网上支付爆发式增长，去年支付宝全民账单中移动支付占65%

移动支付，便利中藏风险

新闻聚焦

本报记者 王晓峰
通讯员 朱君敏 黄一娇

网上购物，菜场买菜，逛超市，用支付宝或微信扫一扫二维码就能买单了。智能手机时代，移动支付成了不少人生活中不可或缺的一部分。虽然生活因此便利了不少，但随之带来的风险也不得不引起重视。如今，各种利用移动支付漏洞的网络诈骗花样频出，让人防不慎防。

今年1月13日，腾讯发布了《移动支付网络黑色产业链研究报告》，报告内容显示去年我国的移动支付在蓬勃发展的同时，面临着安全能力参差不齐的现状；大量虚假手机号成为诈骗分子主要作案工具；用户安全意识偏低给不法分子可乘之机；不法分子窃取用户隐私信息以后进行精准诈骗和恶意营销的事件频发。

如何确保移动支付用得安全又放心？民警表示，市民常常忽视的一些小问题其实很致命，使用移动支付要具备一定的安全“常识”。

庄豪 绘

移动支付成诈骗“新领地”

支付宝盗号“木马”、假冒支付宝页面、利用支付宝手机校验功能……不法分子变着花样进行诈骗。这不，最近又有市民被不法分子利用支付宝新的“借条”功能给坑了。

前些天，家住鄞州钟公庙街道的小王在网吧玩游戏，玩到正嗨时发现游戏账号里没钱了，无法购买相关虚拟商品。小王本想通过网银直接购买，但考虑到网吧里的网络不安全，加上网银U盾落在家里，于是想着用支付宝付款，但账户里面的钱不够用。

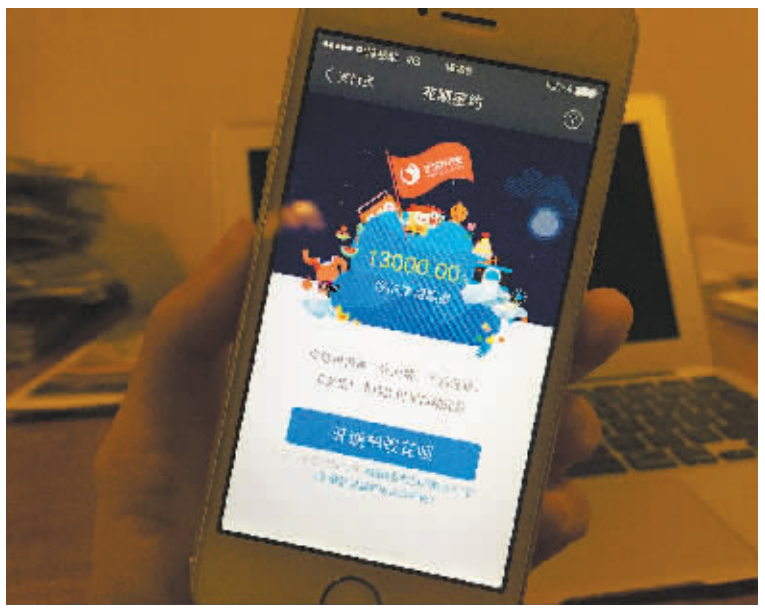
作为资深的“手机控”，小王立马想到了此前在微信上面看到的网络小额借款信息。他按照上面留下的联系方式加了对方为好友，并商讨借款事宜。对方却“建议”他通过支付宝最新的“借条”功能来借款，称使用第三方支付平台才能让双方都放心。

得知小王支付宝内还有几百元钱后，对方就让他通过“借条”功能先转些利息过去。在对方提示下，小王在与其聊天的窗口中，点击下方“+”内的“借条”选项，输入金额并点击确认一周还款，即完成借款操作。打完“借条”后，小王就发现对方把自己拉黑了，无论怎么发消息都发送不出去，对方承诺的千元借款也没有转账到位，自己反而损失了几百元。这时小王才发现自己是遭遇骗子了。由于“借条”已经发出去了，他担心若逾期不打款给对方，会影响自己的信用额度。若打给了对方，只能是“肉包子打狗，有去无回”，小王为此纠结不已。

“本是为了网络交易的安全考虑，第三方支付平台才因此兴起。然而，第三方平台却被不法分子设局利用，越来越不安全，诈骗花样频出。”民警说。

家住象山泗洲头镇的晏女士在朋友的帮助下开通了网上淘宝店。按照相关规定，她与淘宝方面签订了消费者保障协议，并交纳了1000元保证金，冻结在支付宝账户中。去年11月3日晚上，有个“买家”通过阿里旺旺联系了她，称拍下的商品无法付款，让晏女士提供QQ号。随后，一个名为“阿里巴巴客服”的QQ号添加了她，并告诉她新开张的店铺还没有激活保证金，所以有些功能没法开通，导致顾客网购时遇到各种问题。在该“客服”的远程指导下，晏女士毫无怀疑地把钱转给了对方，直到后来迟迟没有回音时，她才意识到自己被骗了。

庄豪 绘



移动支付在日常生活中的使用日益频繁。

此外，利用信用卡套现的骗局，如今也有了“网络版本”，即不法分子利用支付宝推出的“蚂蚁花呗”功能来实施作案。“蚂蚁花呗”是蚂蚁微贷为消费者打造的一款“先买后付款”的网络赊购服务，用户开通后可免费使用“蚂蚁花呗”的消费额度购物，且确认收货后次月再还款。这本是一项为方便消费者而推出的新服务，却被一些不法商家利用，我市警方就曾接到多起此类报案。最为典型的是去年10月21日，家住象山丹城的金女士在微信朋友圈看到了一条关于“蚂蚁花呗”套现的信息，随后就找对方“交易”。最终的结局是点击不明链接，被“消费”了5000元。

背后存“黑色产业链”

随着移动支付市场的不断扩大，一些不法分子逐渐将黑手伸向这些用户。“移动支付的安全问题正在日益凸显，如今这类犯罪更加往高技术化、综合复杂化以及多平台联合使用方向发展。”民警说，其作案手段专业化、团伙化，通过网络的联系，甚至一些素未谋面的犯罪分子开始分工协作，逐渐形成了黑色产业链，使得作案成本更低，打击难度更大。

用户的个人信息是多种网络犯罪手法所需的核心要素，犯罪团伙一旦掌握，就可以根据这些信息进行实时、精准的欺诈和敲诈。从我市目前破获的案件来看，犯罪团伙具有很强的区域聚集性，且主要为年龄介于15岁至25岁之间的无业年轻人。他们对于移动互联网更为熟悉，敏锐地察觉到了其中的敛财机会。

去年我市发生的几起较大的通讯（网络）诈骗案，都有“联合”作案的意味。不法分子先通过伪基站伪装成正规单位并发送“钓鱼”或者含有木马程序的短信。等受害人点击短信里附带的网址链接后，要么被转接到“山寨”网站，要么被植入木马程序，手机内的各种信息随即被盗，然而整个过程用户毫无感知。

前不久腾讯首度发布的《移动支付网络黑色产业链研究报告》也证明了这一点。该《报告》显示，2015年新增的支付类病毒超过32.6万，全年被支付类病毒感染的用户高达2505万。同时，在移动支付安全领域，受骗群体以男性为主，占71%，女性只占29%；受骗年龄则集中在19岁至35岁的青年群体。而且，南方地区的网络诈骗情况尤为严重，资金受损最严重的十个城市中有八个在南方。

此外，用户安全意识低，也给了不法分子可乘之机。据悉，目前有超七成的手机用户存在多账号使用同一个密码的问题。2015年10月，国家网络安全宣传周在启动仪式上曾发布了《我国公众网络安全意识调查报告（2015）》，称在25万多的调查者当中，定期更换密码的被调查者仅占18.36%，更有17.05%的被调查者从来不更换密码。

前不久，北仑就有这样一个案例，受害人曾委托犯罪嫌疑人李某办理小额贷款，为办理方便，还将自己在网上注册的平安易险小额贷款账号和密码告诉了对方。后来，李某在电脑上登录“查找苹果”的网站，抱着试试看的想法，输入了受害人的QQ邮箱，之后又输入了她告知的小额贷款账号的密码，竟然成功登录了。原来该受害人的QQ、微信、支付宝、银行卡等所有账号用的是同一个密码。

养成良好支付习惯防被骗

手机已成为大家日常使用频繁的“电子钱包”，但面临着日益严峻的“移动支付”犯罪，大家应该提高警惕。民警提醒，使用移动支付要养成良好的习惯，具备一定的安全“常识”。

首先说使用手机支付的安全常识。用户请给手机设置开机密码，但千万不要用生日这类易被猜到的数字。民警建议大家将密码设置得独一无二，最好用数字和字母组合，增加破解难度。同时，手机不要频繁刷机，目前最容易被木马入侵并出事的就是“越狱”过的手机。此外，安装手机应用软件时应注意其来源及风险，有些软件是自带“后门”程序的，用户的隐私信息不少就是通过这类途径泄漏出去的，因此请尽量在官方应用商店下载应用软件。

其次说如何确保移动支付平台的安全。同时，将支付工具进行实名认证，绑定身份证，防止手机丢失后被恶意找回密码；关闭支付工具的小额免密支付功能，设定消费限额，避免更大损失；安装密码安全控件，对密码进行加密；设置安全保护问题；申请安全证书，使用U盾、数字证书、手机动态口令等安全必备产品。

此外，大家在手机上登录支付平台时，使用后一定要记得取消“记住用户名”“十天内自动登录”等设置。去年“双十一”，鄞州邱隘一男子丢失手机后，由于该丢失的手机破旧不值钱，他便没多想，“丢了也就丢了”。谁料该手机被人捡到后，对方登录其手机上的淘宝，然后改了他的收货地址，最后网购的东西被别人收了货。

手机丢了，绑定的支付宝、微信怎么办？民警提醒一定要赶紧处理，先致电手机运营商挂失SIM卡，电信是10000，移动是10086，联通是10010；之后拨打95188报案，解绑支付宝，冻结支付宝；登录http：//110.qq.com/冻结微信账号；最后致电银行客服，冻结网银、手机银行。

最后，旧手机处置要谨慎。据悉，目前已经证实，多数旧手机已删除信息可通过软件恢复。旧手机如处理不当，落在不法分子手里，很有可能被其利用，进而成为犯罪工具。

新闻背后的热词

移动支付

2015年是我国移动支付大发展的一年，智能手机用户数量也飞速地增加，移动互联网的普及也极大地促进了移动支付的蓬勃发展。根据央行发布的2015年第三季度支付业务统计数据，第三季度全国银行机构共处理移动支付业务45.42亿笔，金额18.17万亿元，同比分别增长253.69%和194.86%。

移动支付是指消费者通过移动终端对所消费的商品或服务进行账务支付的一种支付方式。客户通过移动设备、互联网或者近距离传感直接或间接向银行金融企业发送支付指令产生货币支付和资金转移，实现资金的移动支付，实现了终端设备、互联网、应用提供商以及金融机构的融合，完成货币支付、缴费等金融业务。

如今，没带钱包，衣食住行、吃喝玩乐照样不受影响，消费时用手机扫一扫二维码就可以轻松搞定，移动支付已经渗透到我们生活中的方方面面。移动支付不仅改变了传统的支付手段，也深刻地改变了公众的消费模式。前不久，支付宝发布了2015年全民账单，数据显示移动支付笔数的占比为65%，比去年增长了15.8个百分点。

随着移动支付的风起云涌，病毒感染、手机漏洞以及诈骗短信等因素给用户带来了严重的安全隐患。根据腾讯手机管家统计数据，2015年手机病毒感染终端数量达7490万次。

数 说

制图：金雅男

相关链接

遭遇通讯（网络）诈骗后如何自救止损

涉及“移动支付”的犯罪，说到底也是通讯（网络）诈骗犯罪中的一部分。那么一旦发生了，受害人想要挽回损失，又该如何处理？民警说，一定要记得“抢”时间，在骗子将你的钱转走之前，这段时间就是止损的“黄金时间”。

首先受害人一定要记住对方的银行账号，这是问题的关键，然后可以尝试这两种办法来临时冻结骗子的银行账户。第一，尝试电话银行冻结。即拨打该诈骗账号归属银行的客服电话，根据语音提示输入该诈骗账号，重复输错五次密码使该诈骗账号冻结止付，时限为24小时。若被骗大额资金的话，在接报案件后的次日零时后再重复上述操作，则可以继续冻结止付24小时。第二，通过网上银行冻结。即登录该诈骗账号归属银行的网址，进入“网上银行”界面输入该诈骗账号，然后重复输错五次密码就能使该诈骗账号临时冻结了，时限也为24小时。

在自救止损的同时，也请记得第一时间报警，警方会通过“通讯（网络）诈骗快速接警和止损流程”尽最大的可能帮受害人挽回损失。