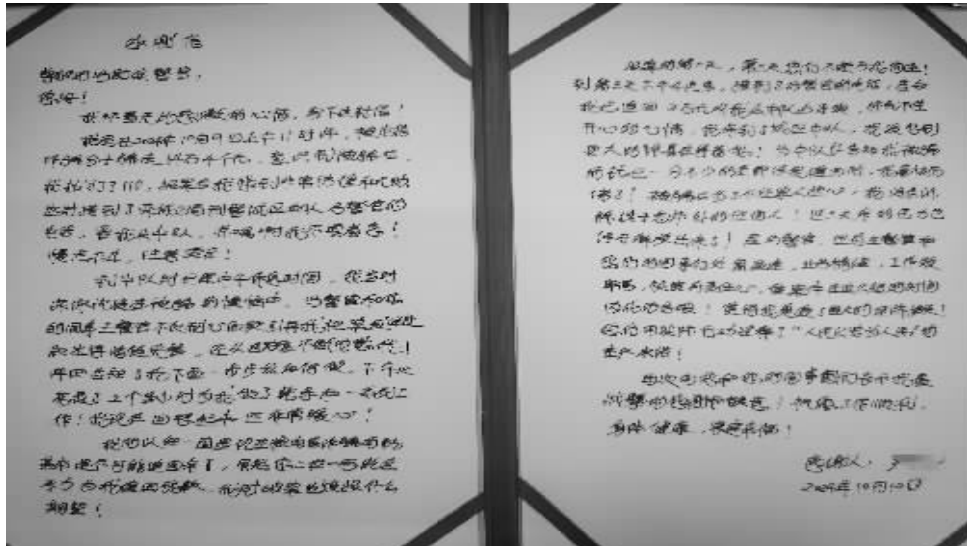


与“女儿”网聊遇电诈 女子被骗 144000 元

办案民警 72 小时将钱款全部追回 民警教你如何反诈防骗



如果你家有在外上学的子女发来信息要钱,请一定多方核实,这是不是孩子本人。近日,石家庄市民尹女士收到在外住校的“女儿”通过聊天软件发来的信息,在未核实对方真实身份的情况下,尹女士便给“女儿”打款 144000 元。而当她意识到自己遭遇电信诈骗后,尹女士没想到,石家庄警方仅用 72 小时便把她被骗的钱款全部追回。



■尹女士手写的感谢信。



■尹女士给警方送锦旗。

□文/图 本报记者 南开宇 通讯员 冀贺

聊天软件弹出好友申请 信息与女儿一模一样

据尹女士介绍,事情发生在今年 10 月 9 日上午。尹女士的女儿在栾城区某重点中学上高中,学习成绩优异。她与女儿的沟通方式一般都是通过电话或者聊天软件。

10 月 9 日 10 时前后,尹女士的手机“叮铃”响了一声,某聊天软件弹出一条好友申请。这条弹出的申请人头像、昵称、个性签名等内容跟她的宝贝女儿一模一样,尹女士虽然疑惑但还是加了对方好友。在随后的聊天中,尹女士被对方语气及所说话术迷惑,以为正在跟她聊天的就是自己的女儿。聊天中,“女儿”告诉她学校请了国内某重点双一流大学教授来授课,但这个培训班名额不多且培训费价格不菲,需要 72000 元,“女儿”希望她能支持自己,报班学习。

听说女儿学习心切,想要报班,尹女士二话不说就按照对方提供的银行卡号转过去 72000 元。但结果却出乎尹女士意料,对方听说尹女士打款后,隔着屏幕跟“妈妈”各种撒娇、唠家常,可半个小时后却突然说钱没收到,让尹女士再次打款。这话引起了尹女士的怀疑,但在对方密集的话术下,尹女士根本没有深思的时间,在对方一步步地引诱下,尹女士再次向同一个账号打款 72000 元。

结束聊天后,尹女士越想越觉得事情有蹊跷:“明明我都转款成功了,怎么说第一次的 72000 元没收到呢?”尹女士便拨通了女儿班主任的电话进行求证。果然,学校根本就没有什么名牌大校教授开设的培训班,也不允许有人假借此名义开设培训机构收钱。意识到自己遭遇电信诈骗后,尹女士焦急地拨打了 110 报警电话。

反诈中心与骗子抢时间 民警开启追赃程序

听尹女士简单叙述了被骗经过后,接警员立刻将专线转接至市局反诈中心,同时将警情指派到栾城分局刑警一中队处警。反诈中心根据尹女士提供的银行卡号迅速进行数据追踪,发现该银行卡号于 11 时 06 分、11 时 07 分在浙江省武义县某银行 ATM 自动取款机上分别取现 10000 元,同时,另有 50000 元正在通过该银行柜台窗口走流程。反诈中心立刻开始与对方抢时间,并于 11 时 15 分临时止付成功。同时,结合该银行卡线索,刑警

一中队民警积极联系涉诈账号所在地浙江省武义县公安局,请求协助查找涉案卡主,并通过极限操作,成功将卡内剩余的 124000 元冻结。

安抚好尹女士后,办案民警随即开启追赃程序,经连续 72 小时不间断工作,10 月 12 日又将此前被取现的 2 万元赃款成功追回。至此,尹女士被骗的 144000 元一分不差地被石家庄市公安局栾城分局刑警一中队民警返还给了尹女士。

尹女士感慨:整个过程感觉像在做梦一样

10 月 13 日上午,尹女士来到石家庄市公安局栾城分局刑警大队一中队办公场所,她将赶制的一面绣有“尽职尽责 完璧归赵”的锦旗和一封手写的感谢信送到刑警一中队办案民警李进存、冯豹庭手中。尹女士坦言:“现在感觉,自己就像在做梦一样,真的太谢谢你们了”。

尹女士在感谢信中写道:“在我的认知里,现在被电信诈骗的钱基本是不可能追回来了,虽然您一直说会尽力为我追回钱款,可我对破案也没报什么期望……报案第二天、第三天你们不断与我沟通,第三天下午 4 点多,您让我去中队办手续,当被告知被骗的钱已一分不少全部追回时,我喜极而泣……你们用实际行动诠释了‘人民警察为人民的庄严承诺’。”

10 月 20 日,接受采访的尹女士表示,她 12 日得知钱被追回的消息万分激动。“当时我是怀着无比感激的心情,写下的那封感谢信。我还记得被骗那天我赶到中队时已经是中午休息时间,我还沉浸在被骗的懊恼中。144000 元可不是一笔小数,当时两位民警不仅耐心细致引导我把案件经过叙述完整,还在不断安慰我,告诉我后面每一步应该如何做。当天下午又用了 2 个多小时做笔录,现在回想起那个过程还非常暖心……”尹女士说。

民警这份“反诈宝典”请牢记

采访中,民警表示,市民应该提高防范电信网络诈骗意识,并总结出防范电信网络诈骗的对策及建议,请广大市民牢记。

一、妥善保管个人信息

1.要保护好个人身份信息。在非必要情况下,不向陌生人提供身份证号码、工作单位、家庭住址、职务等重要

信息。不将身份证照片或号码保存在手机中。

2.要保管好个人账户信息。在相关网站输入账号、手机号码、查询支付密码等重要信息前要认真核实域名真实性,不点击可疑链接,不连接来历不明的无线网络,不扫描非正规渠道获取的二维码,谨防钓鱼陷阱。

二、绝不出租出借“两卡”

要保持警惕,不轻信他人,不贪图小利,绝不出租、转让、出租、分租、出借或者购买银行卡、支付账户(微信、支付宝等),以免给不法分子提供“作案工具”。若发现出租、出借电话卡、银行卡等犯罪行为,要及时向公安机关举报。

三、加强账户安全管理

1.为银行卡、网上银行、手机银行设置复杂程度较高的密码。

2.不在其他任何网站上设置与网上银行、手机银行等相同的用户名和密码。

3.不向任何人透露或转发短信验证码及其他形式的动态密码。

四、提高金融安全意识

1.群众应密切关注媒体报道和网络曝光的诈骗案件,了解近期出现的作案手法,并提醒家人亲友提高警惕。

2.对电信运营商通过短信推送的安全提示信息,以及公安机关通过网站、公众号不定期发布的风险防范要点,应认真研读并牢记。

五、培养良好支付习惯

1.接到熟人通过短信、微信、微博、QQ、邮件、语音等形式发送的转账请求,或询问银行卡、网银密码等重要信息时,要通过电话核实确认。

2.陌生人或长期失联的“熟人”要求汇款时,须保持谨慎多方求证,遇到可疑情况及时向公安机关、银行、电信运营商等机构咨询。

3.如确需向对方转账,应尽量选择次日到账方式并于事后再次核实,如有异常及时申请撤销。

4.具有移动支付习惯的消费者应选择安全性较高的支付产品,并下载安装正版应用软件。

5.避免在与移动支付软件绑定的银行卡中存放过多资金以便分散和锁定风险。

民警最后提醒大家,确保不被骗要做到“四不”,即:不轻信、不泄密、不汇款、不刷单。当您感觉上当受骗时,不要心存侥幸,应当迅速终止交易、保存涉案证据,并及时向公安机关报警,以此减少损失并为公安机关破案争取时间。