新骗局套路深，“老司机”都可能中招

警方提醒：看牢自己的银行卡验证码，千万不要随意给其他人！

骗局几乎每天都在上演，听到的提醒也多了，很多人觉得自己绝不会掉进陷阱。然而，一种最新骗局实在太“高级”了，就算你是警觉性高的“老司机”也难保不中招。近日，市公安局发布预警：看牢自己的银行卡验证码，千万不要随意告诉别人！

记 者 张贻富
通讯员 刘 益 康巍巍 李 绩

民警在进行安全防范宣传。

看看这个在朋友圈热传的最新骗局

网友“@越来越老的未来”是一名自认为能熟识多种骗局的IT男。8月29日下午，他收到两条来自“建设银行95533”的短信，提示他有两笔转账支出，分别是300元和4600元。他平时警觉性就比较高，知道自己的卡没有绑定任何第三方支付，而当时卡又还在身边，所以他怀疑是诈骗分子利用伪基站发送的诈骗短信，因此并没有理会。

可接下来更蹊跷的事情发生了，就在他收到短信不到3分钟，接到170开头的来电，对方自称是“京东商城客服”，说他在异地发生消费，询问其是否本人交易。此时这位网友并不担心。

不过，在对方准确报出他的银行卡号及他绑定的手机号和姓名时，他开始有点慌了，在他告知对方自己没有消费，不许扣款后，对方声称可以帮忙进行拦截。

果然，他的手机收到了银行短信称余额增加了300元。他一边与对方周旋要求其将4600元的消费也拦截下来，一边用另外一个手机拨打建设银行客服电话确认卡内余额。

让他震惊的是：经余额查询，的确与刚刚收到的短信提示余额完全一致。

不过，对方随后声称要拦截1000元以上的消费，需要提供手机验证码，他马上又警觉起来：警方在通讯（网络）诈骗案宣传中曾多次强调，不要轻易将验证码透露给陌生人。

他一直强调自己没有收到手机短信验证码，多次周旋后，骗子意识到他可能识破骗局就挂断了电话。他赶紧拨打建行客服电话，这才搞清楚他银行卡的钱被转到了投资理财-理财商品-保证金管理。

市民姚女士的真实亲历

无独有偶，家住鄞州石碶街道的姚女士近日也碰到了类似情况。姚女士说，她有一张工商银行的牡丹卡，分子母卡，其中母卡在自己手上，子卡在英国读书的女儿手上。

8月31日那天，她的手机突然收到两条短信，称其卡内有两笔扣款交易，金额分别为3000元和36500元。她以为是国外的女儿进行了消费，就打了越洋电话给女儿，可女儿说自己压根没用过卡。

正在她焦躁不安时，接到了自称是“工商银行工作人员”的电话，对方跟其确认这两笔交易是否本人操作时，姚女士当即否认。

对方说：“我们怀疑您的银行卡可能被盗用了，也有可能您的网银账户被盗了。目前我们能做的就是帮您挂失卡片并进行账号冻结，请您提供一下手机收到的验证码。”

这时，姚女士的头脑有点清楚了，她记得以前自己丢过一张信用卡，办理挂失时银行没有让其提供验证码之类的情况，而只是核实了一下她的姓名和联系方式。于是，她借口要询问一下女儿是不是在国外消费了，就赶紧挂断了电话。

随后，姚女士当即拨打了工商银行的客服电话，工作人员告诉她之前有两笔通过网上银行购买了工银货币的交易，金额是从其卡内划到期货币账户名下，钱都还是属于她的。姚女士这才恍然大悟。

警方揭露骗子的套路

据警方介绍，随着通讯技术的不断发展，大多数人都会办理网银、手机银行，绑定三方支付，在网上购物。大多数人面对一连串银行卡余额发生变动的真实信息，往往会乱了阵脚，最终落入骗子的圈套。

警方在总结类似诈骗手段后，也剖析出骗子的诈骗伎俩：

1.通过某种手段获取你的用户名、密码等信息，通过非法手段进入你的网银。

2.把你的钱转到你的投资账户里，这时候钱还在卡内，比如工商银行，只要是购买其银行网站上的基金、原油、贵金属等，全部都不需要验证码，直接可以从本人账户转到投资账户中。

3.转钱到投资理财账户后，银行会给你发信息，通常短信内容是提示你账户中的余额发生了变动，但并未指出钱的走向。

4.大多数人在看到钱莫名其妙被转走后会惊慌失措，骗子就更容易获取你的信任。这时，你就会接到骗子的电话，跟你核实你的卡是否发生了消费，可以帮忙追回钱款或冻结账户等，目的是套取你手机收到的验证码。

5.有时候有些骗子还会把小额的钱从投资账户再转回受害人的网银账户。此时受害人会收到银行发给你的转账信息，结果你就会以为骗子真的在“帮”你。

6.骗子提出另外一笔钱数额太大，需要验证码，当你把验证码告诉骗子后，这笔大额的钱就被真的转走了。

牢记一点：银行账户验证码别给陌生人

警方为此提醒广大市民，切勿点击手机短信中的不明链接、不轻易透露个人银行卡、密码等信息。最关键的是，任何与银行账户或银行卡有关的验证码，一定不要轻易泄露给别人！

银行方面也提醒说，切勿采用来历不明的超级链接方式间接访问网站，切勿提供账户信息及短信验证码。

账户信息及手机动态验证码属于账户支付验证的关键信息，应妥善保管，同时注意银行发送的交易提示短信，不要轻信以退款等名义骗取关键信息的陌生来电。

■相关链接

6条容易泄露个人信息的途径及防范措施

据警方介绍，之所以当前通讯（网络）诈骗案、电话推销如此猖獗，跟个人信息的泄露也存在很大关联。警方为此总结了8条容易泄露个人信息的途径，大家也要学习学习提高警惕。

一、各类单据随意丢。

快递单、车票、登记票、购物小票、办理手机卡的业务单、水电费账单……这些单据都包含大量个人信息，随意乱丢可能让它落入不法分子手中，导致个人信息泄露。

防范方法：无用的单据可以直接撕掉，或将姓名、电话、地址等个人信息涂掉再丢弃。

二、自动连接公共WiFi。

若在智能手机的网络设置中选择了WiFi自动连接功能，就会自动连接公共场所WiFi。但WiFi安全防护功能比较薄弱，黑客只需凭借一些简单设备，就可盗取WiFi上任何用户的信息。

防范方法：公共场所尽量不使用不需要密码的免费WiFi，最好将WiFi连接设置为手动。使用无线WiFi登录网银或者支付宝时，可以通过专门的APP客户端访问。

三、社交媒体露详情。

通过微博、QQ空间、贴吧等和熟人互动时，有时会不自觉说出或标注对方真实信息。有些家长在朋友圈晒出的孩子照片包括孩子姓名、就读学校、所住小区；晒火车票、登机牌，却忘了将姓名、身份证号、二维码等做模糊处理。

防范方法：在微博、QQ空间等社交网络要尽可能避免透露或标注真实身份信息。朋友圈晒照片一定要谨慎，尽量不晒包含个人信息的照片。

四、简历填写太过详细。

很多人通过网上投简历找工作，简历中的个人信息一应俱全，有些公司在面试时还会要求填写一份所谓的“个人信息表”，上面有家庭关系说明、父母的名字、个人电话、住址、毕业学校甚至身份证号等信息。

防范方法：一般情况下，简历上只提供必要信息，不要过于详细填写本人具体信息，尤其是家庭住址、身份证号等。

五、卖旧手机不删信息。

转卖旧手机时，尽管已将其恢复到“出厂默认设置”，甚至将其格式化，但通过技术手段，专业人员还是可以把旧手机里的短信、通讯录、软件设置浏览记录等全部恢复。

防范方法：存储有个人账户资料的手机，尽量避免转卖。如果确有出售必要，在转卖之前，务必做好彻底清理工作。

六、“自动登录”尽量少用。

多数应用程序安装过程中都会弹出询问“向您发送通知”“使用您的位置”等对话框，如果点“允许”，这些应用可扫描并把手机信息上传到云服务器，手机使用者的位置、通话记录等都很容易被人获取。此外，很多人习惯把QQ、微信等设置成“自动登录”，一旦手机丢失或者被黑客入侵，账户和密码很容易被窃取，带来损失。

防范方法：安装手机软件时，慎重选择“允许”。尽量不要把手机软件设置为自动登录，每次登录都应设置密码；密码定期要更换，安全系数要高，不要用简单的数字组合。