手机支付扫一扫？小心躲起来的“假老板”

今日女报 / 凤网记者 陈炜

扫扫二维码，轻松支付——可是，支付二维码带来的财产风险你了解吗？

近日，一段“手机二维码支付被盗刷”的测试小视频被新浪微博推上热搜。视频中，不少消费者在超市排队等待付款时，并没有面对面的扫码过程，却都被“刷”走了一笔钱，并且收款方不是超市。

在A商店消费，却被B“商店”刷走了钱，到底谁才是消费者应该埋单的“真老板”？先别慌！让今日女报/凤网记者带你去湖南（长沙）反电诈中心找寻答案！

■热点回顾

民警也中招：饭店排队买单，钱却不翼而飞

近日，山西晋城市沁水县的郭先生在一家在饭店吃完饭，他走到收银台打开手机上的收付款二维码，准备结账。这时，奇怪的事情发生了——还没轮到郭先生付钱，郭先生的支付宝和短信同时接到了扣款通知，扣款金额是999元，收款方是一家台球休闲会馆。

郭先生人还在饭店，怎么可能分身去台球馆消费？

郭先生是一名警察，他立即要求查看饭店监控。在监控中看到，在郭先生等待付款的时候，身后有一名男子拿自己的手机对着郭先生的二维码拍照后迅速离开。这名盗刷郭先生二维码的男子买某之后被警方抓获。

犯罪嫌疑人是如何通过悄悄盗刷消费者的钱呢？今年3月，新浪微博博主@钱局长本人上传的一个测试小视频就来了个大揭秘。

视频拍摄地址选在人流密集的超市里。一些顾客在排队过程中却奇怪发现手机微微一震，再一看，支付宝或微信提醒“已经扣款成功”，少则数百元，多达上万元，而收款方并非超市。

原来，视频中盗刷客户钱款的测验员靠一款名为“钱方好近商户”的手机软件“作案”，通过提交姓名、联系电话、店铺名称以及店铺地址等信息，待审核通过后，在1个工作日内成为APP的入驻商户。之后，通过APP中自带的“立即扫码收款”功能，让手机变身为“扫码枪”。也就是说，只要排队等候付款的顾客提前打开付款二维码，就有可能被“作案者”盗刷。

视频中还显示，即便测验员没有靠近顾客，只在超市隐蔽角落安装一台摄影设备，通过偷拍付款码，也可在短时间内扫描，同样能盗刷顾客手机中的钱款。

■追踪调查

不让“假老板”坑钱，软件公司正把关

“我们确实了解到，有不少入驻商户非法利用软件中的扫码收款功能盗刷他人钱款。”3月26日，今日女报/凤网记者联系上“钱方好近商户”软件客服人员，“我们公司现在已经加强了入驻商户审核系统，并进一步完善风险控制系统”。

该客服人员表示，如今，入驻商户必须提交真实信息资料，待后台严格审核通过后，才向其开通“立即扫码收款”等权限。如果商户利用该功能非法盗刷他人钱款，公司接到举报并核实情况后，会第一时间向警方提供该商户的信息资料，配合办案。

此外，为保障受害人被盗刷的财产安全，公司采用了“T+1到账”模式。也就是说，商户非法盗刷他人钱款后，即便APP中显示“已收款”，但钱款也要在第二个工作日才能转至商户绑定的银行账户，给消费者留下了反应处理的时间。

该客服人员提醒，市民在购物付款时，不要过早地打开付款码页面，当自己结账时再打开，这样能防止被不法分子悄悄靠近后盗刷钱款。

■话题延伸

4月3日，今日女报/凤网记者从长沙市公安局了解到，2018年，“96110反电信网络诈骗专线”接到相关报警15000余起，成功止付银行卡数3400余张，止付、劝阻金额共计1.2亿元。那么，除了利用APP盗刷他人钱财，还有哪些新招需要消费者高度警惕呢？咱们一起去看看吧！

公共场合蹭Wi-Fi，反被“蹭”走1000元

长沙市民刘妮（化名）一直有蹭Wi-Fi上网的习惯。2018年6月，她在逛街休息期间，搜索并链接了一个不用密码就能直接登录的公共Wi-Fi。谁知，1小时后，她突然收到一条长沙银行发来的信息，其网银账号已经被人转走1000元。

银行卡在身上，怎么会莫名给别人转账？刘妮第一时间赶到距离最近的长沙银行鑫泰支行ATM机上查询，结果显示：“确实已转账1000元。”

反击要点 >>

提高警惕别乱“蹭”

“像刘妮一样被盗刷的情况很多，我们为防止钱款被再次盗刷，通常会协助对方办理银行账户止付业务，并申请账户冻结。”长沙银行鑫泰支行大堂经理阮丽霞告诉今日女报记者，银行工作人员将会带客户去ATM机上打印凭条，以便证明发生盗刷时，银行卡与客户在一起，不可能同一时间或极短时间内发生远距离刷卡消费。

“尽管这笔盗刷费用无法追回，但通过这一系列行为能及时止付，并将相关证据交付警方配合破案。”阮丽霞提醒，市民链接没有密码的网络，会增加误连“钓鱼Wi-Fi热点”的几率。如果非要使用公共Wi-Fi资源，一定要仔细核对用户名。另外，在网络环境下使用网银、手机银行时，应仔细看清网站来源，尽量不要在来源不明的Wi-Fi网络上操作网银，最好是使用银行发布的官方手机银行客户端。这样，比用浏览器登录网银更安全。

网购“POS机”，“隔空盗刷”银行卡

2018年10月，长沙市民张先生在陪妻子逛街时，突然收到了一则消费提醒短信——银行卡和手机都随身携带，未曾消费，怎么突然就被扣钱了？

很快，张先生赶到银行查询发现，被盗刷的1500元钱竟是在一台pos机上进行消费，而终端编号显示为长沙市一家服装店，但长沙市工商局却查不到这家店的注册信息。于是，张先生报了警，并向湖南（长沙）反电诈中心投诉举报。

原来，张先生办理的银行卡带有闪付功能，并支持小额免密免签支付。这意味着他在消费时无需输入密码，也不用本人签字，只需要将卡片靠近POS机就能迅速完成交易。结果，不法分子通过在网上购买到支持银联免密支付的POS机后，趁张先生逛街时疏于防范，遂靠近他并用POS盗刷其钱款。

反击要点 >>

免密支付别乱开

湖南（长沙）反电诈中心民警翟安告诉今日女报/凤网记者，犯罪嫌疑人通过POS机进行“隔空盗刷”需满足一定的条件——首先，受害人的银行卡需具备闪付功能；其次，受害人的银行卡开通了小额免密支付功能；最后是犯罪嫌疑人使用的POS机距离该银行卡比较近。

“很多受害人并不知道自己的银行卡开通了小额免密支付功能。”翟安提醒，如若无法保证银行卡的安全，尽可能要关闭免密功能。出于安全考虑，市民应在手机上设置锁屏与开机密码，有指纹密码功能的手机应开启指纹功能等。

另外，手机作为私人物品，应减少外借，并妥善保管手机与个人信息，切勿将身份证，银行卡等照片存入手机相册中。一旦发现手机丢失，要及时报警，并及时冻结关联银行卡、信用卡。

一觉醒来存款没了，原是“短信拦截”作祟

据《长沙晚报》报道，2018年8月5日，宁乡市公安局玉潭派出所接到群众报警：早晨起床后，发现手机在半夜收到多条验证码和银行扣款短信，银行卡莫名被盗刷，损失在数千元至数万元不等。

办案民警走访侦查发现，与以往的盗窃案件不同，嫌疑人不需要与受害人接触，而是在受害人完全不知情的情况下，盗取了受害人手机验证码等信息，然后对银行卡进行盗刷犯罪。

经过10多天的案件攻坚，专案组民警锁定湘西籍男子符某有重大作案嫌疑。随即，专案组在开福区某宾馆内将正在作案的符某抓获，当场缴获“短信拦截”设备2台、作案电脑2台、银行卡12张、他人身份证10张、电话卡13张、涉案资金12万余元。

反击要点 >>

4G网络更安全

“嫌疑人作案手法刁钻，分为三个步骤。”宁乡市公安局玉潭派出所办案民警介绍，第一步，用“短信拦截”设备采集手机号码。符某会寻找人流密集的居民小区，然后入住附近的小旅馆或者短租房，启动设备，以获取更多的手机号码及验证码；第二步，获取身份证及银行卡信息。符某获得手机号码后，通过网络上的“黑色渠道”购买与手机号码对应的银行卡号及身份证号码；第三步，实施联合盗刷，洗钱提现。符某将获得的银行卡账号、身份证号码、手机号码及验证码发送给“黑色渠道”，“黑色渠道”利用事主的银行卡在各大电商平台购买话费、充值油卡等，交由专门负责洗钱的团伙成员“销售”提现，再返点给符某。

民警提醒，犯罪分子的黑科技手法似乎让人防不胜防，但也不必过分恐慌。警方侦查发现，2G网络下的手机更容易被盗刷，4G网络的安全性能更高，所以尽可能不要为了省流量关掉4G。