



“来一下我办公室”过时了，
“帮你提高银行额度”接着骗

网络安全新威胁 不得不防

事件——

日前，记者从腾讯手机管家方面获悉，继“你明天到我办公室一趟”肆虐一时后，“可以帮你提高信用卡额度”类的诈骗电话正在成为新“潮流”，直接威胁到广大用户的信用卡安全。与此同时，随着岁末的到来，其他类型的电信诈骗、木马病毒等互联网安全威胁开始越发严重。对此，业内专家发出提醒：“即使再有钱，也不能任性地把骗子给骗走了！”

“提额”诈骗案件频发

据了解，近来信用卡“提额”诈骗频发，屡屡有人中招。不久前，广州的王女士接到“020955××”的电话，对方自称××银行的客服人员，称她的信用记录良好，年底可将信用卡额度提高至 10 万元，并且准确地说出了王女士的姓名、家庭地址等信息。于是王女士按该“客服人员”的要求，提供了信用卡卡号、有效期、卡片背面三位数卡片安全码(CVV2)等信息。对方称最后一步是验证手机动态验证码，需要王女士在收到验证码后提供给客服人员，便可完成提升额度。于是王女士便将验证码告诉了对方，结果挂掉电话后，她收到了一条该银行的短信：“您的信用卡消费了 2900 元。”

2014 年 12 月，广州的刘先生接到“××银行”打来的电话，称可以提高信用卡额度，在刘先生提供了信用卡卡号、有效期、卡片背面三位数卡片安全码(CVV2)码等信息后，发现信用卡被盗刷三笔，总额 2 万余元。

腾讯手机安全专家陆兆华分析称，诈骗分子首先通过非法渠道获取到了受害者的姓名、电话、家庭住址等个人信息，然后利用“网络改号”软件将电话伪装成相应银行的客服电话，骗取受害人的信任，要求对方提供卡号、卡片有效期、卡片背面三位数等信息。最后，诈骗分子便利用这三个信息在网上消费、快捷支付的方式对受害者的信用卡实施了盗刷。

针对此类诈骗，陆兆华表示，银行基本不会通过打电话的方式通知客户信用卡“提额”，即便是打电话，也不会跟持卡人索要卡号、卡片有效期、卡片背面三位数字等信息，只会对持卡人的身份信息进行核实。另外，据银行工作人员表示，各大银行对于信用卡提额，都是建议持卡人自行登录银行的信用卡官方网站，提交提额申请，如审核通过即可提高额度。

诈骗高峰期“如期”来到

“年底本来就是各种诈骗案件的高发期，而且近来频频出现互联网个人信息泄露的事件，更加诱发了大量的诈骗案件的发生。”据 360 的互联网安全专家介绍，不久前 12306 遭到“撞库”攻击，泄露了大量的用户信息，其中就涉及用户的姓名、身份证甚至银行卡和订票的信息，部分内容甚至出现在类似 58 同城等的分类信息网站上出售，不法分子往往会利用这些信息进行诈骗。“在发生多起用户个人信息泄露的事件后，互联网安全领域就曾预测，大量的网络诈骗现象将会随即出现，如今到了岁末，各种诈骗现象开始抬头也是意料之中。”

所幸的是，随着网络诈骗现象频繁发生，更多的用户也开始意识到了安全软件的重要性，近期猎豹安全大师、腾讯手机管家等的网络安全软件，其下载量就有大幅攀升。据猎豹移动介绍，其于 2014 年初推出的免费手机杀毒软件猎豹安全大师(CM Security)，则仅仅用了不到一年的时间就完成一亿用户的目标，更在 Google Play 全球工具类排行榜高居第二名。根据猎豹移动 2014 年安全报告统计，过去一整年，猎豹移动安全实验室共监控到 744 起信息外泄事件，是 2013 年的 2.06 倍，影响人数超过 817 万人。

“对于花样不断翻新的网络诈骗和信息安全威胁，普通市民最重要的还是要提高安全意识，同时要学会善用安全软件，同时留意最新诈骗手法的相关信息。”陆兆华表示，虽然目前网络安全威胁形势依然严峻，但是在用户和安全软件企业的共同努力下，中国的网络安全问题正在得到不断的改善，但预防诈骗最核心的还是用户的安全意识问题，这个实在马虎不得。

(南方)

四部委联手出台新规定

电信诈骗将不能再任性了

苦于无规可循，一直以来电信诈骗防范的重要一环——“资金冻结”的效率都不高，导致很难有效保护存款人的财产。近日，银监会联合最高人民检察院、公安部、国家安全部四部委，公开发布《银行业金融机构协助人民检察院公安机关国家安全机关查询冻结工作规定》(以下简称《规定》)。该《规定》要求，对于手续齐全的涉案资金，银行等金融机构应当立即办理冻结手续。

对此，业内人士指出，《规定》发布后，存款人遭遇电信诈骗后，眼睁睁看着钱从账户被转走却无能为力的现象将得到改善，公安、银行之间相互“踢皮球”的

情况也将成为过去，这也意味着电信诈骗“事后处理”和案件侦破将取得突破性进展。

事实上，在快速拦截涉案资金方面，此前已有警企合作的模式进行了尝试。早在 2013 年底，腾讯联合广东省公安厅、深圳市公安局反信息诈骗咨询专线、中国互联网协会、银监局、银行协会、三大运营商等组织及企业，共同发起国内首个天下无贼—反信息诈骗联盟，已在致力于提高警方、银行、存款人之间的联动效率，不仅涉及电信诈骗的“事后处理”和案件侦破，还涉及电信诈骗的“事前预防”。

资料显示，警方、银行、腾讯安全通过共享数据的方式，建立了国内首个“恶意诈骗银行号码库”，恶意诈骗银行号码库将通过大数据、云安全技术实现腾讯双管家(电脑管家和手机管家)，守护用户在 PC 端和移动端的网络支付。当发现用户转入账号属于恶意诈骗银行账号时，安全软件会在第一时间提醒网民，“此账号疑似恶意诈骗银行账号，请不要继续转账汇款，以免遭受财产损失”。

此外，天下无贼—反信息诈骗联盟内的警方、运营商、银行、腾讯安全以及大众点评等组织成员还将共享恶意电话号码数据库，该数据库目前拥有 1 亿数据，从而实现手机管家对各类陌生来去电号码的识别以及对恶意电话号码的智能提醒。

安全专家表示，大数据、云计算的运用对于防范信息诈骗起到了未雨绸缪的作用，再配合四部委发布的《规定》，让电信诈骗的事前防范、事后处理两个重要环节的效率得到提升，解决了一直以来防范电信诈骗的重大难题。

(北商)

