学习防诈知识公益讲座

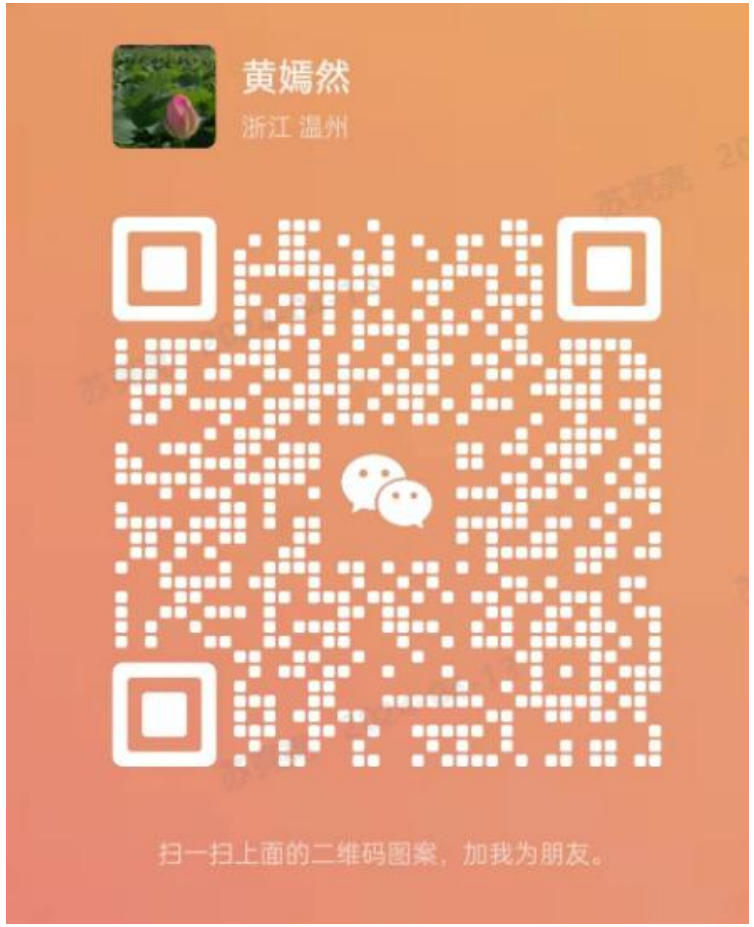
浙江健泽律师事务所 | 黄嫣然律师

乐清市城东街道总部经济园4幢1102室

浙江健泽律师事务所

黄嫣然律师

13306777158



听到别人被电信诈骗，你的反应是？

年龄大？

太单纯？缺少阅历？

贪小便宜？

“人傻钱多”？

常见误区

01 老年人被骗多？年轻人被骗少？

据统计电信网络诈骗的受害者中，年龄在45岁以下受害者的占比高达90%，每年受骗的人群中，18岁以下的受害者占9%左右，00后到70后受害者占绝大多数。

02 没钱就不会被骗？

事实上，在很多被骗案件中，受害人在骗子的指导下通过花呗、借呗、京东白条、金条等各式金融平台贷款大额资金转账给骗子的案例比比皆是。在互联网时代，骗子消耗的不一定是我们现有的资金，还有可能消耗我们的未来和信用。

03 被骗的都是“人傻钱多”吗？

电信网络诈骗有三大特点：一是诈骗手段与互联网技术紧密相连，任何新的技术手段都可能被用于电诈；二是组织公司化行为产业化，诈骗团伙很多采取公司化运作模式，呈现出明显的集团职业化特点。此外，由于分工不断精细，已经演化出相互依存、相互合作的黑灰色产业，诈骗犯罪由团伙运作变成了体系运作；三是利用社会热点和新的应用程序不断翻新诈骗手段。将社会热点融入骗局中，既能吸引更多人关注，也能为诈骗分子提供掩护，使被害人放松警惕。犯罪分子再借题发挥，也更容易得手。这些特点，都使得电信网络诈骗方式手段更加隐蔽，让人防不胜防，如果警惕性不搞，极容易被骗。

诈骗类型

01. 虚　假　征　信

02. 虚假网络投资理财

03. 刷　单　返　利

04. 网　络　贷　款

05. 假　冒　身　份

06. 虚　假　服　务　类

虚假征信

骗子冒充银行、网贷、互联网金融平台（蚂蚁金服、360借条、京东金融、银监会等）工作人员，称被害人之前有网贷、分期记录、会对个人征信产生不良影响，以可以帮助注销账号、消除分期记录等为由，诱骗受害人转账汇款、从而事实诈骗。这个是2023年发案较多的一种情形。

案例：近日，市民杨某某连续接到一个 189***0937 的陌生电话，因为号码陌生，杨某某并未接听，**当该号码第四次响起，杨某某以为是重要事情于是接起了电话**，电话里对方自称是“京东白条”的客服，称杨某某在“京东白条”上的年化利率超过了国家规定的 3.25%，被归纳为高利息网贷，若不及时关闭将会影响征信或者产生额外费用。杨某某称自己并没有操作过，对方以杨某某身份信息被盗用为由，依旧要求注销账号。杨某某心存怀疑，可对方对自己个人信息非常了解，**且收到了国家反诈中心 APP 的身份验证信息**，当对方询问有无收到银行信息时，**杨某某收到了工商银行的短信，而且所有的操作均在京东官方 APP 上进行**，于是杨某某放松了警惕，对方又称杨某某账号关闭失败，需要在 APP 设置里的“第三方共享清单”查看杨某某共享出去的信息。随后会有“后台工作人员”进行对接，杨某某在“后台工作人员”的引导下**下载了自带屏幕共享功能的 APP**，在骗子的各种忽悠下，杨某某将钱转到指定安全账户，损失了 26 万，被对方拉黑后才意识到被骗。

诈骗手法：

①伪装“客服”主动联系被害人

骗子往往冒充金融机构、互联网金融工作人员等身份（如：银监会、蚂蚁金服、360借条、京东金融、某学贷、分期乐等贷款平台“客服”）主动联系被害人，近期发案以冒充京东金融、银监会等工作人员较多，其中冒充京东金融客服类占比较大。

②准确说出受害人个人身份信息，获取信任

为了获取受害人信任，骗子会利用非法渠道获取的个人信息，在电话中准确报出受害人的姓名、身份证号、家庭住址、贷款等信息，进而实施精准诈骗。

注意：现在骗子非法渠道非常多，可以查到你极其详细的个人信息，如果报出你的身份情况并不能代表其系真正的平台工作人员。

③虚实结合 打消顾虑

在征信类诈骗中，骗子往往会诱导受害人登录中国人民银行或者银监会等官方平台进行征信查询，以增加可信度。近期多为利用国家反诈中心 APP 中的身份核实功能，向受害人发起身份核验，此时受害人会收到国家反诈中心发送的验证短信。

注意：身份核实只是国家反诈中心 APP 的一项功能，为市民提供陌生人身份核实便利，只需输入手机号被核实方就会收到短信。

或者在骗子询问是否收到银行短信时，受害人会收到银行发送的短信。原因在于部分手机银行 APP，只需录入手机号点击登录，就可触发银行向用户发送登录验证码。**实际上并非由你来验证对方的身份，而是由对方验证你的身份。**

这些官方发送的信息，会让受害人产生误解，以为通话方确实为官方客服，骗子正是利用市民对这些官方平台信息的不知情，从而增加信任度。

④以“会影响个人征信”为由，让受害人恐慌

当受害人放松警惕后，骗子谎称与国家相关政策不符合，利率过高，需注销账号或资金冲正，否则会影响个人征信产生严重后果。若是受害人未曾注册京东金条或白条，骗子则谎称其身份信息被盗用注册了贷款账号，也需要配合注销。

注意：可以自己上相应平台进行查询，并再次联系该平台客服核实。

⑤要求转账完成“清零和销户”。
骗子称只有清空贷款额度才能完成“清零”和“销户”，于是要求受害人前往各大网贷平台借款，并将所有资金打入指定账户；或诱导受害人离开官方平台登入诈骗网站，诱导受害人向指定账户转账，以此实现诈骗。

注意：只要让你打钱去某个账户的都需要警醒，可能是编造剧本谎骗你。

⑥要求下载其他软件

骗子经过前期铺垫，取得受害人信任后，正式开始实施诈骗。一是通过诱导受害人下载自带屏幕共享功能的 APP，如云视讯、钉钉、腾讯视频等，以此窃取账号密码等个人信息。

注意：在很多骗局里面，骗子都会诱导你开启“屏幕共享”，这个功能开启后，你在手机上的任何操作对方都可以看到，包括你输入验证码、密码、解锁的全过程。

电信网络诈骗手法不断推陈出新，虚实结合，令人防不胜防，预防电信网络诈骗需要加强学习，提升自身识诈防诈能力是关键。

征信类诈骗，骗子实施诈骗常用的理由有注销校园贷、降低贷款利率、消除不良记录、注销借贷账户以及扣除违约金、利息费等，当你接到的电话中提及了这些理由的时候，请务必保持高度警惕。再次强调，陌生来电不要接。

虚假网络投资理财

①以专业“导师”为饵的高回报、高收益投资理财。
骗子通常在股票、虚拟币等论坛发布广告，以专业“导师”荐股、免费上课为由吸引受害人入群，并引导受害人下载0指定 APP 进行投资理财。主要投资项目通常为打新股、炒虚拟币、炒股、投资新三板等。

案例：倪先生接到炒股电话，询问他是否需要学习炒股。在确定能通过炒股赚钱后，倪先生便加入了炒股群。群内有两个“专业老师”开语音直播讲课，助理每天会私法给倪先生一两只潜力股，然后倪先生就跟着对方买股票。几天下来倪先生卖的几只股票赚了 5000 多元，后来群里的“导师”说有一个翻倍股的平台，接着倪先生就通过“导师”提供的二维码下载了“大辉证券”平台，“导师”替他注册了账号，并要求倪先生分 4 次将大量资金转至指定账号代为操作，直至平台无法提现倪先生才意识被骗，损失 74 万元。

②以感情投入为铺垫的投资理财，俗称“杀猪盘”。
骗子伪装为成功人士，通过婚恋网站、网络社交工具寻觅、物色诈骗对象，聊天交友，确定男女朋友、婚恋关系，甚至远程下单赠送昂贵礼品，取得信任。在取得受害人信任后，骗子推荐博彩网站、赌博 APP，谎称系统存在漏洞、有内幕消息、有专业导师团队等，只要投注就能稳赚不赔，甚至先提供自己的账号让受害人帮忙管理，进行体验，一步步引诱受害人投注。

案例：
6 月底，崔某某在抖音相亲时通过红娘认识了一名男子，两人相谈甚欢。该男子自称从事金融工作，现有一个难得的赚钱机会却无暇顾及，希望崔某某能帮忙操作。随后崔某某在该男子的指示下下载了一个“中银国际”APP，帮男子购买期货，一天两次，都能盈利。在男子的诱导下崔某某也注册了账号开始操作。一个月后 APP 无法登陆，崔某某发现被骗，损失 20 余万元。

注意：投资理财类诈骗通常有以下几个关键词：“网友”、“内幕”、“漏洞”“高收益”。切记，凡是打着“一倍投资、多倍收入”类似标语的都是诈骗。不要被所谓的高回报迷了双眼，切勿相信稳赚不赔的“买卖”。投资理财要选择合法正规的平台和机构，网友推荐或百度搜索的投资项目都要谨慎对待，多方验证。

刷单返利

注意：不论如何包装，本质依然是**“完成任务一小额返利一大额收割”**的刷单。

①“兼职刷单”诈骗。

骗子通常在各种网络平台发布兼职广告，以“零投入、高回报、日清日结”为诱饵，诱骗受害人参与其中。随着网络社交平台的发展，刷单诈骗已从最初的“购物刷单”到“点赞、关注、投票、为主播打赏、公益捐款”等，形式灵活，紧跟社会热点。

案例： 小刘接到陌生电话，声称有“福利兼职”渠道，只要她下载指定 APP，并在该 APP 上帮主播“投票”，就能赚一笔不少的零花钱。于是小刘便按照指引每天在 APP上进行签到，并完成给指定主播“投票”“点赞”的任何。在完成任务后，小刘收到了几十元至几百元不等的佣金。正当她以为自己找到了赚零花钱的小诀窍时，“客服”称有部分任务“超时”，导致漏掉了后续一整轮的任务，要求她自行补全大额任务，否则将会“违约”。小刘信以为真，便陆续向对方提供的指定账户转账，直至发现 APP 无体现，“客服”也将她拉黑，小刘这才意识到自己被骗，损失1.9万元。

②虚假色情类刷单诈骗。
骗子通过短视频平台、网站或小卡片，发布虚假色情广告设置诱饵，再由“客服”下发任务指令，引导受害人开通指令 VIP 会员做任务，完成不同额度任务匹配相应的美女，再缴纳各种“套餐费、保证金、会费”等费用。

案例：市民李先生在我市某停车场取车时发现车窗上有张香艳小卡片，心动的他扫描了卡片上的二维码，下载了名叫“Monice”APP，注册账号后，平台上马上有“客服”联系他，自称可提供上门服务，但需办理会员套餐，充值不同价位的会员就可享受相应等级的服务。李先生信以为真，交了会员费后，“客服”发来许多大尺度美女照片，让李先生完成指定任务后选美女。完成多次线上任务后，对方称李先生“操作失误”，要求缴纳解冻金才能继续。李先生在连续缴纳多次解冻金仍被告知“解冻失败”后，他才意识到被骗，损失超百万。

注意：骗子会根据人的欲望进行广撒网制造诱惑，如果你没有抵制住诱惑，就可能变成被待宰的羔羊，一旦需要你支付费用，都要警醒可能存在陷阱，切勿因欲望冲昏了头脑。

网络贷款

注意：请从正规渠道进行借贷，现在经济环境较差，应量入而出，适当消费。

骗子会以“无抵押、无担保、秒到账、不查征信”等幌子，吸引你下载虚假网贷网站。诱惑其尽快下载手机APP后注册信息，签订“贷款合同”，让你以“手续费、刷流水、保证金、解冻金”等名义先缴纳各种费用。利用受害人急需用钱的心理，需要验证还款能力为由，反复要求受害人汇款，待诱骗成功后，便会关闭诈骗APP或网站，并拉黑受害人。

案例：市民陈先生在浏览网页时，看到一款网络贷款APP，声称“无抵押、无担保、超低息，只要注册，贷款立马到账”。正巧陈先生近期手头资金困难，遂下载注册了指定贷款APP，然后客服发送一份合同给陈先生，答应出来签好字发送回去。期间“客服”以“手续费、保证金”等为由，要求陈先生在指定账户缴纳相关费用。多次缴款后仍无法房款，陈先生意识到被骗，损失7万元。

假冒身份

通过非法渠道获取你的手机号和相关信息，通过网络社交软件（QQ、微信、微博等）方式，冒充“亲朋好友”编造如以人在国内代买机票、代交学费、遇交通事故需救治或赔偿、病重需手术费等危急事故，诱骗你转账或代付。或冒充领导、公司老板、上级管理者身份（冒充领导身边的秘书、司机等，同样是以领导的名义），以与其他公司合作伙伴签合同、送礼、遇事急需用钱等事情为由，催促受害人付款。

案例：“我是 XX（某领导），这是我的新号码，之前的已停用，请惠存！方便日后联系，收到回复！”近日 陈先生收到“领导”发来的短信，他不假思索地更新了通讯录信息，随后通过了“领导”发来的微信好友验证。不久，“领导”以家里亲戚公司需要经费周转且自己身份不便为由，要求陈先生汇去一笔钱，自己同时将同等金额打到陈先生账户上，并附上了一张银行转账截图。一想到“领导”有私事相求，而且只是“过一道手”的工作，陈先生不仅快速卸下防备，内心甚至还有点窃喜，马上操作完成了 60万元转账。结果，陈先生的钱被转走了，“领导”的钱却迟迟未到账，他这才意识到自己被骗：转账截图是合成的，再想联系却已被微信拉黑，电话忙音。

诈骗手法：（一）“领导”找上门

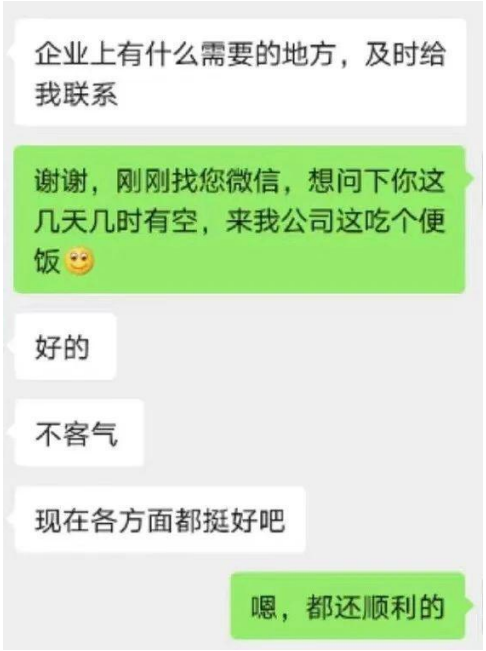
“领导”主动发送短信或添加微信好友（盗用领导微信头像昵称），冒充相关“领导”与你主动联系。

（二）寒暄关怀，获取信任

诈骗分子会用平常领导关心下属的口吻对你进行暖心关怀，降低你的防备之心。

（三）帮忙转账，伪造截图

当你感觉与（领导）更亲近时，诈骗分子便会趁势而起，以资金周转、不方便出面等为由，伪造转账凭证(24 小时到账)，要求受害人尽快帮忙转账至指定账户。过程中骗子会模仿领导口吻，使用“尽快”“马上”“你办事我放心”等命令、催促性词语，营造紧张气氛，并利用时间差降低当事人核实真伪的可能性。



诈骗对象：
第一类：冒充党政干部，如市长、市委书记等，诈骗企业主；
第二类：冒充乡镇领导，如镇长、书记，诈骗村居干部；
第三类：冒充单位领导，诈骗本单位员工

注意：凡是自称“领导”、“亲友”通过短信、微信、QQ 等方式添加好友的，一定要再三核实对方身份信息。在对方提出借款或帮忙汇款时，一定要提高警惕，切勿轻易转账。
苹果手机用户收到 iMessage 信息时一定要小心谨慎，仔细核实短信内容的真实性，提及金钱，涉及转账汇款的一定要与对方电话或见面核实，电话核实的，一定要从自己通讯录信息获得号码，切勿以回拨方式通电话。

②虚假色情类刷单诈骗。
骗子通过短视频平台、网站或小卡片，发布虚假色情广告设置诱饵，再由“客服”下发任务指令，引导受害人开通指令 VIP 会员做任务，完成不同额度任务匹配相应的美女，再缴纳各种“套餐费、保证金、会费”等费用。

案例：市民李先生在我市某停车场取车时发现车窗上有张香艳小卡片，心动的他扫描了卡片上的二维码，下载了名叫“Monice”APP，注册账号后，平台上马上有“客服”联系他，自称可提供上门服务，但需办理会员套餐，充值不同价位的会员就可享受相应等级的服务。李先生信以为真，交了会员费后，“客服”发来许多大尺度美女照片，让李先生完成指定任务后选美女。完成多次线上任务后，对方称李先生“操作失误”，要求缴纳解冻金才能继续。李先生在连续缴纳多次解冻金仍被告知“解冻失败”后，他才意识到被骗，损失超百万。

注意：骗子会根据人的欲望进行广撒网制造诱惑，如果你没有抵制住诱惑，就可能变成被待宰的羔羊，一旦需要你支付费用，都要警醒可能存在陷阱，切勿因欲望冲昏了头脑。

虚假服务类

注意：购买网上物品时收到类似信息，请联系官方客服核对，并通过官方平台退款退货退款。

①冒充电商物流客服：骗子冒充购物网站客服工作人员给你打电话，说出通过非法渠道获取你的购物信息和个人信息，谎称你购买的产品质量有问题，需要给你退款理赔。诱导你在虚假的退款理赔网页填入自己的银行卡号、手机号、验证码登信息，从而将你银行卡内的欠款转走，或者是利用你对支付宝、微信等支付工具中借款功能不熟悉，诱导你从中借款，然后转给骗子。

案例：市民王先生接到陌生电话，自称是“某海淘旗舰店”的售后客服，称其在旗舰店购买的联名款耳机，订单编号为358470516，因耳机产品批次存在设计缺陷，可能会在使用中产生佩戴不舒适感，现主动为其办理售后保障服务。王先生立即查看旗舰店自己下单编号，与“客服”说的一样，气愤斥责“客服”为何发货前不检查产品质量，“客服”耐心解释称他可享受退款不退货服务，同时额外获赠一张店铺优惠券的权益。王先生一听退款不退货，还有优惠券？念叨说不会是骗人的吧。“客服”又称自己有王先生购买的全部记录，骗子怎么会知道的这么详细呢？王先生心想言之有理，便询问是否直接在平台申请退款，“客服”称可直接在线转接王先生常用的银行“客服”，直接在线办理退款服务。王先生信以为真，按“客服”指引在邮箱内点击指定链接，在网页中输入了银行卡号、个人信息、退款金额等。期间又被银行“客服”卡号输错为由，银行卡已被冻结，要求王先生在卡内存入大量资金，资金需在账户中存放24小时即可解封，解冻后再次按链接填写信息并提交便可获取退款。就这样，王先生往卡里存钱，输入验证码后钱不翼而飞才意识到被骗，损失12万元。

②航班改签、取消：

案例：城南街道赵阿姨在网上购买机票后就接到陌生电话，自称是“航空公司”客服，如实报出赵阿姨航班信息，称可帮她改签到当天的航班，并赔偿她“300 元改签费”。赵阿姨根据“客服”指引下载“ZOOM”软件，开启了“屏幕共享”功能，在所谓的“理赔链接”中填写个人信息及银行卡号，期间还输入了动态验证码。挂机后承诺的理赔金并未到账，银行卡账户钱款却不翼而飞，损失 2.8 万元。

诈骗分子会利用伪基站发送诈骗短信，以“可以提供代办机票业务”为由，冒充客服身份，诱骗受害人直接向指定账户转账汇款。除此之外，骗子还可能通过非法渠道，获取市民的票务信息，以“票务退改签、飞机延误”等为由，诱导受害人下载指定 APP，通过“屏幕共享”获取受害人银行卡密码及动态验证码，或要求受害人向指定账户转账汇款，从而实施诈骗。

注意：在收到类似“航班取消、航班变动、机票退签改签”等内容的短信时，应通过航空公司客服电话、机场客服电话、官方网站等多方正规渠道进行核实确认，不要盲目轻信来路不明的信息。

③ETC退费：

案例：芙蓉镇李先生收到“ETC”续签否则停用的提醒短信，李先生信以为真，点击短信内的链接进入到“ETC 在线认证中心”网页，李先生根据提示在网页内输入身份证号、银行卡号及密码、手机号等个人信息。提交后，李先生收到了来自银行的本人操作确认验证码提示，但李先生并未细想，只想赶紧验证完让自己的 ETC 恢复正常，之后，银行卡内的钱被转走。

骗子冒充 ETC 中心、高速管理中心等机构的名义发送短信，以 ETC 无法继续使用为幌子，诱导受害人点击短信中的网站链接。无论点击哪里都要填写银行卡号、身份证号、短信验证码等个人信息。当完成所谓的认证时，银行卡帐户也早已在骗子的掌控之中。

注意：收到“ETC 认证失效”、“ETC 卡被冻结”或“ETC 已停用”等短信时，先别急着操作，可通过官方平台咨询核实，切记不要轻易点击短信里的陌生链接。

④代办签证：

案例：潘先生在某书上刷到一则可以代办签证的视频信息，于是便添加了微信，支付了 3850 元代办费。二天后，对方称已经为潘先生办理好签证，并要求潘先生前往市区指定地点领取文件，待潘先生赶到后却发现市区并没有这个门牌地址，微信也被对方拉黑，潘先生这才意识被骗，损失 3850 元。

骗子在社交平台上发布“签证办理”“代办签证”等服务信息吸引受害人，并声称有内部渠道可快速办理签证，不少受害人信以为真，直接将“代办费”转至对方指定账户，因此被骗。

注意：如需代办签证，需选择正规的、具有合法资质及良好信誉的代理机构，切勿轻信所谓的快捷办理途径，更不要向陌生人转账汇款。

⑤退学费类：

案例：柳市镇孟某收到一封快递，近期并未采买的她，出于好奇打开了这封快递，发现里面是一张关于《教育部 7.24 双减政策对**教育机构学费退还通知》，提示扫二维码添加客服专员办理退款事宜。由于前期孟某确实在网上购买过课程，因此她深信不疑。添加客服后，被要求下载一个名为“12345 国家清退中心”的 APP。注册登录后，“客服”发来退款流程，称将通过证券增值的方式将其 3280 元报名费退还。孟某根据指示在 APP 上购买证券，前两笔均能成功返利提现，便放松了警惕。当大额购买后无法提现时，对方以其操作错误导致账户冻结为由，告知孟某要继续汇款才能解冻，孟某才意识到被骗，损失 20 万元。

诈骗手法：骗子在非法获取培训机构用户信息后，通过电话或短信联系受害人谎称办理退还学费，诱导受害人添加好友或加入 QQ 群。骗子还会**伪装成退费专员，贴出伪造的课程缴费记录**骗取受害人信任。
在骗取受害人信任后，骗子谎称退款必须要在指定 App 内完成，引导点击指定网址链接下载指定 App，从而获取银行卡、验证码等重要信息。
骗子称按照指引投入资金便能获得本金和返利，在收益的驱动下，受害人会不断加大投入资金。此时，骗子不再返还，以操作完一次性返还、操作错误、账户冻结、交解冻金等理由不断诱导受害人转账，从而达到利益最大化目的。

注意：正规培训机构退费一般会按照付款渠道原路返还或直接转入你的银行卡内，无需你做任何操作！对方一旦让你下载操作其它软件以完成退款，一律不要理会。不要随意提供身份证号、银行卡账号、验证码等重要信息，切勿随意扫描对方发来的“二维码”，更不要轻易点开来历不明的“网页链接”，谨防中木马病毒或误入钓鱼网站。

⑥交通违法处理：
案例：市民张先生收到一条交通违法短信，点击链接后发现，网页上写着“交通违法查询平台”，内容看起来很正规，于是填写了个人信息、银行信息和手机验证码，完成后系统显示要等待 2 到 3 分钟才能看结果，他等不及就退出了网页。没想到过了一会，张先生就收到了银行扣款信息，共被骗8500 元。

不法分子通过不正当的手段获取到受害者及车辆相关信息，通过改号软件给车主发送“交通违法”短信，并在短信中附上虚假网站的网址链接。车主收到此类违法信息，一旦点击链接进入虚假网站，骗子就会进一步诱导车主填写身份证号、银行卡号等个人信息，从而实现盗刷。
还有一种套路，骗子在短信中网址链接中植入木马病毒，盗取机主的个人信息。

注意：交通违法可通过 12123APP 等官方平台进行查询，不要轻信任何不明链接。

如何防范电信诈骗?

1、**警惕屏幕共享。**在很多骗局里面，骗子都会诱导你开启“屏幕共享”，这个功能开启后，你在手机上的任何操作对方都可以看到，包括你输入验证码、密码、解锁的全过程。

2、**非必须请主动关闭境外来电服务。**据统计，通过电话联系方式进行诈骗约占40%左右，其中境外来电占了较大比例，如无境外关系，建议主动关闭境外来电服务功能，降低被骚扰风险。

关闭办法：移动用户：编辑短信1901，发送到10086，机主二次确认即可关闭。联通用户：编辑短信GBGJLD，发送到10010，机主二次确认回复Y，即可关闭。电信用户：编辑短信1901，发送到10001，机主二次确认回复1901Y，即可关闭。

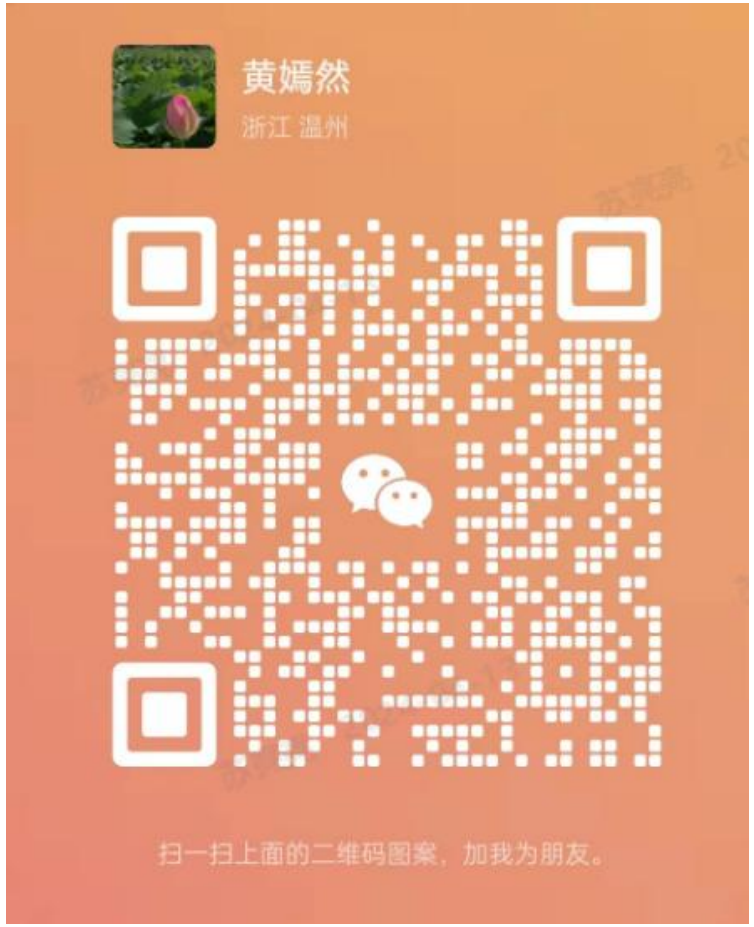
或使用运营商提供的防护服务：移动用户：关注“机伶”微信公众号，我的机伶-智能防骚扰-拦截设置，按需启用防骚扰拦截。电信用户：关注“天翼防骚扰”微信公众号，业务设置中点击“智能拦截设置”，按需启动“高频呼叫”、“诈骗电话”和“国际长途电话”拦截等功能。联通用户：关注“中国联通微厅”，在办理中选择“智慧沃服务”选中“终结你的通信烦恼”点击免费订购，立即订购。

3、**国家反诈APP。**该APP不仅具有宣传反诈骗知识的作用，还可以只能识别涉诈电话、短信、安装，并预警提示一键举报诈骗线索。
下载国家反诈中心APP后，要启用来电预警功能才能实现无感拦截或预警。
4、**警惕iMessage消息**，近期iMessage信息出现冒充领导、熟人诈骗，这个诈骗形式是针对苹果用户实施，苹果手机注意识别。4、可以关闭imessage功能避免被骚扰。
步骤路径（可以让大家自己看）：“设置栏”-“信息”-关闭“imessage”，关闭iMessage以后可以拒收所有的iMessage信息。不想关闭iMessage功能的用户，可以通过过滤未知发件人来减少收到垃圾短信。这样设置后，信息会分成两类。通过iMessage发送的短信都将被划分为“不在通讯录一列”，并且不会有短信提示音。步骤路径：“设置栏”-“信息”-“过滤未知发件人（打开状态）”。大部分的垃圾短信都是通过邮箱地址发送的，所以取消邮件的发送地址可以屏蔽大量的垃圾短信。步骤路径：“设置栏”-“信息”-“发送与接收”-“删掉邮箱联系方式”。
5、**正确对待96110来访。**这个是反电信诈骗专用号码，专用用于对群众的预警劝阻、防骗咨询、涉诈举报等工作，如果收到96110的电话，一定要及时接听，耐心听取劝阻员的讲解，如实回答询问。对于因预警上门见面的民警，一定要积极配合，切勿抗拒或编造谎言欺骗。如果平时对自己遇到的事情心存疑惑，也可以拨打96110进行咨询。

浙江健泽律师事务所

黄嫣然律师

13306777158



YOUR LOGO

感谢大家的观看！

浙江健泽律师事务所 | 黄嫣然律师

乐清市城东街道总部经济园4幢1102室