热线：96060 E-mail:xdkb@kuaibao.net 现代快报
责编:刘伟 美编:时芸 组版:王盛吉 2015.5.14 星期四


制图 李荣荣

最近，不少南京市民收到“你老公(老婆)跟人开房时被拍照片，想看全部照片，请点击……”类似的短信，你想要不去点击网址链接，确实有点难。不过，一旦你点击进入，那就落入了骗子的圈套，绑定手机的银行卡、支付密码等信息就会被骗子获取，银行卡内的钱也会被盗。这是昨日南京警方曝光的最新通讯网络诈骗手法。同时，警方还发布了其他常见的通讯网络诈骗手法，并做了提醒。

通讯员 苏宫新 宁公宣 秦公轩 现代快报记者 李绍富 陶维洲

## “你老公跟人开房时被拍照片，想看全部照片，请点击……”

# 市民请注意！“相册诱惑”诈骗来了

### 这8种通讯网络诈骗“杀伤力”大，要当心！

**1 “相册诱惑”诈骗**

**这是今年才出现的一种新型诈骗方式。诈骗分子短信群发含“相册”的木马病毒，机主出于好奇点击短信链接的网址后，病毒程序自动下载运行，盗取手机内的通讯录、绑定操作的银行卡、支付密码等信息，从而实施盗刷、转账等犯罪。**

**2 淘宝退款网络诈骗**

骗子预先通过非法渠道获取了淘宝网店的大量客户购物信息，冒充淘宝客服，通过电话或短信方式，以其购买物品的订单存在问题无法发货为由，要求受害人到指定网址办理退款事宜进行诈骗。

**3 “画皮”QQ诈骗**

**骗子事先设置一个各种资料都跟被骗人公司领导一样的QQ号，要求转账汇款。**

**4 “积分兑换”诈骗**

骗子利用伪基站冒充955开头的银行客服、10086等客服号码群发短信，以积分兑换现金、网银升级等为名诈骗。

**5 电话冒充领导诈骗**

骗子打电话冒充受害人的领导、老师等，以给领导送“红包”不便为由，让受害人垫付汇款实施诈骗。

**6 冒充公检法办案诈骗**

骗子冒充“公、检、法”等办案人员身份，以涉嫌洗钱、贩毒等犯罪为由恐吓受害人，骗人把钱转到所谓指定“安全账户”来诈骗。

**7 钓鱼网站票务诈骗**

骗子事先制作了虚假网站，提供虚假的航空公司、演唱会门票售票方等联系方式，并以400电话等专业号码增加可信度，骗取受害人信任后盗取受害人银行卡内资金。

**8 补贴类短信诈骗**

骗子以刚买房、买车、生育或有老人死亡的家庭为诈骗对象，以各种补贴为诱饵进行诈骗。

## 最新短信诈骗 “相册诱惑”藏病毒，会掏空手机里的信息

最近一段时间以来，不少市民都会收到短信，内容都与自己或是身边的人被拍照片有关。“这是上次我们一起玩时拍的照片，我制成了相册，你点击……就可以查看所有照片”“这是你老公跟别人到宾馆开房时，被人拍的照片，全部照片都在相册里，你点开……就可看全部照片”。

据南京市公安局刑侦局的相关民警介绍，南京目前收到这类诈骗短信的人不少，这是今年才出现的新诈骗方式。诈骗分子以短信群发器等方式发送类似相册的木马病毒，点击短信链接的网址后，病毒程序自动下载运行，盗取手机内的通讯录、绑定操作的银行卡、支付密码等信息，从而实施盗刷、转账等犯罪。同时，手机也会因中病毒无法使用，而相应的病毒会向通讯录内的人员发送病毒，形成连锁诈骗的局面。

目前，南京不少市民都收到了类似的短信，但上当受骗后报案的，暂时还没有。不过，据南京警方介绍，目前在江苏省其他地区，已有人因遭遇类似的诈骗，损失了数十万。

### [防骗提醒] 别随意点击链接,别轻易转账汇款

1.只要不随意点击来历不明的网站链接，并记住天上不会掉馅饼，不要贪任何小便宜，不轻易转账汇款，骗子就拿你没办法。2.用于网络交易的银行卡里，不要留有太多的钱，单笔交易的额度最好设置一个较低的限度,或设置当日消费限额，以免被盗刷时损失惨重。3.最安全的方式是，在网络交易前，先临时修改一个密码，交易结束后，再改为自己常用的密码。

## 最新诈骗案件 女会计输错3次密码冻结骗子账户，追回20万

不法分子QQ上冒充老板诈骗女会计案再次在南京发生。

南京市民徐女士是一家公司的会计。5月10日晚上9点多，公司李总对徐女士说，老板刚通过QQ与其联系，要求汇款20万元。随后，李总把老板周总的QQ号给了徐女士，让其通过QQ和周总沟通汇款事宜。因为QQ号是李总给的，而且指定要通过QQ联系，徐女士根据“周总”指示，将20万元汇入苏州一个账号用于支付货款。

说来也巧，刚打完款，徐女士就接到了周总的电话，对方询问公司财务状况。徐女士当即提起了刚刚汇出的20万元。没想到周总一头雾水，根本不知道这回事。徐女士赶忙叫来了李总，三人在电话中一合计，知道肯定是被骗了。

于是，几人分工合作，李总打电话报警，徐女士则根据之前警方的提示，通过网上银行连续三次输错骗子账号的密码，将其账户暂时冻结。接到报警的朝天宫派出所民警深知，这样的暂时冻结过了午夜12点就会失效，必须彻底将账户冻结住。经过查询，骗子账户在苏州吴江一家银行。当晚10点半，民警便从派出所出发，连夜赶往吴江。

路上，民警便通过各种方式联系吴江方面银行负责人进行交涉，要求继续冻结该账户。凌晨1点半，当民警赶到吴江时，银行账户上的钱还在。在递交相关公安文书后，该账户被长时间冻结，钱保住了。

### [防骗提醒] 受骗后，“输错密码”补救还来得及

遭遇这样的骗局后，骗子还没来得及转走汇款，可立即通过网上银行等途径连续输错骗子账号的密码多次，将其账户暂时冻结。

## 其他案例披露 信用卡在身上，却被人透支消费50多万

昨天，江苏省公安厅经侦总队发布盗取银行卡信息诈骗典型案例，为你揭秘。

去年8月，江苏睢宁警方接到山东警方发来的协查线索，称在侦破一起网上制售半成品银行卡（仅有卡面信息的克隆卡）案件中，发现嫌疑人杨某通过快递，将克隆卡邮寄到睢宁。通过银行查询，警方发现杨某快递过来的银行卡被人在澳门消费300多万元。经过进一步调查，睢宁人樊某浮出水面。去年9月27日，民警将樊某抓获。经审讯，樊某交代了自己的作案经过。去年5月开始，樊某和朋友晋某从网上获取他人银行卡信息，然后通过QQ发给山东的杨某，让其制作成半成品克隆卡。当卡片寄回来后，樊某再通过写卡器，将银行卡信息写入半成品克隆卡中，再去澳门套现。

到底是谁动了我们的银行卡？下面这个案例，大家也许能找到答案。去年6月20日，淮安警方接到辖区一家企业负责人报警，称他于6月18日收到银行短信提醒，信用卡被消费50多万元。而信用卡一直在自己身上，对此他感到很疑惑。经查询，警方发现受害人的银行卡在安徽亳州市谯城区三处地点分六次刷卡消费507217元。很快，两名嫌疑人潘某和詹某落网。面对民警，詹某等人交代，他们从网上获得信用卡信息，然后进行克隆盗刷。

民警梳理发现，被克隆的卡有个共同点，都在广东一家酒店消费过。“该酒店的刷卡设备可能被不法分子动了手脚，有人进行刷卡消费时，银行卡信息泄露。”

### [防骗提醒] 建议记下信用卡CVV码，然后刮掉

1.选择正规商家消费，并全程跟踪刷卡流程，最好卡片不离手。2.注意信用卡信息的保护。卡背面签名的位置有一串数字，其中最后三位为CVV码，当进行网上交易时，只要输入信用卡卡号、有效期和这三个数字就可以进行交易。民警建议，将CVV码牢记于心，然后将卡上的数字刮掉。