



# 趋势科技新闻稿

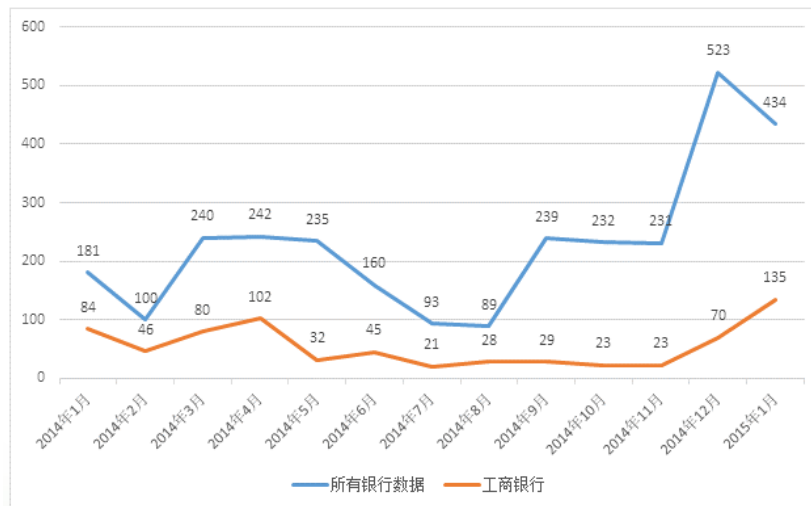
[即时发布]

## 3 天增加 40 个工商银行钓鱼网站 趋势科技发现金融钓鱼网站井喷式增长

### 钓鱼网站高度模仿官方网站 暗中窃取用户信息与网银资金

**[趋势科技中国]- [2015 年 1 月 30 日]**近日，全球服务器安全、虚拟化及云计算安全领导厂商趋势科技监测发现，金融钓鱼网站数量在近两个月出现了井喷式增长的趋势，针对工商银行的钓鱼网站更是在短短 3 天内增加了 40 个。这些钓鱼网站在界面和域名上高度模仿银行官方网站，以骗取用户的银行账号、密码甚至个人财产。趋势科技提醒用户，在登录银行网站的时候一定要认真核对网站域名，并使用具备钓鱼网址封锁功能的趋势科技 PC-cillin2014 云安全版来保护个人金融及信息安全。

据趋势科技（中国区）病毒实验室监测显示，在最近两个月，针对银行的网络钓鱼网站数量出现爆发式增长，峰值数据一度达到 523 个。而针对工商银行的钓鱼网站则从 11 月份的 23 个大幅攀升到现在的 135 个，创下近一年来的新高，这很可能导致大量用户误入钓鱼网站。



**【趋势科技监测：近两个月，针对银行的钓鱼网站数量出现大幅增长】**

为了让用户误以为访问的是银行官方网站，不法分子对工商银行等银行官网进行了全面山寨。这些网站多数会使用 and 官方网站类似的域名(如 icbc\*\*\*.com)，或者包含有和银

行客服电话一样的数字(如\*\*\*95588.com)。而且，其界面与官方网站也极为相似，识别难度很高。

当用户点击这些钓鱼网站并试图访问网上银行时，网站会弹出和官方网站相似的登陆框。一旦用户输入账号、密码、身份证号并点击登录，这些机密信息就会被不法分子偷偷上传到指定的服务器。而且，不法分子还会谎称用户需要升级密码器，以诱导用户输入密码器中的密码来进行“验证”。实际上，这个“密码器”内嵌恶意代码，用户输入的密码会被不法分子直接获取。



【钓鱼网站域名与官方网站相似，并谎称“密码器”需升级以获取用户密码】

趋势科技（中国区）技术总监蔡昇钦指出：“银行类钓鱼网站不仅在数量上出现了大幅增加，复杂性与识别难度上也有所提升。这些钓鱼网站涉及到不同的黑客和诈骗团伙，有着不同的犯罪手段，很难找出一个统一的识别标准。而且，随着移动金融的进一步普及和流行，仿造手机银行的钓鱼网站也开始增多，手机用户切不可掉以轻心。”

要防范钓鱼网站的威胁，趋势科技提醒用户务必通过正规的渠道来访问银行网站，并特别警惕那些通过论坛、短信、社交平台等非官方平台传播的网址。如果用户在访问网站之后发现数据泄露，要及时与银行联系，更改密码等个人信息。



【假冒手机银行的钓鱼网站】

用户还需要谨记防范钓鱼网站的识别法则，即官方网站域名+浏览器+搜索引擎+第三方软件验证，钓鱼网站很难同时满足以上几种验证。趋势科技还建议用户安装 PC-cillin2014 云安全版等安全、高效的信息安全软件，PC-cillin2014 云安全版后台中具有全球钓鱼网站监控体系，以及爬网系统、网页安全分级功能等最新的防控技术，能全面监测和甄别网页中的恶意代码，并通过“主动式云端拦截技术”提前一步甄别出恶意网站及链接，帮助用户防范钓鱼网站威胁，安心享受春节假期。

###



### 关于趋势科技 (Trend Micro)

趋势科技是全球虚拟化及云计算安全的领导厂商，致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念，基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构，为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全，保障信息与财产的安全。同时，遍布全球各地的 1,500 余名趋势科技安全专家可为各国家和地区的企业级个人用户提供 7×24 的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息，请访问：

[www.trendmicro.com.cn](http://www.trendmicro.com.cn)。请访问 Trend Watch：[www.trendmicro.com/go/trendwatch](http://www.trendmicro.com/go/trendwatch) 查询最新的信息安全威胁的详细资讯。