全民国家安全教育日:金融网络安全典型案例

今年4月15日是第5个全民国家安全教育日。金融安全是国家安全的重要组成部分,是经济平稳健康发展的重要基础。为切实提高全民金融安全法治意识,中国人民银行嘉兴市中心支行整理了六个金融网络安全典型案例,提醒广大群众谨防金融网络诈骗。

网络贷款陷阱

2019年5月16日,赵某在某QQ群看到一则无抵押贷款广告,遂在网上向放贷人申请贷款1000元。放贷人让赵某打了1200元的欠条,扣除利息200元后,在网上付给他1000元。由于各种原因赵某无法按期还款,原放贷人便向赵某推荐一名新的放贷人,而第二个放贷人也需要扣掉相应利息。就这样,赵某陷入了和之前一模一样的借贷套路。等到他还不起时,第三个、第四个和第五个放贷人会陆续登场。而此时,利滚利、本金滚本金,再加上违约金、滞纳金等等,赵某需要偿还的贷款越滚越多,已经累计到100多万元。此时,放贷人威胁赵某还钱,并恐吓他已到法院起诉,将要拍卖他的房屋和车辆。

安全提醒

不法分子从一开始就以非法占有借款人的财产、房产为目的,利用借款人社会经验不足的弱点,处心积虑地通过"双倍借条"或"平账"等手段,将原来的小额借款,变成难以偿还的债务,进而逼迫当事人抵押房产、签订长期租房合同,或者勾结黑中介直接"网签"卖房,一环套一环骗取受害人的房产。

防范此类情况发生,可采取以下措施:一是到正规的金融机构或平台贷款;二是不要被"无需抵押,快速房贷"等广告诱惑;应详细了解后再做决定;三是如不幸受骗,应第一时间向公安机关报案,同时保留好相关的借款合同,微信、短信的转账及聊天记录等证据,并及时提交公安机关。

伪基站陷阱

2019年7月28日,李女士正在玩手机,突然收到一条XX银行发来的银行卡消费积分兑换短信,没有多想就点开了链接,并按提示输入了自己的银行卡卡号和身份证号码,又输入了XX银行短信发来的验证码,没想到短短数十秒后,就收到多条共计转款99998元的短信,李女士这才意识到自己被骗了。

安全提醒

不法分子利用伪基站伪装成银行或运营商发送诈骗短信,引诱手机用户点击短信中的链接,从而将木马病毒植入用户手机,盗取用户账户、密码等敏感信息,实现骗取钱财的目的。

防范此类情况发生,可采取以下措施:一是发现手机信号突然中断,应提高警惕,因为靠近伪基站时,手机一般会脱网,几秒后才恢复正常;二是当收到"中奖""转账"等短信时,一定要提高警惕,不要轻易点击短信中的链接,更不要转账汇款;三是不要轻信各种积分兑换,正常的积分兑换应通过官方渠道;四是手机要安装安全类软件,它们可以有效拦截垃圾短信。

代办信用卡诈骗

2019年1月19日,嘉兴市桐乡一男子接到一个自称信用卡办理公司客服的电话,称事主在平台上办理信用卡申请通过了,要求提供身份信息。接到对方发来一个网站,让事主填写个人信息,受害人在填写完银行账户和验证码后发现卡内6000元全部被取走,才意识到被骗。

安全提醒

诈骗分子瞄准的是那些急需用钱又对信用卡缺乏了解的人,精心杜撰剧本,受害人很容易上当。诈骗分子有的通过网页、微信群、QQ群等发布可以提升信用卡额度、信用卡套现、办理大额信用卡或办理大额低息贷款等信息,有的假冒银行发送短信,拨打电话邀请持卡人提额,诱导持卡人按照其要求操作,骗取公民个人信息,实施诈骗。

目前,有不少银行把信用卡业务外包,所以一些公司提供办理信用卡并不奇怪,关键在于如何分辨真伪。申请办理任何可透支的金融类卡时,都会受到申请单位的严格审查,并核定金融类卡的消费额度。绝对不会是所谓的"工作人员"承诺您多少就是多少。整个申请过程都是免费的,即使涉及交费,也会让你到单位或银行办理,并给予相关收据、收条。切莫被所谓的"高额""低息"或"无息"诱惑。

投资理财诈骗

2019年3月8日,嘉兴市秀洲一男子接到一个电话,向其推荐股票,之后使用微信添加事主好友并将其拉进一个微信群,在群内事主了解到一个股票软件,诈骗分子谎称该软件可以融资,里面的股票都是经过分析的,稳赚不亏,之后事主按着对方说的操作先后在软件内投资了17万,当事主想要取出时发现钱无法取现,才意识到被骗。

安全提醒

诈骗分子在社交平台上鼓吹自己能准确预测股票、期货的涨跌,塑造所谓的"专家""大师""白富美"形象,有的诱骗受害人参与投资,收取高额"会员费""服务费";有的推销各类"荐股软件""荐股平台",以"免费试用"和"高盈利"为诱饵,将用户导流到软件平台,参与贵金属、艺术品、邮币卡等现货交易或境外期货交易。其实这些交易系统都是伪造的。骗子可以在后台实时操纵行情,伪造交易记录,骗取受害人大量资金。

投资有风险,投资理财一定要到正规平台,在微信群、QQ群等交流理财知识并不靠谱,一旦涉及汇款转账就要警惕了。此外,不要被社交平台上所谓高回报的贵金属、原油、期货等投资,"推荐股票"之类的说辞所迷惑。

冒充网购客服退款诈骗

2019年1月11日,嘉兴市海宁一买家接到一个自称网购平台客服的电话,称事主买的床单存在质量问题要退款给事主。之后发给事主一个二维码,事主扫描以后填写了自己的银行卡号,之后事主连续收到了扣款短信,第一次被扣了4998元,第二次被扣了5000元,第三次被扣了2000元,事主才意识到自己被骗了。

安全提醒

受害人接到电话后,诈骗分子自称是淘宝、京东或其他购物平台的客服或卖家,可以详细报出受害人的个人订单信息,并称订单无效要"退款"、或者"退货给补偿"等,引诱受害人点击钓鱼链接、或引导受害人扫描二维码等,将钱卷入自己的账户。

防止此类诈骗可采取以下措施进行防范,一是当遇到自称卖家的电话说需要退款或者重新支付时,要亲自登陆官方购买网站查询,或者拨打正规客服,不要轻易点击所谓店家提供的网址,更不能在这些网页上填写相关信息。二是银行卡号、验证码信息一定要保管妥当,不要轻易外泄。各类购物平台的客服人员不会需要用户个人银行卡信息及转账要求。

机票改签诈骗

2019年1月6日,嘉兴市海盐一女子接到诈骗分子发来的一条短信称事主的航班因故障被取消,要给事主退款300元,于是事主就打该电话,案犯自称是航空公司人员,问了事主的银行卡,并说要退300元,接着会有验证码发过来,事主信以为真,就将收到的验证码都告知给对方,结果银行卡被多次消费共54983元和44988元,共计被骗99971元。

安全提醒

在此类诈骗中,诈骗分子先购买乘客的订票信息,然后发短信到乘客的手机上,说"您定的机票,航班要取消了,你是要改签,还是要退票,改签或者退票收取20元的手续费。"留一个手机号码,为了看起来像客服电话,在号码前加了"0086"。如果乘客回电话,诈骗分子就冒充航空公司客服,以退款的名义骗取对方的银行卡信息进行转账。

对此类诈骗,一是收到航班延误、取消短信时,应拨打航空公司官方客服电话向机场工作人员核实。二是切记退票、退款是不需要输入密码和验证码的,更不需要先行汇款。

(华闻)