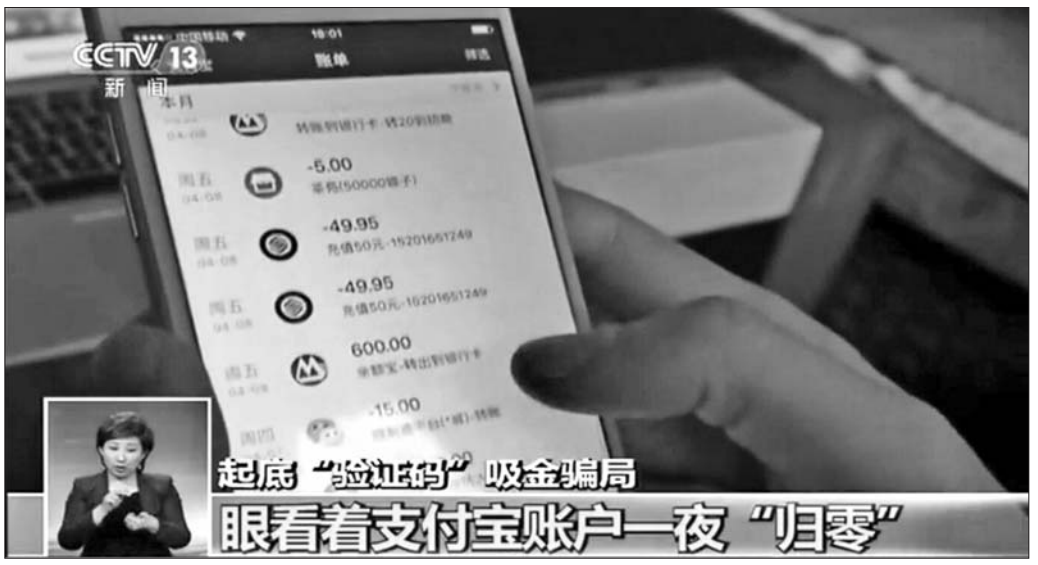
回了一条短信，一夜间“倾家荡产”

一种全新骗术正在蔓延，短信验证存重大安全漏洞

“因为一条短信，一夜之间，我的支付宝、所有的银行卡信息都被攻破，所有银行卡的资金全部被转移……那是一种一无所有的绝望。”最近，一篇受害人自述被骗经历的长文在网络上广为流传。作者称，由于回复了一条短信，他的支付宝、银行卡以及百度钱包里所有的资金一夜之间被“洗劫一空”。真相究竟如何？记者在调查中发现，一种全新的骗术已经出现并正在蔓延，我们不可不知、不得不防。



小许眼看着自己的支付宝账户“归零”。央视截图

发完验证码 支付宝网银一夜“归零”

当事人小许是一名刚参加工作不久的大学毕业生。“4月8日傍晚，挤在北京晚高峰的地铁里，小许连续收到了几条显示来自中国移动官方号码的短信。短信称，他已成功订阅了一项“手机报半年包”服务，并且实时扣费造成手机余额不足。

小许很纳闷，他根本就没有订阅这个服务。紧接着又一条短信接踵而至，内容显示，只要回复“取消+验证码”即可退订该项服务，且3分钟之内退订免费。

当小许正在琢磨“验证码”到底是什么时，手机上又收到了一条来自中国移动客服电话“10086”的短信，内容显示“您的USIM卡验证码为******(6位数字)”。小许并未多想，便编辑了“取消+6位验证码”的短信回复了过去。原以为成功避免了一次手机用户经常碰到的“吸费业务”，但他却惊讶地发现，自己的手机突然显示“无服务”，无论重启多少次都没有响应。

当晚8点左右，小许的手机在无线网络下，接连收到支付宝的转账提示，有人在另一个终端上操作他的支付宝账户。

由于手机无法呼出挂失，情急之下，小许通过操作客户端解除了支付宝与3张银行卡的绑定，并且委托亲友拨打支付宝客服电话冻结账号。但是，当小许挂失完成后，发现支付宝没钱了，而且还在网银里跨行转账，每张银行卡余额均为零。

第二天他发现名下的招行、工行两张储蓄卡被人绑定在另一个在线支付平台“百度钱包”上，加上小许原本在“百度钱包”绑定的另一张中国银行卡，3张卡在事发当晚均进行了资金转移操作，并最终通过招行和工行的手机银行，以“短信验证码转账”全部转入了两个陌生账号。

“劫持”手机号 编造诈骗“剧本”

从收到可疑短信，直到眼见自己的所有账户被彻底“洗劫一空”，整个过程只有3个多小时。骗子到底是通过怎样的手段“发起攻击”的？记者通过调查复盘了整个骗术过程，这实际上是一个“连环计”。

先是破解移动官网密码，“劫持”手机发动攻击。记者登录中国移动北京分公司官方网站，找到了“中广财经半年包”业务。自助订阅后立即扣费，记者收到的短信和小许接收到的内容完全一样，都来自“10086”。中国移动的内部查证：4月8日17:54，有人通过海南海口的一个IP地址，以小许的手机号成功登录了北京移动官方网站，不仅发起了手机报订阅，还在18:13成功办理了一项名为“自助换卡”的业务。

然后，发“退订”短信，制造验证码假象。骗子在攻破移动网站的登录密码后，给小许订阅了“手机报”，并发了所谓“取消+验证码”的退订信息。这么做一是通过手机欠费让受害者产生担心心理；二是制造“退订”时需要“验证码”的假象。

最后，启动换卡流程，“退订”变“换卡”。套取验证码是本次骗术的关键所在，骗局的核心就是“自助换卡”。

骗子在登录移动官网后发起了“自助换卡”业务。这是中国移动推出的一项在线服务，用户不必跑营业厅，直接通过在官方网站操作就可更换4G手机卡。新卡立即生效，旧卡同时作废。

信息安全专家把此类电信诈骗称作“补卡攻击”。据了解，这种“白卡”和领取人的手机号没有绑定关系，因而领取后可以写入任何手机号，不仅可以免费从官方途径获得，甚至在淘宝等网站上有人公开售卖。这就意味着，攻击者要“劫持”小许的手机卡，只需要以小许的手机号成功登录中国移动网上营业厅，并骗到那个没有任何提示说明的6位验证码，剩下的条件都可以轻易获取，不需要任何身份验证。

自助换卡时系统会向用户发一个二次确认的验证码。这个验证码可以直接把之前手机的SIM卡废掉，原来的号码将会转移到另一张SIM卡。这是设局的关键，诈骗分子制造“退订”假象，就是要拿到这张新SIM卡。

而小许收到的这条来自10086系统自动发出的验证码，并未说明用途，也没有对验证码的泄露风险进行安全提示。骗子正是在这个绝大多数用户不清楚的“信息盲点”上做文章，“嫁接”起了两项中国移动的官方业务，编造了整个骗局的“剧本”。

个人信息地下数据库 触目惊心

尽管已经向警方报了案，而且支付宝和百度钱包也在案件侦破之前对小许在该支付平台上损失的金额进行了先行赔付，但小许仍在通过各种途径寻求答案。他恐惧的是，不知自己还有什么关键信息已经被他人所掌握。

记者对本次事件所涉及的第三方支付平台和手机银行的关键业务进行操作汇总后发现：所有的在线支付都可以用手机号和静态密码登录，百度钱包直接可以用短信验证码登录；“更改登录密码”和“转账支付”也无一例外地需要依靠短信验证码完成；而对于第三方支付最重要的“支付密码”，支付宝也简化到仅凭短信验证码就可以更改。

信息安全专家张耀疆介绍，个人信息已形成地下数据库。这个库里面会有大量非常完整的个人信息的链条。如姓名、家庭住址、手机号、银行卡号、银行的密码，其实在网络黑市里都有，而且是整理好的，不是零散的。“而验证码这个东西，它可以做各种各样的动作，比如说找回你的账号密码，那么这样就导致个人的账号密码和验证码变为一体了，它变成一个因素了。那么原来设计当中的双因素的功效就大大降低。就像把所有的鸡蛋都放在这么一个篮子里面，导致了种种的问题。”张耀疆说。

对于小许的移动手机号是如何被他人成功登录网站的，移动公司表示，目前不能准确解释，但如果密码设置过简，或与其他安全级别较低的网站密码相同，就可能会被攻破。工商银行客服介绍，只有取钱密码、银行卡号和手机完全掌握才能在网银上进行操作。因而可以断定，小许的手机卡被“劫持”之前，他更多的“成套”个人信息已经被攻击者掌握了，而第二把钥匙“手机验证码”也因手机卡“被劫”落在了攻击者手中。

据央视新闻

短信验证码的诈骗“剧本”

第一步 破解移动官网静态密码

骗子破解密码登录移动官网 → 订阅增值业务从手机扣费

第二步 发诈骗短信 骗取手机验证码

骗子再发短信，告诉受害人可免费退订，但需回复验证码

第三步 退订增值业务变成“自助换卡”

受害人急于退订，但找不到验证码

骗子趁机在移动官网操作“自助换卡”业务 → 系统向受害人发送“自助换卡”业务的验证码

第四步 受害人“乖乖”回复验证码

受害人以为收到退订业务的验证码 → 把“自助换卡”验证码发送给骗子

第五步 骗子换卡成功，取得手机控制权

骗子利用验证码完成“自助换卡” → 劫持手机，受害人手机瘫痪

第六步 利用短信验证码，成功转走余额

骗子可以接收各类短信验证码 → 对受害人所有账户发起攻击

相关链接

如何防范验证码诈骗

静态密码一定要复杂

信息安全专家孟卓表示，现在互联网发展到这个地步，计算机服务器的运算能力已经很高了，在行业里做的一个测试中，4位数验证码不到一万次就猜出来了，基本上几分钟就能搞定。

专家提示，电脑和手机都面临着木马病毒、“钓鱼”网站等黑客技术的安全威胁。所以，静态密码首先要足够复杂，并妥善保管防止泄露。

仔细甄别“干扰信息”

攻击者经常利用各种手段对短信进行伪装，并千方百计地对攻击对象进行误导甚至恐吓。所以一定要对“运营商”、“银行”等身份的手机短信和来电进行认真甄别，冷静应对。

手机“瘫痪”先挂失

如果手机通讯出现瘫痪，一定要马上查清故障原因。如非手机本身或信号故障，要立刻挂失手机卡，并及时冻结第三方支付和银行账户，避免攻击者趁用户处于“信息孤岛”时，冒名顶替机主身份窃取账户。

验证码别告诉任何人

从电信运营商到第三方支付平台，再到正在进军互联网的银行系统，构成了如今我们每个人信息和财产安全的链条。

电信运营商和提供相关服务的企业只会将短信验证码下发给用户，绝对不会要求用户通过短信或电话进行所谓“回复验证码”的操作。

据央视新闻