半年网购诈骗案过万起 每万名网购者中就有一人“中招”

网购诈骗来势汹汹

如今网购已经成为人们主流的消费方式，而木马犯罪产业也大规模“转行”，把攻击重心从游戏盗号放在了网购消费者身上，利用钓鱼网站结合电话诈骗、木马劫持等方式盗取网购资金。

据360互联网安全中心最新发布的《2014年上半年中国网购安全报告》（下文简称《报告》）基于大数据统计分析，今年上半年，360网购先赔服务共接到网络欺诈报案约1.3万例，占开启网购先赔服务用户的比例接近万分之一。这意味着，每一万名网购消费者中，就会有一个人实际遭遇到网购损失。尽管万分之一的比例很低，但由于国内网购用户基数庞大，再加上部分“裸奔”用户更容易被钓鱼网站和木马侵害，网购安全威胁仍不容忽视。而在网购受害人群中，90后的比例达到59.8%，男性的比例更是高达63.2%。在诈骗形式上，P2P网贷、贵金属交易、外汇买卖等新型的互联网金融投资诈骗也日益活跃，消费者应对此予以警惕。

◆现象——

诈骗新花样层出不穷

今年5月，郑州的吉先生网购了一个充电器，不久就接到了自称是“卖家客服”的电话，对方告诉吉先生，由于系统临时维护升级，吉先生的订单失效，需要他填写退款协议办理退款。吉先生便通过QQ打开对方发来的退款链接，并按提示输入了银行卡号、密码、身份证号、手机号及短信验证码等信息。结果，本以为是办理退款，他的银行卡却被消费了3000元。

像吉先生碰到的这类以“退款”为由，实施电话混搭钓鱼诈骗的案例不在少数。《报告》显示，2014年上半年，360网购先赔收到的近1.3万例网络欺诈举报中，“退款”欺诈占到了11.2%，是仅次于网络兼职欺诈的流行骗局之一。退款欺诈受害人的人均损失高达3760元，远超过网购诈骗人均损失的总体平均值，从受害人数量、黑产值到人均损失，均排在第二位。

“画皮”网络诈骗团伙专骗“财务人员”

7月中旬，有网友通过110.qq.com向腾讯雷霆行动项目组举报，称在广西南宁市宾阳县芦圩镇发现了一个网络诈骗团伙的窝点，其中有负责实施诈骗者，还有专职取款者。网友提供了犯罪团伙详细的个人身份和社会关系链信息，腾讯雷霆行动项目组随即向警方进行了反馈。警方对其中一个被举报的窝点进行了多方打探和蹲点，随后进行突袭，将当中两名犯罪嫌疑人控制。据警方透露，在突袭时，犯罪嫌疑人还在进行网络诈骗活动。

据了解，警方查扣了作案电脑10台、手机11部、银行卡数十张、上网卡、网银口令卡及其他作案工具。值得注意的是，警方发现这些银行卡里有多宗全国各地的入账记录。通过串并案分析，警方确认他们就是多起“画皮诈骗”案的主要犯罪嫌疑人。经过查证，这两个“师徒”团伙长期协同配合，盗取一些“公司老板”以及“供应商”的社交聊天工具，然后自行伪装成这些角色诈骗“财务人员”，已查证的涉案金额超过50万元。

腾讯互联网犯罪研究中心秘书长朱劲松表示，监测数据显示，“画皮诈骗”的案件近期开始抬头，主要针对公司的财务人员和会计人员进行诈骗，而且这种手法的迷惑性非常大，一旦被骗，少则几万元，多则上百万元。

互联网金融火爆 P2P网贷欺诈猛抬头

根据Enfodesk易观智库《2014年第二季度中国P2P网贷市场监测报告》数据显示，2014年第二季度，为把握市场机遇，新进者数量增多，同时业内企业加大了市场推广力度，中国P2P网贷市场相较第一季度有明显增长，行业交易规模达381亿元，环比增长26.0%。迅猛发展的P2P网贷市场，也让不法分子看到了可乘之机。

《报告》显示，360网购先赔服务接到223例投资理财欺诈报案，在各欺诈类型中仅排第八位，但受害者人均损失却高达9533元，远超其他欺诈类型，排在榜首。其中，P2P网贷跑路事件频发，今年上半年，P2P网贷平台的受害人占各类理财诈骗的61.6%，在互联网金融诈骗中占据榜首。360安全专家刘福军指出，互联网金融风头正劲，信用卡理财、外汇买卖、P2P网贷、博彩投资等各类新型投资方式先后出现。不过，由于准入门槛低、无监管，导致P2P网贷平台野蛮生长、鱼龙混杂。仅2013年至今，已经有百余家P2P网站跑路，受害者往往难以追回资金，损失惨重。

◆趋势——

手机支付安全也堪忧

随着移动互联网的快速发展，通过移动智能终端进行网购的消费者也呈现爆发式的增长。易观最新数据显示，2014年第二季度，中国手机购物市场交易规模达1680.9亿元，同比增长256%。但是，通过手机等移动智能终端进行网购，在享受便利的同时，手机支付的安全性也成为移动购物过程中不能忽略的一个问题。

日前，腾讯移动安全实验室发布了《2014年上半年手机安全报告》（以下简称《报告》），该报告显示，Android手机病毒在经历了2012~2013年的几何式高速增长之后，在2014年上半年逐步趋于平缓，同比增长7.9%。手机支付类病毒进一步蔓延，上半年感染手机支付类病毒的用户数达到693.4万，其中可拦截并转发用户支付短信验证码的手机病毒大规模增加，支付类病毒呈现出多种特征融合化发展的趋势。

二维码传毒2年增3倍

随着二维码的流行，目前其已成为增长最快的染毒渠道，据了解，通过二维码传播的病毒传播比例已达到9%，而在2013年的全年报告中，二维码的病毒传播比例还只有7.42%，2013年上半年，该渠道占比为6%，2012年全年只有3%，占比2年翻了3倍，呈现加速上升趋势。据悉，在腾讯手机管家最新发布的5.0版中，就新增了安全扫码功能。通过安全扫码，可以有效地减少用户因扫描二维码而下载安装手机病毒、登录钓鱼网址的风险，最大限度地避免个人隐私信息泄露，保障资金账户安全。

手机安全专家解释称，二维码可以包含网址链接、安装包下载等各种内容，用户扫码后，很可能会下载一个木马病毒到手机中，然后导致用户的支付宝账号密码被盗，遭遇财产损失。此前，腾讯手机管家曾截获过名为“盗信僵尸”的手机病毒，该病毒可将中毒手机变成“肉鸡”，私自发送短信注册淘宝账号，同时可以拦截屏蔽自动回复系列支付确认短信，盗取手机支付确认验证码，窃取手机用户资费，甚至威胁支付宝账户余额。

新型伪装病毒专盗隐私

如今，小小的手机已经承载了每个用户大多数的个人资料，不仅涉及到个人隐私，同时隐私问题也直接影响到了手机购物的安全。近期，瑞星“云安全”系统拦截到一款新型Android病毒，该病毒伪装成知名社交网站“Facebook”的应用程序，引诱网民下载安装，手机一旦中毒，就会按照黑客的指定命令发送短信或拨打电话，造成巨大的资费消耗。此外，该病毒还可窃取用户的短信、联系人列表、通话记录、图片文件等隐私信息，并发送至黑客指定的地址。瑞星安全专家指出，该病毒一旦被安装，几乎无法用正常方式卸载，因此用户需特别小心。

“Facebook”病毒囊括了资费消耗和隐私监听两类病毒的特点，该病毒可接收指令，并在用户不知道的情况下让手机发送短信、拨打电话。黑客可利用该功能群发垃圾短信，并使用户手机拨打吸费号码，造成巨大的资费消耗。此外，病毒还会诱导用户激活设备管理器，使用户无法用正常方式对其进行卸载。因此，手机一旦中毒，用户将面临网银账号丢失、社交账号丢失、验证码被截取、短信及电话被监视、隐私照片遭泄露等一系列风险。

◆对策——

网购安全如何保障

面对越来越严峻的网购安全问题，互联网安全专家表示，网民的电商账户几乎成了网络身份ID，通常绑定网银快捷支付，一旦电商账户密码信息泄露，就会面临网银被盗刷的风险。对此，360安全专家刘福军建议，消费者要重视个人账号安全，定期修改密码，并使用安全浏览器的“网站名片”，识别网站的真实身份，避免在非可信网站上提交个人信息。

此外，投资者在网上搜索金融理财信息时，往往被一些“加V认证”的空壳网贷平台蒙蔽，从而使得骗子平台轻易获取投资者的信任，迅速敛财。刘福军建议，投资者要高度警惕那些宣称收益奇高、纯资金吸纳的互联网金融投资项目，并认真调查其担保投资机构的合法资质，以免落入投资陷阱。

对于越来越普遍的二维码威胁，手机安全专家提醒广大手机用户，不要见到二维码就扫，通过安全软件的的安全扫码功能，可以有效降低因扫描二维码感染病毒的概率。同时，配合安全软件的病毒查杀、钓鱼网站识别功能，可以基本上彻底远离扫码风险，避免信息泄露，最大限度保障资金账户的安全。

在手机应用也呈现出“鱼目混珠”的现象后，手机安全专家建议，广大手机用户要使用官方认可的正规渠道下载APP，谨慎授权，拒绝APP申请与自身功能无关的操作权限，安装专业的手机安全软件，定期为手机进行全面杀毒。（南方）