

假福利真套路 警惕电销POS机诈骗

“为回馈老用户，免费给您邮寄一台POS机进行升级。”近日，北京商报记者收到了这样一通电话。客服称，机器人筛选记者为“符合条件的用户”，可以免费赠送一台POS机。免费得、易激活、无押金，这到底是天降的福利还是隐藏的陷阱？



A

电销POS机、刷卡费率玩套路

“POS机免费升级，激活后刷卡费率0.48%、扫码0.25%，没有押金没有开卡费，但需要刷信用卡1000元流水激活机器。”在电话中，客服向记者这样宣传。填写收货地址后，记者收到了开店宝品牌的POS机。之后，客服要求关注“开惠宝官方服务号”微信公众号激活注册机器。记者查阅发现，该公众号认证主体为“江西省泽迅科技有限公司”，具有“开惠宝”的商标保护。

随POS机一起送达的，还有一张“使用说明”。在说明书上介绍了分润后台以及刷卡手续费提现的步骤。工作人员表示，“这是老用户的优惠政策”。

对此，一接近开店宝的人士透露，“江西省泽迅科技有限公司”为其合作公司，上述情况非开店宝官方行为，开店宝并不知情。开店宝商户交易的标准费率是0.6%，而合作公司正是利用“手续费返现”的方式进行营销包装，使费率“降”到了0.48%。

北京寻真律师事务所律师王德怡评价，合作公司的这种POS机存在交易复杂、消费不透明的情形，有损消费者的公平交易权和知情权。一旦产生纠纷，用户取证难度大，维权成本十分高昂。

在北京市中闻律师事务所律师李亚看来，电话销售也是一种违规行为，同样会存在POS机代理商信息不真实、不准确、不一致的情况，这种情况可能成为POS机刷卡套现以及洗钱、赌博等犯罪行为的路径。未经消费者同意，通过电话销售的方式宣传、介绍所推销的产品和服务的行为同时也违反广告法、消费者权益保护法的相关规定。

事实上，POS机电销、费率不符的违规行为，不仅使用户资金受到侵犯，还严重威胁到支付行业健康发展，扰乱市场秩序。

2023年5月，中国支付清算协会发布的《关于加强收单外包服务市场规范管理的意见》明确要求，收单外包机构需要维护客户资金安全，业务真实合法，诚实守信经营。在此之后，以拉卡拉为首的多家持牌第三方支付机构接连发布声明，要求代理商在开展业务时不得使用“零扣率”“即时到账”等涉嫌不正当竞争、误导消费者的文字。若有违反，代理商将有可能面临终止合作的处罚。

上述接近开店宝人士对记者表示，获悉情况后，已对合作公司进行了通告处罚。

B

POS机硬件中可能被植入木马

虽然记者遇到的情况还未涉及欺诈和资金损失，但是这样的电销套路仍然值得警惕。免费送POS机的背后，究竟是福利还是陷阱？

在黑猫投诉平台上，有多个电销POS机相关投诉，有的是未退押金，有的是首刷不到账。“说的是0.38%的费率不再扣别的费用，结果激活就扣了99元，利率也严重不符”“打着邮政工作人员的旗号办理信用卡和POS机，骗取押金399元一直未退”。虚假宣传、扣费不退、交易不透明是众多消费者投诉的主要理由。

而日前，多地警方也披露了以免费安装、退押金为名的电销POS机诈骗案件。警方表示，犯罪团伙先从黑灰产业中非法获得用户信息，由专业的客服人员联系用户，客服人员会以“免押金、免手续费、免安装”为统一话术吸引用户注意。若用户在一连串的“免费政策”下表露出了心动，客服人员将会提出POS机首周刷卡额达标，不仅能享受秒到账政策，还可领取其他福利。在“优厚福利”的吸引下，一些用户开始尝试申请该POS机。

之后，客服人员通常会以激活POS机、激活收款账号、激活秒到账功能等不同的名义分别诱使受害人刷卡。还会通过分散刷款的方式，再次降低用户警惕心。在用户刷款金额迟迟不到账时，客服人员会以各种原因搪塞用户，并在一段时间后不回应或拉黑用户。

“这种POS机可能在硬件中植入了木马，用户的数据安全也无法保证。”王德怡表示，建议消费者不要贪图小利而忽视自身数据的安全性。

记者注意到，已有开店宝、国通星驿等多家POS机厂商发布公告对消费者作出提示。“近期，有不法分子冒充品牌支付机构客服人员，通过电话形式，以免费更换低费率POS机、免费寄送新款POS机等欺诈信息，诱导用户更换终端设备，并随意扣取费用，导致用户资金受损。”上述公司皆声明，公司未通过短信或电话等形式进行终端更换等活动，将对相关信息及线索排查到底，涉嫌违法犯罪的，将上报监管机构处理。

易观分析金融行业高级咨询顾问苏筱芮同时指出，不法分子冒充品牌支付机构客服人员，通过电话形式，发布免费更换低费率POS机、免费寄送新款POS机等欺诈信息，对于用户来说是一种权益的侵害。不法分子正是利用用户与POS机厂商的信息差，企图浑水摸鱼进而牟利。对于厂商来说，应当通过下游渠道及时将此类欺诈信息传达至终端用户，避免其因为轻信所谓的客服电话而上当受骗；而对于用户来说，则应当在核实来电是否为正规厂商的同时，与原有的收单服务渠道及相关人员再次进行核实确认，不轻易使用来源不明的收单设备。据《北京商报》

安全大讲堂

“拟声”“换脸” 小心AI新型诈骗

当前，AI技术的广泛应用为社会公众提供了个性化、智能化的信息服务，也给网络诈骗带来可乘之机。如不法分子通过面部替换、语音合成等方式，制作虚假图像、音频、视频，仿冒他人身份实施诈骗，侵害消费者合法权益。国家金融监督管理总局发布消费者权益保护风险提示，提醒广大金融消费者警惕新型诈骗手段，维护个人及家庭财产安全。

利用AI新型技术实施诈骗主要有“拟声”“换脸”两种手段，即通过模拟他人声音或形象骗取信任，进而诈骗钱财。不法分子通常先以“网店客服”“营销推广”“招聘兼职”“婚恋交友”等为借口，通过微信、QQ、电话等方式联系消费者，采集发音、语句或面部信息。再利用“拟声”“换脸”等技术合成消费者虚假音频或视频、图像，以借钱、投资、紧急救助等借口诱导其亲友转账汇款，或提供银行账户密码等敏感信息，随后立即转移资金。此外，不法分子还可能对明星、专家、官员等音视频进行人工合成，假借其身份传播虚假消息，从而实现诈骗目的。

此类诈骗手段迷惑性、隐蔽性较强，诈骗金额较高，为保护广大金融消费者合法权益，国家金融监督管理总局提示：

网络渠道“眼见不一定为实” “拟声”“换脸”等合成技术的一大特点即“以假乱真”，不法分子可利用此类技术轻易伪装成他人，并通过快速筛选目标人群、定制化诈骗脚本，精准实施诈骗。因此，在涉及资金往来时，一个“声音很熟的电话”、一段“貌似熟人的视频”都可能是不法分子的诈骗套路，消费者应提高警惕。

转账汇款务必核验对方身份 面对自称“熟人”“领导”等通过社交软件、电话等以各种理由诱导汇款，务必核验对方身份。如可在沟通过程中提问仅双方知晓的问题，也可利用其他通讯方式或见面核实，或向对方的朋友、家人阐明身份和情况。在无法确认对方身份时，应尽量避免转账操作。

保护好照片、声音等个人信息 消费者应提高个人信息保护意识，不随意下载陌生软件、注册陌生平台或添加陌生好友，对个人社交账户的安全状况保持警惕。尽量避免在互联网过多暴露个人照片、声音、视频等信息，不贪图方便把身份证、银行卡的照片等直接存放在手机内。如不慎被骗或遇可疑情形，应注意保存证据并立即向当地公安机关报案。

据《中国消费者报》