2015年信用卡6大诈骗手法大起底

年关临近,老百姓的生活将迎来一波消费高峰,不法分子也会瞅准时机蠢蠢欲动,实施各类信用卡诈骗。近日,交通银行信用卡专家总结了2015年关于信用卡常见的六大诈骗手法,提醒大家在即将到来的年末节庆购物高峰中,一定要提高警惕,遇招拆招不中招。

骗术1：变身银行官方号码+伪基站,发送钓鱼网址

案例：王女士曾收到由“95×××”发来的“积分换礼品”信息,短信内容大致是“登录×××××网站可激活领取礼品”,落款为“某某银行”。好在细心的王女士发现网站要求提供自己的身份证号、信用卡卡号与密码等,疑心这是个钓鱼链接,没再继续下去。

分析：违法犯罪分子通过“伪基站”设备,向周边地区发送大量的虚假银行客服短信,以提供升级网银服务、积分兑换现金等为幌子,欺骗事主登录虚假银行网站并上传银行卡账号、密码、手机号等关键信息,并在短信中内置恶意网址链接,然后在事主手机中安装木马病毒,用于盗取手机支付验证码,从而盗取事主银行卡存款。

利用伪基站群发“假冒银行官方号码+钓鱼网址”短信依然占据很大比重,上当受骗者众,涉案金额巨大。接到类似短信的市民有很多,不少市民收到短信后,乍一看信以为真,有的按照提示操作后,银行卡里的钱就被直接网上盗取。

提醒：如遇到类似情况难辨真伪,可致电相关银行信用卡官方热线进行核实。

骗术2：冒充网店客服“退款”发送钓鱼网址

案例：沈阳市民田女士“双十一”网购后,付款没多久接到一个电话,对方开口就流利地报出详细的订单信息和姓名、地址等,“对方自称是客服,问我是不是在几点几分买了什么商品,我一看所有资料都对得上,就信了。”而后对方通过QQ发来退款链接,田女士一步步被骗子牵着走——申请退款、再重新拍、发送卡号、泄露验证码。几分钟后,她的储存卡累计被刷走3720元。

分析；诈骗分子利用消费者的真实购物信息,充当网店客服致电客户,声称商品断货,需要客户提供信用卡卡号、有效期、CVV2码等信息进行“退款”,随后引诱消费者进入钓鱼网站填入上述信息。一旦消费者上当泄露信息,信用卡就会被盗刷。

提醒：有些不法分子发现常规的诱骗已经不起作用,他们还会冒充老同学、老乡发送假相册,甚至冒充“小三”通过激将法诱骗用户点击链接,其诈骗实质依然是钓鱼网

址。

骗术3：微信互动页面、“微信红包”嵌入钓鱼网址

案例：群里有人发了红包链接，“链接写着某某公司,我也没多想这个公司是不是真有,就立即点击了‘抢红包’,显示抢到了200元的现金礼包。”青岛市民邱先生随即点击兑换取现,但系统要求输入姓名、身份证号和银行卡号等信息。邱先生没有引起警觉,按要求输入了个人信息。没过几分钟,他收到网站发来的验证码短信,他立即输入了短信中的验证码。最后,邱先生收到的不是红包的确认消息,而是信用卡被刷走1000多元的短信通知。

分析：很多不法分子会在微信互动界面中嵌入钓鱼网址,用户点开链接的同时,其相关个人信息便被盗取。例如,有位吴女士曾随手转发了微信群里一条祝福页面并填写了个人信息,随后却频频收到信用卡消费短信,幸亏她赶紧联系银行冻结卡片,才避免了更大的损失。

此外,微信红包也被不少不法分子利用,这些人会潜藏在人数较多的微信群中,通过分发嵌入钓鱼网站的红包,来盗取用户的信息。

提醒：消费者千万不要贪图小利,不要点击不明来路的链接与“红包”,特别是当其要求输入个人信息时,尤其要警惕。

骗术4：“山寨”微信公众号或APP推送钓鱼网址

案例：许多不法分子采取了更“高端”的诈骗手段——建立“山寨”的微信公众号或企业APP。赵先生是某手机游戏的热心玩家,他在微信上搜索到某游戏的公众号便添加关注,之后在优惠活动界面购买了游戏套餐产品,输入了信用卡信息,结果发生了盗刷事件。

提醒：关注公众号时,一定要认真核对企业的公众号名称以及是否取得微信认证。在下载APP时,也要去正规网站下载,安装可靠的安全软件,并注意安装时软件是否试图获取敏感度较高的用户授权。

骗术5：免费Wi-Fi存陷阱,勿扫不明二维码

案例：“在一家便利店呆了2小时,用公共Wi-Fi看了一会儿电视剧,其间收到短信提示,称有人登录了我的支付宝。前往银行柜员机查询,发现卡内800多元被盗刷。”王女士想起,她的银行卡与支付宝进行了绑定,随即前往银行自助柜员机查询发现,卡内余额只剩下1.11元。

王女士网购了一件600元的毛衣,网店告知扫描二维码可返还10元红包,她随即扫描了店方提供的二维码,但领取红包的界面并未出现,而王女士的银行卡不久后便出现了取款记录,而她本人并未取钱。事后王女士才发现,银行卡被盗刷,原来她扫描的二维码中含有木马。

提醒：尽量不要在公共场合随意连接来源不明的无密Wi-Fi,如果需要连接,也不要涉及支付类的操作。不要随便扫描不明来源的二维码,对于填信息免费送礼品的活动,也不要贪图小便宜。一旦不慎中了木马病毒,应该第一时间修改用户账户密码,立即解除所有网上支付绑定,联系信用卡发卡行,确保信用卡安全。

骗术6：代办大额信用卡广告?小心财产都转走

案例：泸州市民李女士介绍,去年7月1日,一名叫兰某某的女子找到她,自称能帮其办理可透支5万-10万元的信用卡。李女士和兰某某并不熟,只知道对方在一家贷款公司上班。她简单核实对方身份后,同意办理并付给对方2000元预付款,随后由兰某某介绍,李女士跟着一名叫吴某的男子到了成都,在对方介绍下分别办理了两家银行的信用卡,同时花费100元办理了一张成都的电话卡。此后,吴某联系李女士要将办好的信用卡交给她,但由于没有同时拿到办理的成都电话卡,李女士拒绝接收该信用卡。去年10月5日晚,李女士的QQ邮箱突然收到一条信息,其办理的两张信用卡分别透支了12031.60元和16341.29元。李女士大吃一惊,“我确实曾经委托他人办理信用卡,但至今信用卡都没到手,怎么就透支了?”

分析：诈骗分子通过冒充银行的客服电话、聊天软件或网页等发布虚假办卡信息,号称可以办理高额度信用卡,实际上是用你的身份信息盗办大额信用卡。办理信用卡需要申请人提供详尽的个人身份信息,有些骗子利用这些身份信息以及虚假的资产证明(临时打入账户,开卡后再转出),偷偷办了一张甚至数张大额信用卡,盗刷信用卡,因为这张信用卡是在你名下的,所以这些消费也都是在你名下的。

不法分子还会以“管理费”、“保证金”等各种名目不断收取高额费用,或以办卡需要提交“存款证明”做“流水账”,要求对方提供银行借记卡卡号以及该卡预留的手机号,暗中利用到手的信息将对方借记卡中的资产进行转移。

提醒：消费者切勿轻信他人能代办大额信用卡,一定不要听信任何非法渠道办理信用卡的宣传。信用卡应通过正规渠道办理,银行不会收取任何费用,更不会向客户索要密码等支付信息。