



手机卡一再被“劫持” 银行卡多次被盗刷 被害人哭诉——

通信运营商不补规则漏洞，无解！

首席记者 潘高峰
新民网 胡彦珣

谁动了我的手机卡？

身份证没丢
SIM卡却被更换

7月10日下午5时许，市民杨先生在下班途中，随手打开手机准备上网消磨下时间，却发现无论如何连不上网络。“怎么回事？”他想拨打10000号投诉，结果发现连电话也打不出去。

回家后，杨先生赶忙用座机拨打10000号咨询，工作人员告诉他一个令他吃惊的消息：当天下午4时，有手机机主持身份证在营业厅办理了换SIM卡业务，新卡启用，原卡就作废了，自然无法使用。

“手机在我身边，身份证也在我身边，我就是机主，究竟是谁把我的卡换掉了？”一瞬间，杨先生有些不寒而栗。

7月11日，一到上班时间，杨先生就赶到家附近的电信营业厅，用身份证将SIM卡换了回来。他从营业厅得知，昨天的手机换卡业务是在浦东永泰路营业厅办理的。于是杨先生又赶往永泰路营业厅了解情况。营业员告诉他，昨天的换卡人与身份证上的照片是同一人，所以没有怀疑，只复印了身份证留底。杨先生提出要查看身份证复印件，营业员表示只有警方才有权查看。于是杨先生拨打110报警。

东明路派出所民警很快出警来到现场，调取了身份证复印件后查询发现，这是一张假的二代身份证，使用的是杨先生的姓名、身份证号和地址，但照片却是犯罪嫌疑人的。最让杨先生感到奇怪的是，身份证上的地址用的是他多年前丢失的一张一代身份证的地址，当时他还没有来沪，地址是湖南的。

假身份证为何可以轻易办理业务？对此，营业员的答复是：按照公司规定，初次办理新卡是要核对身份证真假的，之后的业务只需要复印留底即可，没有核对身份证真假的要求。

杨先生对此很不满，经过沟通，电信公司答应杨先生会在他的电话卡后台信息下备注，要求每次办理业务都验证身份证的真伪。因为没有什么经济损失，杨先生当时向警方备了案后，也没有继续追究此事。

谁刷了我的银行卡？

手机卡停用
银行卡也被掏空

原本以为一切到此为止，杨先生万万没想到，7月26日他的手机卡再次无法使用。这一回杨先生有了经验，他很快赶到电信营业厅换回了手机卡。

奇怪的是，没过多久杨先生接到了一个电话，是支付宝网监打来的，询问他的支付宝是否有购买消费。杨先生连忙否认，支付宝网监告诉他，因为“购买者状态不稳定、消费异常”，支付宝此前拦截了杨

先生账户的两笔网上消费。这一切，让杨先生有一种不祥的预感。

果然，没过多久，杨先生担心的事情发生了。7月27日晚，杨先生的手机收到银行的两次交易提醒短信，显示他的银行卡先后发生了一笔6950元和一笔3030元的转账交易。杨先生前往银行查询消费记录，结果发现除了这两笔大额转账，还有很多未经短信提醒的消费记录，除了用于购物，还有微信发红包和转账，总计万余元。

杨先生终于意识到自己手机卡一再被换的缘故。7月28日，他前往普陀分局报案。普陀警方目前已经受理此案，并全力开始侦破。

尽管警方已经开展侦查，但杨先生的安全感却没有丝毫增加。在他看来，如果运营商的规则没有改变，自己的手机卡仍然有随时被换掉的可能。“对方可以随时找个地方换卡，谁能担保每一位营业员都是认真负责的？”

为此，杨先生将大部分银行卡冻结并与手机解绑。“但我还要生活，不可能把所有的卡都取消，我是一个市场销售，手机也不能轻易更换，我该怎么办？”

谁盗了我的支付宝？

“补卡解码”

先废手机再取钱

那么，手机卡被人“劫持”，究竟意味着什么？杨先生银行卡内的钱又是怎样被转走的？记者就此做了一番测试。

登录支付宝、网银一般需要输入帐号和支付密码。记者了解到，很多人为了图方便，把手机号直接设成支付宝账号，杨先生就是如此。这使犯罪分子轻松破解了盗号的第一步。

在输入密码的旁边一般有一个选项是忘记登录密码。点击“忘记密码”之后，相关的银行或支付宝客服会向绑定的手机发送短信，类似“您正在找回登录密码，校验码XXXX”。这时只要输入校验码和身份证号就可以重新设置新密码，轻松破解账号。

记者发现，很多密码的重置过程中需要两个重要号码，一个是身份证号，一个则是校验码。在已知身份证的情况下，只需获取校验码。而校验码只会发在绑定的手机号上，当手机卡在别人手中时，验证码的获取也就轻而易举了。

有人会说，支付宝一般会有两个密码。一是登录密码，一是支付密码，两者并不相同。记者进一步测试发现，用支付宝网上银行转账时，首次输错支付密码，系统会跳出“重新输入”、“忘记密码”两个选项，选择“忘记密码”，重置密码时需输入姓名、证件号和卡号，也可更改银行的支付密码。

那么，是不是不把手机号设成账号就安全了？记者就此采访了上

海警方刑侦部门，警方表示，杨先生的身份证被冒用，并不一定就是当初身份证丢失导致，更大的可能性是他的个人信息泄露，而这种泄露现今非常普遍，一个人泄露的信息很可能包含身份证号、手机号、银行卡号、微信号、QQ号、支付宝账号等等，从这起案件的作案手法来看，一旦掌握这些信息，对于犯罪分子来说，要拿走你的钱，只需要用这些个人信息办一张假身份证，然后利用运营商的疏漏骗取手机卡即可。

也就是说，这个局的核心，是手机。

谁为我的损失负责？

疏忽或漏洞

没有识别身份证

昨天，记者就此采访了上海电信。电信承认此事确有发生，经过和杨先生所说基本一致。

上海电信相关负责人在回复记者采访时表示，按规定，在进行业务登记时，要求用户提供真实有效的本人身份证原件进行身份信息登记；委托他人办理业务的，代办人应同时提供委托人、代办人的有效身份证件原件，营业员需通过二代身份证识别仪识别用户证件真伪。但电信同时表示，由于该用户是老用户，系统中已有实名信息，故营业员根据用户出示的身份证原件和本人进行比对后，感觉无误，就为其办理了补卡，漏做了二代身份证读卡识别的步骤。

而针对7月26日杨先生再次被换卡，并造成了经济损失一事，上海电信通过IT手段查证后表示，此次为远程异地补卡，即此卡在外地被补领。

上海电信表示，近年来一直尝试通过各种技术手段和管理措施来最大限度的防范，目前配备了800台二代身份证验证仪，覆盖全市所有营业厅。在今后的工作中，将强化培训，加强营业员对身份证识别操作规范的检查力度，纳入专项检查考核内容。

对于上海电信的回应，杨先生认为，这并没有打消他的疑虑。“第一次被换卡后，我曾向电信投诉，对方答应为我备注，一旦有人换卡，一定要核对身份证真伪。显然，他们没有做到。”

因此，杨先生认为，仅靠营业员的自觉是不可靠的，一定要成为一个规则。杨先生说，随着智能手机的普及，手机已经不再仅是通话工具，而被赋予了更加重要的功能。随着越来越多人的手机号绑定了银行卡、支付宝，移动支付在给人们带来便捷的时候，也给了犯罪分子可乘之机。这要求每个环节都安全可控。杨先生建议，运营商应该把核对证件真伪做进系统流程，如果不核对无法进行下一步操作，这样才能为更多人守护财产安全。

的地位。

“如果运营商的安全漏洞不补上，每个人都可能是受害者。”杨先生认为，他遭遇的一切完全“可复制、可推广”，要解决目前面临的“危机”，只能寄望于通信运营商改变规则。

那么，杨先生究竟碰到了什么样的难题？



新民图表 制图 戴佳嘉

相关链接

湖北荆州警方侦破多起“补卡解码”案

记者查询发现，这种诈骗案在全国多地都有发生，情节大致相同。

湖北荆州警方此前就接报并已侦破“补卡解码”系列案件10起，涉案金额达百万元。很多用户一开始发现手机无法接听，还以为是手机出了问题，没太留意，等到去银行查询余额时，发现钱已经被转走。

警方介绍说，这是一种新型的信用卡诈骗手段，其犯罪手法可以简单地概括为四个字，即“补卡解码”。所谓“补卡”就是犯罪嫌疑人利用伪造的受害人身份证，到通讯运营网点补办与银行卡绑定的手机卡。所谓“解码”就是犯罪嫌疑人补

卡成功以后，在盗刷、盗转受害人银行卡时，利用所截获的短信等动态验证码信息，在没有银行卡密码或网银支付密码的情况下也能将钱转出。警方调查发现，该犯罪团伙已经形成了一条完整的犯罪链。

警方提醒，身份证号和手机号一定要保管好。如果手机使用中出現长时间没信号或无法使用时，要警惕是否被他人补办了自己的手机卡。开通网银的账户，最好不要有大额存款，一旦发现手机卡被调换、被挂失要立即报警，如果更换手机号，一定要及时解绑相关的银行卡。

潘高峰 胡彦珣