你不知道的电信新陷阱

冒充熟人借钱，冒充公安局、检察院、法院人员查案，短信、二维码中暗藏木马链接……这些骗术，想必大家都有了免疫力。但是，你知道吗？一些你闻所未闻的电信业务，也开始成为骗子设置的新陷阱。

手机被锁定 卡上5万多元被盗

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。

“副号”≠“亲情号”

不用身份证，不用银行卡，甚至连真实姓名都不用知道，钱就这样不翼而飞。副号究竟是什么东西？

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。副号则是由运营商提供的“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个真实手机作为副号。主副两个号码可同时待机，并可根据需要自由选择其中任一号码拨打、接听电话、收发短信。

那么，何先生的手机号是怎么成为犯罪分子的“副号”的呢？

犯罪手法还原

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，一旦你误回复了，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”业务也不太安全

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。

案情回顾——

某天清晨，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？

犯罪手法还原

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，保证登陆安全的动态验证码，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成受害人，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”。

冷门业务的漏洞被骗子盯上

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，要养成良好的上网习惯，陌生链接勿点，不在安全性未知的网址界面中填写自己的个人信息，定期修改社交账号密码，避免手机联系方式等信息遭到泄露；提高安全意识，养成良好的手机使用习惯，避免遭受手机病毒。

（人民）