**开通手机银行前必须知道的事**





360公司联合包括新闻晨报在内的中国手机反骚扰反欺诈联盟，以及中国支付清算协会等共同发起“支付安全＋”行动，并发布了《2015中国移动支付安全绿皮书》（以下简称《绿皮书》）。



　　《绿皮书》透露，在今年一季度中，支付购物类恶意程序达到1147个。最近随着股市利好，大智慧、同花顺等APP也常被恶意程序盯上。

　**平均每天拦截垃圾短信1.07亿条**

360安全专家裴智勇表示，自去年中国手机反骚扰反诈骗联盟成立以来，反骚扰效果显著。今年一季度，360手机卫士共为全国用户拦截各类垃圾短信约96.9亿条，较2014年第一季度同比下降53.6%，较2014年第四季度环比下降21.9%，平均每天拦截垃圾短信1.07亿条。在所有垃圾短信中，诈骗短信占12.1%。而在诈骗短信中，冒充熟人的最多，占28.5%，其次是虚假中奖占25.6%，冒充银行占19.9%。



    不过手机诈骗形势仍旧严峻，2015年1—3月，360互联网安全中心共接到网络诈骗报案4920例，报案总金额高达1772.3万元，人均损失3602元。其中，360手机用户报案1147例，报案总金额为831.8万元，人均损失7252元；　电脑用户报案3773例，报案总金额为940.5万元，人均损失2493元。可见，尽管目前手机用户的报案数量还不及电脑用户多，用户遭遇手机诈骗时的人均损失却为电脑诈骗人均损失的2倍。



    从手机用户的报案类型上看，虚假中奖数量最多，占22.2%，其次是钓鱼盗号占18.5%，虚假兼职占12.8%。根据用户报案材料的描述分析统计，用户遭遇诈骗的首要途径是诈骗短信，占比53.8%排在首位，其次是钓鱼网站32.3%，诈骗电话12.7%，木马病毒仅占1.2%。而在不同类型手机欺诈的人均损失排名中，虚假中奖、钓鱼票务排在前两位，人均损失分别为14148、11651元，此外，欺诈博彩8252元、伪基站7151元、冒充他人6993元分列其后。



　　**农行掌上银行等4款应用被篡改最多**

    伴随着移动支付技术深入人心，不少不法分子将诈骗由PC 端移至移动端。《绿皮书》显示，今年一季度，360共截获假冒或篡改各类移动支付及购物程序的恶意程序1147个。尽管此类木马的数量并不算大，但由于极具迷惑性，普通用户很难识别，用户手机一旦感染这些木马，就将会面临短信劫持、资金劫持、账号被窃及网银盗刷等一系列巨大风险，最终造成重大经济损失。



　　从恶意程序的制作方式上看，此类恶意程序主要可以分为两大类别：一种是篡改特定官方客户端程序并植入恶意插件的篡改类木马；一种是纯粹假冒其他应用程序的假冒类木马。在这1147个篡改恶意程序中，篡改类木马共有795个，占比为69.3%，假冒类木马共有352个，占比为30.7%。

　　在这795个篡改类恶意程序的篡改对象中：农行掌上银行最多，占比约为28.4%；其次是美团团购，占比约为21.4%；接下来的是手机淘宝和1号店，占比分别为16.9%和13.3%。针对这四款应用的篡改样本占到了篡改类恶意程序样本总量的80.0%。

    而在352个假冒类恶意程序的假冒对象中，大智慧占比最高，达到20.1%；支付宝钱包和同花顺排在二三位，占比分别为16.8%和14.8%。



    另外，近年来FakeTaobao （假淘宝）家族木马日益猖獗。监测显示，自2014年9月份以后，该木马家族的样本数量开始激增，短短半年时间里，样本总量就已经从3万多个激增到接近13万个，每月新增样本量超过一万个以上，成为目前最为广泛流行的一个移动支付类木马家族。从形态上看，该木马早期的主要形态是将自身伪装成手机淘宝客户端，但随着该木马家族样本数量的激增，木马所假冒对象也开始逐渐转变为运营商软件、合同订单表格、系统软件、照片图片以及手机银行等。



    通过对木马内容、木马签名、木马首次出现地以及其他多种大数据综合分析方法发现，Fake-Taobao木马的作者主要分布在广西、广东和北京三地，分别占比17.7％、16.4%和6.1%。分析还显示，上海是该木马使用者最多的地区之一，占比13.3%。

**移动支付安全面临恶意程序、钓鱼网站、诈骗短信和诈骗电话四大威胁**

    只因关注了一个虚假的微信公众号，用户就被诈骗了近3000元。信息安全专家表示，目前恶意程序、钓鱼网站、诈骗短信和诈骗电话是威胁移动支付安全最主要的四个因素，用户在进行网上消费，需要移动支付时一定要注意保护好自己的钱财。



    有数据显示，截至去年年底，我国网上支付用户规模超3亿，其中移动支付用户超过2亿，庞大的市场规模吸引黑客盯上了移动支付。2015年第一季度，360互联网安全中心共截获安卓移动平台新增病毒409万个，比2014年全年截获的新增病毒量还多83万个。



**案例：**

**扫二维码扣近三千元**

    广州的赵利是手机游戏“太×熊猫”的热心玩家。2015年4月，他在微信上搜索“太×熊猫”时，看到一个名为“太×熊猫限量礼包”的公众号，于是就添加关注了这个微信公众号，随后他看到该公众号有充值兑换的优惠活动信息，就在活动界面购买了968元的套餐产品。付款后，从收款的消息界面上可以看到，共有8个人参与了这个活动，总共付款7744元。



　　刚完成付款没多久，一个自称是客服的名为kefu568的微信号联系了赵利，称其购买的商品出现了问题，资金已被冻结，需要给赵利退款，并提供了两种解决方案，一个是再付一次款，这样前一次的付款就会自动退回，另一种方法是等9~10个工作日后到银行去办理退款手续。

　　由于这两个方法都很难接受，赵利继续和这个客服号沟通，最后kefu568给其发了一个二维码，要其扫描这个二维码即可以完成退款，但当赵利扫描了这个二维码后，账户中又被转走了968元，收款人为“李传×”。

　　赵利立即向kefu568询问是怎么回事，对方表示可能还是交易异常，请他再扫一次二维码。结果扫过二维码后，又被扣款968元。而且kefu568劝说赵利，要解除异常，就必须继续充值或扫描二维码退款。

　　赵利此时才感觉不妙，拒绝继续操作。kefu568称，72小时后钱会自动退款到赵利网银账户。次日，赵利再次询问kefu568自己的钱什么时候能退，对方则继续劝其等待。又过了半天，kefu568已经联系不上了，而“太×熊猫限量礼包”的公众账号也找不到了。

**数据：短信诈骗冒充熟人的最多**

　　在中国手机反骚扰反欺诈联盟成立一周年之际，昨日360公司联合中国支付清算协会以及20余家国内O2O厂商、电商、支付厂商共同发起“支付安全+”行动。信息安全专家表示，目前恶意程序、钓鱼网站、诈骗短信和诈骗电话是威胁移动支付安全最主要的四个因素。

    而据媒体披露，从去年年底到今年年初，全国各地爆出了伪基站假冒运营商客服号码发来的积分兑换现金的短信，不少用户上当并损失钱财。



　　除了恶意程序之外，2015年第一季度，360手机卫士统计显示，共为用户拦截钓鱼网站攻击3.3亿次，占钓鱼网站总拦截量的5.5%。预计到2015年底，钓鱼网站对手机用户的攻击量可能会超过钓鱼网站攻击总量的10%。

　　同时，2015年第一季度，全国用户拦截各类垃圾短信约96.9亿条，其中诈骗短信占12.1%，冒充熟人的最多，占28.5%；其次是虚假中奖占25.6%，冒充银行占19.9%。

**支招：**

**使用移动支付防骗**

　　信息安全专家提醒用户应注意不要扫描陌生人从聊天工具中发来的二维码；在向微信公众账号付款前，先联系官方客服进行确认；由于有伪基站技术的存在，即便是自己熟悉的客服号码发来的短信也需要电话确认；当有人告诉你交易存在异常时，应直接登录电商网站并查询自己账户的状态；定期修改购物账号的密码