假冒银行网站“钓”走百万存款

网警揭秘钓鱼网站四大“歪招”

□据 新华社

随着信息网络技术的高速发展，方便快捷的网上银行在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。

假冒银行网站“钓”走百万存款

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。上述案件中，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，让其尽快登入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，其网银账户内的款项就被迅速转走。

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、广西等三省区六地，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、银行卡等大量作案工具以及若干诈骗案例教材和赃款15万余元。据警方介绍，这是浙江首次侦破盗窃网上银行犯罪案件。

“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告诉记者。

据不完全统计，2010年12月以来，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，涉案金额巨大。

揭秘钓鱼网站四大“歪招”

在很短的时间内，这种冒充银行网站实施诈骗、盗窃的犯罪在全国蔓延，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逞？”

绍兴市公安局网警支队副支队长吴佳瑾告诉记者，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了解，具体有以下几个特点：

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网银用户作为作案对象。由于这些对象文化层次相对较高，防范意识较强，普通的诈骗手法已无法得手，犯罪团伙进而选择“密码丢失索取”、“网络升级提示”等“善意”提醒诱惑他们。

二是在境外注册网站域名，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是在国内注册的，都是在境外网站注册的免费域名。目前对境外域名注册行为无法实施有效管理，域名注册人的信息也难以获取。

三是制作高仿真网站，欺骗网民透出账户密码。犯罪团伙要获取网民的网银账户及密码，必须配套几可乱真的假银行网站。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。在网民登录此类网站后，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记录。

四是以连贯的转账操作，迅速转移网银款项。在获取网民的网银账户密码后，犯罪嫌疑人迅速登录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。

吴佳瑾表示，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，公安机关侦破此类案件有很大难度。

倡网民自我防范，唤部门给力监管

绍兴市公安局网警支队支队长倪炳水表示，根据警方掌握的情况，在官方网站上进行正确操作交易，安全是有保障的。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网银内的款项，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表示，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些人员主动防御，在网上实时监控，一旦发现假冒淘宝网、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。

也有网民表示，从犯罪分子实施犯罪的过程看，他们利用的短信、电话、虚假网站等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，对一些存在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。

■延伸阅读

如何防范钓鱼网站

所谓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URL地址（网页地址）以及页面内容，或者利用真实网站服务器程序上的漏洞在网站的某些网页中插入危险的HTML代码（构成网页文档的主要语言），来骗取用户银行或信用卡账号、密码等私人资料。

钓鱼网站近来在全球频繁出现，严重地影响了在线金融服务、电子商务的发展，危害公众利益，影响公众应用互联网的信心。钓鱼网站通常伪装成银行网站，窃取访问者提交的账号和密码信息。它一般通过电子邮件传播，此类邮件中一个经过伪装的链接将收件人连到钓鱼网站。钓鱼网站的页面与真实网站界面完全一致，要求访问者提交账号和密码。一般来说钓鱼网站结构很简单，只有一个或几个页面，URL和真实网站有细微差别。

专家提醒，网民在查找信息时，应该特别小心由不规范的字母数字组成的cn类网址，不要上一些不太了解的网站。

防范办法主要有：

第一，查验“可信网站”。

通过第三方网站身份诚信认证辨别网站的真实性。目前不少网站已在网站首页安装了第三方网站身份诚信认证——“可信网站”，可帮助网民判断网站的真实性。

第二，核对网站域名。

假冒网站一般和真实网站有细微区别，有疑问时要仔细辨别其不同之处，比如在域名方面，假冒网站通常将英文字母I替换为数字1，CCTV被换成CCYV或者CCTV-VIP这样的仿造域名。

第三，比较网站内容。

假冒网站上的字体样式不一致，并且模糊不清。假冒网站上没有链接，用户可点击栏目或图片中的各个链接看是否能打开。

第四，查询网站备案。

通过ICP备案可以查询网站的基本情况、网站拥有者的情况。没有合法备案的非经营性网站或没有取得ICP许可证的经营性网站，根据网站性质，将被罚款，严重的将被关闭。

第五，查看安全证书。

目前大型的电子商务网站都应用了可信证书类产品，这类网站的网址都是“https”开头的，如果发现不是“https”开头的，应谨慎对待。

公安机关缴获的犯罪分子使用的银行卡。（新华社发）