“钓鱼网站”频盗网民存款

浙江绍兴曾一天发案六起案值百万

随着信息网络技术的高速发展，方便快捷的网上银行在人们日常金融活动中愈发普及。然而，近期全国各地频发假冒银行网站骗取客户密码、实施网银盗窃的案件，给群众造成重大经济损失。网络金融安全遭遇侵害，引发广大网民的高度关注。

解读“钓鱼网站”

“钓鱼网站”是一种网络欺诈行为，指不法分子利用各种手段，仿冒真实网站的网址以及页面内容，或者利用真实网站服务器程序上的漏洞在站点的某些网页中插入危险的网页代码，以此来骗取用户银行或信用卡账号、密码等私人资料。

“钓鱼网站”的源码只需几十元即可买到，近年，在网络上也出现了批量生成“钓鱼网站”的工具。而“钓鱼网站”使用的域名（网站地址），也大多可以免费申请。“钓鱼网站”的生存周期一般只有几天，当“钓鱼网站”被安全公司拦截或被停止域名解析后，“钓鱼者”可以很快将网页内容切换到另一个域名，继续实施诈骗。

伴随着互联网应用的日益广泛，互联网上的“钱”越来越多。而“钓鱼”欺诈的方式与传统的病毒产业链相比，整个“钓鱼”欺诈过程，一个人即可完成，“钓鱼者”可以更直接、更快速的获取经济利益。

“钓鱼”欺诈流程：“钓鱼网站”代码贩子（木马作者）-“钓鱼网站”经营者-通过流氓软件产业链为“钓鱼网站”带流量（或通过游戏内置的聊天频道、虚拟物品交易平台推广）-诈骗受害者钱财或个人信息-收集出售个人信息-获取利益。

“钓鱼网站”假冒银行网站盗存款

2010年12月9日，浙江绍兴市连续发生6起网上银行盗窃案件，累计案值上百万元。在这几起案件中，受害人均收到陌生手机号码发送的短信，提示其银行网银动态口令将于次日过期，让其尽快登陆中国银行的官方网站进行升级。受害人在按照短信提示的网址登录该网站并按照指引操作后，其网银账户内款项被迅速转走。

绍兴警方在浙江省公安厅网警总队的指导下，转战广东、福建、广西等三省六地，经过一个多月的缜密侦查，于2011年1月13日成功摧毁一个以福建泉州籍人员为主的网银盗窃犯罪团伙，抓获包括主犯叶某、易某、莫某等在内的8名犯罪嫌疑人，缴获电脑、短信群发器、银行卡以及若干诈骗案例教材等大量作案工具，扣押赃款15余万元。据警方介绍，这是浙江首次侦破盗窃网上银行犯罪团伙。

“当前，这种针对中国银行网银动态口令卡的智能型网银盗窃侵财型案件，已呈高发态势，并且正在以惊人的速度向全国蔓延。”绍兴市公安局网警支队支队长倪炳水介绍。

据不完全统计，2010年12月份以来，仅浙江省已发同类案件40余起，涉案金额上千万元。另据了解，江苏、广东、北京等地也有很多类似案件发生，涉案总额巨大。

警方披露 “钓鱼”欺诈有四大特点

在很短的时间内，犯罪分子利用“钓鱼网站”实施诈骗、盗窃的犯罪行为在全国迅速蔓延，很多从未开通网络银行的百姓也曾接到类似的手机短信。不少网民发帖质问：“这种针对网络金融的犯罪手段为何能屡屡得手？”

绍兴市公安局网警支队副支队长吴佳瑾说，警方在对同类案件实施分析后发现，犯罪嫌疑人的作案手法均采取诈骗与盗窃相结合的形式，其对银行业务流程及互联网应用技术有较深的了解，该类犯罪具体呈以下几个特点：

一是短信群发“善意”提醒，诱使网民上网操作。在此类案件中，犯罪团伙有针对性地选择江浙等经济发达地区的用户作为作案对象。由于这些对象文化层次相对较高，防范心理较强，普通的诈骗手法已无法得手，进而选择“密码丢失索取”“网络升级提示”等“善意”提醒诱惑网民。

二是境外注册网站域名，逃避互联网监管。在所有已发案件中，犯罪嫌疑人开设假网站使用的域名均不在国内注册，都是在境外网站注册的免费域名。由于目前对境外域名注册行为无法实施有效管理，使得域名注册人的信息难以获取。

三是高仿真网站制作，欺骗网民透出账户密码。要获取网民的网银账户及密码，必须配套几可乱真的银行假网站。在同类案件中，犯罪嫌疑人均制作极为精美、与真实网站相似程度极高、普通用户无法识别的“钓鱼网站”。在网民登录网站后，网站页面有相应的提示性指引，简单操作后，网民的账户密码就被“钓鱼网站”所记录。

四是连贯的转账操作，迅速转移网银款项。在获取网民的网银账户密码后，犯罪嫌疑人迅速登陆真实银行网银网站窃取资金。网银的动态口令卡所提供的动态口令只有时间很短的有效期，犯罪嫌疑人在极短时间内完成网银转账操作，达到窃取的目的。

吴佳瑾说，由于此类犯罪具有极强的欺骗性，网民稍不注意就容易上当，而犯罪分子具有极强的反侦查意识，整个作案过程不与受害人见面，全部通过网络完成，公安机关侦破案件有很大难度。

网民声音 银行应弥补安全漏洞

绍兴市公安局网警支队支队长倪炳水说，根据警方掌握的情况，在官方网站上进行正确操作交易，安全是有保证的。网民要增强自我防范意识，不要相信不明邮件、短信和电话发布的金融信息。

网民“一叶知秋”发帖认为，尽管被害人是上了虚假网站后被盗走了存款，但作为银行方面应该主动干预，尽早发现“钓鱼网站”，弥补安全漏洞，发布防范信息。

阿里巴巴公司副总裁邵晓峰说，作为国内最大的网络支付平台，支付宝也面临大量“钓鱼网站”的困扰。为此阿里巴巴公司专门组织了一批人员主动防御，在网上实时监控，一旦发现假冒淘宝、支付宝的“钓鱼网站”，立即向公安和电信部门举报，清除此类网站，同时公司还频繁地向网民发布预警信息，提醒用户不要上当。

也有网民说，从犯罪分子实施犯罪的过程看，他们利用短信、电话、虚假网站等工具都与电信部门有关系。虽然犯罪团伙注册的假冒网站地址在境外，但网络空间是向国内电信运营商租用的，希望工信部门能加强管理，对一些假冒银行和国家机关的域名加以甄别，对可疑用户进行调查，并及时向公安机关举报。

（据新华社电）

相关链接

“钓鱼网站”危害首超病毒木马

近日，国内信息安全厂商瑞星发布的《瑞星2010上半年互联网安全报告》（以下简称“报告”）指出，2010年全年，我国互联网上新增病毒750万个，比去年下降56%；但新增“钓鱼网站”175万个，比去年增加11倍；其中，“钓鱼网站”的受害网民高达4411万人次，损失超过200亿元。

瑞星报告指出，在所有“钓鱼网站”中，假淘宝、假QQ、假非常6+1、假银行和假新浪是五大常见的假冒网站，占据“钓鱼网站”的76%。此外，假机票网站在节假日期间也活动频繁，假冒的南航网站在“钓鱼网站”中也占到2%。这些“钓鱼网站”使用与假冒对象网站相似的域名，采用聊天软件、电子邮件等方式传播。

瑞星报告介绍，尽管病毒、木马和挂马网站造成的威胁得到遏制，但以“钓鱼网站”、网络诈骗为特征的新型互联网威胁急剧增加，并首度超过了病毒和木马，其中医药、美容、成人用品、证券咨询等行业受此危害最为严重。

瑞星报告同时认为，现在的网络“钓鱼”，网民要防范其实也不难，可遵循以下几个原则：

一是网上交易时，不要随意接收他人以调查表、报价表等名义发送的文件，以及自己不确定的链接；

二是，在网银支付过程中，一定要看清商户名称，收款方的账号和身份必须严格确认；还有不能贪小便宜，网购有折扣优势，但过度便宜往往隐藏危险；

三是还要勤杀毒，保证电脑上网时无病毒等。

反病毒专家表示，要防止“钓鱼网站”，关键仍在提高防范意识，比如小心识别虚假网址，在任何情况下都不要将密码告诉他人（包括银行员工或警方），不要轻信任何套取网上银行用户名和密码的行为，另外不要在公共场所（如网吧、公共图书馆等）使用网上银行，以防止这些计算机可能装有恶意的监测程序。（王文）

2010年十大“钓鱼网站”

1 item.taobao.com-uik.co.cc（淘宝钓鱼网站）
2 item.taobao.com uuc.co.cc（淘宝钓鱼网站）
3 ffejixq3.info（腾讯钓鱼网站）
4 icbc-be.com（工商银行钓鱼网站）
5 www.cctv3.cc（非常6+1钓鱼网站）
6 qq2010mb.info（腾讯钓鱼网站）
7 mybank.icbc.com.cipoc.info（工商银行钓鱼网站）
8 www.cctv9669.com（非常6+1钓鱼网站）
9 qqffo.net（腾讯钓鱼网站）
10 sina3.t3.to（新浪钓鱼网站）