探路

车票“首轮”没抢到,瞅准退票捡个漏

本报记者 王琳

今年春运期间火车票调整为提前60天预售,且提前15天退票不收退票费,这在方便广大乘客的同时,也使一人抢多票的情况明显多起来。铁路部门对此提醒,现在春节前热线票“首轮”已被抢得差不多,还没有抢到票的乘客,看准退票时间点有机会“捡漏”。

“年年都有人会多订票‘备用’,而今年情况尤其多。”潍坊火车站工作人员说,企业放假时间往往到了临近春节才能确定,为既不耽误工作又能顺利购票回家,于是不少人就抢购了不同日期的火车票,到放假时间确定时,再将不用的车票退回去。目前就已有少量的退票情况,但想捡漏不太容易,更多的退票差不多还得等一个月。

对于那些最初放票时没能抢到票的市民,铁路客运工作人员建议,不妨多上12306网站刷一刷看是否有退票。“一般退票时间集中在上午8点到下午3点,也就是上班时间。”工作人员说,同时电话订票未取,订单过期失效后,车票将会在每天12:00和24:00后重新投入系统。想抢票要注意这两个时间点。不过退票采取的是“延时随机返库”原则,也就是一趟车的退票将分不同时段、随机分配到各个销售渠道中,因此除了“23时至次日7时”期间不返库,其他时间都有可能出现返库余票。

此外,一些“囤票”的旅客确定行程后且想要享受提前15天退票免退票费的优惠,会集中在这一时间段退票。一般来讲,铁路客流高峰日为腊月廿三到腊月廿九,那么这部分退票则最可能集中在明年1月20日前后到2月初。另外,除了提前15天抢退票外,在发车前一到两天时间里,也会有部分未来得及提前半月退票的乘客,选择在此时将自己多余的车票退回。因此,开车前1到2天,也是旅客“捡漏”的好时机。

卡没离身却被离奇刷走28万

警方汇总坏人各种盗取银行卡信息手段,告诉咱如何防范

今年10月份的一天,泰安肥城李女士的手机突然收到银行客服短信,显示她的银行卡于当日在POS机上支出28万余元。该卡一直在李女士本人手中,从未丢失,最近也没有刷过卡,怎么钱被刷走了呢?当地警方经过侦破,日前终于破案,警方借此也特别提醒市民,个人银行卡重要信息特别是密码千万不要泄露。

本报记者 刘真
通讯员 刘洋

惊奇:

卡和密码都未丢 钱咋没了

李女士是肥城的一个个体商户,这张被盗刷的银行卡她一直随身携带,密码也没有其他人知道,卡上的钱怎么会无端被人偷走了呢?案发后她立即报了案。

接到报案后,肥城市公安局立即成立专案组,经过调查,民警发现李女士的银行卡刷卡地址在合肥,民警立即赶赴合肥。通过查询发现,刷卡的POS机是一个姓马的合肥人办理的,李女士的钱在被盗刷后当即被转到马某的账户上,后在不到半小时的时间内就被转账到了14张在全国各地不同银行开户的银行卡上进行提现,提现的地点是天津。

由于这14张银行卡是不同的开户人在全国各地不同的银行开户,民警推测这些银行卡极有可能是复制卡,卡主本人也许对此并不知情,但民警还是将14张银行卡的卡主信息打印出来,与监控录像中的提款人进行逐一比对,一个姓张的卡主进入了警方的视线,经过反复比对,民警确定张某就是其中一名提款的犯罪嫌疑人。

经过一段时间的调查取证,日前专案组先后对张某和马某等几名嫌疑人实施了抓捕。据犯罪嫌疑人张某供述,他以代办POS机和信用卡为业,过去与受害人李女士有所接触,他在为李女士办理POS机时,李女士对他几乎没有什么戒备,于是在帮助李女士试用机器时,他偷偷记下李女士的银行卡号和密码。此后复制了李女士的银行卡,随后与马某等几名同伙一起盗刷了李女士卡上的28万元,为迷惑警方视线,他们特意赶到天津进行提现。

当心:

坏人这些手段偷银行卡信息

据肥城市公安局经侦大队民警介绍,大家一般认为,卡只要在自己手中,卡里的钱就是安全的,其实并非如此,银行卡被人复制后盗刷的案子已发生很多。不法分子只要获取了他人银行卡的主要信息和密码,就会复制一张卡后,将卡里的钱偷走。

那么不法分子是如何盗取他人的银行卡信息和密码的呢?警方介绍,除了像上面案子借代办POS机或信用卡当面盗取信息外,其他主要盗取手段还有几个:

一是使用便携式信息采集器。这种采集器像充电宝一样大小,很隐蔽,不法分子拿到他人的银行卡后,迅速刷一下,就可窃取该卡的用户名、身份证号、家庭住址、存入或支取金额的时间地点以及账户余额等信息,不法分子据此可以复制一张卡,如果再设法得到该卡的密码,就会将卡里的钱划走。

二是在ATM机的插卡口加装高仿真的卡槽,里面装有读卡器,同时将微型摄像头安装在ATM机上方,拍摄密码输入过程。读卡器可像上面的采集器一样获取银行卡的主要信息,摄像头则用于盗取银行卡的密码。还有,有的自助银行门口,也会被不法分子偷偷安装上读卡器,卡主在刷卡进门的时候,一不小心就同时也刷了这个读卡器。

三是在ATM机按键上方安装微型摄像头。ATM机按键上方都会有一处用来遮挡的地方,市民认为有了它就可以安心使用ATM机了,其实不然,有些不法分子会在遮挡处上方用胶带粘贴微型摄像头,且不易发现,这样信用卡密码很容易泄露。

四是不法分子利用安装了读卡器的假的POS机获取卡主信息。

另外,还有的是通过网上购买银行卡信息。一些粗心的网民,在网上交易时不小心留下自己银行卡的基本信息,这些信息被不法分子或不良商家获取后,常会倒卖出去。获取这些信息的不法分子如能再获知银行卡的密码,就会偷走卡主的钱。

支招:

输密码时一定要用手挡一下

见招拆招,肥城市公安局经侦大队民警提醒,保护好银行卡密码是第一位的,市民在公共场所刷卡消费和输入密码时,要用手或遮挡物遮盖保护密码,这样可以避免旁人通过各种方式偷窥或者记忆密码,不法分子如果不知道密码,任凭他采取何种方式,都不能对信用卡进行盗刷。

信用卡刷卡时,不要让卡离开自己的视线,即使是卡交到别人(如服务生)手上也是如此,这样就不会给不法分子以可乘之机。

完成交易后,各种金融单据妥善保管或彻底销毁,防止犯罪分子通过此类单据掌握用户的信息;网上交易时也要注意不要留下银行卡主要信息。

还有,市民设置的密码最好不少于12位数字,且最好采用数字和字母组合的方式,这样也增加了被盗取的难度。

持卡的市民最好定制银行短信提醒业务,这样便能在最短时间里发现卡内资金的异常变动,并及时通过银行客服电话挂失。

另外,市民在使用手机支付宝时,尽量不要将银行卡号自动保存在手机中,最好不要在手机支付宝中开通快捷支付。如果在支付宝中存有余额,那么手机一旦丢失,这些钱就意味着一起丢失。

相关新闻

收到“银行”短信 1万多元被套走

本报烟台12月24日讯(记者 张倩倩 实习生 马彩红) 22日,烟台龙口的黄先生收到一家银行发来的短信,称黄先生的手机银行已过期,需要重新激活一下。他信了,没想到却是一个陷阱。

22日黄先生的手机收到这样一条短信:“您的手机银行今天过期,请登录我行管理网站激活升级。”黄先生点击进入这条短信提供的网站链接。随后黄先生手机又收到一个激活码,按照提示,他输入了该六位激活码和自己的手机银行密码。本以为自己的手机银行就这样升级完毕了,却没想到自己卡里的钱没了。操作完毕后不一会儿,黄先生就收到了一条短信,他卡里被转走了14200元。

黄先生后来才知道,原来那个链接是个假的网址,比真正的官方网址多了两个字母。加上之前他每次用手机银行付款时,总会有个验证码的短信提醒,这次只是激活,所以他才按照提示操作了。

发现被骗后,黄先生去东莱派出所报案,并得知,与他情况相同被骗的不在少数,金额多则四五万元,少则一两千元。民警称,确实有多名市民来报案,警方也在立案侦查此事。

网银莫名 被盗刷6000元

本报菏泽12月24日讯(记者 赵念东) 23日晚上,家住菏泽牡丹区的林女士刚吃过晚饭突然收到一条余额短信提醒,自己的银行卡被支走金额4288元,“我以为自己的银行卡丢了,被别人捡到后利用。”于是,林女士立即寻找自己的银行卡和U盾,结果发现两者都在。

发现不对头,林女士立即拨打了银行卡上的客服电话,对自己的银行卡申请止付。而待林女士拨打完电话后,发现其银行卡又被刷走2521元,两次时间间隔不到20分钟。菏泽市公安局牡丹分局经侦大队民警介绍,近日,牡丹区警方陆续接到群众关于网上银行账号被盗刷的报案,这很可能是因为银行卡信息被不法分子盗取。民警提醒市民,在开通网上银行时要谨慎,对于自己比较重要的银行卡,比如工资卡等用于存储大额资金的银行卡,尽量不要开通网银;如果需要开通网上银行,最好设置每天的最高消费限额,同时开通短信余额提醒服务。另外,在使用网银时,最好单独办理一个银行账户,以避免出现问题时,造成更多经济损失。目前该案还在侦破中。

微观 逸周末

想知道“逸周末”最新内容,扫一扫吧!

最新研究揭露感冒的三个真相

感冒常有,而知道感冒真相的人却很少。大家都知道:感冒最早出现的症状主要包括咽喉肿痛、打喷嚏、鼻塞流涕、身体疲倦。天冷却穿的衣服很少、光脚走在冰冷的地上,刚洗完头头发还没干就出门……这些是感冒的原因吗?它们都不会导致你感冒——但是会导致抵抗力下降,让病毒们有机可乘。

感冒到底是怎么回事?感冒后应该怎么办?美国最新研究为我们揭示了这一系列问题的答案。关注逸周末公众微信号(qiluyizhoumo),可查看全部详细内容。点击逸周末微信页面右上角头像,还可以查看历史消息哦!

逸周末粉丝QQ群(384365359)——逸家人现在也开通了,欢迎亲们回家!