



反欺诈宣传

守护老幼,远离欺诈

上海索迪斯万通服务有限公司 二〇二一年七月

目录

一、电信网络新型违法犯罪	3
1、2021年八大高发网络诈骗	3
2、转账汇款注意事项	4
二、违法犯罪行为及其危害	5
非法贩卖"两卡"	5
三、个人金融信息保护	7
1、金融个人信息包括什么内容	7
2、个人金融信息安全注意事项	7
四、防范欺诈案例	8
1、老人防范欺诈案例	8
2、青少年防范欺诈案例	8

一、电信网络新型违法犯罪

1、2021年八大高发网络诈骗

1) 网络贷款

诈骗手法: "低门槛"广告 + 网贷 APP

警方提醒: 当有人向你推销贷款时,一定要小心。诈骗分子先让你在虚拟贷款网站或 APP 上填报个人信息,再以信息报错、贷款额度被锁等理由,诱骗你缴纳保证金或者解冻金。任何声称"无抵押、低利率"的网贷平台都有极大风险。

2) 网络刷单

诈骗手法: 兼职刷单 + 网络博彩

警方提醒:所谓刷单,就是通过网上购物方式为网店刷信誉或者充值刷流水,网店向刷单者返还贷款并支付佣金的违法行为。诈骗分子往往以兼职刷单名义,先以小额返利为诱饵,诱骗你投入大量资金后再把你拉黑。

千万不要轻信兼职刷单广告,所有刷单都是诈骗,不要缴纳任何保证金、押金。

3)"杀猪盘"

诈骗手法: 网上"美女"+投资"赢利"

警方提醒: 当有陌生人加你为好友时,一定要小心。诈骗分子往往先以甜言蜜语或者献殷勤等方式博取好感和信任,再向你推荐所谓"稳赚不赔、低成本高回报"的网络投资平台。当你越投越多时,就会把你拉黑。

从网恋"一见钟情"开始,到参与网络赌博或投资诈骗结束,知道受害者倾家荡产甚至背负巨债,就是"杀猪盘"诈骗。

4) 冒充"公检法"

诈骗手法: "公安调查"+"冻结账户"

警方提醒:凡是自称"公检法"要求你转帐汇款自证清白的,都是诈骗。

5)"荐股"

诈骗手法: "理财导师"+ 虚假平台

警方提醒:一进股票群,套路深似海。"老师""学员"都是托儿,炒股软件都是假,只有你是"真韭菜"。

6)冒充客服退款

诈骗手法: "客服主动退款"+申请平台贷款

警方提醒:接到自称"卖家"或"客服"的电话说需要退款或重新支付时,当事人一定要登陆官方偶购物网站查询相关信息,不要点击对方提供的网址链接,更不能在这些网址上填写任何个人信息。

7) 虚假购物

诈骗手法: 网络广告 + "购物送抽奖"

警方提醒: 在网络购物中发现商品价格远低于市场价格时,一定要提高警惕,谨慎购买,不要将钱款直接转给对方。

8)注销"校园贷"

诈骗手法: "注销不良记录" + 指导贷款

警方提醒:凡是声称你有"校园贷"记录需要注销、否则会影响征信的,都是诈骗,切勿转账汇款。

2、转账汇款注意事项

【看】

一看:对方身份

进行转账汇款前,首先应确认对方真实身份。可以通过拨打电话、视频或面对面等形式与对方进行身份信息确认,切勿轻易转账汇款。

二看: 收款账户

转账汇款时,建议与对方确认收款账户信息是否正确。

三看: 转账金额

进行密码支付前,与对方核实转账金额是否正确。

【问】

问: 是否到账

转账汇款后,应及时向收款方确认是否到账。若发生未到账等异常情况, 应及时联系银行进行核实。

【注】

当转账汇款时,建议通过添加转账汇款用途、收款方等备注信息的方式进行留痕。若为借款性质的转账,建议在转账汇款备注中添加"借款"、"借钱给 xxx"等字样。

特别提示:如果不慎发生被骗的情况,建议及时报警,积极寻求公安机关帮助,尽可能挽回资金损失。请广大消费者擦亮眼睛,谨防被骗。

二、违法犯罪行为及其危害

非法贩卖"两卡"

1、什么是"两卡"

两卡是指:银行卡和电话卡。

电话卡包括移动, 联通, 电信手机卡和虚拟运营商的电话卡, 物联网卡。

银行卡包括,个人银行卡(储蓄卡),企业对公账户,和第三方支付账号(如支付宝,微信账号和收款码)。

2、非法贩卖"两卡"的危害

"实名不实人"的卡,不但被犯罪分子用来搞电信诈骗,还会用来搞网络贩毒、网络赌博等犯罪。据新闻报道,每年网络赌博流出资金就达万亿级别,而这些钱大部分都是通过买卖的银行卡、对公账户或者第三方支付账户走账,难以追查和打击。

非法买卖的银行卡、身份证等可能被用于洗钱、逃税、诈骗、送礼和开店刷信用等行为,扰乱了正常的社会秩序。同时,卡内存储了很多个人信息,如果贪图小便宜出售自己名下的卡,有可能被收卡人用来从事非法活动,给自己带来巨大的法律风险,甚至承担刑事责任。一旦所售卡出现信用问题,最终都会追溯到核心账户,导致个人信用受损,甚至承担连带责任。

3、安全提示

妥善保管

妥善保管身份证、银行卡、网银 U 盾、手机等,不借给他人使用;不随意 丢弃刷卡交易凭条;不向任何人发送带有银行卡信息和支付信息的图片等。

有效防范

不点击短信、网络聊天工具或网站中的可疑链接,不登陆非法网站;慎扫 不明来历二维码;不轻信陌生电话;使用资金较少的银行卡用于网络支付等。

及时报警

如个人相关信息泄露或银行卡被盗刷,应尽快挂失银行卡,并及时向公安机关报案,提供有关证据配合公安机关开展案件调查。

案例:涂某通、万某玲帮助信息网络犯罪活动案

1、基本案情

涂某通,1998年8月出生,系某大学在校学生。

万某玲,1998年9月出生,作案时系某职业技术学校在校学生,案发时系某医院员工。

2018年起,涂某通明知他人利用信息网络实施犯罪,为牟取非法利益,长期收购银行卡提供给他人使用。2018年,涂某通与万某玲通过兼职认识后,涂某通先后收购了万某玲的3套银行卡(含银行卡、U盾/K宝、身份证照片、手机卡),并让万某玲帮助其收购银行卡。

2019年3月至2020年1月,万某玲为牟利,在明知银行卡被用于信息网络犯罪的情况下,以亲属开淘宝店需要用卡等理由,从4名同学处收购8套新注册的银行卡提供给涂某通,涂某通将银行卡出售给他人,被用于实施电信网络诈骗等违法犯罪活动。经查,共有21名电信网络诈骗被害人向万某玲出售的上述银行卡内转入人民币207万余元。

2、 法院判决

鉴于万某玲犯罪时系在校大学生,因找兼职误入歧途而收购、贩卖银行卡,主动认罪认罚,江油市人民检察院对其提出从轻处罚的量刑建议。涂某通在审查起诉阶段不认罪,也不供述银行卡销售去向、获利数额等情况。2020年12月31日,江油市人民法院作出一审判决,以帮助信息网络犯罪活动罪判处涂某通有期徒刑一年四个月,并处罚金人民币一万元;判处万某玲有期徒刑十个月,并处罚金人民币五千元。涂某通、万某玲未上诉,判决已生效。

从近年来的办案情况看,手机卡、银行卡(以下简称"两卡")已经成为电信网络诈骗犯罪分子实施诈骗、转移赃款的重要工具。工作中发现,部分在校学生由于社会阅历不足、法治观念淡薄,已成为非法买卖"两卡"的重要群体之一。在利益诱惑面前,有的学生迷失方向,一步步陷入违法犯罪泥潭,从办卡、卖卡发展到组织收卡、贩卡,成为潜伏在校园中的"卡商",他们不仅出售自己的银行卡,还在学校里招揽同学出售银行卡。这些银行卡经过层层周转,落入到诈骗人员等犯罪分子手中,用于流转非法资金,危害不容小觑。对于从"工具人"转变为"卡商"的在校学生,将综合其犯罪事实、情节和认罪态度,依法追究刑事责任。

三、个人金融信息保护

1、金融个人信息包括什么内容

个人身份信息: 个人姓名、性别、国籍、民族、身份证件种类及有效期限、职业、联系方式、婚姻状况、家庭状况、住所、工作单位地址及照片。

个人财产信息: 个人收入状况、拥有的不动产状况、拥有的车辆状况、纳税额、公积金缴存金额等。

个人账户信息: 账号、账户开立时间、开户行、账户余额、账户交易情况等。

个人信用信息:信用卡还款情况、贷款偿还情况以及个人在经济活动中形成的,能够反映其信息状况的其他信息。

个人金融交易信息:包括银行业金融机构在支付结算、理财、保险箱等中间业务过程中获取、保存、留存的个人信息和客户在通过银行业金融机构与保险公司、证券公司、基金公司、期货公司等第三方机构发生业务关系时产生的个人信息等。

衍生信息和其他反映特定个人某些情况的信息:包括个人消费习惯、投资 意愿等对原始信息进行处理、分析所形成的反映特定个人某些情况的信息。

2、个人金融信息安全注意事项

切勿把自己的身份证件、银行卡等转借他人使用。

在日常生活中切勿向他人泄露个人金融信息、财产状况等基本信息,也不 要随意在网络上留下个人金融信息。

尽量亲自办理金融业务,切勿委托不熟悉的人或中介代办,谨防个人信息 被盗。

提供个人身份证件复印件办理各类业务时,应在复印件上注明使用用途。

不要随意丢弃刷卡签购单、取款凭条、信用卡对账单等,对写错、作废的 金融业务单据,应撕碎或使用碎纸机及时销毁,不可随意丢弃。

不要轻信来历不明的电话号码、手机短信和邮件。警惕向您询问个人金融信息的电话及电子邮件,在任何情况下,法院、警方都不会要求您告知银行账户、卡号、密码或向来历不明的账户转账,如遇到此类情况,应予以拒绝,必要时立即报警。

四、防范欺诈案例

随着互联网和手机成为人们生活的重要组成部分,越来越多的数据表明老年人和青少年正在成为犯罪分子实施欺诈的重要对象。为进一步防范生活中的诈骗,提高公众反欺诈意识和能力,切实保护广大人民群众的财产安全乃至人身安全,应当加强自身防范意识,学习生活中关于诈骗的防范知识。

1、老人防范欺诈案例

2019年10月,腾讯110平台发布的《中老年人反欺诈白皮书》指出,2019年上半年,腾讯110平台共受理中老年人受骗举报量超过两万人次。其中,97%受骗的中老年人曾遭资金损失,涉案金额从百元到数万元不等。白皮书还显示,从诈骗受害人群来看,60后群体更容易落入虚假投资等骗局,人均被骗金额最高。这些数据说明,尽管中老年人生活经验丰富,但面对纷繁复杂的网络环境和真伪难辨的诈骗手法时,他们极易落入诈骗团伙的陷阱中。再加上网络时代,各种诈骗手段不断翻新,而老年群体,对于网络时代的种种骗局缺乏认识,更容易受骗上当。年轻人可以经常给老人提供关于诈骗的真实发生的案例,经常与他们分享新型骗局,从而降低老年人轻信诈骗信息的程度。

•冒充熟人诈骗

【案例详情】方爷爷在公园遛弯时接到电话,对方自称是战友"老乔",说自己得了病在住院治疗,急需资金周转,希望他能帮老战友一把。方爷爷确曾有个久未联系的战友叫老乔,便信以为真,就汇款2000元到对方账户。过了一段时间又接到"老乔"电话,声称病情加重,还需要8000元。方爷爷汇过去后,再联系"老乔",接过电话已被拉黑,此时方爷爷发现被骗了。

【防范提醒】如遇到自称朋友、熟人通过电话联系或社交软件添加好友,并要求转账汇款时一定要提高警惕,务必通过视频电话或当面核实确认后进行操作!

•冒充"公检法"诈骗

【案例详情】退休后的佟奶奶接到一通自称是"公安局民警"的来电,对方称 佟奶奶名下的银行卡涉嫌洗黑钱,要求其配合协助调查。佟奶奶信以为真,便 按照对方的要求将自身名下所有存款,都转账至其声称的"安全账户"里。完 成转账后,佟奶奶发现打不通"公安局民警"的电话,这才意识到自己被骗 了。

【防范提醒】公检法机关会当面向涉案人出示证件或法律文书,不会要求远程转账汇款至所谓的"安全账户"。

• 虚拟投资理财诈骗

【案例详情】爱炒股的姜爷爷在盯盘时接到电话,对方自称从事证券交易,可提供更低交易手续费,好奇的姜爷爷便按照对方的指示,下载指定 APP。之后一个多月里,姜爷爷在这款 APP 中不断"盈利",并陆续追加投入。等到姜爷爷想要提现,平台显示账户异常无法提现,联系 APP 客服后处理无效,随后甚至无法打开 APP,姜爷爷这才报警。

【防范提醒】投资理财,请选择银行、证券公司等正规途径!切勿盲目相信所谓的"炒股专家"和"投资导师"。

2、青少年防范欺诈案例

近年来,除老年人之外,大学生群体也成为电信、网络诈骗受害者的重灾区。各类贷款、兼职广告充斥校园,紧抓在校生的需求,打着零成本兼职赚钱的噱头,实则背后风险重重,个人信息泄露、容易受到诱惑、社会经验不足和防骗教育的缺失等问题是学生频频被不法分子盯上的关键原因。

• 网络游戏虚拟交易诈骗

【案例详情】正在打游戏的小狄在"世界"频道看到有人发布消息"出售传说 橙装,价格美丽,非诚勿扰,有意者 M"。小狄心动了,立即联系对方。对方说,需预先支付 500 元。小狄在对方指定的网络平台付了钱。然而他登录游戏后,却发现装备迟迟未到。心急的小狄急忙联系"卖家",却发现自己被"拉黑",这才意识到被骗了。

【防范提醒】当在网络游戏充值、买卖账号或游戏装备时,一定要小心! 诈骗分子会以低价充值、高价回收等为由,引诱你在对方提供的虚拟连接内进行交易。买卖游戏币、游戏点卡,请通过正规网站操作,一切私下交易均存在被骗风险。

•注销"校园贷"诈骗

【案例详情】课间活动室,小赵接到电话,对方称小赵在上学期间注册过某校园贷账号,如不注销,就要缴纳高额滞纳金,影响个人征信。对方以指导销户为由,要求小赵添加工作人员联系方式,并让小赵遵循其指示操作,诱导其到某平台借款,然后转入到所谓的"安全账户",还让小赵随时截屏保留证据。一个月后,小赵接到平台催款电话时,才发现上当受骗。

【防范提醒】不要轻信陌生人声称你之前有"校园贷"行为。如遇以"校园贷"或"注销校园贷"为借口要求转账,都是诈骗!

• "杀猪盘"诈骗

【案例详情】小陈通过异性交友 APP 认识"小骗",经过多日聊天,两人确立 网恋关系,"小骗"趁机声称自己在做投资,想带小陈一起赚钱。经过几轮诱惑后,小陈通过对方发送的连接登陆理财投资平台,在开始盈利几次之后发现 有利可图,小陈便不断往平台充值,且金额越来越大,最终充值近 23 万元。小陈准备回收资金,却无法提现时,才发现自己被骗!

【防范提醒】素未谋面的网友、网恋对象推荐你网上投资理财、炒数字货币 (虚拟币)、网购彩票、博彩赚钱,谨防上当受骗!

更多链接

1、国务院打击治理电信网络新型违法犯罪工作部际联席会议决定

https://www.mps.gov.cn/n2255079/n4876594/n5104076/n5104077/c7386967/content.html

2、《中国人民银行关于加强支付结算管理 防范电信网络新型违法犯罪有关事项的通知》(银发[2016]261号)

http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3154362/index.html

3、网络违法犯罪举报网站

http://www.cyberpolice.cn/wfjb/html/index.shtml

4、防范打击电信网络新型违法犯罪 | ②国家反诈中心《防范电信网络诈骗宣传 手册》

http://www.pcac.org.cn/eportal/ui?pageld=598354&articleKey=612153&columnld=595124

5、"国家反诈中心"APP

https://news.cctv.com/2021/06/17/ARTI1INjDKe0IDDxI8jhGSSZ210617.shtml ?spm=zm1033-

001. 0. 0. 1. fxXw5C&file=ARTI1INjDKe0IDDxI8jhGSSZ210617. shtml

上海索迪斯万通服务有限公司

福泉北路388号东方国信商务广场A座9楼 200335 - 上海 - 中国

Tel: 400 920 6001 - Fax: 6209 6002

www.sodexo.cn

