郑荐

银行卡3天异地盗刷32次 57万多元全被买成Q币

报警后骗子还打来电话:“我刷走了你的钱,不信可以报警” 提醒:遭遇异地盗刷先取100块钱,证明卡在自己身上

在银行快捷支付否认函上,记录了被盗刷的32笔资金的内容

3天时间,银行卡遭遇盗刷32次,卡内57万多元现金被陆续转走,而卡主发现异常报警时却接到骗子“刷走了你的钱,不信可以报警”的挑衅电话。

事情发生后,银行拒绝了卡主索赔要求,称此事系客户误点虚假短信泄露个人信息所致,警方调查得知被盗刷的资金转入了广东一家公司,随后又通过网络充值被全部购买成了Q币。

郑州晚报记者 汪永森 实习生 敬晨宇 文/图

卡主 银行卡遭盗刷,3天转走57万元资金

18日15时,青年路万翔公寓租户郭女士发现自己的芯片银行卡功能受限,她求助城东路上该卡开户银行得知卡内57万多元资金已被分为32次转走。

郭女士很震惊,不知卡内资金通过什么途径被转走,转走的钱中一半为购房款,一半为各地商户的货款。

“银行卡开通了短信提醒,这几天怎么没收到一条提醒。”她说,如此频繁的转账操作,3天时间共转走57万多元资金,自己的手机竟然没有收到一条提醒短信。

在银行快捷支付否认函上,她登记下了被盗刷的32笔资金的内容,盗刷时间集中在4月17日至18日。

这两日被盗刷的资金第一笔为1000元,第二笔只有0.01元,此后出现5笔5万、1笔3万、10笔2万、7笔1万的转账记录,现在卡上只剩四五千元。

骗子 “我刷走了你的钱,不信可以报警”

在确定大量资金被盗刷后,郭女士希望银行方面进行解释和赔偿,此后双方出现纠纷并拨打了110,二里岗分局民警赶到进行调查处理。

民警进入银行协调双方之时,郭女士的手机突然响起,来电是一个183开头、归属地为广东深圳的陌生号码,她按键接听后血压再次上升了。

“广东的电话,就说了45秒时间,南方口音的普通话,先确认我的名字,接着告诉我钱是被他取走了。”郭女士称,来电充满挑衅和调侃意味。

这名男子不但在来电中自称骗子,还建议郭女士查完账报警,“你查查看,不相信,去试试,也可以报警”,再拨打该号码已处于关机状态。

警方 已立案调查,盗刷的钱全部购买了Q币

在二里岗分局民警的协调下,这家银行向郭女士公开了资金流向,而交易清单中取款方一项绝大多数为代签,所有对方客户名都是“广东天翼银行划扣资金过渡户”。

警方随后的调查显示,郭女士被盗刷的资金转入广东天翼银行划扣资金过渡户后,又流向山东烟台一家名为“鼎信网络”的充值公司。

“购房款和货款,民警说被骗子全部买成了Q币。”郭女士说,自己的存款、家人的退休金及货款都被取走,目前卡内余额已不足5000元。

记者通过网络查询得知,广东天翼银行划扣资金过渡户是一个连连支付的支付通道,第三方支付,与国内部分银行有合作。

目前,二里岗分局案件侦办大队已经立案调查此事,民警也已南下广东搜集证据。

银行 客户误点虚假短信,泄露信息所致

20日上午,该银行郑州分行一负责人表示,客户在此前的操作中误点号码伪装为某通信运营商的积分短信并输入个人信息,导致账户信息泄露,短信功能被屏蔽。

“银行门口的LED屏上有提醒,有不法分子利用伪基站假冒‘10086’和‘95533’向持卡人发送虚假短信,提醒客户不要将信息和验证码透露给他人。”该负责人说。

郭女士承认点击过积分短信,但输入的信息不包括银行卡号,更没有涉及密码信息。

她认为银行在监管方面存在漏洞,而钱被分为32次转走,银行也未进行提醒,情况未明时银行还曾要求她在“因个人原因导致信息泄露”的情况说明上签字。

该负责人说,通过网路转账一般满足银行卡、身份证号、密码以及验证码四个条件,银行系统并不能评估出风险,而短信提醒是因遭到屏蔽才未起到作用的。

线索提供 吕先生(稿费50元)

提醒

遭遇异地盗刷先证明卡在自己身上

二里岗分局民警表示,银行卡信息被盗刷集团盗取,主要通过ATM机上设置的陷阱,饭店、酒店刷卡的时候让服务员来刷,银行泄露信息,手机上的木马病毒四种途径实现。

中央财经大学经融学教授韩复龄建议,银行卡应该使用指纹识别降低盗刷风险,即不是卡主本人不能刷卡,但是这种卡又会增加使用成本。

此外,持卡人在用卡过程中,要注意用卡环境,保护个人信息,一旦发现银行卡被异地盗刷,首先要证明卡在自己身上,可以立即去银行存取100块钱,然后保存好存取凭证,这样可能帮助自己维护自己的合法权益。

短信附加网站能不点就不点

常见的高仿诈骗短信主要有:机票改签、法院传票、电视节目中奖、银行通知短信、10086短信、信用卡提额短信、交通违法短信、孩子成绩单短信、订餐短信、聚会合影短信等。

诈骗短信都会附加一个链接,即便再像,也是假的。无论哪家银行,如果发送的短信附加网址,肯定是官网,比如工行是“www.icbc.com.cn”而收到的短信是“wap-icbcnj.com”,尽管都有icbc的字样,但还是会发现不同。这样短信由于迷惑性高,很容易被当成真的。很多不法分子往往使用和真实网址非常相似的域名,其网站LOGO、图标、新闻内容都以假乱真,确实难以判断。

如收到疑似诈骗短信,该如何辨别真伪呢?首先不要轻易点击链接,能不点就不点,不要让钱包为好奇心买单。如果真的有点击的必要性,最好是自己打开官网,然后找相关的内容。