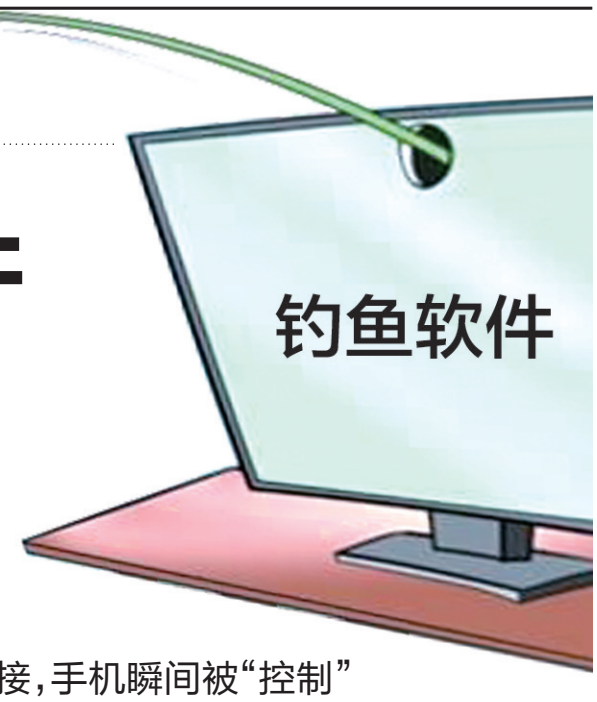
合肥一老板遭钓鱼软件“钓走”60万

网络犯罪成高发势头，警方已开展“净网行动”



□ 记者 王玮伟

同样的网银页面、同样的操作方式，可账户里的60万元怎么会瞬间蒸发？日前，合肥某企业老板谢军（化名）向市场星报，安徽财经网记者反映，他被骗子利用“钓鱼网站”转走他银行卡里的60万元钱。

市场星报、安徽财经网记者从合肥警方了解到，今年以来，各类电信网络诈骗层出不穷，给受害群众带来巨大损失。为此，针对近期出现的一些电信网络诈骗案件，记者选出部分案例，让广大市民擦亮眼睛，避免今后再次落入网络电信诈骗陷阱。

案例一：输两次验证码，账户“蒸发”60万

10月6日上午发生的一幕，谢军仍记忆犹新。当天上午9点左右，打开网银准备转账，打开银行网站，突然电脑屏幕跳出一个页面，谢军大概看了下，与银行网站类似，需要输入验证码。其以为是银行网站的弹窗，先后输入账户、密码，及两次验证码。

同样的网银页面、同样的操作方式，这些都如平常一样。让谢军没有想到的是，没多久他发现网银账户的数额出现变动，账户里的60万元被转走，而他的手机并未收到转款提醒。

意识到网银可能被盗，谢军一边报警求助，一边联系银行寻求解决方法。经过银行查询了解，从谢军账户“蒸发”的60万，被转至兰州的某个账户，随后该笔款项被先后拆分，转至近百个账户内。目前，辖区警方接警后，已展开调查。

提醒：市民需提高警惕，不登录不熟悉的网站，键入网站地址时要校对，以防输入错误误入钓鱼网站。使用银行网站的市民在登录前也要留意浏览器地址栏，如果发现网页地址不能修改，最小化IE窗口后仍可看到浮在桌面上的网页地址等现象，请立即关闭IE窗口，以免账号密码被盗。

案例二：点开短信链接，手机瞬间被“控制”

今年3月份以来，安徽芜湖警方接到举报，不少居民频繁收到带有可疑链接的短信，有人点击链接后手机被非法控制。芜湖警方当即成立专案组开展侦查。经对木马程序进行分析和比对，网安民警成功锁定了嫌疑人的真实身份和活动地点，并将其抓获。

经查，犯罪嫌疑人周某提供制作贩卖手机木马服务。嫌疑人何某从周某处定制购买手机木马，将木马放入自建网络空间，然后从网上搜索获取大量人员手机号，并冒充熟人发送带有木马链接的短信。

据介绍，该木马具有秘密获取手机通讯录和短信，并自动向通讯录好友发送木马链接的功能。嫌疑人在成功控制手机后再非法获取受害人身份信息和银行卡信息，最后通过互联网第三方购物平台购物、手机充值等方式来盗取银行卡资金。据统计，该团伙涉嫌非法获利数十万元。

提醒：遇到“奇怪”的短信或没有核实的链接不要轻易点击。安装软件时建议到正规渠道下载应用，对手机内的重要资料定期备份。

案例三：大学生网络兼职，刷单遭骗1.5万元

小童是一名应届大学毕业生，毕业后在合肥包河苑附近工作。7月15日，小童在网上看到一家北京公司有招聘，通过QQ聊天，她与一位自称该公司负责人的沈女士进行了交流，并成功“入职”。随后，小童根据沈女士QQ消息发来的指引，点击了一个网址，并根据网站提示，一步步完成刷单操作。

“整个过程不到3分钟，非常快。”据小童介绍，之后对方要求她支付5100元的“本金”，称完成所有流程后，5分钟内便会退还本金及10%的佣金，“也就是说，不仅还给我这些钱，另外还能得到500元佣金。”她并未多考虑，便将钱转给了对方。

然后沈女士告诉小童，“你的账号被冻结了，需要再进行一笔刷单才可以解冻。”听闻自己的账户被冻结，小童有些紧张，慌乱中顺着对方的指引，又分别两次支付了5000和4000元的本金。当第三笔刷单进行到一半时，“还是没有解冻，我感觉很有可能被骗了。”

至此，银行卡内将近1万5千元已经划给了对方。之后，小童与沈女士经过多次交涉，但对方表示在未完成所谓“剩余工作”前，拒绝退款。7月17日下午，小童拨打了该公司负责人号码，但两个手机均处于关机状态。目前，小童已向辖区警方报案。

提醒：网上兼职刷信誉几乎都是骗局，切勿轻信。同时，市民上网找兼职时，千万不要轻信网上关于购物返利、付费刷信誉等信息，一旦遇到对方要求先支付、交纳保证金、押金、购买充值卡、游戏卡等，多数都是骗局，不要为“小利”而上当受骗。

案例四：网络发布假电话卖机票，8个月非法获利500万

3月18日，淮南市民朱某通过百度搜索“机场客服电话”，并按照该电话要求向指定账号进行汇款，后发现卡内余额被全部转出。淮南公安机关接到报案后，迅速成立专案组开展侦破。

经侦查发现，嫌疑人将盗取的资金通过福建泉州POS机刷卡进行消费。经进一步扩线侦查，发现该取款团伙共持有12台POS机，刷卡金额高达500万元。近期，专案组在海南儋州将犯罪嫌疑人郑某某、朱某某等4人抓获，查实受害人涉及全国20余个省市300余人。

经审查，犯罪嫌疑人交代，自2014年9月至2015年5月，其先后通过网络购买银行卡、“400”电话等作案工具，并雇佣网络推手将购买的“400”电话发布到互联网并使其在百度等搜索引擎中排名靠前，以购买低价机票、办理机票退改签及托运行李等收取手续费为由实施诈骗。

提醒：此类骗子主要是通过设置网站，在各论坛、贴吧及搜索引擎发布“低价打折机票”的信息，等受害人来电订购机票。旅客应选择正规、信誉较好的专业机票代理网站或民航售票处。

警方：电信网络诈骗高发，开展为期半年“净网行动”

随着网络、电信技术的飞速发展，伴随而来的电信网络诈骗犯罪日益呈现高发势头，逐渐成为诈骗犯罪的主流。记者从合肥警方了解到，统计显示，去年合肥网络诈骗占涉网案件总发案数的94.6%，是最为高发的涉网案件。 当前，合肥网络购物诈骗、冒充QQ好友诈骗、冒充公检法诈骗、虚假信息诈骗等四类诈骗高发。今年以来，合肥也有不少居民遭到电信网络诈骗，最多的一笔约600万元。

据介绍，针对当前网络违法犯罪活动多发，危害我国互联网络安全、侵害人民群众合法权益的情况，自今年7月起，公安部组织全国公安机关开展为期半年的打击整治网络违法犯罪“净网行动”。