不法分子截获验证码盗刷银行卡

警惕“手机短信嗅探”犯罪

凌晨，突然发现手机信号从4G降为2G，收到来自银行、支付宝和移动公司的各类短信验证码。随后，银行账户被转空、支付宝余额被转走、手机自动订购了一堆无用的增值业务……这并非科幻电影中的场景，而是现实世界中短信嗅探设备对手机用户实施的不法侵害。

近期，全国多地发生利用短信嗅探技术窃取钱财的案件，有的涉案金额逾百万元。“新华视点”记者调查发现，一些不法分子通过社交网络兜售相关技术及设备。

犯罪分子利用嗅探技术“隔空取物”，短信验证码也被截获

今年8月，一位新浪微博网友向警方和相关金融机构报案：凌晨2时至5时，手机先后收到100余条来自支付宝、京东金融和银行等金融机构的短信验证码，相关账户内的余额及绑定银行卡内的余额全部“凭空蒸发”。

事后经安全技术专家鉴定，认为这是一起较为典型的利用短信嗅探技术实施财产侵害的案例。据中国电子技术标准化研究院技术专家何延哲介绍，短信嗅探技术是在不影响用户正常接收短信的情况下，通过植入手机木马或者设立伪基站的方式，获取用户的短信内容，这其中就包括来自银行、第三方支付平台和移动运营商的短信验证码。

一位业内人士介绍，除了盗取用户金融账户内的资金外，短信嗅探技术还可以截获移动运营商给手机用户发送的验证码，用来办理各类增值扣费业务，从而盗取手机用户的话费。

公开报道显示，近期，全国已有多地破获相关案件：7月，河南新乡公安机关破获一起利用短信嗅探技术使用他人金融账户购买虚拟物品实施销赃的案件，抓获犯罪嫌疑人10名；8月，厦门警方破获一起利用短信嗅探技术盗刷他人金融账户的案件，抓获犯罪嫌疑人1名，涉案金额10余万元；同样在8月，深圳警方打掉一个全链条盗刷银行卡团伙，抓获10名犯罪嫌疑人，查缴伪基站等电子设备6套，带破同类案件50余宗，涉案金额逾百万元。

记者暗访：社交网络售卖嗅探设备软件，声称“包教包会”

这些非法设备从何而来？记者在互联网和社交软件搜索，发现大量嗅探设备交易帖和交流群。

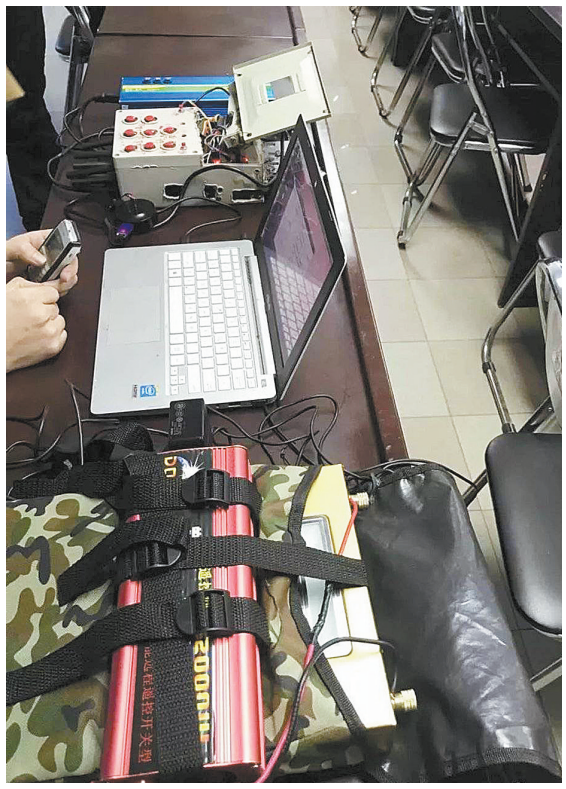
在一个名为“嗅探吧”的百度贴吧中，不少卖家除了介绍嗅探功能，留下QQ、微信等联系方式外，还时常分享一些拦截短信成功的截图，诱导他人购买相关设备。

根据一篇交易帖的指引，记者添加了尾号为0960的QQ用户。对方称，只需要8500元即可将盗取话费的全套设备软件卖给记者，盗取支付宝账户余额的相关设备则需2万元。为打消记者的顾虑，对方甚至还表示可以通过快递公司“货到付款”，在快递网点开机现场验证设备性能后再付款，并承诺将通过傻瓜式教程“包教包会”。

一位售卖设备的卖家告诉记者，他们有一个专门的工作室，有人负责制作硬件，有人负责软件编程。

有卖家提醒记者，要遵守“行规”。例如，在盗取他人话费时，一天盗取的话费上限不能超过3000元。

还有卖家给记者发来了大量的照片和视频录像，证明所售卖的设备真实可靠。在一段视频影像中，嗅探设备正在运行，对方还演示了如何操作软件，并成功截获了一条发自银联的短信验证码。



办案民警做了一番思想工作后，使用嗅探攻击设备（伪基站）的嫌犯决定配合警方还原犯罪过程。（虎嗅）

据深圳市反电信网络诈骗中心透露，今年夏天，深圳市公安局龙岗分局龙新派出所查获了一套车载“嗅探攻击设备”，并让犯罪嫌疑人对作案手法进行了全程还原。

嫌犯向警方供述，要想实现盗刷，只需知道一个人的手机号、姓名、身份证号、银行卡号、验证码就足够了。具体步骤如下：

第一步：用伪基站（藏在美团外卖箱子里的设备）捕获受害人手机号

前提是受害者的手机必须处于2G状态下。即手机号必须是中国移动或中国联通，因为这两家的2G是GSM制式，传送短信是明文方式，可以被嗅探。

第二步：实时嗅探手机短信

光知道手机号码其实没太大用，因为很多网站至少需要知道验证码才可以登录。这个时候，短信嗅探设备就要发挥很大作用了，短信嗅探设备包括一部电脑+一部最老款的诺基亚手机+一台嗅探信道机。受害者手机要保持静止状态，这也是嫌犯选择后半夜作案的原因。

第三步：实现盗刷

掌握了一个人的姓名、身份证号、银行卡号、手机号，并能实时监测手机短信验证码后，就可以去盗刷了。因为很多网站在设计的时候，只需要输入这些就可以完成支付，甚至可以通过这些内容来更改登录、支付密码。（虎嗅）

嗅探攻击设备藏在一个“美团外卖”的箱子里，以便在公共场所流动捕获受害人的手机号。（虎嗅）

专家建议：运营商加快淘汰2G网络技术，金融机构加强安全因子的多重验证

非法买卖、使用短信嗅探设备触犯哪些法律法规？福建省瀛坤律师事务所张翼腾律师认为，由于出售人未经有关主管部门批准，未取得电信设备进网许可等资质，非法生产、组装、销售“伪基站”设备的行为可能构成非法经营罪。

如购买者擅自设置、使用无线电台（站）或者擅自使用无线电频率，干扰无线电通信秩序，造成公用电信设施不同程度中断，使不特定多数的个人无法正常进行通信联络活动，其行为可能构成破坏广播电视设施、公用电信设施罪、扰乱无线电通信管理秩序罪。

此外，若使用者实施了盗刷银行卡的行为，则可能同时构成盗窃罪、信用卡诈骗罪等。

何延哲表示，在2G通道下进行的短信和通话信息使用明文传输。为成功劫持信号完成短信嗅探，不法分子有时还会干扰3G和4G信号，强制让用户“降维”到2G网络状态。

腾讯安全玄武实验室负责人于旸建议，用户可以要求运营商开通VoLTE功能（一种数据传输技术），让短信通过4G网络传输，防范无线监听窃取短信。

于旸表示，在网络安全领域存在一个“不可能三角”，即无法同时实现安全、便捷和廉价三个要素。从短信嗅探技术盗刷他人金融账户的案例来看，目前，被多数金融机构采用的基于账户登录密码和短信验证码的“双因子安全认证”虽然方便，但在该环境下有失效风险。

何延哲等业内专家建议，通信运营商应考虑加快淘汰2G网络技术，确保用户的短信和通话内容不被他人截获窃取。此外，有关专家建议，在“双因子安全认证”出现漏洞的情况下，包括银行和第三方支付平台在内的金融机构应加强安全因子的多重验证，推出更为完善可靠的校验手段。

（新华社北京10月18日电）