

海归等成电信诈骗新“易感人群”

近期上海警方接报一起外籍人士被骗 2000 万元大案



首席记者 潘高峰

提起电信诈骗被害人,人们脑海中总会浮现出社区、中老年、女性这几个关键词。殊不知,一些人眼中的高智商、高收入精英阶层,有时也会对骗子言听计从。

记者昨天从警方获悉,除了新型骗术不断涌现,电信诈骗的“易感人群”也在发生变化。其中,境外人士、海归族、候鸟族(在本市或外省市有多处住房,经常或定期调换居住场所的人员)、圈圈族(一心忙于工作或科研,人际圈、信息圈相对封闭的人员)已成电信诈骗“新宠”。由于他们或对中国法律缺少了解,或一心忙于工作和科研,人际圈、信息圈相对封闭,几乎没有什么电信诈骗的防范知识,很容易让骗子轻松得逞。

老骗术屡骗老外巨额钱款

今年10月28日,上海浦东警方接报一起电信诈骗大案。被害人在骗子冒充公检法机关的威胁和蛊惑下,在连续一周的时间里,不断通过网上银行向所谓的“安全账户”转账超过2000万元。这是近期上海发生的单笔被骗金额最高的电信诈骗案件。

被害人之所以毫无防备,很大程度上因为他是一名外籍人士,对于骗子的伎俩几乎没有什么免疫力。同一天,也是在浦东,还发生了一起被骗400余万元的案件,被害人同样来自境外。

境外人士、海归族、“候鸟”族、“圈圈”族成为电信诈骗新的“易感人群”,对于警方来说,也是一个新的挑战。上海市公安局刑侦总队二支队警官糜一鸣告诉记者,虽然警方近年来在防范宣传上花了大量人力物力,几乎每个人都生活在防骗的环境中,无论是电梯口、电子宣传栏、阅报栏、信箱,都有警方张贴、投递的防骗宣传资料,电视上、广播里、报纸上、交通工具的移动视屏里,也充斥着各类案例的警示提醒,但是对于一些特定人群,还是缺少好的宣传手段。

“比如一些企业高管、科研人员、境外来沪工作或定居的人士,往往生活在特定的圈子里,加上对自己的分辨力和判断力往往十分自信,很少会把这些东西纳入视线。”对于糜一鸣来说,如何让电信诈骗的防范知识进高端商务楼、科研院所,进入一些高档别墅和全封闭的小区,是一个新的课题。

网银升级已成为最“火”骗术

“易感人群”的拓展,伴随的是骗术的不断翻新。以往的电信诈骗,大量是通过电话拨打,ATM机或银行柜面转账来行骗,但随着行骗目标向高端商务人士“拓展”,行骗的手段和媒介也都在不断变化。

据警方统计,今年9月,本市接报电信诈骗案件千余起,同比基本持平,但网银密码器升级类诈骗首次超越假冒公检法等司法机关行骗,占有案件类型的14%,成为最“火”骗术。

“其实这种手法并不是最新的。最早在2009年就曾经出现过,只不过当时是以‘中行E令’升级的形式出现,而现在换成了工行电子密码器升级。”糜一鸣告诉记者,这种骗术一度大行其道,但经过警方建议,中行真的升级了密码系统,到2010年2月,这种骗术基本上销声匿迹。

“其实很简单,我们建议银行增加了一个手机验证的环节,因为骗子其实并不掌握具体哪些人在使用工行电子密码器,所以也不可能知道对应的手机号,而是通过群发短信乱枪打鸟碰运气。一旦有了手机验证这一环节,行骗难度大幅提升。”

糜一鸣提醒,此类诈骗都是短信诱骗被害人登录钓鱼网站,输入账号和电子密码器上的随机密码进行所谓升级,结果账号和密码被掌控钓鱼网站后台的骗子看得一清二楚,只需拷贝下来,在真实网站上同步登录网银,就能把钱



警方提示遍布大街小巷,但「易感人群」熟视无睹

本报记者 张龙 摄

电信诈骗 谁在扮演“帮凶”

滥开卡 化整为零瞬间提款

骗子为何能神速提款?现在的电信诈骗团伙分工更专业,细分为“电话组”、“网银组”、“取款组”等。警方此前抓获的一名专门负责网上银行转账操作的犯罪嫌疑人交代,他一边受上级老板雇佣,一边又招了3名马仔负责ATM机取款及银行卡收购。所得赃款85%上交老板,余下的15%按照4:2:2:2的比例分

配。由于ATM机取款额度限制,诈骗团伙需要大量的银行卡。

一旦被害人中招,“网银组”立即接到网络电话,深谙此道的他们立即将钱款在数分钟内拆分,水银泻地般流入多个银行卡账号之中,每张卡不超过2万元——这正是大部分ATM取款的限额。与此同时,被称为“车

手”的“取款组”成员早已经启动,提着垃圾袋在全城取款,最后汇总,除了提成之外,都交给老板,通过地下钱庄转到境外。

每一起案件侦破,警方缴获的作案用银行卡往往都有数百张,这正是“滥开卡”的恶果。许多银行为了经济利益,对于“滥开卡”不但制止,反而鼓励。上海警方从2011年就在努力推动银行卡开卡设限,如今两年过去了,真正响应者寥寥。

透传改号 骗子电话竟显示110

“骗子打来的电话竟然显示110,叫我哪能办?”冒充公检法或者银行客服的骗子为了戏演得逼真,通过一种名为“透传”的改号服务,增加骗局的可信度。所谓透传技术,是VOIP网络电话的一种功能,用户可以随意指定显示电话号码,这种技术原本是为解决号码变更带来的不便,却成为骗子的帮凶。

据公安部五局披露的数据显示,近年发生的电信诈骗案中,使用网络改号电话作案的占90%以上。“电信诈骗团伙99%在国外,大多盘踞在东南亚各国,租用国内电信部门的信道后,通过国内某一城市端口落地,再跳过多地基站接入受害人所在城市,追查起来非常难,破案成本很高。”

公安部有关负责人介绍,电信运营商向外租出一个信道能收20多万元,要想彻底遏制电信诈骗,电信运营商加强对信道管控和监督是治本之策。公安部曾向工信部了解到,境外网络改号电话的识别、拦截,诈骗短信、垃圾短信的封堵、过滤,技术上可行。为何无法根治,主要还是利益作祟。运营商应当按照电信条例的规定,为用户提供“准确、安全的电信服务”,确保来电号码的真实性。

钓鱼网站 注册容易查封难

最近爆发式增长的“网银升级”电信诈骗,除了群发短信之外,还有一个必备的作案工具:钓鱼网站。

许多市民在被骗很多天后,震惊地发现令自己上当的网站竟然还开着。“警察难道无所作为吗?”实际上,网警们也有苦难言——有的是关不掉,很多网站服务器在境外,只能屏

蔽,但犯罪分子往往换个域名链接又死而复生;而大多数时候则是关不胜关,因为开一个假网站太轻松,关一个网站却需要很多手续。

注册一个网站非常简单,买一个域名不到50元,租一个服务器好的也不过数百元,稍微懂些网页编程的技术,就可以轻易搭建一个钓鱼网站,主管部门对此几乎没什么审核。

另外,对垃圾短信的监管不力甚至纵容,对骚扰电话缺少限制,银行账户异地冻结手续繁琐等等,都在无形中帮了骗子一把。近年来,警方一直在努力推动建立银行推出金融产品前的风险评估机制,对于那些容易产生漏洞的服务,及时提出修改建议,但也一直没有得到回应。由于银行的措施变革要得到总行的支持,地方分行即使有想法,往往也难变成现实。首席记者 潘高峰

轻易转走。

“其实,要洞察骗术非常简单,只需查看银行卡背面,一般都有真正的银行网址,如果短信上的网址链接与其不符,那就是骗局。”

诈骗新手法瞄上机票网购

除了网银升级诈骗,一种通过以航班取消、机票改签、网购退货等为由,套取被害人信用卡卡号和后三位号码实施盗刷的行骗方式,也是近期常见的诈骗新手法。

骗子同样通过群发短信的方式,发布“航班因机械故障被取消,请您拨打400-xxx-xxx电话退票、改签”这样的短信,碰上正好订购了机票的市民,很可能以为自己预订的航班真的出了问题,拨打电话咨询后,被要求提供信用卡卡号和验证码等信息,以便退款或改签。许多人难免信以为真,殊不知这些信息已经足以让骗子通过快捷支付的形式刷空甚至透支信用卡。

警方“虎口夺食”

今年8月6日下午3时21分,杨浦警方接到市民朱女士的紧急报警。她父亲接到一陌生男子电话,声称父亲的银行卡涉嫌洗钱,要求将存款转到新的安全账户中,父亲对此深信不疑,可能已将钱款转给对方。

这是一起典型的电信诈骗。殷行派出所民警立即兵分两路:一路赶赴辖区内各银行搜索拦截,另一路赶往国和二村朱老先生家中,万一老人转款回家,可以亡羊补牢。

当民警来到居民家门口时,遇到一位老先生正在和人打电话,依稀就是存钱、密码等内容。民警立即上前询问,证实他就是朱女士父亲。朱老先生说已将两万元打入骗子要求他开设的建设银行卡中,并已告知骗子卡号和密码。

眼看骗术即将得逞,民警立即从朱老伯手中接过电话,自称是朱老伯的儿子,佯装对骗子的话深信不疑,并透露父亲还有一张10万元存折,询问如何转入安全账户。就在民警与骗子周旋、假装询问如何一步步转入安全账户拖延时间之际,朱老伯飞速赶到银行,抢先一步将2万元存款取出。至此,一起既遂的电信诈骗案成功被民警拦截。

然而,并不是所有人都有朱老伯那样的运气。如此“虎口夺食”只是极小概率事件。很多时候,即使当事人事后突然醒悟,想要冻结钱款,也赶不上骗子取款的速度。大部分案件即使侦破,也追不回钱款。

首席记者 潘高峰