

宣传诚信理念



守牢钱袋子,谨防新骗局

——节假日期间反诈温馨提示

文 / 记者 殷志军 陆翔 图 / 资料

近日按照中国支付清算协会要求,工商银行上海市分行结合以往电信诈骗典型案例,提醒广大市民节假日期间不要輕易泄露个人信息、不接来历不明电话、不回复来历不明短信,做好自身防护工作。



典型案例 1

房先生收到一条短信息,称“凡是接种过疫苗人员,可点击链接录入个人信息登记备案,领取疫苗接种库补偿款,补偿额度是2000元”。房先生查询发现自己疫苗接种正是这种疫苗,于是点击短信链接并进入了看似正规的网站,并根据网站指引填写了银行卡号、密码、身份证号等信息。输入完成后,房先生开开心心地坐等补偿款到账,谁知等来的却是银行扣款信息,此时才知受骗上当。

防范提醒:新冠疫苗接种信息均由权威部门发布,辖区卫生健康行政部门或疾控机构是按要求公布可进行新冠疫苗接种的信息,请市民关注官方信息发布平台,不要轻信非官方渠道,遇到问题或疑惑可拨打官方电话予以核实。



典型案例 2

乔女士近日发烧嗓子疼,抗原检测后发现自己感染了新冠病毒。为缓解症状,乔女士便上网搜寻,看到有“售卖治疗新冠特效药,服用后15分钟内消除头痛及浑身酸痛症状”。于是病急乱投医的乔女士主动联系对方,并按照对方提示点入链接支付货款,然后等待快递。可一周过去,乔女士症状基本消退,药物还没送到,再联系对方却发现已被拉黑,此时乔女士才发现被骗。

防范提醒:不法分子假冒政府部门、药物研究(医疗)机构等,通过拨打电话、发送短信、网络发布等形式进行推销,谎称有“特效药”,诱导市民点击钓鱼链接购买,从而盗取账户信息或款项。因此,不要轻信非专业医疗机构或陌生人推销,要在正规平台或专业资质药店及医院购买药品。



典型案例 3

杨女士前些时间在某网络平台认识了一位网友,谈到当前疫情防控形势时,对方表示正在投资研制“新冠特效药”项目,预期收益很高,询问杨女士是否想参加。杨女士对此深信不疑,于是在对方的提示下给指定银行账户转账一万元,不久后对方告知药品已初步研制成功并获利2000元,并将收益转给杨女士。尝到甜头后,杨女士在对方诱导下又转账五万元。但此后,杨女士发现再也无法联系上对方,这才意识到被骗。

防范提醒:网络交友需谨慎,一定要警惕,不轻易转账。同时要谨慎看待“低成本高回报”“稳赚不赔”“内部渠道”等投资话术,切勿进入虚假投资理财网站、APP,避免落入诈骗陷阱。



典型案例 4

小邵是网游爱好者,春节前夕游戏平台推出“特别活动”和“神兵利器”,小邵很喜欢。看到在游戏聊天栏内有出售“神兵利器”装备的信息后,他便主动联系对方。对方称以低价将装备出售,但需在指定平台交易,于是小邵进入该网址充值后发现对方已下线,而且充值资金也无法取出,此时小邵才意识到被骗。

防范提醒:孩子放假在家,家长给孩子玩手机时,须谨防孩子被诱导支付购买虚假游戏账号装备,一旦发现被骗,请及时报警。



典型案例 5

晁先生收到“您的3000积分即将过期,请登录激活并领取现金礼包”。晁先生并没过多怀疑,点击链接后进入页面填写姓名、身份证号、信用卡号、交易密码等信息,并按要求下载“安全控件”。不久后,晁先生收到多笔消费短信,此时才发现自己遭遇了电信诈骗。

防范提醒:当收到积分兑换短信,其中但凡有网址链接的,一定不要随意点击,有可能是木马病毒或是假冒钓鱼网站。遇到要输入姓名、银行卡及密码等信息时,一定要多留心。



典型案例 6

周某、赵某、温某利用QQ群或微信群,寻找学校家长群,先冒充家长私信班主任,谎称微信换号或者手机丢失,骗取班主任信任,加入班级家长群。随后,趁班主任上课之际,将账号改成班主任的头像和昵称,要求家长缴纳新冠疫苗费用350元。学生家长没有过多怀疑,很快在群中响应,通过其提供的收款码付款。等班主任发现并进行提示时,已有多名家长被骗。

防范提醒:群聊管理员应严格进行群管理,不能让身份不明的人混入群聊。遇到群聊里汇款转账要求时,家长也要通过电话或者当面核实等方式与校方取得联系,若遭遇网络诈骗,保留好转账的账户明细和聊天记录,及时报警。

