿捏受害者的心理弱点，看懂骗局背后的底层运作机制，从源头理解风险产生的原因。

02 高发衍生陷阱

聚焦校园场景，拆解5类伪装性极强的新型诈骗套路。涵盖虚假兼职、游戏交易、校园贷、冒充公检法等高频案发类型，看清各类骗局的真实面目。

03 统一破局逻辑

掌握一套可复用的应对体系。包含事前如何有效防范风险、事中如何快速识别异常、事后如何科学止损的核心法则，化被动为主动，建立心理防火墙。

04 总结与倡议

强化全员反诈安全认知，凝聚校园安全共识。倡议大家不仅要自身练就“火眼金睛”，更要成为反诈宣传员，共同筑牢校园安全防线，守护师生财产安全。

守护校园净土，反诈刻不容缓

高校人群社会经验相对不足，是诈骗分子的重点觊觎对象，各类新型骗局也在不断变种升级。本次宣讲不仅是知识普及，更是为了帮助大家建立反诈“防火墙”。面对可疑信息保持高度警惕，面对利益诱惑坚守原则底线，让诈骗套路在校园无缝可钻，共同维护平安、和谐的校园生活环境。

PART 01

网络涉黄诈骗核心底层逻辑

精准拿捏两大人性弱点

猎奇侥幸心理

大学生社交活跃，对网络新奇内容充满强烈的探索欲。总抱着“只是随便看看、聊聊不会有事”的侥幸心态，从而主动降低了安全戒备，为不法分子提供了可乘之机，成为被骗的起点。

警示：好奇心是陷阱的诱饵，侥幸是被骗的开端！

羞耻恐惧心理

一旦陷入骗局，受害者往往因碍于个人脸面、害怕隐私曝光或被亲友知晓，产生强烈的羞耻感和恐惧心理。这种心理使其不敢报警、不敢向学校上报，最终选择私下妥协，成为骗子长期勒索的突破口。

警示：沉默是纵容的帮凶，退让只会让损失扩大！

核心危害：骗子正是利用这两大心理弱点，从“引君入瓮”到“持续勒索”，形成了一套完整的诈骗闭环。打破沉默、拒绝侥幸，是摆脱诈骗陷阱的唯一有效途径。

固定行骗三步闭环

01

低门槛诱惑引流

以“免费福利”“轻松兼职”“同城交友”等轻量化话术降低防备，不直接暴露目的，先通过温和手段将目标引入预设陷阱，消除初步警惕心理。

02

取证锁死拿捏

诱导受害者进行私密互动并悄悄录屏，同时恶意窃取手机通讯录与个人敏感信息。一旦获取关键证据，就掌握了后续威胁、胁迫的核心筹码。

03

持续敲诈收割

利用受害者的羞耻感与恐惧心理进行恐吓施压，先以小额资金试探，一旦得手便不断加码勒索金额。通过反复威胁曝光隐私，对受害者进行无限度的钱财榨取。

核心反诈提醒

不是只有裸聊才属于涉黄诈骗！只要遭遇色情内容引流，后续被以隐私、名誉相要挟进行索财或胁迫，无论形式如何，本质上都是典型的诈骗犯罪行为，请立即报警处理。

PART 02

高校最常见的5类衍生陷阱

陷阱一：“色情+刷单”复合型诈骗

男生最高发，本学期校园发案最多

诱饵：免费福利的虚假承诺

以“免费私密交友”“解锁独家私密视频”为噱头，诱导受害者参与看似简单的刷单、点赞任务。利用年轻人的猎奇心理和贪小便宜的心态，降低警惕性，一步步将其引入预设的骗局之中。

套路：小额返利后的大额收割

初期给予小额返利建立信任，让受害者尝到“甜头”。随后以“任务未完成”“操作失误导致账户冻结”为借口，要求受害者进行大额充值解冻。此时受害者因前期获利心理，往往会选择继续投入以挽回成本。

威胁：隐私泄露的精神逼迫

一旦受害者产生怀疑或犹豫，骗子便会立刻变脸，拿出前期诱导的低俗聊天记录、个人信息作为筹码进行威胁，声称若不继续转账就将内容曝光给家人、学校或在网络上公开，利用羞耻感迫使受害者就范。

本质：色诱为钩，刷单为刀

这是一种复合型的新型网络诈骗，将“色情诱惑”作为吸引用户的钩子，把“刷单返利”作为实际的资金收割工具。两者结合极大地降低了受害者的防备心理，且具有极强的隐蔽性和传播性，是当前校园反诈工作中需要重点防范的类型。

陷阱二：陌生私密APP/网站钓鱼诈骗

“违法+被骗”双重困境

诱人诱饵

利用“私密影视”“专属交友”等猎奇内容发送陌生链接，诱导用户下载小众APP或违规翻墙访问境外网站，利用好奇心降低用户防备心理。

暗藏套路

软件或网站内置恶意木马程序，一旦安装或访问，瞬间窃取通讯录、相册、银行卡及校园个人敏感信息，全程在后台静默运行，难以察觉。

勒索威胁

骗子冒充客服以“检测到违规浏览”为借口，威胁曝光隐私信息并索要高额封口费，更有甚者直接利用窃取的支付信息盗刷用户资金账户。

法律风险

私自翻墙访问境外非法平台的行为本身已违反相关法律法规。受害者不仅面临财产损失，还可能因违规行为承担相应的法律责任，得不偿失。

⚠ 关键警示：猎奇心理的致命代价

这类诈骗手段极其隐蔽，不仅会造成个人隐私泄露和财产被盗刷，更会让你陷入“浏览非法内容+遭遇诈骗”的双重违法困境。请务必守住好奇心，不点击陌生链接、不下载不明APP、不参与翻墙行为，保护好个人信息与法律底线，避免落入精心设计的诈骗陷阱。

陷阱三：“高薪私密陪聊”兼职诈骗

精准瞄准想兼职赚钱的同学，看似轻松的“线上陪聊”实则是步步惊心的诈骗深渊

诱饵：虚假的“轻松高薪”承诺

骗子利用学生渴望灵活兼职的心理，发布“日结几百元、足不出户、不限经验”的线上陪聊招聘信息。用极具诱惑的薪资和轻松的工作描述作为糖衣炮弹，降低受害者的防备心理，将其引入预先设计好的圈套。

套路：诱导私密互动并秘密取证

在取得信任后，逐步诱导受害者进行低俗露骨的聊天互动，进而要求发送私密照片、开启视频通话。在此过程中，诈骗分子全程进行隐蔽录屏和截图，获取受害者的隐私影像资料，以此作为后续实施敲诈勒索的“致命把柄”。

威胁：隐私曝光与连环勒索

掌握证据后立刻翻脸，以“将私密照片视频发给学校、家人和朋友”为要挟进行精神施压。同时编造“保证金”“违约金”“消除记录费”等各种名目，不断向受害者索取钱财，一旦妥协，就会陷入无休止的层层收割。

恶果：人财两空的惨痛结局

不仅没有赚到承诺的兼职费用，反而被诈骗分子掏空积蓄甚至背上债务。更严重的是，隐私泄露的风险成为悬在受害者头顶的达摩克利斯之剑，带来巨大的精神压力、名誉损失和难以修复的心理创伤。

陷阱四：短视频/社交平台私信引流诈骗

伪装成同龄学生、高颜值网友，以“交友”之名设下隐私陷阱

诱饵：情感伪装搭讪

在抖音、QQ、微信等主流社交平台主动发起私信，伪装成校友、同乡或志趣相投的高颜值网友。通过嘘寒问暖、暧昧互动营造“灵魂契合”的交友假象，让受害者放松警惕。

关键手段：利用青少年情感需求，从线上“陌生搭子”快速升级为“亲密好友”，为后续诱导做铺垫。

套路：私密诱导取证

取得初步信任后，以“平台监管严、聊天不方便”为由，诱导受害者转战无监管的小众私密软件。进而以“确认关系、加深了解”为借口，要求视频裸聊或发送私密照片/视频。

核心陷阱：全程隐秘录屏、截图，非法获取受害者隐私素材。此时的“亲密互动”已变成被锁定的“把柄”。

威胁：隐私胁迫勒索

掌握证据后立刻变脸，利用学生对“社会性死亡”的恐惧心理，威胁将私密内容发送给其父母、老师、同学或发布至网络。以此逼迫受害者按要求转账，实施敲诈。

严重后果：受害者往往因羞耻和恐惧不敢报警，陷入反复被勒索的恶性循环，造成巨大的身心和财产双重伤害。

陷阱五：AI换脸、虚假不雅合成诈骗

诱饵获取

无需与你进行视频裸聊，仅通过你社交平台公开的自拍、生活照，就能获取制作虚假影像所需的人脸素材，门槛极低且不易察觉。

技术合成

利用AI深度伪造技术，快速将你的人脸合成到虚假不雅视频、图片中。生成的内容画面逼真，在缺乏专业鉴定的情况下，普通人几乎无法分辨真伪。

精准恐吓

骗子精准报出你的姓名、班级、学校等真实个人信息，谎称已掌握你的“私密影像”，以“将视频全网曝光、告知家人和学校”为威胁，逼迫你就范。

被迫转账

面对逼真的合成影像和个人信息泄露的事实，受害者极易陷入极度恐慌，在心理防线彻底崩溃后，往往来不及冷静核实，只能按照骗子要求进行转账。

新型高发，隐蔽性极强！

这是一种针对学生群体的新型非接触式精准诈骗。犯罪分子无需与受害者实时互动，仅靠网络公开信息即可完成全套作案流程。由于AI合成技术带来的视觉冲击和个人信息的精准命中，极易让受害者产生“把柄被抓”的错觉，在巨大的名誉和心理压力下丧失判断力，最终导致财产损失。保护个人隐私，切勿随意泄露生活照，是防范此类骗局的第一道防线。

PART 03

所有陷阱的统一破局逻辑

事前防范：源头止损“三不”原则

陌生链接不点

坚决拒绝一切来源不明的链接，尤其是涉及私密内容、高额福利、轻松兼职的诱导性链接。此类链接往往是钓鱼网站的入口，点击即可能导致个人信息泄露或财产损失。

陌生好友不加

对社交平台上主动搭讪、嘘寒问暖的陌生账号保持高度警惕，不轻易通过好友申请。这类账号背后多是诈骗团伙，建立联系后会逐步诱导参与投资、赌博或进行低俗互动，最终实施诈骗。

低俗互动不碰

坚决抵制网络裸聊、发送私密照片、参与不明低俗网络互动的行为。这是“杀猪盘”和“裸聊敲诈”的典型套路，一旦参与，个人隐私将被对方掌控，进而面临无休止的勒索与威胁。

核心警示：认清本质，零侥幸心理

网络空间并非法外之地，更没有绝对的“匿名”。所有看似“天上掉馅饼”的福利、“投缘”的陌生人、刺激的低俗互动，本质上都是诈骗分子精心设计的陷阱。任何一次放松警惕的侥幸，都可能成为财产受损、名誉扫地的开端。唯有坚守原则，才能从源头切断被骗的可能。

事后应对：守住底线，正确处置

遇骗底线：绝不转账！

无论对方以隐私曝光、家人安全等何种理由进行恐吓威胁，绝对不要向陌生账户转一分钱。骗子的核心目的永远是骗取钱财，一旦转账，只会陷入被反复勒索的无底深渊，止损的唯一方式就是从一开始就拒绝转账。

第一步：立刻拉黑

立即删除并拉黑对方所有联系方式，停止一切沟通。这能有效切断骗子的持续施压渠道，避免对方进一步的精神控制和信息轰炸。

第二步：保留证据

完整保存所有聊天记录、涉事链接、APP界面及通话录音/录屏。这些电子证据是后续警方立案、学校处理以及法律维权时不可或缺的关键材料。

第三步：上报报警

不要独自承受，第一时间告知辅导员和学校保卫处。同时立即拨打110或前往就近派出所报警，依靠法律和行政力量制止侵害，保护自身合法权益。

关键认知：骗子的“威胁”只是纸老虎

传播淫秽物品、敲诈勒索本身就是严重的违法犯罪行为，骗子比受害者更害怕事情败露。他们所谓的“公开曝光”大多是虚张声势的恐吓，只要我们坚守底线、果断报警，就能让不法分子受到应有的法律制裁。

守住底线，远离陷阱

一旦受骗，被骗的钱99.99%是找不回来的！！！