多一份金融了解 多一份财富保障

大学生2分钟被“客服”诈骗八千

莱山警方三年接学生被骗案821起

近日,各媒体爆出大量电信诈骗的案例和预防常识,但仍有诈骗分子变着花样实施诈骗,也总有学生不小心上当。近日,烟台一大学生收到某通讯公司兑换奖励的信息,他点开后不久,银行卡内的8000多元钱被转走。

近日,烟台某高校学生小李收到一条某通讯公司给他发的信息,内容为:您的话费积分(28868分)即将失效,可以登录网站兑换288.68元现金。

因与之前收到的通讯公司发来的业务短信没什么不同,小李就没有任何怀疑,直接登录短信中的链接网站,按照提示将姓名、手机号、身份证号码、银行卡号及密码一并输了进去。

仅仅2分钟后,小李就收到了4条农业银行的信息,内容为卡里总共被扣了8142元,小李这才意识到被骗了,然后就打电话给农业银行让其把银行卡封住,第二天到派出所里报了警。

据派出所民警介绍,近日有不少市民也收到了通讯公司发的类似诈骗短信。该通讯公司客服回复称目前公司并没有积分兑换现金的活动,这是不法分子利用伪基站冒充客服发送积分兑换现金的短信,骗取客户的银行卡号和密码等信息实施的诈骗。

在记者的采访中,每隔几天就会遇到电信诈骗的案例,大学生受骗的案件更是司空见惯。

记者从莱山公安分局获悉,从2014年到现在的两年多时间,该局接到辖区大学生被骗警情821起,平均每周就有6人被骗。这其中,电信诈骗又占其中的大多数。最让民警们忧心的是,尽管每年他们都会针对大学生进行多种形式的安全教育,但这些年轻人的防骗意识依然淡漠。

防范建议:

电信诈骗是指以非法占有为目的,利用手机短信、电话、网络电话、互联网等传播媒介,以虚构事实或隐瞒事实真相的方法,骗取数额较大的公私财物的行为(又称非接触性诈骗或远程诈骗)。针对此类情况,广大市民要提高警惕,不要被他人的花言巧语而迷惑,更不能轻信陌生人;收到陌生电话或短信时要有警觉,并非“标准”普通话和其声称的国家工作人员的身份就是真实的,对其冒充银行工作人员称冻结账户、信用卡刷卡透支等内容,不要轻信,要多咨询一下身边的亲朋好友或子女,同时及时主动向公安机关报警。

(本报记者 柳斌 通讯员 闫红双)

谎称航班取消改签退款诈骗104万元

跨区域作案,破案成本高

烟台开发区警方曾经破获一起数额104万元的“航班改签退款”诈骗案。在开发区做生意的台湾客商左先生之前预订了机票,骗子用400开头的电话联系他,对左先生的航班架次、身份证信息等了如指掌。骗子称航班取消,改签退还200元差价,指导左先生在电脑上一步步操作,将卡内104万元转给了骗子。

办理此案的开发区公安刑警赵璞回忆,104万元转出后,几秒钟内分成了25笔汇入7个人持有的14个一级账户,一天之内又转入几十个二级账户,最后通过POS机套现、柜台提款、ATM提款等方式被全部提走。“速度之快非常惊人,也可以看出骗子的专业程度以及产业化程度。”赵璞说,所以,电信诈骗的案件破案难度极大,加之犯罪分子多在南方甚至境外,破案成本也是极高。

据了解,电信诈骗多是远程、非接触式犯罪,所以线索更少、隐蔽性更强、人员结构更复杂、打击难度更大。

目前,电信诈骗通过手机短信、打电话、电子邮件、QQ、MSN、虚假网站等方式进行违法犯罪活动,与被害人零接触,隐蔽性极强。随着打击力度的加大,跨区域作案特征越来越明显,犯罪分子在省外甚至境外设置服务器或直接通过省境外网络信息技术等方式实施诈骗,加大了调查取证与打击的难度。

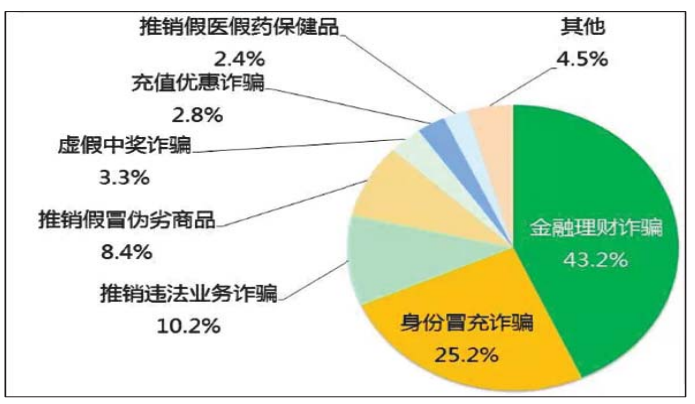
《2016中国网民权益调查报告》显示

个人信息泄露已成重灾区

根据《2016中国网民权益调查报告》,近八成的网民个人信息被泄露,37%的网民因此遭受财产损失。在央视记者的调查中,有人表示可以提供江苏省10万名高三考生的信息,一条只要三分钱。快递员、银行职员、教育培训机构甚至交警协勤人员泄露和倒卖个人信息的新闻屡见不鲜,一包辣条的钱就能买上百条个人信息。

另外,犯罪分子利用网站的漏洞窃取用户信息,也是信息泄露的重要途径。大学生徐玉玉被骗案中,大量考生的信息就是通过网站被窃取的。

在一桩典型的电信诈骗案里,骗子先是通过短信或者电话引诱受害者汇款,再用多张银行卡把赃款化整为零,快速分批取走,这让追查起来非常麻烦。



为了方便管理和遏制犯罪,除了实行银行卡实名验证,工信部还从2010年开始推行电话实名制。但是,即便电话卡完全实现实名制,骗子也有空子可以钻。

目前,全国电话实名率已经超过了90%。但是,在实名制普及率高达96.24%的广东地区,呼出诈骗电话位居全国前列。徐玉玉案中的两个诈骗电话,都经过了实名制认证,很多时候骗子会利用捡拾或者冒用他人身份信息开卡。

电信诈骗冻结资金有望3日内返还

近年来,电信网络新型违法犯罪愈演愈烈,造成人民群众巨大财产损失。9月20日,中国银监会和公安部联合发文,要求公安机关、银行业金融机构对已查明的冻结资金,及时返还人民群众,并明确银行业金融机构办理返还应当在三个工作日内办理完毕。

不法分子往往利用电信、互联网等技术,通过发送短信、拨打电话、植入木马等手段,诱骗(盗取)被害人资金汇(存)入其控制的银行账户,实施电信网络新型违法犯罪。而银行则是“挽救”被害人的“最后一道防线”,能够协助公安机关依法对特定银行账户实施冻结措施。

为减少电信网络新型违法犯罪案件被害人的财产损失,确保依法、及时、便捷地返还已冻结资金,银监会和公安部联合印发了《电信网络新型违法犯罪案件冻结资金返还若干规定》,明确了返还工作原则、职责,返还条件、程序和方法以及被害人的义务。

规定要求,公安机关负责查清被害人资金流向,及时通知被害人,并对权属明确的被害人财产作出资金返还决定,实施返还。公安机关要主动与被害人联系,依法办理资金返还工作,不得以权谋私,收取任何费用。

规定明确,银行业金融机构要依照有关法律、行政法规和规定,及时协助公安机关实施涉案冻结资金返还工作。能够现场办理完毕的,应当现场办理;现场无法办理完毕的,应当在三个工作日内办理完毕。

电信诈骗常见的六种骗术

日前,山东、广东发生三起学生遭遇电信诈骗案件,导致受害者猝死或自杀,引发社会对电信诈骗的广泛关注。如今的电信诈骗,已经不只是发个短信通知中奖,或者“领导”打电话让你去办公室那么简单的伎俩了,电信诈骗现在也有套路了。

◓套路一:冒充公安局、检察院、法院人员

骗子冒充“公安局”“检察院”“法院”等单位“工作人员”打来电话,告知受害人涉嫌洗钱、贩毒、经济犯罪等违法行为,利用受害人急于“摆脱干系、减少损失”的心理,诱使受害人将钱款转入骗子提供的所谓安全账号,以达到诈骗的目的,这也是最常用的招数。现在很多骗子通过改号软件伪装成官方客服电话,甚至还出现了“升级版”:骗子以赠送免费物品为由,引导用户通过电话下单,以货到付款的形式邮寄,若用户拒绝签收快递或者退货,诈骗者便以公检法的口吻对用户进行威胁恐吓,进行诈骗。

支招:“公检法”没有所谓的“安全账户”,“安全账户”=诈骗!

◓套路二:“请您及时领取××补贴”

犯罪分子以领取新生儿补贴、贫困补贴、助学补贴等为由行骗,由于他们能说出受害人的详细信息,让受骗人信以为真。骗子在获取受害人银行账号之后,通常会要求受害人到ATM自动取款机操作,按照对方的“引导”进入英文操作界面。由于受害者看不懂ATM机上的英文提示,往往把转账程序当成输入验证码,最终上当。

支招:此类电话或短信,切勿轻信,更不要到ATM操作。

◓套路三:“您乘坐的××航班取消了”

手机订机票成了网络诈骗的风口。骗子谎称改签退票等理由,引导民众进入钓鱼网站,虚假号码,进行到汇款的陷阱。有数据报告显示,这一诈骗类型高达44%,成为网络诈骗主流。骗子能够准确说出受害者的姓名、航班信息,多以可以获得改签补偿金的名义进行诈骗。

支招:机票退改签业务,通过航空公司、票务代理商等正规渠道的网站、电话、服务厅办理,别相信任何电话、短信,即使与本人信息完全相符。

◓套路四:用伪基站冒充10086等运营商客服电话

诈骗分子通过“伪基站”伪装成10086等号码群发诈骗短信,以“积分兑换现金”的方式诱骗下载安装一个带有木马病毒的App,窃取账号、密码、验证码等,从而盗刷资金。

支招:最简单的一招,就是遇到这种事情,反打10086来咨询,一打电话就什么都明白了。

◓套路五:“网上购物退款”诈骗

犯罪分子冒充淘宝等公司客服拨打电话或者发送短信,以受害人拍下的货品缺货或者交易失败为由,告诉受害人需要退款,要求购买者提供银行卡号、密码等信息,从而实施诈骗。

支招:淘宝等公司网购退款会直接退到支付宝内,不需要知道银行卡号等信息。遇到此类事情,千万不要贸然把银行卡号等信息告诉别人,直接向卖货商家咨询就知道真假。

◓套路六:“你的账户有资金异常变动”

骗子首先窃取了受害者网银登录账号和密码,通过购买贵金属、活期转定期等操作制造银行卡上有资金流出的假象。然后假冒客服打电话确认交易是否为本人操作,并同意给用户退款骗取用户信任。接下来,骗子会使用受害者网银进行转账操作,或开通快捷支付操作,并选择短信验证码的方式进行验证,这样一来,受害者的手机上就会收到一条验证码短信。最后,骗子再以限时退款为由,要求受害者立即提供自己手机收到的验证码,受害者一旦把短信验证码提供给了对方,对方就得手了。

支招:立即直接拨打银行的官方客服电话进行核实,别相信任何主动呼入的、自称是客服的电话。