截至3月底，全国已认定处理了4万多个“钓鱼网站”；然而在企业管理和国家监管存在漏洞的情况下，网民网购维权越发艰难

网络购物 “钓鱼”诈骗何时休

□据 新华社

辽宁网民孙林不久前在网购平台淘宝网上以7710元的价格购买电脑时，被诈骗人员植入木马病毒，支付的货款被骗汇到诈骗人员在知名网游公司网龙公司开设的游戏账户下，随后被消费或折现。

全国像孙林这样的网民不在少数。随着互联网的迅速发展，网络购物已成为诈骗分子行骗的新领域。根据中国反“钓鱼网站”联盟发布的信息，截至2011年3月底，已认定处理了43842个“钓鱼网站”，大多集中在网购、电子商务等领域。专家认为，网购领域虽然个体金额大多较小，但涉及面广、总量大，有关部门应加强监管，为网络交易提供一个安全的环境。

1 网购“钓鱼”近期高发 数百网民被骗百万元

“3月1日下午，我在淘宝网一个卖家那里购买一部三星手机。进入支付宝付款页面点击建行网银付款时，支付宝网页突然很快地跳转到了网龙公司旗下的91充值平台。当时我也没留意，点击确定付款，进入建行付款页面，输入账号密码和U盾的支付密码后，页面跳出一行字显示支付失败，我就起了疑心。”网民董晓麦说。

董晓麦回忆：“当时，我立刻登录建行网站查了卡上余额，发现已经被扣费了，但返回淘宝账号后显示未付款。查询建行的支付记录发现，原本通过支付宝支付的金额并没有充入支付宝，而是通过即时转账转到一个在福建网龙计算机网络信息技术有限公司开设的游戏账号上。”

“我突然意识到被人‘钓鱼’了。前几天，我在阿里旺旺买手机接收到一个图片压缩包，里边有一个文件打不开，可能那时候，电脑就被人植入木马了。”董晓麦说。

数百网民遭遇类似骗局，这些受害者自发组织QQ群集体维权。“中国网事”记者加入一个群号为“141686037”的受害者群里看到，这个群已经有194人，受害者的网名都是由地区加被骗数额组成，从网名可以看出受骗人员来自全国各地，受骗金额少则数百元，多则数千元，有一些甚至达到十万元。

“中国网事”记者在另外一个群号为“142316878”的受害者群里看到，里面有102人。像这样的受害者群还有很多，反映的情况大同小异。据粗略统计，涉及金额已达一百多万元。

被诈骗分子利用为“钓鱼台”的网龙公司接受“中国网事”记者采访时表示，从2010年年底至今，出现大量不法分子利用在网龙公司开设的游戏账户“钓鱼”诈骗网民的案件。在这些案件中，当事人无一不是登陆了网络购物平台，并轻信网络骗子发来的木马程序，从而导致骗子成功窃取当事人的付费存款，并用于各种消费。

2 “钓鱼”诈骗呈现“升级版” 网购维权越发艰难

“这种通过在国内某知名购物平台上种植木马盗取卖家账号，在和买家进行交易时，向买家传送藏有木马的文件进行盗窃的案例近年来屡见不鲜。”网龙公司透露，不仅网龙公司，凡是具备开设私人游戏账号功能的网游公司也都有涉及。

据介绍，近年来，“钓鱼”诈骗方式不断升级。传统的“钓鱼”方式是指网民在网购过程中，当进入第三方支付平台付款时，链接到了诈骗分子做的虚假页面，该页面在页面形式、扣款金额等方面做得与原网购网站非常相似，而通过这个虚假页面进行支付的金额则自动进入了诈骗分子的账户。

近期出现了比较严重的木马型“钓鱼”方式。“这是一种更隐蔽、更可怕的方式。”业内人士介绍说，当电脑中了这种木马病毒，在网购交易中的支付平台到银行扣款的环节当中，木马程序会自动在后台生成另一笔交易，新的交易指向了一个新的账户，银行的扣款自动到了诈骗分子的账户，而网民毫无察觉。

诈骗发生后，网民大多选择立即与第三方支付平台和网游公司联系，但他们普遍反映维权很难。

网民黄东生说，他在意识到自己被“钓鱼网站”诈骗后，立即与上海汇付网络科技有限公司联系，但客服人员说资金只是经过他们公司，已经实时转到了网龙公司的“91充值平台”。随后他又致电“91充值平台”客服，要求取消交易或至少先冻结这笔资金，但客服人员说钱已经充值到账户中，无法取消；他们没有接到公安局通知，无权冻结账户。

受骗网民向公安机关报案，也大多是无功而返。“这样的案件不会引起足够重视，公安部门投入大量人力去解决几千块钱并且是跨省的案件，难度可想而知。”黄东生说，诈骗人员就是抓住了受害人员分散在全国各地，每一个个体涉案金额不大的特点大肆行骗。

（资料图片）

3 打击网络犯罪 何时“魔高一尺，道高一丈”

网龙公司表示，不法分子的犯罪行为严重损害了网民的经济利益，也严重伤害了网龙公司的声誉。公司已汇总相关材料，向公安机关报案，将配合公安机关作出必要的协助，以使木马植入者早日被绳之以法。他们还向相关购物网站作出情况通报，提醒相关购物网站做好技术防范，并提醒网民注意网络支付安全。

“此前，众多网购用户因类似事件在各大网络平台上纷纷向网易公司发起维权，从现有情况来看，风波已经蔓延并且很有可能蔓延至包括网龙在内的其他上市网游企业。”网龙公司说。

福建八闽律师事务所主任林柏冬认为，对网民而言，通常对知名网站心理不设防，诈骗分子就是抓住了网民这一心理特征，大肆制作“钓鱼网站”实施网络诈骗；对企业而言，它们对“钓鱼网站”缺乏事前防御机制和事后处理机制，使网民成为不法分子的“鱼肉”。

林柏冬表示，有些网游公司在账户管理上存在漏洞，致使犯罪分子利用这种管理疏漏，用虚假身份开设多个银行账户，进行资金转移。

据公安部公共信息网络安全监察局主办的2010年全国信息网络安全状况网上调查显示，网络盗窃、网络“钓鱼”已占网络安全事件的8.1%。

专家建议，为有效防范“钓鱼”事件，大型的购物网站、第三方支付公司、网游公司等应建立完善的防范“钓鱼网站”的机制，堵塞高科技犯罪漏洞，保障网络用户资金安全；同时，公安等政府管理部门要切实加强网络安全监管，加大打击力度，为网络用户提供一个安全的交易环境。

■相关链接

经常上网购物 怎样防止被“钓”

为了打击骗子网站，淘宝网曾多次发布公告，表示只有“www.taobao.com”一个域名。我们归纳了网友的防骗方法，为您提供参考。

1.骗子如果用QQ与你联系，发来的网址前会有一个带“?”号的盾牌标志；真正的淘宝地址前，则会出现一个绿色带对勾的盾牌标志。

2.打开高仿淘宝网站，你会发现店铺提供的旺旺号不在线，而骗子也不会轻易通过淘宝旺旺与你沟通，因为这样容易被淘宝监控到。

3.买家咨询某种商品时，点开卖家发来的链接后，正常情况下，不用输入登录信息；凡是提示让你输入登录信息的，大多是“钓鱼网站”。买家登录淘宝账号后，一直处于活动状态，除非服务器发生故障，否则不会突然让你重新登录。

4.对方发来的链接，结尾以“.jpg”、“.swf”等结尾的，一定要小心。

5.由于骗子制作的是虚假淘宝网站，对于已有淘宝账号的网友，可以先尝试将用户名输错。如果在你明显输错的情况下，网站仍提示登录成功，说明你登录的是骗子网站。

6.在付款环节，骗子会询问你使用的是什么银行卡，这样，他才能生成相应的银行订单；而在真正的淘宝网交易，卖家不会关心这些。