

加强防骗能力的学习和掌握 警察带你走进电信网络诈骗“现场”

□通讯员 吕信思

近期,随着相关部门对电信网络诈骗的防范宣传、打击的力度不断加大,电信网络诈骗发案有所下降。但随着大家识骗能力、防骗能力的不断提升,骗子们也“紧跟时代”,升级诈骗手段,不断翻新花样,企图混淆视听实施犯罪。

据浙江省打击治理电信网络新型违法犯罪工作联席会议办公室发布,用大数据分析去年前11个月全省电信网络诈骗受害人年龄得知,年龄在21-50岁的人群被骗的比例高达81%。这部分人是社会的中坚力量,拥有财富最多,也是最大的涉网人群,社会活动频繁,信息泄露也较为严重,是骗子重点攻击的对象。防范电信诈骗离不开政府相关部门对此类案件的打击和治理,也离不开民众自身加强防骗能力的学习和掌握,更离不开亲友之间的沟通与协助。

下面,由我市警方带您一同走进今年初的几个电信网络“犯罪现场”,回顾这些诈骗案件的全过程,听听警方怎么说。

案例一 “银行客服”要验证码,小心有诈



一天,家住东城街道的吴女士收到号码显示为01057151457发来的短信,称其名下的一张信用卡因逾期未还已被冻结。吴女士记得这张信用卡欠款已还清,但又怕信用受影响,便主动联系了短信中提到的电话号码。电话那头一名自称银行工作人员以查询的名义,要求吴女士提供银行卡背面的7位数字,以及吴女士随后收到的银行短信验证码。

吴女士没有多想,按对方的要求走完所有流程。结果,吴女士没有等到问题的回复,却收到了一条银行短信,提示其卡内的9300元被消费。再联系对方时,电话里却只有忙音。

警方提醒 骗子就是利用吴女士自己提供的验证码以及信用卡背后的最后3位数的附加码,成功用吴女士的卡进行消费。请一定要严密保管与个人账户有关的验证码,特别是信用卡背后的附加码,不能轻易透露给他人,以免被骗!

案例二 充10元游戏币反被转走一万元



市民肖某在家中玩网游时添加了一名游戏里的玩家好友,对方称可提供抵扣为五折的游戏充值优惠,肖某想先充10元钱试一试。于是,他便添加了其QQ,随后对方通过QQ发来一个文件让肖某下载安装,并称这是完成优惠充值必不可少的插件。肖某信以为真,完成安装后,肖某又根据对方的提示打开自己的支付宝,在界面上输入了账号密码。谁知过了不到5分钟,肖某手机上竟收到短信,提醒其银行卡内10000元余额已被转走,他才发现自己被骗。

警方提醒 不论何种充值务必走官方渠道,不要轻易接收或点击陌生人发来的文件和链接,里面很可能潜藏着为盗取个人账户信息的病毒和木马。

案例三 假老板找上门,糊涂会计竟不知

一天,我市某公司会计徐某接到一个陌生的来电,电话里的人说这是老板狄某的私人号码,徐某一听声音,果然与老板说话的口气很相像,便深信不疑。第二天一早,对方打来电话,以急需给其他两家公司转账为由让徐某取出10000元,通过现金转账的方式到ATM机上转存,并称为其报销。转完之后,对方又称还需

再转10000元。这时,徐某才感觉到不对劲,就去找真正的老板狄某核实,得知老板根本没有这个电话号码,也未叫其汇过款,这下徐某才得知被骗。

警方提醒 犯罪分子冒充老板行骗的老套路屡见不鲜,想要识破其中骗局,核实对方的真实身份是关键。

案例四 满是陷阱的违规刷单



一天,在网上做生意的市民胡某收到有过生意往来的“大乔”的一条消息,称可以帮其在

网上刷单清库存。

当时胡某正好有1万余只的闹钟需清仓,他便与“大乔”谈好每件,以一单1元的佣金刷单。第二天,胡某的网店上果然多了2000余订单,随后“大乔”提出闹钟销售质量不行要求涨佣金,胡某同意向对方转账6000元。胡某本以为网上的订单还会源源不断,谁知过了一天却没有了,反而接到了一个陌生女子来电,问其为何不结清佣金。紧接着,胡某又发现之前的订单均被取消,再联系“大乔”时,已无人回应。

警方提醒 刷单行为本就违规,近两年因刷单被骗案件时有发生。请记住,不论是刷单还是被刷单都极有可能掉入诈骗分子设计的陷阱。

案例五 新手卖家遭遇网店风险陷阱

大学刚毕业的丽丽想自主创业,于是,在某网站上申请准备开网店。

申请下来不久,丽丽的手机便收到一条短信称其店铺存在风险,若不解除这个风险,网店就会被立即冻结,且在网店解封之前还不能进行其他操作。慌张之下,丽丽添加了短信中注明的可快速办理解冻服务的微信账号,并按对

方的要求将4000元钱用支付宝付款的方式转账。随后再联系时,丽丽发现自己已被拉黑,这才明白被骗了。

警方提醒 犯罪分子会盯上新手就是利用对方不了解不熟悉相关流程的特点实施诈骗。其实需要添加微信账号进行操作这一步就已十分可疑,还要要求向其汇款更可认定是诈骗。

案例六“小额贷款”引诱受害者步步上当



外来务工者高某看到了一张写有“无抵押办理小额贷款”的网络图片,他就在QQ上添加

了该图片上所示的网友“哥吸的是烟”为好友,并告知对方自己需要办理5万元的“微粒贷”。

对方收到信息后,让高某通过微信充值740元Q币,作为办理贷款的费用充值到指定帐号上。接着,对方以高某账号未激活和信用积分不够为由,让其再充值2500元,并承诺激活成功后便会退还。两小时后,高某询问进展,对方又称其账号存在使用频率低的问题需要再充值。此时,高某想要讨回之前所付的钱款,却被对方直接拉黑了。

警方提醒 骗子利用受害者急用钱、图便利等心理,编造不存在的“低门槛小额贷款”信息,进而步步引诱受害者上当受骗。

案例七 9张迪斯尼门票背后的骗局

春节长假期间,很多人会计划带着小孩到上海迪斯尼乐园游玩。市民老胡也想带着家里的几名小孩去上海迪斯尼玩一玩。

2月2日14时许,老胡通过微信朋友圈找到了一名自称是某旅游公司的客服人员安某,向其购买了9张迪斯尼电子门票及该旅游公司提供的导游服务项目,共计4950元。2月5日,当老胡带着一家老少按照约定时间到达迪斯尼乐

园门口时,却怎么也找不到之前说好在门口口等待的导游,更不用说那几张电子门票了。老胡再联系安某时,发现已被拉黑,这才知道被骗了。

警方提醒 不难看出这个安某是藏在朋友圈里的假客服,一旦骗到钱款便会拉黑对方。网络购票务必走官方渠道,如遇类似情况请留足证据即刻报警。