

移动支付覆盖合肥大小商超,支付安全成最大隐患

别慌刷手机,请先看看这篇报道



□ 记者 祝亮

细心的市民会发现,近期在合肥许多商场和超市的收银台,移动支付已经成为一种潮流。使用微信或支付宝扫码支付,已经成为许多市民,除现金支付、银行卡支付以外的第三大选择。越来越多的商场超市、餐饮酒店、交通工具支持移动支付,意味着:市民出行只需带上手机就能完成一路支付。日前,某网站进行的一项调查显示,9成受访合肥市民都使用过移动支付,但也有相同比例的市民对手机支付带来的安全隐患表示担忧……

现状:移动支付遍布合肥商场超市

几年前开始,移动支付在网上交易中早已被广泛使用,用手机网购早已不再是新闻。自去年开始,移动支付方式就开始出现在合肥的一些商场。今年4月底,支付宝钱包宣布与家乐福和华润万家达成合作关系。6月下旬开始,合肥家乐福门店基本都实现了支付宝支付。除了家乐福,永辉超市、苏果超市、红府超市也同样都支持微信或支付宝支付。

在合肥万达广场、新地中心、华润五彩城、银泰城等综合商业中心,涵盖餐饮、服饰、百货的多家商店均支持移动支付。连肯德

基、必胜客、DQ等知名连锁店也纷纷借移动支付的“东风”。还有一些商场的停车场车费也支持移动支付。团购、优惠买单等手机APP让合肥多数餐馆饭店都能移动支付。

在出行方面,网络约车都可以使用移动支付,机票、火车票、长途汽车票均已实现移动支付……

现在,市民出行只需要带上自己的手机,就可以享受到各种便捷的服务。移动支付已经遍布合肥各商业领域,正在悄然颠覆传统的货币交易方式。

体验:整个支付过程不到半分钟

昨日下午,市场星报、安徽财经网记者来到位于合肥市桐城路的红府超市尝试移动支付。记者在店内挑选了几样物品,便来到收银台结算。在收银台醒目位置,也有标识提示消费者可用支付宝支付以及微信钱包支付。

在收银员指导下,记者打开支付宝钱包,点击“付款”,便出现了一个条码和二维码为一体的付款码。收银员用扫描枪对着付款码

扫了一下,只听“滴”的一声,手机界面显示出“支付成功”及支付金额,无需输入密码。点击“完成”后,支付宝会自动显示出商品信息、交易单号、交易时间、付款方式及交易状态等信息,耗时不到半分钟。

同样,记者也在位于合肥市祁门路的永辉超市体验了微信支付。整个支付过程也是不到半分钟。

背后:支付宝、微信烧钱抢市场

市场星报、安徽财经网记者采访中了解到,支付宝和微信支付在年轻人的圈子颇受好评。为了在合肥市抢占商超支付市场,支付宝、微信可谓煞费苦心,自登录线下以来就不断开展烧钱让利活动。

据了解,支付宝将每个月的28日定为“支付宝日”,只要是在这一天使用支付宝进

行支付,就可以享受“支付宝价”。在合肥,包括华润万家、家乐福、屈臣氏等知名连锁超市或便利店,用户在“支付宝日”使用支付宝支付,就能享受到超市购物8折,10元封顶的优惠。除了支付宝,微信也大打优惠牌,近期,某超市就推出“微信支付立减5元再送5元”的优惠项目。

调查:9成受访市民使用过移动支付

日前,某知名网站对合肥地区移动支付使用现状进行问卷调查,受访对象以在职群体为主,调查结果显示,93%的受访对象使用过移动支付;73%的受访对象坚信移动支付很快可以取代现金、银行卡等应用到所有货币结算领域;充值话费、购物、银行业务等成为移动支付的主要目的;80%受访对象在

使用第三方支付;超过9成的受访对象认为方便快捷是选择移动支付的主要原因。

合肥市民贾小姐接受记者采访时说:“不用再担心没有零钱,被找好多零钱,不用再担心会收到假币,现金用完了也不着急去银行了……现在习惯手机购物能给自己省很多时间,少很多麻烦。”

担忧:

市民担忧手机支付安全隐患

当然,一个新事物有它的便利性,自然也会有弊端。在问卷调查中,88%的受访对象认为移动支付安全机制不健全,交易风险高,另外个人隐私也可能面临威胁。

合肥市民汪先生说:“现在智能手机确实给我们带来了很大便利,但风险并存。比如说,捆绑了自己银行账户的手机丢失了怎么办?就算钱没被盗走,个人信息也会面临泄露;网上每天还有各种各样的病毒软件,诈骗信息时时刻刻在威胁我们的账户安全,有的时候真的是防不胜防。”

支招:

指纹支付比常规密码更安全

互联网安全专家表示,除了看好手机,不随意丢弃或转卖手机之外,喜欢用手机网购的“剁手党”更应该养成科学使用手机的习惯。

“指纹识别支付较传统密码具备更加可靠的安全性,目前在我国尚无被破解的案例。而且现在越来越多的智能手机开始引入指纹识别功能,不再是苹果手机专利,千元级国产智能手机魅蓝metal等也具备指纹识别功能。因此,使用移动支付时,有条件的尽量开启指纹识别。”

专家告诉记者,“此外,要通过正规渠道购买手机,不少二手手机、水货机有可能事先已经植入木马病毒,以便窃取手机支付账号等信息,然后进一步盗走账号里的财物;设置登录密码和支付密码时,尽量不要重复,同时也不要使用出生日期、手机号码等‘显性’信息做密码。”

“再就是手机操作系统也要经常更新,例如最新版的Flyme操作系统,就可以将支付安全功能接入阿里的安全模块,它能使每一个支付相关应用的进程都变为隐形状态,可以从根源上阻断支付账户的风险,让每一笔交易都在最安全的环境下完成。”

常见手机支付隐患

虚假WIFI

很多持卡人习惯于用手机购物、转账、汇款,不法分子利用持卡人支付习惯,专门在一些购物中心、休闲场所建立免费的虚假WIFI,不明真相的消费者一旦连接其个人信息就有泄露的风险。如果持卡人进行移动支付、网银转账等敏感操作,黑客可通过后台程序记录下上网者的手机IP地址和信息,其用于支付的卡号和密码就有被盗取的可能。

病毒“二维码”

近年来,携带木马病毒的二维码也成为了骗子套取信息的新方式,有时不小心的扫一扫,就有可能带来被盗刷的风险。据了解,不法分子在网上下载一款“二维码生成器”,再将病毒程序的网址粘贴到二维码生成器上,就可以生成一个“有毒”的二维码。诈骗分子会利用这些二维码将手机木马植入被害人手机并自动提取相关信息,几秒钟时间,手机号、卡号、密码等私人信息可能已传到他人手中。

钓鱼网站

这是近年来较为常见的一种窃取信用卡信息的方式,不法分子会使用“改号器”软件把电话号码“伪装”成银行的客服号码,再利用流动伪基站,发送诈骗信息,引诱受害人登录其设计好的足以以假乱真的假冒银行网站,一旦受害人在这个网站输入账户和密码等关键信息,信息就会被不法分子所得,再利用这些信息通过网络把账户资金转走。