

附件 1

反诈宣传视频

(扫描下方二维码或通过后方链接下载)



链接：<https://pan.baidu.com/s/1euFy-JLz3OCCAREWBKgt-BQ?pwd=0803>

提取码：0803

附件 2

电信诈骗典型案例及防范知识

一、云手机里无链接登录,“投资理财软件让你一步掉陷阱!”

云手机是一种基于云计算技术的虚拟化手机服务,用户通过终端设备可在云端服务器上构建一部虚拟手机系统,如电猫云、红手指、双子星等,这种虚拟手机系统运用于专业人士的游戏挂机、远程办公、应用测试等功能。

(一)案例简述

贵阳某地周先生在“伊对”社交平台上,结交了“程女士”,“程女士”在聊天中透露自己是“证券公司高管”。两人在素未谋面的情况下,感情升温,成为互相信任的“恋人”。

在恋人“程女士”的请求下,周先生用个人银行卡帮其接收“6万元的别人欠款”,接着又将这笔资金转到对方提供的陌生人陈先生账户上,并称钱打到这个账户上是为了投资理财。

完成此次操作后,“程女士”将自己投资收益截图发给周先生,并以“专家指导”“高额收益”等理由诱导周先生参与投资。在“程女士”指引下,周先生进入“**云手机”小程序,使用对方提供的手机号+验证码登录进入“**交易所”进行账号注册和银行卡绑定,并开始转账进行“投资理财”。当周先生的投资金额高达60余万元时,某天平台突然显示“打开失败”,同时恋人也消失,周先

生意识到自己被电信网络诈骗,遂报警。

在案发的同一时间里,与周先生一案关联的陈先生也遭遇了同样的诈骗:如前所述,周先生为了帮助其网恋“爱人”接收“他人欠款”,在不加思索的情况下用自己的银行卡接收了所谓别人的“6万元欠款”,并转入对方提供的陌生银行卡上(即另一名受害人陈先生账户上),而陈先生的银行卡入账(6万元)这笔资金时,也同样是在“伊对”交友里,受网恋“爱人”的深度洗脑,也使用了自己的银行卡帮助“恋人”接收“别人的欠款”,接着又将收到的“欠款”转入“恋人”提供的下一个指定陌生银行卡上(即下一个受害人)。

以上一案关联多名受害人,这是诈骗分子利用“杀猪盘”的深度感情洗脑,诱骗受害人虚假投资理财时,为了躲避金融机构的异常账户风险监测,以“恋爱”伪装,让受害人听信谎言,提供自己的银行卡帮助接收不明资金入账(即涉诈资金),又转进下一个受害人的银行卡里,使自己不仅是受害人,更成为一名帮助犯罪工具人!

(二)作案手段解析

诈骗分子先在XX云手机(比如电猫云、红手指、双子星)等平台上注册账号并购买云手机设备,在所购买的云手机设备上构建一部虚拟手机,通过手机号+验证码实现无链接登录后,可进入已搭建在互联网上的虚假投资理财软件。此时诈骗分子只需要通过在伊对、探探、陌陌、珍爱网、抖音、快手、微博、租售房屋等各

类平台寻找目标受害人,当受害人放松戒备,持续与诈骗分子进行深度交往时,诈骗分子将引诱其接收陌生资金入账→转入陌生账户投资充值→显示高额回报→进入圈套→使用自己的真金白银开始投资→平台消失、恋人消失,最终被骗。

(三)防范要点

1.网络交友时擦亮眼睛,如果遇到了特别殷勤主动的网络陌生人,短时间内着急确定恋爱关系的,且聊天话题涉及转账、收账和投资理财的,需提高警惕。

2.遇到“稳赚不赔、高额收益”的投资理财项目时,切勿相信,尤其当对方是自己婚恋对象的,更要保持冷静,做到果断拒绝,避免落入“甜蜜陷阱”。

3.不管和对方是多么亲密的关系,当其以各种理由,借用你的银行卡进行资金入账时,一定要多加核实,确认入账资金的合规合法性,避免因接收涉诈资金而成为电诈犯罪“工具人”,给自己造成麻烦。

4.投资理财要通过正规金融机构或国家已备案的合规证券公司平台进行购买,请勿随意下载进入国家未备案的投资理财软件进行理财投资。凡通过云端手机进入理财软件进行投资的,一定是诈骗!

如遇可疑情况拨打96110举报、咨询!

若不慎被骗拨打110或前往附近派出所报警!

二、机票“退改签”要注意

(一)案例简述

每逢春节前后、寒暑假、五一小长假等重要时间节点,是我省旅游高峰旺季,电信网络诈骗方式多呈现诈骗分子冒充航空公司客服人员,以陌生电话致电给广大人民群众,称航班延误、航班故障、天气影响等为由,可以进行机票退改签理赔服务,诱导点击陌生链接进入互联网里的虚假“中国民航”客服网站(或诱导下载虚假 XX 服务 APP、远程控制软件等互联网会议软件开启屏幕共享),通过语言诱骗挑起群众紧张情绪,在不经致电官方客服进行核实的情况下,盲目做出机票“退改签”的决定,最终向陌生账户进行转账(或在屏幕共享下打开银行账户进行退款检测或流水检测等而导致银行信息泄露,银行卡资金被远程盗刷)。

(二)防范要点

1. 正规平台,避免泄露。出行购票请在正规平台、官方途径购买机票,尽可能避免信息泄露;

2. 官方渠道,核实真伪。当被告知航班延误或者取消,应通过航空公司官方客服电话、官方网站等多个正规渠道核实航班信息是真实性;

3. 两卡信息,小心保管。银行卡账号、密码、验证码务必小心保管,不要透露给任何人;不要随意下载软件、不要和陌生人创建并接通视频共享会议或电话会议。

4. 牢记防范电信网络诈骗“三大法宝”。陌生电话不轻信、未知链接不点击、银行信息不透露

如遇可疑情况拨打96110举报、咨询！

若不慎被骗拨打110或前往附近派出所报警！

三、线上的甜言蜜语 线下的意外“惊喜”

浪漫的情人节、传统的七夕节、旅游的五一节等等重要节日，当你沉浸在快乐中时请留个心眼，莫让诈骗分子钻了空子。

诈骗分子通常潜藏在各大社交平台，例如陌陌、探探、伊对，甚至“珍爱”婚恋网站，寻找合适的时机以交友、婚恋等理由与你联系，获取信任成为好友或恋人；又或者潜藏在58同城、安居客等，抓住你急于出租、出售房屋的需求和你取得联系，聊天交往中成为暧昧的朋友，总之以上这些都会转向投资理财，带你一起发财致富！当自己开始点击和下载对方提供的陌生链接和理财软件，并将钱财转给对方指定的陌生账户，资金不断投入到诈骗分子为你量身定制、五花八门的虚假投资理财平台时，“提现不成功”“系统故障”“输入超时”“需缴纳本金的？%才能全额提款”等这样的诈骗话术，会让你从甜言蜜语的情绪价值中一下子跌入噩梦般的深渊，惊出一身冷汗！以上这样的骗局，你或者身边的人遇到过吗？

（一）案例简述

贵阳的王女士为了寻求真爱，下载了“珍爱”APP。在该平台上，她结识了幽默风趣又绅士有度、从事证券分析师的沈先生，两人很快以交往为目的开始深入了解。随着感情升温，沈先生向王女士展示了自己惊人的理财投资回报。在沈先生的诱导下，她开

始在对方指定的投资理财软件中从小金额到大投入,前后往沈先生提供的20余个账户转账,共计90余万元。最后在“输入超时”“系统故障”等导致“提现不成功”情况出现时发现自己被电信网络诈骗,同时温柔贴心的沈先生和投资理财平台也消失得无影无踪。

(二)防范要点

1. 网络交友需谨慎,不要相信“有缘千里来相会”,理性交友,理性看待感情。特别是对那些没见过的人,尤其在涉及金钱往来时,一定要提高警惕,并与身边亲朋好友多沟通、多询问,防止落入“圈套”。

2. 对于引导在网上投资、理财之类,先给尝甜头再引导继续投入的,必是骗子无疑。谨记“天上不会掉馅饼”没有“一本万利”低成本、高回报”的事情,正常投资尚有风险,“赚大钱”更不会无缘无故降临,守好自己“钱袋子”。

3. 谨慎对待陌生链接和软件。不随意点击陌生人提供的链接,不下载来源不明的软件,更不随意跟随网络陌生人进行投资理财。

如遇可疑情况拨打96110举报、咨询!

若不慎被骗拨打110或前往附近派出所报警!

四、警惕! 二维码里藏陷阱,刷单返利是诱惑

当你收到网购快递包裹时,会发现包裹里时常会有一些中奖卡、刮刮卡、购物卡和蟹卡等,亦或者你并没有下单,也会收到莫

名其妙的快递,这些包裹里同样有以上这些卡片。这些小卡片上会附有客服二维码或者群聊二维码,以领取福利为由诱导你扫描二维码与客服取得联系或进入群聊完成领取福利操作。

(一)诈骗流程

收到陌生快递→扫码进群→领取价格不等的小福利(获取信任)→点击进入群主发布的新链接,开始做小任务领取佣金→进入刷单获取小佣金,尝到赚钱红利→任务升级,对方开始推荐新的链接和刷单 APP→由小到大向陌生账户充值转账,平台显示高额获利,但无法提现(无法提现的原因根据每位受害人的实际情况,诈骗话术各不相同)

(二)作案特征

这类诈骗因返利周期短、引流进群成功率高,并且利用众多官方商户的合法性、合规性伪造公司保障合同,骗取受害人信任进行刷单返利任务,已逐渐演变成当下诈骗手法最为繁多、变化最为迅速的诈骗类型。

(三)防范要点

1. 刷单返利是违法,不要轻信任何声称“刷单能赚钱”的信息,天上不会掉馅饼。
2. 不随意扫描陌生的二维码,不进陌生的群聊,不点击来路不明的链接。
3. 不轻易向陌生人转账汇款,保护好自己的银行账户和支付密码。

五、便捷支付时代,慎用手机NFC功能,谨防成为境外诈骗分子远程“提款机”

NFC是一种近距离的数据交换,主要用于移动支付业务。在我们的生活中,公交卡、门禁卡、支持闪付的信用卡和POS机,都是NFC技术的产物,极大地提升了生活和工作效率。但诈骗分子却利用NFC功能的便捷性进行诱骗转账。

(一)作案手段

诈骗分子通过陌生电话联系受害人,自称XXX客服,以航班故障、会员扣费取消、银行流水检测等事由引起受害人关注。接着诈骗分子以帮助受害人办理退款、退费等为由,要求受害人通过手机进入互联网XX会议室(比如钉钉、瞩目会议室,甚至有些虚假会议室,如云视听等),在会议室内开启屏幕共享,随后又要求受害人打开手机NFC功能,诱导受害人下载可以通过手机NFC远程支付的软件(即NFO“隔空读卡”软件)。如果此时你信以为真,拿着银行卡贴近手机或打开银行账户APP办理退款、退费时,卡里的资金则被诈骗分子通过与受害人进行通联的手机,利用NFC功能远程“隔空读卡”进行盗刷。

(二)防范要点

1. 牢记防范电信网路诈骗“三大法宝”

(1)接到自称客服等陌生人的电话,须通过官方渠道核实身份;不点击或扫描未知的链接或二维码;不下载来路不明的陌生软件。

(2)拒绝与陌生人进行屏幕共享,正规机构或平台不会通过屏幕共享的方式核实信息或解决问题。

(3)不向陌生人透露个人信息,不将自己的银行卡和手机交给陌生人操作,保护好银行卡账号、密码、验证码等重要信息,避免造成重大财产损失。

2. 谨防 NFC 功能被盗刷的防范措施

(1)关闭不常用的 NFC 功能。在不需要使用 NFC 时,关闭手机的 NFC 功能,避免被不法分子利用。

(2)谨慎使用公共 NFC 设备。避免在不明来源的 NFC 设备上刷卡或进行支付,防止信息被窃取。

(3)避免绑定过多 NFC 卡片。减少携带 NFC 卡片数量,及时检查手机钱包,根据实际情况,适当解绑不常用的银行卡,尤其是存储大额资金的银行卡,以此降低信息泄露风险,减少资金损失。

3. 加强支付安全的防范措施

(1)使用安全的支付方式。优先选择有密码或指纹验证的支付方式,增加安全性。同时定期查看银行卡交易记录,发现异常及时联系银行工作人员。

(2)谨慎开通“免密支付”,如开通了“免密支付”功能,不要将收款码、付款码随意展示给他人,同时启用手机的锁屏密码和支付应用的二次验证功能,以增强安全保护。

如遇可疑情况拨打 96110 举报、咨询!

若不慎被骗拨打 110 或前往附近派出所报警!

附件3

应了解的电信网络诈骗相关知识

互联网便捷时代,不仅可以线下交友,更可以在网上冲浪,网上社交平台寻找到自己心仪的“恋人”,灵魂的“挚友”,更可以在“恋人”“挚友”“理财大师”“客服”等等的指导下,进入投资理财、刷单返利、办理退费、修复征信、取消抖音自动扣费、关闭百万保障自动扣费等等五花八门的骗局中,似乎自己通过陌生人或导师的指引,可以在网上找到解开各种人生“困局”的“金钥匙”!此时此刻你对网络上那个陌生的“TA”充满着无比的信任,在“TA”的耐心引导下,你开始义无反顾的踏入一个又一个为你精心定制的骗局中!

为此,了解一些电信网络诈骗的常用套路,有百利而无一害!

诈骗分子找到你的方式:除了常规的陌生电话寻找你外,其他寻找你的引流方式有:抖音、快手、陌陌、探探、伊对、珍爱网、安居客、58同城、招聘、二手交易、涉黄涉赌等互联网平台发送虚假信息或吸引受害人注意,等待主动靠近后,进行私聊,完成引流。

引诱进入涉诈网站登录通道:

1.通过手机浏览器搜索栏(百度、UC浏览器、夸克、谷歌等)、官方小程序对话框输入对方提供的陌生链接,进入搭建在互联网上的虚假诈骗网站。

2.通过短信、软件等方式发送携带病毒的陌生链接,当受害人点击该链接,便自动进入诈骗群聊或网站,又或者直接下载诈骗软件,被引流进入。

3.利用云手机(电猫云、红手指、双子星等)的游戏挂机、远程办公、应用测试与开发功能,引导无链接登录,进入搭建在互联网上的虚假网站、诈骗软件等。

虚假 APP,屏幕共享、控制软件进行远程盗取:

利用虚假 APP(例如银联会议 APP)冒充客服,称帮助关闭直播会员、百万保障业务自动扣费、影响征信,诱导下载涉诈 APP,通过屏幕共享,窃取银行卡密码、验证码,或直接远程操控转账,从而达到诈骗目的。

被骗后的各类转账方式:

1.线上支付。使用手机银行 APP 进行卡转卡

2.ATM 转存资金至第三方陌生账户。以汇集资金为目的,诱骗受害人使用 ATM 机多次取现,再通过 ATM 机向陌生账户转账。

3.委托朋友将现金于线下转交给陌生人,或线上帮忙转账。

4.柜面取现,本人线下交付或线上邮寄给陌生人。

5.购买大额黄金等贵重金属,线下交付或线上邮寄给陌生人。

6.购买等价购物券、奢侈品券、大额油卡等线下交付,或线上邮寄给陌生人。

7.提供银行卡给他人接收不明资金,又帮助转给陌生人等。

为什么电诈案件报警后破案时间长、难度大?

你以为是电信网络诈骗——受害人立马报案,把受骗过程交代清楚→警察立马锁定犯罪嫌疑人→冻结资金,开上警车去抓人→人赃并获,案件破获。

实际的电信网络诈骗——少部分受害人被骗后立即报案,能够完整描述受骗过程,并将完整的证据资料提供给警方;而大部分受害人慌慌张张、语无伦次,不能清晰、完整地描述整个被骗过程,也无法将证据资料(比如聊天记录、下载的涉诈 APP、登录的虚假链接、对方的个人信息等)完整的提供给警方。

锁定犯罪嫌疑人——通过警方的侦破,微信是诈骗分子用买来的信息注册的、IP地址是用软件改过的、电话号码是用 GOIP 处理过的,就连跟受害人聊天的视频甚至都是 AI 合成的,别说锁定嫌疑人,就连要确定嫌疑人是男是女都不容易,整个侦破扑朔迷离,如同互联网里“捞针”。

冻结资金——诈骗分子引诱受害人把钱转出时,你以为警察可以立即把接收资金的那张银行卡进行立即冻结,进行退赃。实际上银行卡内的钱不到半个小时就已经通过刷单、投资理财等方式转入下级卡、境外账户、取现、购买虚拟币等方式给转移走了,运气好点的还能被银行自动止付住,但绝大多数资金会在立马之间被诈骗团伙馋食殆尽。

锁定犯罪嫌疑人,立即抓人——嫌疑人在缅甸、菲律宾、老

挝、迪拜,公安机关指定管辖裁定、司法协助、跨国抓捕都没有那么容易。

所以说电信诈骗案件报警后破案时间长、难度大!运气好的会通过抓捕卡商和帮信人员等中间人,让他们退钱来帮助你挽回损失。但想想,为了千把来块钱就把自己的银行四件套给卖掉的人又能有多少钱赔给你?对于这些嫌疑人,很多是宁愿坐牢,都不愿意赔钱。所以说,在目前情况下,电信网络诈骗是全世界一个无解的难题。只有积极提升自身的防范意识,尽量做到不被骗,才能有效避免财产损失。