

近年来,网络电子支付已成为日益普遍的支付方式。近日,中国人民银行对电子支付中存在的问题进行了发布,其中支付机构在迅速发展的过程中,相关问题和风险不断显现,消费者未能得到有效保护,同时,央行提醒消费者在使用网络支付等服务时自我保护意识和风险识别能力亟待提高。

# 电子支付存漏洞 消费者需自我保护



## 网络支付类 投诉占大多数

央行表示,满足金融消费者的有效需求、维护消费者权益是金融工作的出发点。罔顾安全,简单地迎合消费者的金融需求,往往是造成金融风险乃至金融危机的重要原因。

央行表示,美国次贷危机爆发前,金融机构为消费者提供零首付房贷服务,极大地便利了消费者,但经过长期的风险积累,过度创新导致相关金融衍生品风险聚集,引发连锁反应,导致金融机构倒闭,全面爆发金融危机,最终还是由消费者承担了沉重损失。

央行表示,消费者在使用网络支付等服务时自我保护意识和风险识别能力亟待提高。在追求和享受支付便捷性的同时,消费者忽视了自身金融信息的保护,对支付业务内在风险的警惕性不足,风险不断积累。伴随着日益频繁支付活动,个人支付信息泄露风险大大增加,消费者面临更大的资金被盗和欺诈风险。

据统计,人民银行全系统金融消费者权益保护部门受理的网络支付类投诉占互联网金融类投诉的95%。

## 部分支付机构存在严重漏洞

近年来,非银行支付机构(以下简称支付机构)以服务电子商务发展和为社会提供小额、快捷、便民的小微支付服务为宗旨,适应公众日益增长的个性化、差异化支付需求,网络支付服务得到快速发展。但支付机构在迅速发展的过程中,相关问题和风险不断显现,消费者未能得到有效保护。

当前,支付账户普遍未落

实账户实名制。记者从央行获悉,据公安部反映,不少机构为“黄赌毒”、洗钱、恐怖融资及其他违法犯罪活动提供便利。某支付机构通过开立大量假名支付账户,为境外赌博机构提供支付交易高达数千亿元,非法跨境转移资金风险巨大。并且挪用客户资金事件时有发生,多地屡次引发消费者上街和围堵政府部门事件,严重影响社

会稳定。

此外,部分支付机构风险意识薄弱,客户资金和信息安全机制缺失,安全控制措施不到位,对消费者的信息和财产安全构成严重威胁,甚至可能将相关风险引导至消费者的银行账户。去年初,某支付机构泄露了上千万张银行卡信息,涉及全国16家银行,截至去年上半年,因伪卡形成的损失已达

3900多万元。同时,一些支付机构缺乏消费者权益保护意识,夸大宣传、虚假承诺,普通消费者维权困难。

通过非银行支付机构办理支付业务的客户资金风险案件频发,暴露出部分支付机构一味追求支付便捷而忽视支付安全、支付系统存在严重漏洞、客户资金安全和信息安全难以得到有效保障等问题。

随着移动互联网消费时代的来临,信用卡网上消费越来越普及,随之而来的是不法分子瞅准了这个特别的时机实施各类信用卡诈骗事件。对此,银行专家总结了过去一年关于信用卡的一些诈骗手法,提醒大家在购物时,一定要提高警惕。

# 谨防钓鱼 信用卡消费要留心

## 一号骗术 变身银行号码+伪基站 发送钓鱼网址

专家指出,通过手机和移动互联网实施的诈骗中,利用伪基站群发“假冒银行官方号码+钓鱼网址”的短信依然占据很大比重。例如王女士曾收到由“95×××”发来的“积分换礼品”信息,短信的内容大致是“登录××××网站可激活领取礼品”,落款为“某某银行”。但细心的王女士却发现网站要求提供自己的身份证号、信用卡卡号和密码等,疑心这是一个钓鱼链接,才没有再继续下去。

银行信用卡专家提醒,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。

## 二号骗术 冒充网店客服“退款” 发送钓鱼网址

诈骗分子通过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,信用卡就很可能被盗刷。

据专家介绍,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。

## 三号骗术 微信互动页面 微信“红包”嵌入钓鱼网址

很多不法分子会在微信互动页面中嵌入钓鱼网址,用户在点开链接的同时,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的一条祝福页面并填写了个人信息,随后就频频收到信用卡消费短信,幸亏其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,这些人会潜伏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。专家提醒,消费者千万不要贪图小利,或因为是熟人就点击不明来源的链接和“红包”。

## 四号骗术 开发“山寨”微信公众号 或APP推送钓鱼网址

许多不法分子也采取了更为“高端”的诈骗手段——建立“山寨”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。

银行信用卡专家提醒,在关注公众号的时候,一定要认真核对企业的公众号名称以及是否取得了微信认证。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。

## 五号骗术 免费WiFi存陷阱 勿扫不明二维码

银行信用卡专家提醒,尽量不要在公共场合随意连接来源不明的无密WiFi,如果需要连接,也不要涉及支付类的操

作;如果看到不明来源的扫二维码、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,从而确保信用卡安全。

## 六号骗术 代办大额信用卡广告诱人 财产损失悄无声息

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。不法分子以“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。

银行信用卡中心专家特别提醒,广大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。

