城商行是我国银行业的重要组成部分，像浙商银行、北京银行等都属于城商行。本文作者下载了134家城商行的手机银行APP，对其中的身份安全模块进行了体验与调研，一起来看一下吧。


这家大行人脸识别系统被攻破：被人6次识别成功，43万被盗走

澎湃

近日，交通银行人脸识别系统被攻破一度冲上热搜。犯罪分子骗取受害人马某个人信息及人脸影像，通过假人脸信息成功转走马某储蓄卡中近43万元。

01

假人脸活检成功6次

据了解，与马某同样经历的共有6名储户，诈骗分子通过冒充执法人员，通过“李鬼”APP获取受害人个人信息和人脸影像，再诱骗他们将钱存入交通银行储蓄卡，使用假人脸通过了银行“人脸识别”系统窃取他们资金。据了解，6名客户损失超过

身份安全是身份认证的基础，身份安全的底层则是由设备安全所建立的，没有设备安全，即使我们倚重的人脸识别也能被不法分子轻易攻破。

二、城商行手机银行APP身份安全功能分类

与国有银行不同，在我们的固有印象中，大多数城商行即便拥有自己的APP，也只是为了方便群众办理理财、信贷等线下金融业务，这样一来缩小了用户范围，即便出现风险事件损失也能完全可控，因此城商行对于身份安全的需求并没有股份制或国有银行那么强烈，然而事实真的如此吗？

134款APP中，在应用市场无法搜到的有30家，无法直接线上开户的有38家，另外还有9家无法登录或是正常完成认证。也就是说在这134家城商行中，超过40%的银行都支持线上直接开展业务，比我们想象中的比重要大的多。

而且，这也并不意味着无法线上开户的银行就不涉及任何身份安全的风险。一样的

道理，即使你在线下完成开户，你开通手机银行只是为了转账方便，依然有人能够绕过重重关卡直接盗取你的账户。

我们在往下看，57家支持线上开户的城商行中，有47家APP具备身份安全功能，占比82.45%。这些身份安全功能不外乎设备管理、登录管理、支付管理、证书管理等，我们做了如下归类整理。

- 设备管理：查看常用设备、常用设备删除、常用设备绑定
- 登录管理：
  密码设置、手势解锁、指纹解锁、人脸解锁、声纹解锁、微信/支付宝绑定
- 支付管理：交易限额、指纹支付、面容支付、蓝牙U盾、安全锁、pin码
- 证书管理：云证书、动态令牌、芯盾

三、曾用设备不等于可信设备

按照设备类型我们可以划分为三种，
即：陌生设备、曾用设备、常用设备。
根据不同的设备类型，我们可以进行风险分级，目前少数手机银行APP根本就没有做设备管理的功能，也就意味着无法对风险做进一步的细分把控，即使做了相关功能，做法上也是错误的。

我们调研的这些城商行APP中，全部把用户曾经用过的设备，默认叫做常用设备。虽然从语言文字的逻辑上是说的通的，但是曾用设备却并不等于常用设备。一旦有了常用设备的设定，风险等级也就会对应进行降级，但我只是经常用这部手机登录我的手机银行账户，并不代表这部手机就是可信任的。比如我会经常使用朋友的手机、公司的公共手机、无法时长保障安全的备用机等等。

我们也可以把常用设备改个名字，直接叫做“可信设备”，可能会更加直观的理解我的意思。可信设备应该是需要我去主动授权或绑定的，但现在银行的做法是我登录过的即为可信，这是根本上的错误。

完成对设备的分层之后，我们就可以结合其他金融科技能力，来搭建我们的风险管理体系。

四、手机银行APP如何基于设备安全搭建风险管理体系？

1. 基于设备进行分层

针对陌生的设备，我们就用最高安全级别的认证方式来让用户验明自己的身份，比如需要完成人脸识别、甚至是使用NFC去完成证件真伪的辨别。

对于常用设备，我们可以使用相对较轻的认证方式，比如输入密码、pin码，完成身份二要素核验等等。

对于用户主动绑定过的可信设备，则通过最基础的方式来进行认证，比如指纹、手势码等等。

这里是基于设备本身做的风险分层，我们也可以通过不同场景，进一步分层。

2. 基于场景进行分层

比如，登录是一个相对来说风险较轻的动作，可以通过低风险措施完成认证，比如常见的指纹、手势码登录。

查看账户余额，更新身份信息等操作，属于较高一层的风险操作，可以输入密码、pin码等方式完成认证。

转账、购买理财产品等场景，属于最高风险操作，必须采用最严格的核验方式，完成核验或对应进行风险降级。

如果
将这两个维度进行组合，我们就形成了一套基于安全设备管理的数字银行全场景身份风险控制方案。

此外，我们也会发现，当前的城商行APP中，大多是基于设备号去做的设备管理，这种方式其实也不太适用当下的环境。

随着个人信息保护法、反电信诈骗法的相继出台，对用户信息的获取及滥用进行了有效控制，设备号也属于个人身份敏感信息，在可以预见的将来，一定会退出历史舞台。我们近年来也一直在寻找解决方案，并且近期也发现了一种不依赖设备号数据也可以完成设备管理的方法，可以关注我之后的文章。

题图来自 Unsplash，基于 CC0 协议。

该文观点仅代表作者本人，人人都是产品经理平台仅提供信息存储空间服务。