购物平台账户一夜被盗刷5万多元

小心了！手机“副号”或成诈骗新目标

春节期间，随着用户各类消费行为的增多,互联网诈骗案件迎来高发期。除了常见的中奖诈骗、短信诈骗等手段不断滋扰群众外，骗术也在不断升级，电信诈骗案件出现新一轮高峰。其中，有用户遭遇新型手机卡副卡钓鱼欺诈，引发了社会关注。

新型“副号”漏洞被不法分子利用

最新的电信欺诈便是利用运营商一卡多号业务进行的新型欺诈手段。手机卡副号为某些运营商提供的一卡多号业务，在不换手机、不换SIM卡的基础上，用户可以增加最多3个真实手机号作为副号。

犯罪分子首先利用猖獗的黑产交易，获得涵盖用户姓名、银行卡号、身份证号以及银行预留手机号等个人敏感信息，然后利用运营商主副号绑定业务不验证实名一致性的漏洞，将受害者手机号绑定为副号，进而接管受害者手机号，劫持银行卡交易的短信验证码，然后透过系列复杂手法完成对受害者账户的资金窃取。此手法较为新型，跨平台作案，涉及到运营商、手机云服务商、银行、第三方支付平台、消费金融服务方，说明行业需要联防联控，筑高防护壁垒的必要性。

没用身份证、银行卡,钱却不翼而飞了

一觉醒来，深圳的何先生发现自己的手机被锁定，同时，某购物平台账户遭陌生人盗刷，犯罪分子使用白条消费和申请贷款，一夜间洗劫了5万多元。

随后何先生发现，自己的手机曾经被一个陌生号码接管。来自运营商的短信显示，这是一项办理添加“副号”的业务，何先生的手机号码被犯罪分子添加为副号。当副号手机关机，所有短信都会被主号接收，犯罪分子在此期间接收何先生的短信验证码，进而作案。

没用身份证、没用银行卡，钱就这样不翼而飞了。副号究竟是什么鬼？很多人首先会联想到“亲情号”，但“副号”和“亲情号”并不是一回事。

亲情号通常指不同机主、不同号码，为了彼此之间通话更便宜而开通的话费套餐。那么，何先生的手机号是怎么成为犯罪分子的“副号”的呢？

第一步：买料。犯罪分子在网上购买泄露的姓名、银行卡号、身份证号和预留手机号，俗称为“四大件”。

第二步：钓鱼。犯罪分子向已经掌握了银行卡信息的用户，发起绑定副号的业务申请，以广撒网的方式寻找作案对象。一旦你误回复，就上钩了。

第三步：强迫关机。由于主号只有在副号关机的情况下才能接管短信，犯罪分子这时一般会采用两种手段，一是利用短信轰炸强迫目标把手机关机。二是利用手机云服务，对手机进行远程操作。

第四步：空手套白狼。利用主号收到的短信验证码，犯罪分子对手机号码绑定的网购账户进行洗劫。

花样叠出，防不胜防！对于这类诈骗来说，在接到各类短信通知后，一定要看清短信内容，不可随意回复。

“短信保管”也不太安全

被钻空子的电信类业务还不止手机副号。短信保管业务开通后，便可以在运营商的服务器上保存你的手机短信，现在，不少手机厂商的云服务也在做同样的事情。然而，这却是个暗藏危险的功能。

丁小姐看见手机上有两条来自银行和手机运营商的短信，发送时间分别是凌晨3：43和4：12。一查账户，10万多元的余额在一夜间归零！不仅如此，丁小姐还遭遇了信用卡盗刷，“被申请”了7万元的银行万用金贷款。

这一切究竟是如何发生的？

第一步：撞库，获取各类账户信息。所谓“撞库”，就是利用软件对高概率数字序列进行尝试，利用这种简单粗暴的方法，用户的网络身份、网银账号、手机营业厅等账户便一览无遗。

业内人士称，撞库的速度真的很快，每分钟至少上千个，如果用一些好的设备，效率更高，成功率在50%以上。

第二步：开通短信保管和短信拦截业务，获取验证码。这是最关键的一步。开通这一业务后，保证登录安全的动态验证码就顺利成了犯罪分子的囊中之物。

第三步：开通实体SIM卡。此时，犯罪分子就可以伪装是受害人，在网上营业厅申请4G换卡业务。为了便民，有些运营商会直接把卡快递到指定地址。

既拦截了短信，又复制了SIM卡，诈骗分子就能“为所欲为”了。

大家知道，许多重要服务都依赖手机验证，如果你将手机短信同步备份到服务器上，就增加了暴露机会，一旦网上营业厅服务密码被盗，或云服务登录权限被盗，就等于在“裸泳”。

手机卡以及冷门业务成为诈骗新目标

反诈骗举报平台“猎网平台”发布的《2016年网络诈骗趋势研究报告》提出，2016年以来，网络诈骗主要呈现几个明显的特点：

手机卡成为新的盗窃目标；利用短网址、微云分享链接跳转到钓鱼网站；知名招聘网站、语音平台进行公开招聘；真假难分的钓鱼网站；精准诈骗的实施；诈骗专业度越来越高；利用新业务和冷门业务漏洞实施诈骗；利用云盘、同步软件进行信息窃取。

这其中，便提到了手机卡以及冷门业务的漏洞。安全专家建议：

1、尽量不要去注册小型不安全的网站，避免个人信息被盗用。

2、在不同的互联网平台尽量使用不同的登录密码和支付密码，避免使用出生年月、或者比较简单的数字排列作为账户密码;在公共场合不要轻易连接免费Wi-Fi，不要点击不明来路的短信链接，以免被木马病毒入侵。

3、保护好自己的手机号，用户手机号所属的运营商也是黑产的活跃点，运营商服务密码一定要牢记，不要透露给别人。

4、如果手机出现无故停机状况，建议用户第一时间联系手机运营商，切莫忽视手机异常，谨防手机号被不法分子控制。

>> 诈骗步骤

骗子向已经掌握了银行卡信息的用户发起绑定副号的业务申请

↓

部分手机用户不看短信内容，随意回复,手机号码被骗子添加为副号

↓

骗子利用短信轰炸强迫目标手机关机或利用手机云服务,对手机进行远程操作

↓

当副号手机关机,所有短信都会被主号接收

↓

骗子利用接收的短信验证码，在网上消费或贷款

相关链接：

360手机卫士最新发布的《2016年中国手机安全状况报告》显示，“响一声”仍是最多的骚扰电话；不法分子热衷于异地作案，全国诈骗电话异地呼叫率近七成。

电信骚扰与诈骗问题已经成为2016年度热点安全事件。这份报告显示，2016年，用户通过360手机卫士标记各类骚扰电话号码约2.34亿个，总体来看，相比2014、2015年，2016年骚扰电话标记量首次呈现下降的趋势。其中“响一声”电话以54.6%的比例位居用户标记骚扰电话的首位。

从拦截量来看，360手机卫士去年共为用户拦截骚扰电话385.1亿次，创历史新高，比2015年大幅增长41.3%。其中广告推销类骚扰电话占比15.5%位居首位，其次为诈骗电话、“响一声”、房产中介和保险理财类骚扰电话。

同时360手机卫士还对诈骗电话进行了专项研究，数据显示，诈骗电话异地作案的情况十分显著。

报告指出，全国范围内，诈骗电话的异地呼叫率为68.8%。而对于电信诈骗分子来说，跨地域作案往往会大大增加案件调查和侦破的难度。

安全专家提醒广大市民严防电信诈骗，应做到不明信息勿轻信，不明链接勿点击，不明电话勿理会。

综合新华网